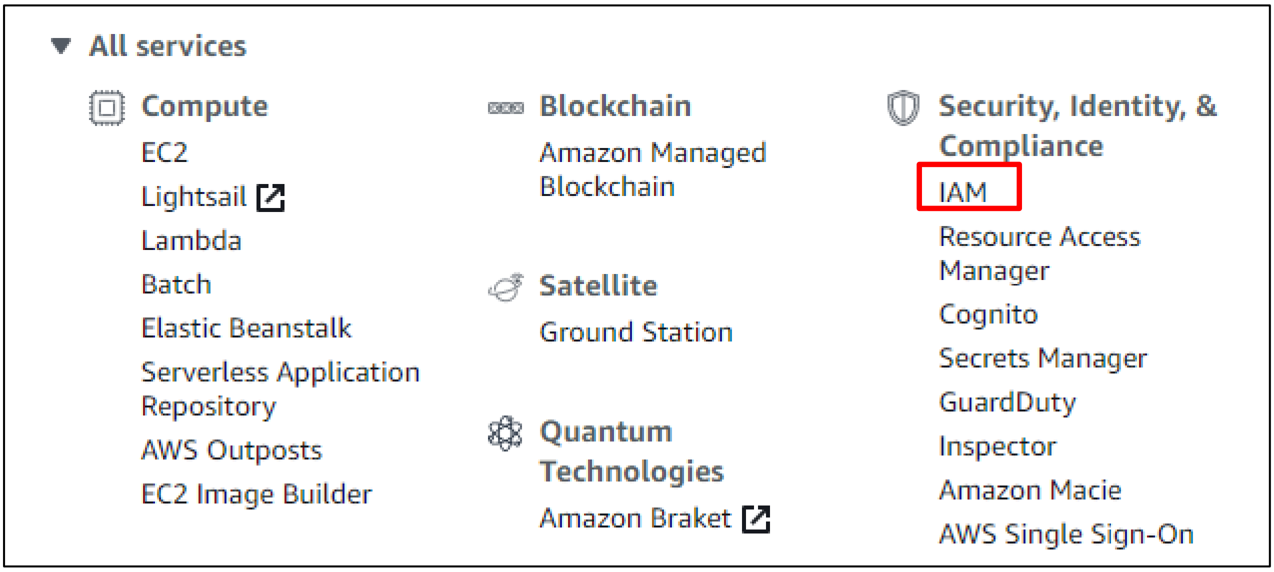
AWS IAM

Demo Document 6

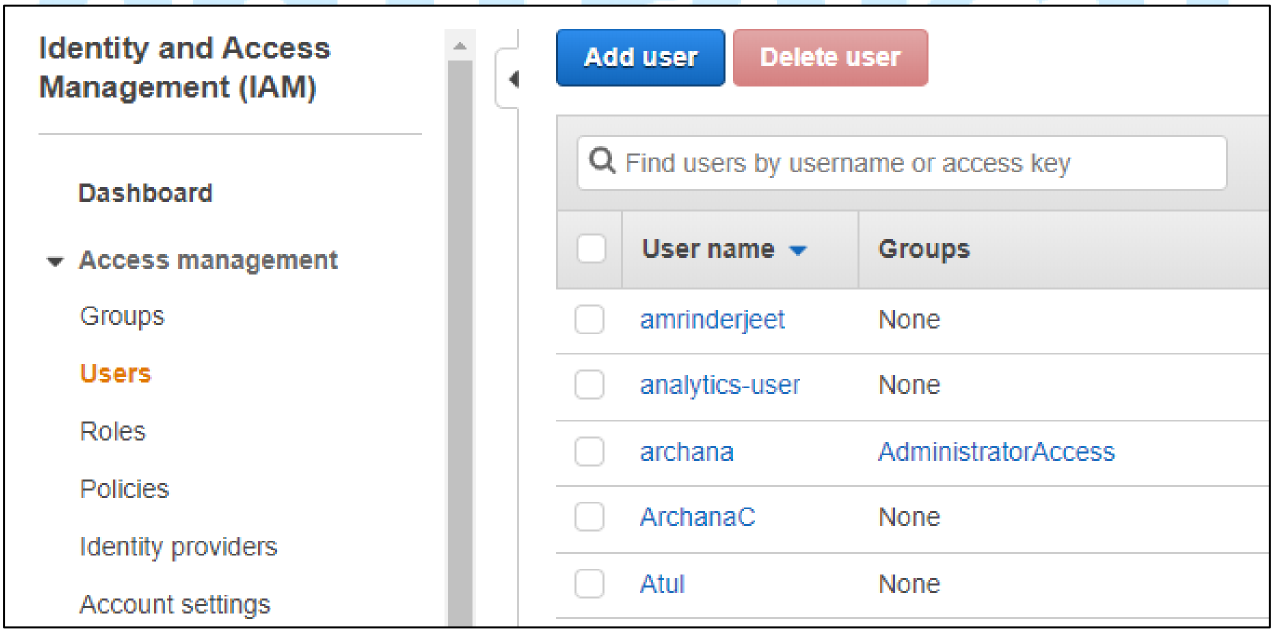
edureka!

