

Assignment 1: Create an account in AWS and configure a budget.

Creating an AWS Account:

1. In browser, open the AWS home page.
2. Choose **Create an AWS account**.
3. Enter account information, and then choose **Continue**. Review account information.
4. Choose **Personal** or **Professional**.
5. Enter company or personal information.
6. Read and accept the AWS Customer Agreement.
7. Choose **Create Account and Continue**.

At this point, we'll receive an email message to confirm that AWS account is ready to use.

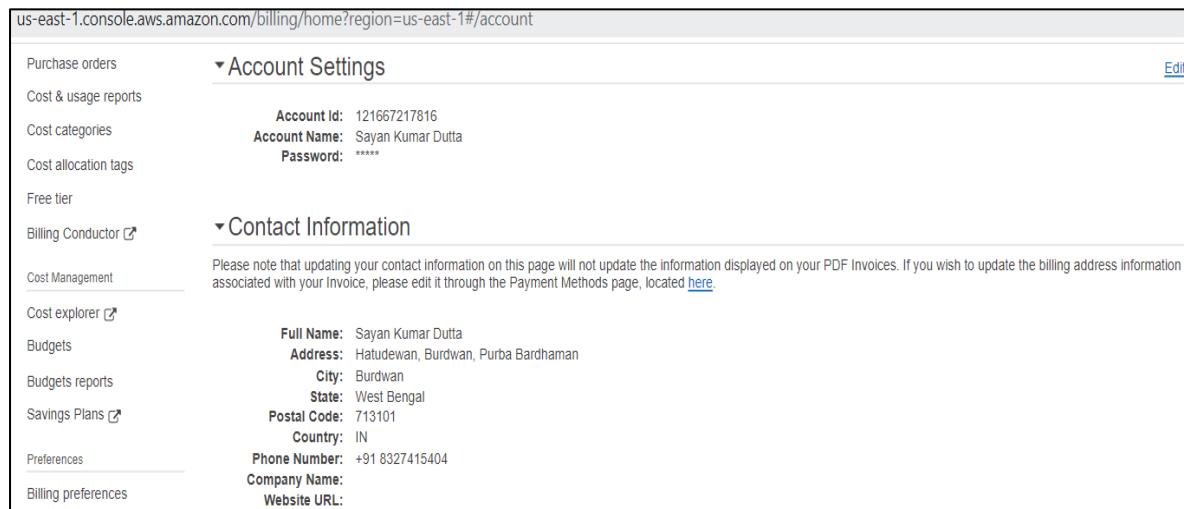
On the Payment Information page, enter information about payment method. If we want to use a different address for billing purposes, choose Use a new address.

8. Choose **Verify and Add**.
9. To verify our phone number, choose country or region code from the list, and enter a phone number where we can be called in the next few minutes. Enter the CAPTCHA code, and submit.
10. When the AWS automated verification system calls us and provides a PIN, enter the PIN using the phone, and then choose Continue.
11. Select the AWS Support plan.

A confirmation page appears that indicates that our account is being activated.

12. Check the email and spam folder for an email message that confirms our account was activated.

After we receive the activation message, you have full access to all AWS services.



The screenshot shows the AWS Account Settings page in the AWS Management Console. The URL in the browser is `us-east-1.console.aws.amazon.com/billing/home?region=us-east-1#/account`. The page is divided into two main sections: Account Settings and Contact Information.

Account Settings

- Account Id: 121667217816
- Account Name: Sayan Kumar Dutta
- Password: *****

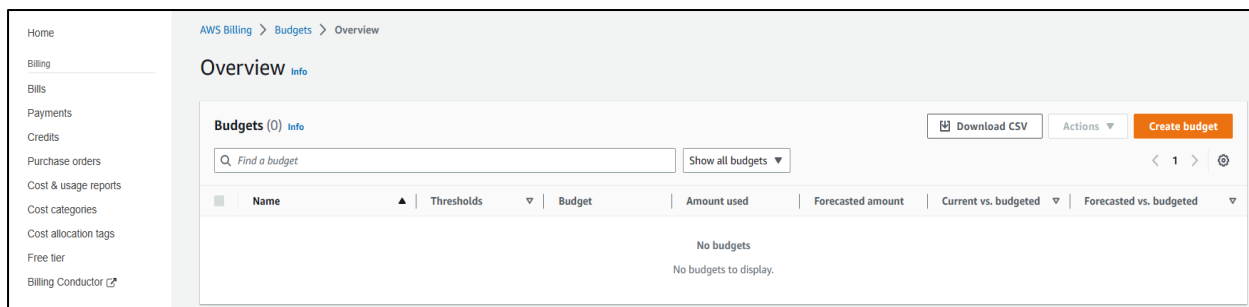
Contact Information

Please note that updating your contact information on this page will not update the information displayed on your PDF Invoices. If you wish to update the billing address information associated with your Invoice, please edit it through the Payment Methods page, located [here](#).

