

AWS Tasks On IAM Service.

Task 1 :- “ Create User And Attach the S3 Permission For One Hour Only.”

1 . Create A User In IAM Service.

Users (2) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Acc
rajaa	/	0	18 days ago	-	18 days	-	Act
shree	/	0	18 days ago	-	22 days	-	Act

Create user

2. Enter New User Name.

Specify user details

User details

User name

Akshada

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.

3. Enter The Password.

The screenshot shows the AWS IAM console 'Create user' page, Step 3: Enter the password. The page is titled 'credential for emergency account access.' and has a 'Set as default' button. The 'Console password' section has two options: 'Autogenerated password' (selected) and 'Custom password'. The 'Custom password' option is selected, and a password 'Akshada@123' is entered in the text field. Below the text field, there are two bullet points: 'Must be at least 8 characters long' and '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) = [] { } | ' '. There is a 'Show password' checkbox which is checked. Below this, there is a checkbox for 'Users must create a new password at next sign-in - Recommended' which is unchecked. A note states: 'Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.' At the bottom, there is a blue box with an information icon and text: '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](#)'. At the bottom right, there are 'Cancel' and 'Next' buttons.

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.

Akshada@123

- 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.

Info 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

4. Click To Create User

The screenshot shows the AWS IAM console 'Create user' page, Step 4: Retrieve password. The page is titled 'Permissions summary' and has a 'Set as default' button. The 'Permissions summary' section shows a table with columns: Name, Type, and Used as. The table is empty, and the text 'No resources' is displayed below it. Below the table, there is a section for 'Tags - optional'. It states: '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.' and 'No tags associated with the resource.' There is an 'Add new tag' button. At the bottom right, there are 'Cancel', 'Previous', and 'Create user' buttons.

Step 4
Retrieve password

Permissions summary

Name	Type	Used as
No resources		

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

5. Your User Is Successfully Created .

The screenshot shows the AWS IAM console in the 'Users' section. A green banner at the top indicates 'User created successfully' with a 'View user' button. Below this, the 'Users (3)' section shows a table of users. The table has columns for checkboxes, User name, Path, Group, Last activity, MFA, Password age, Console last sign-in, and Actions. Three users are listed: Akshada, rajaa, and shree. The 'Last activity' column shows '18 days ago' for Akshada and '18 days ago' for rajaa and shree. The 'Password age' column shows '18 days' for Akshada and '22 days' for rajaa and shree. The 'Console last sign-in' column shows '-' for all users. The 'Actions' column shows 'Act' for all users.

	User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Acc
<input type="checkbox"/>	Akshada	/	0	-	-	-	-	-
<input type="checkbox"/>	rajaa	/	0	18 days ago	-	18 days	-	Act
<input type="checkbox"/>	shree	/	0	18 days ago	-	22 days	-	Act