Rotate Credentials Regularly

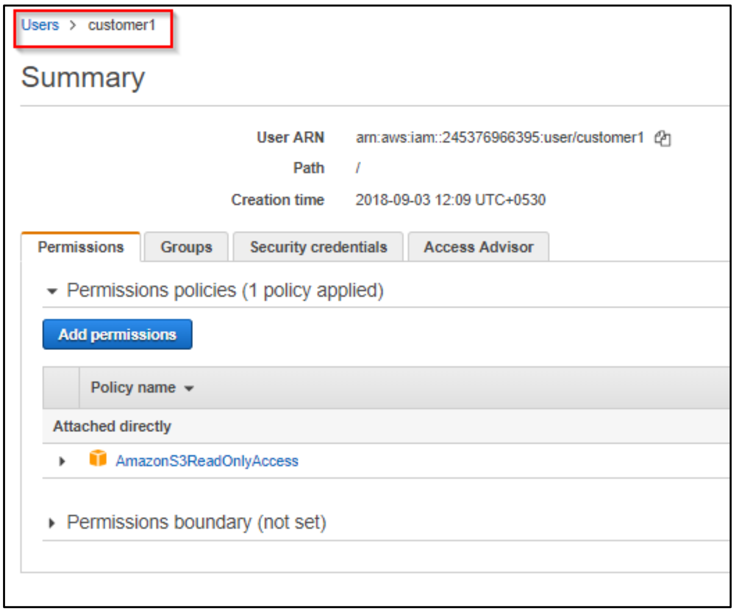
Step 1: Go to the AWS Management Console and select **AWS services**. Under the Security, Identity & Compliance, click on **IAM.**



Steps 2: Go to **Users** and then click on add user.



□	User name	Groups
□	amrinderjeet	None
□	analytics-user	None
□	archana	AdministratorAccess
□	ArchanaC	None
□	Atul	None



Users > customer1

Summary

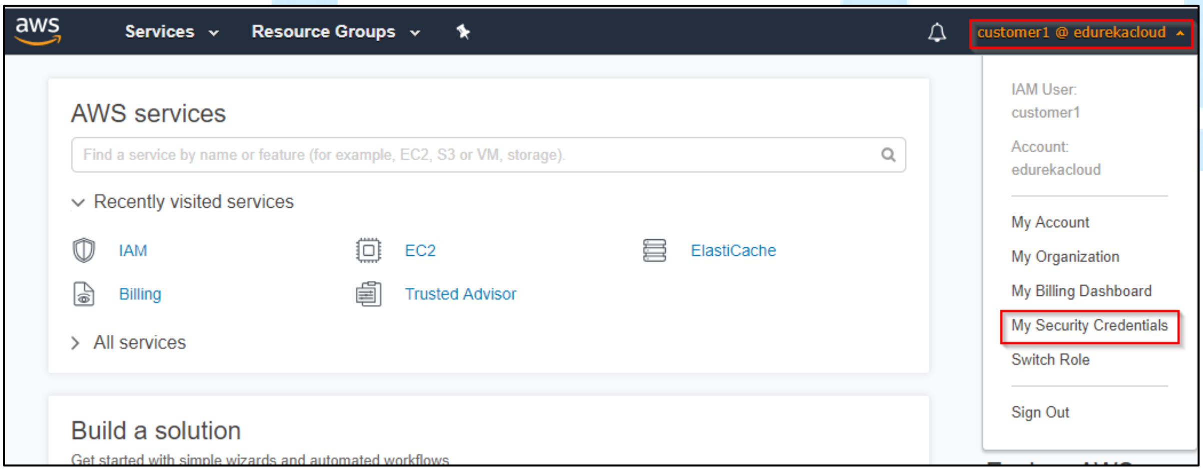
User ARN arn:aws:iam::245376966395:user/customer1