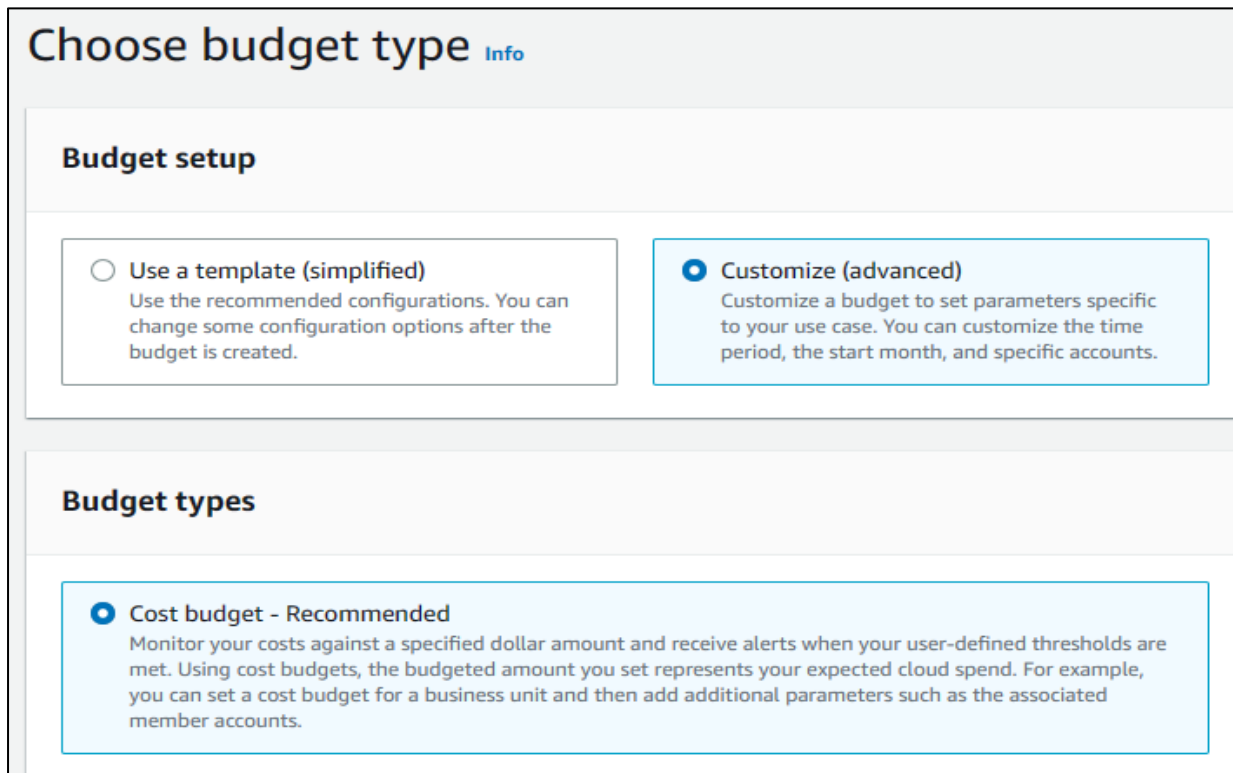
- Full Name: Sayan Kumar Dutta
- Address: Hatudewan, Burdwan, Purba Bardhaman
- City: Burdwan
- State: West Bengal
- Postal Code: 713101
- Country: IN
- Phone Number: +91 8327415404
- Company Name:
- Website URL:

Creating a cost budget:

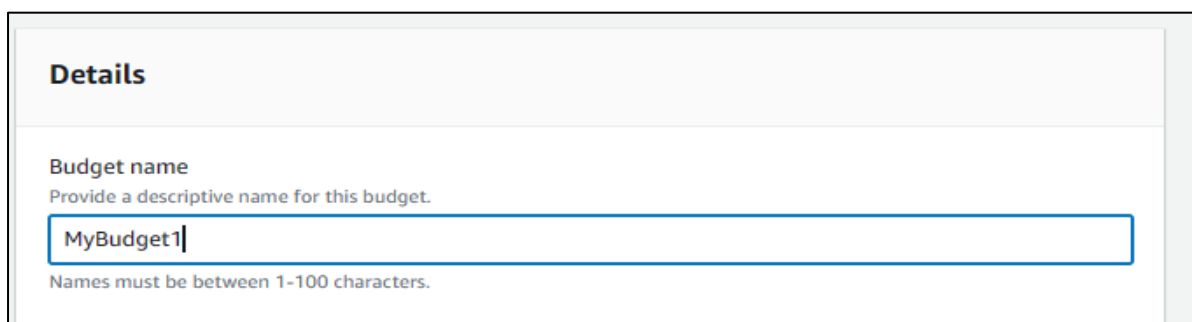
1. Sign in to the AWS Management Console and open the **AWS Cost Management console**
2. In the navigation pane, choose **Budgets**.
3. At the top of the page, choose **Create budget**.