6. Now Create AWS Customer Managed JSON Policy (S3-full-access-1hr) IAM → Policies → Create Policy → JSON.

The screenshot shows the 'Create policy' page in the AWS IAM console. The 'Specify permissions' step is active, showing a 'Policy editor' with a JSON policy document. The policy is titled 'S3-full-access-1hr' and allows 's3:*' actions on all resources for a duration of 1 hour. The 'Visual' tab is selected, and the 'JSON' tab is also visible. The 'Edit statement' section on the right shows a 'Select a statement' button and a 'Add new statement' button.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "AllowS3AccessForOneHour",
6       "Effect": "Allow",
7       "Action": "s3:*",
8       "Resource": "*",
9       "Condition": {
10        "DateGreaterThan": {
11          "aws:CurrentTime": "2024-12-08T15:55:00Z"
12        },
13        "DateLessThan": {
14          "aws:CurrentTime": "2024-12-08T16:35:00Z"
15        }
16      }
17    }
18  ]
19 }
```

7. Specify Policy Name, Then Click On Create Policy.

The screenshot shows the 'Review and create' step in the AWS IAM console. The breadcrumb navigation is 'IAM > Policies > Create policy'. On the left, a progress bar shows 'Step 1: Specify permissions' and 'Step 2: Review and create' (active). The main content area is titled 'Review and create' with a sub-header 'Policy details'. It contains two text input fields: 'Policy name' with the value 's3-full-access-one-hr' and 'Description - optional' which is empty. Below these is a section 'Permissions defined in this policy' with a search bar. The bottom of the screen shows a Windows taskbar with various application icons and a system tray with the date and time.

Step 1
Specify permissions

Step 2
Review and create

Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

s3-full-access-one-hr

Maximum 128 characters. Use alphanumeric and '+,=,@,-' characters.

Description - optional
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+,=,@,-' characters.

Permissions defined in this policy

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

8. Policy Created Successfully.

The screenshot shows the 'Policies' page in the AWS IAM console. A green banner at the top states 'Policy s3-full-access-one-hr created.' with a 'View policy' button. The page title is 'Policies (1314)' with an 'Info' link. Below the title is a search bar with 's3-full' and a 'Filter by Type' dropdown set to 'All types', showing '1 match'. A table lists the policies with columns for Policy name, Type, Used as, and Description. The table contains one entry: 's3-full-access-one-hr' with Type 'Customer managed' and Used as 'None'. The left sidebar shows the 'Identity and Access Management (IAM)' menu with options like 'User groups', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Root access management'. The bottom of the screen shows a Windows taskbar with various application icons and a system tray with the date and time.

Policy s3-full-access-one-hr created. View policy

Policies (1314)

A policy is an object in AWS that defines permissions.

Search s3-full Filter by Type All types 1 match

Policy name	Type	Used as	Description
s3-full-access-one-hr	Customer managed	None	-

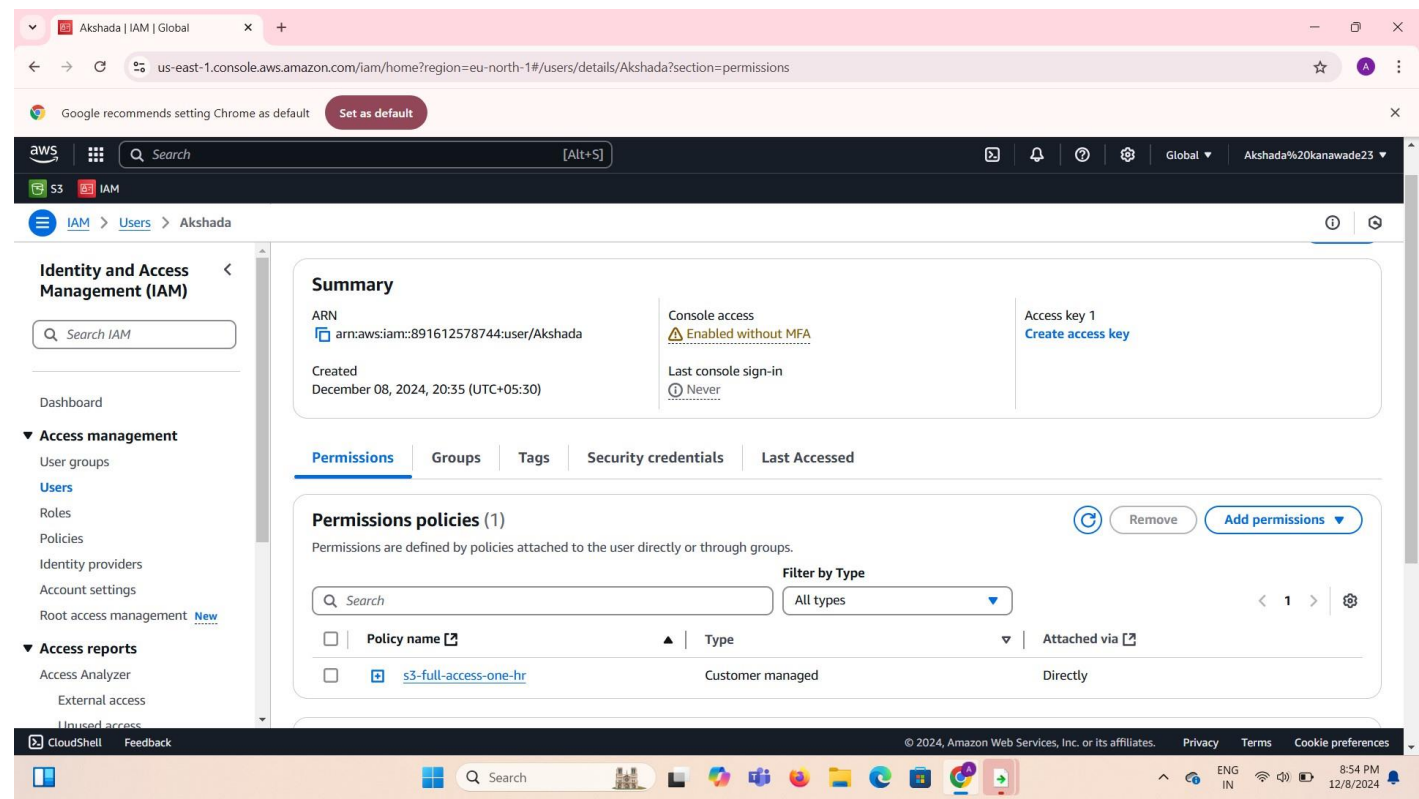
9. To Attached Policy To User , Go to User → Select User → Permission → Add Permission.

The screenshot shows the AWS IAM console for user 'Akshada'. The left sidebar shows the navigation menu with 'Users' selected. The main content area shows the user's details under the 'Permissions' tab. The 'Permissions policies (0)' section indicates that no permissions are currently attached to the user. The 'Add permissions' button is visible, and a dropdown menu is open showing options: 'Add permissions', 'Create inline policy', and 'Remove'.

10. Then , Attach Policies Directly → Select Policy → Next → Attach Policy.

The screenshot shows the 'Add permissions' wizard in the AWS IAM console. The 'Permissions options' section has three radio buttons: 'Add user to group', 'Copy permissions', and 'Attach policies directly'. The 'Attach policies directly' option is selected. Below this, the 'Permissions policies (1/1316)' section shows a search for 's3-fu' with one match: 's3-full-access-one-hr'. The 'Next' button is highlighted in orange.

11. S3-full-access-one-hr Policy is Attached To The User.



THANK YOU !!