Path /

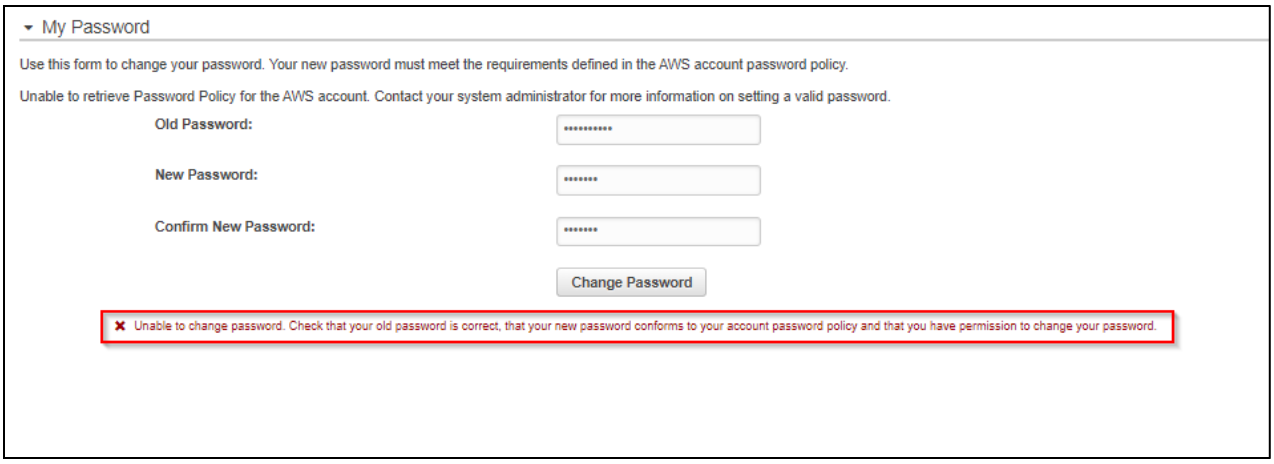
Creation time 2018-09-03 12:09 UTC+0530

Step 3: Sign out of the root account and sign in using the created user credentials. Here, as we have attached only the S3 read policy, you will be able to access only that.

In the right corner, select the **My Security Credentials** to check whether you can change your password or not.



Step 4: Enter the current password, new password, and click on **Change Password**. If it throws an ***error***, you won’t be able to change it because you don’t have the permission.



▾ My Password

Use this form to change your password. Your new password must meet the requirements defined in the AWS account password policy.

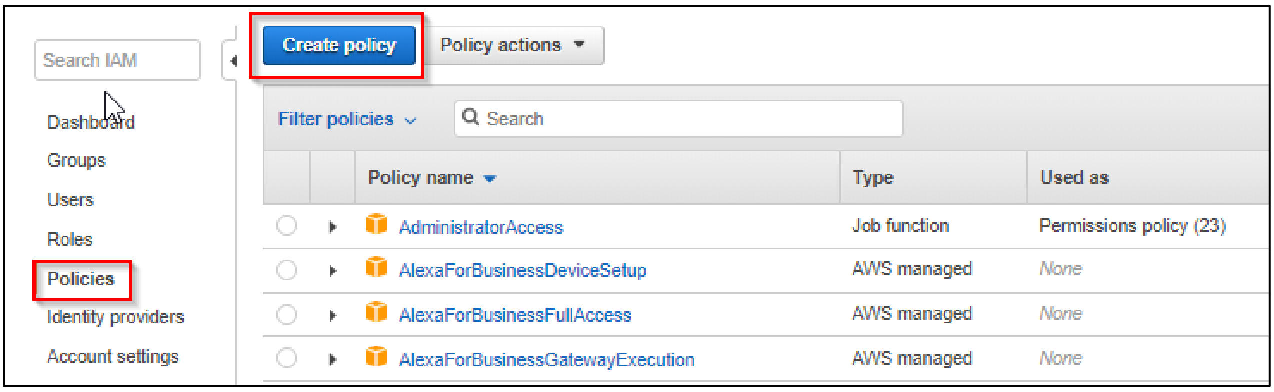
Unable to retrieve Password Policy for the AWS account. Contact your system administrator for more information on setting a valid password.