4. Under Budget setup, choose **Customize (advanced)**.



5. Under Budget types, choose **Cost budget**. Then, choose **Next**.
6. Under Details, for **Budget name**, enter the name of the budget.



7. Under **Set budget amount**, for **Period**, choose Daily/Monthly/Quarterly/Annually.
8. For **Budget renewal type**, choose Recurring budget or Expiring budget .
9. Choose the start date or period to begin tracking against the budgeted amount.
10. For **Budgeting method**, select the way that we want our budget amount to be determined each budget period: Fixed/ Planned/ Auto-adjusting.
11. Under Budget scope, select “**All AWS Services(Recommended)**”.

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

Feb ▼

2023 ▼

Budgeting method [Info](#)

Fixed ▼

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

Enter your budgeted amount (\$)

Last month's cost: \$0.00

1.00

Budget scope [Info](#)

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

Scope options

☒ All AWS services (Recommended)

Track any cost incurred from any service for this account as part of the budget scope

☐ Filter specific AWS cost dimensions

Select specific dimensions to budget against.
For example, you can select the specific service "EC2" to budget against.

12. Choose **Next**.
13. Choose Add an alert threshold and set the Alert threshold.
14. Under Notification preferences, for Email recipients, enter the email addresses that we want the alert to notify.
15. Choose **Next**.
16. Review, and then choose **Create budget**.

▼ Alert #1

[Remove](#)

Set alert threshold

Threshold

When should this alert be triggered?

Trigger

How should this alert be triggered?

Summary: When your actual cost is greater than **50.00% (\$0.50)** of your **budgeted amount (\$1.00)**, 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.

Maximum number of email recipients is 10.

- **Amazon SNS Alerts - *Optional Info***
- **AWS Chatbot Alerts**

[+ Add alert threshold](#)[Cancel](#)[Previous](#)[Next](#)

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	Start date	Budget amount
MyBudget1	Feb 2023	\$1.00
Period	End date	
Monthly	-	

► Additional budget parameters

Step 3: Configure alerts

[Edit](#)

Alerts

Alert #1

Threshold

50% of budgeted amount

Threshold measured against

Actual costs

Step 4: Attach actions - optional

[Edit](#)

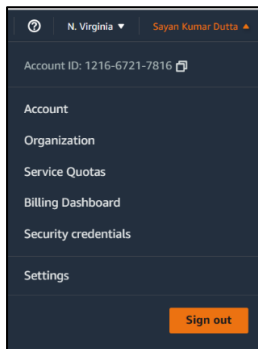
Actions

You have no budgets actions

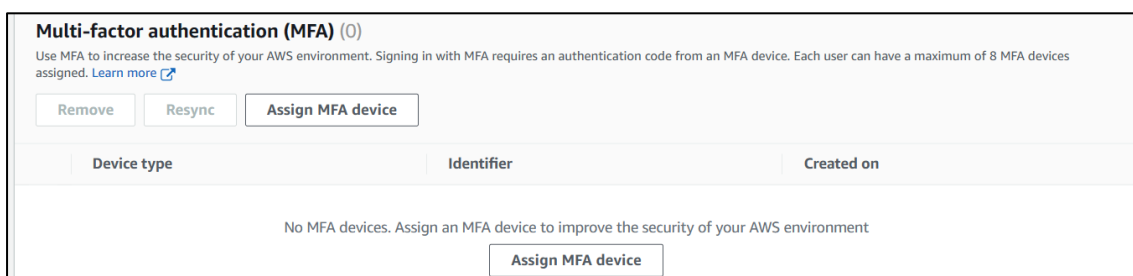
[Cancel](#)[Previous](#)[Create budget](#)

Assignment 2: Create MFA for Authentication.

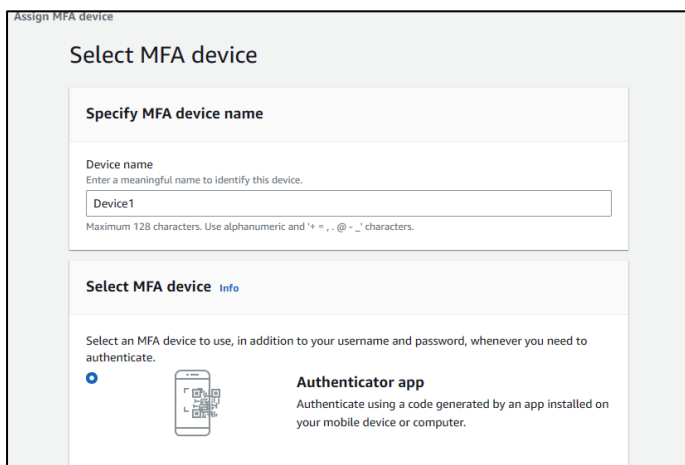
1. Sign in to the **AWS Management Console**.
2. On the right side of the navigation bar, choose account name, and choose **Security credentials**



3. In the Multi-Factor Authentication (MFA) section, choose **Assign MFA device**.



4. In the wizard, type a **Device name**, choose **Authenticator app**, and then choose **Next**.




5. Open the **virtual MFA app** on the device.
 - Scan the QR code. To use the QR code to configure the virtual MFA device, from the wizard, choose Show QR code. Then follow the app instructions for scanning the code.
 - In the Set up device wizard, choose Show secret key, and then type the secret key into the MFA app.
 - The device starts generating six-digit numbers.
6. In the wizard, in the MFA code 1 box, type the one-time password that currently appears in the virtual MFA device. Wait up to 30 seconds for the device to generate a new one-time password. Then type the second one-time password into the MFA code 2 box. Choose **Add MFA**.

Set up device

Set up your 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, chose **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 Fill in two consecutive codes from your MFA device.
MFA code 1:
MFA code 2:

Cancel Previous **Add MFA**


The device is ready for use with AWS.

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		Now



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: sayandutta0587@gmail.com

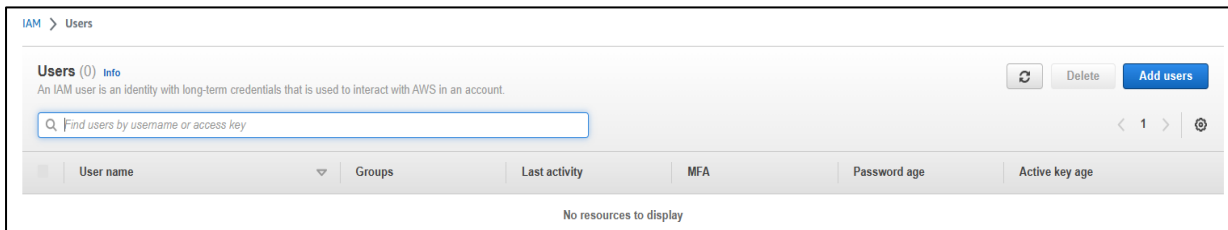
MFA code

Submit

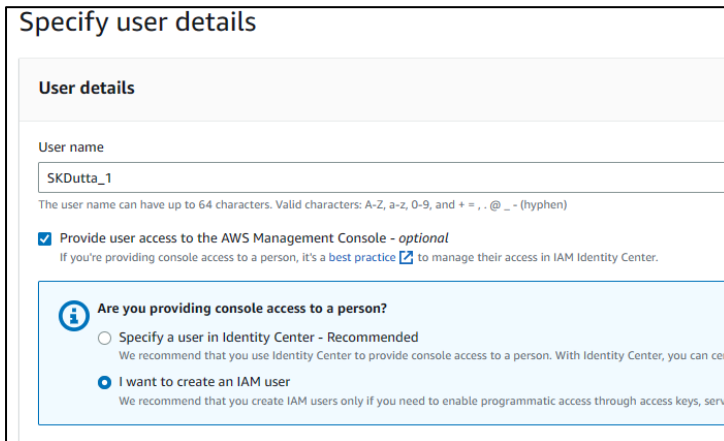
[Troubleshoot MFA](#)
[Cancel](#)

Assignment 3: Create IAM User giving full access of S3.

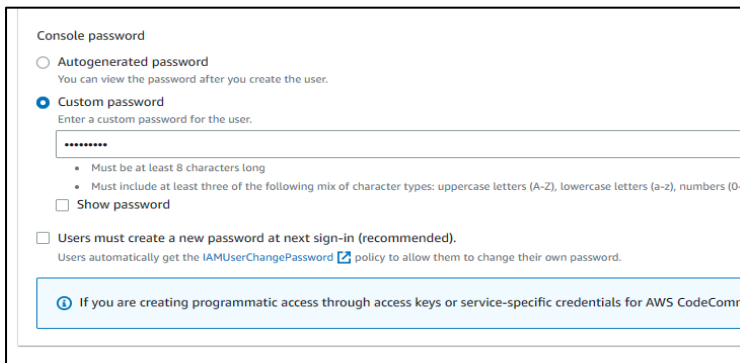
1. Sign in to the AWS Management Console and open the **IAM console**.
2. In the navigation pane, choose **Users** and then choose **Add user**.



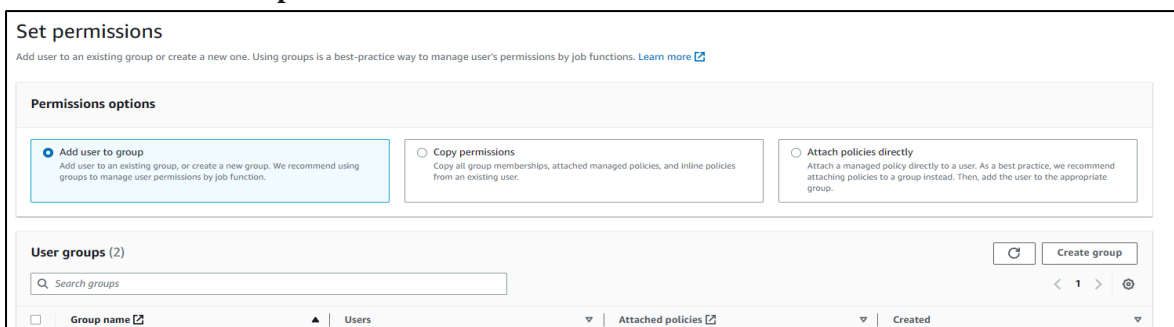
3. Type the user name for the new user. This is the sign-in name for AWS.



4. Select the type of access this user will have.
 - Select **Enable console access**. This creates a password for the new user.
 - **Custom password** – The user is assigned the password that you type in the box.



5. Uncheck **Users must create a new password at next sign-in (recommended)**
6. Choose **Next**.
7. On the **Set permissions** page, specify how you want to assign permissions to this set of new users. Choose **Add User to Group**.



- Choose **Create group** to create a new group.
- Give the **User Group Name**
- Give the required **Permission Policies**
- Click **Create User Group**

Create user group

Create a user 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](#)

User group name
Enter a meaningful name to identify this group.
S3FullAccess2
Maximum 128 characters. Use alphanumeric and "+", "@", "-" characters.

Permissions policies (1/816)

Q s3 9 matches < 1 > ⚙

<input type="checkbox"/>	Policy name	Type	Used as	
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	AWS man...	None	P...
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS man...	Permissio...	P...
<input type="checkbox"/>	AmazonS3ObjectLambdaExecutionRolePolicy	AWS man...	None	P...
<input type="checkbox"/>	AmazonS3OutpostsFullAccess	AWS man...	None	P...
<input type="checkbox"/>	AmazonS3OutpostsReadOnlyAccess	AWS man...	None	P...
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS man...	None	P...
<input type="checkbox"/>	AWSBackupServiceRolePolicyForS3Backup	AWS man...	None	P...
<input type="checkbox"/>	AWSBackupServiceRolePolicyForS3Restore	AWS man...	None	P...
<input type="checkbox"/>	QuickSightAccessForS3StorageManagementAnalyti...	AWS man...	None	P...

Cancel Create user group

8. Check the Group and Choose **Next**.

User groups (1/3)

Search groups

<input type="checkbox"/>	Group name	Users	Attached policies	Created
<input type="checkbox"/>	EC2fullaccess	0	AmazonEC2FullAccess	2023-02-15 (3 days ago)
<input type="checkbox"/>	S3fullaccess	0	AmazonS3FullAccess	2023-02-15 (3 days ago)
<input checked="" type="checkbox"/>	S3FullAccess2	0	AmazonS3FullAccess	2023-02-18 (Now)

► **Permissions boundary - optional**
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more](#)

Cancel Previous **Next**

9. On the **Review and create** page, after reviewing choose **Create user**.

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: SKDutta_1
Console password type: Custom password
Require password reset: No

Permissions summary

Name: S3FullAccess2
Type: Group
Used as: Permissions group

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**

10. To save the password, choose **Download .csv** and then save the file to a safe location.

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://121667217816.signin.aws.amazon.com/console>

User name

SKDutta_1

Console password

***** [Show](#)

[Download .csv file](#)[Return to users list](#)

11. Provide the user with their credentials.
12. New IAM User is being created with S3 Full Access.