Old Password:	••••••••••
New Password:	•••••••
Confirm New Password:	•••••••

Change Password

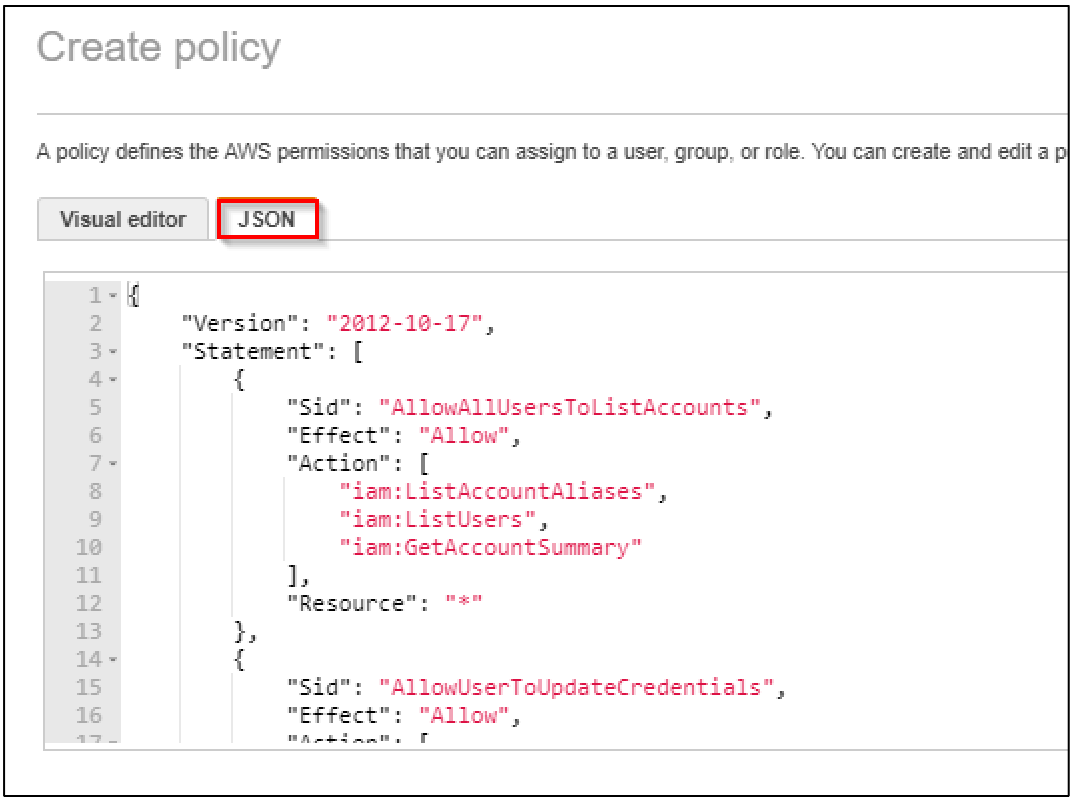
✖ Unable to change password. Check that your old password is correct, that your new password conforms to your account password policy and that you have permission to change your password.

Step 5: Go back to the root account, and under IAM, select the policies to create a new policy.



		Policy name ▾	Type	Used as
○	▸	AdministratorAccess	Job function	Permissions policy (23)
○	▸	AlexaForBusinessDeviceSetup	AWS managed	None
○	▸	AlexaForBusinessFullAccess	AWS managed	None
○	▸	AlexaForBusinessGatewayExecution	AWS managed	None

Step 6: Enter the ***JSON code*** and click on **Review Policy**.

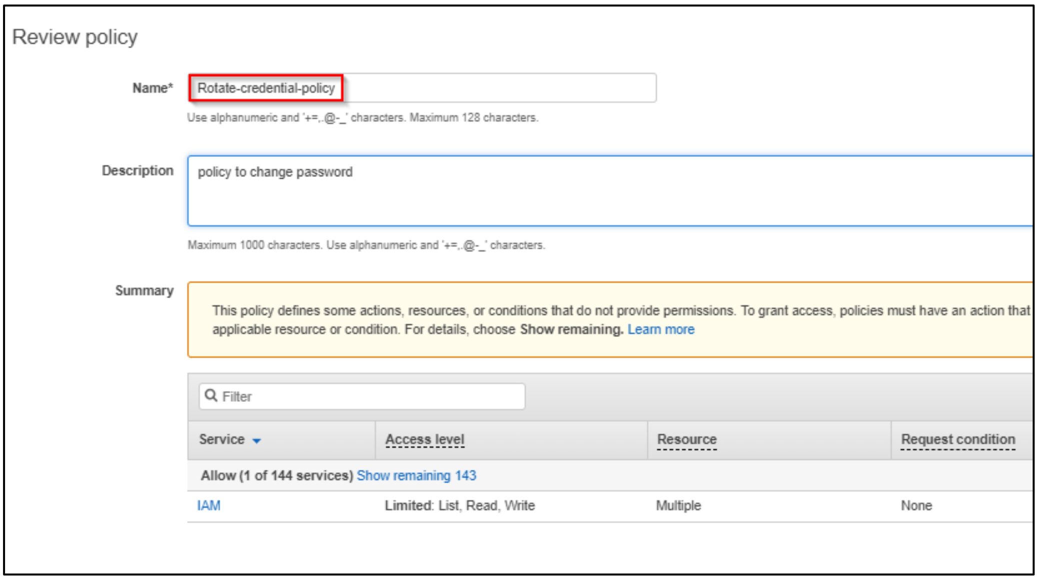


Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a p

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllUsersToListAccounts",
            "Effect": "Allow",
            "Action": [
                "iam:ListAccountAliases",
                "iam:ListUsers",
                "iam:GetAccountSummary"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUserToUpdateCredentials",
            "Effect": "Allow",
            "Action": [
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllUsersToListAccounts",
            "Effect": "Allow",
            "Action": [
                "iam:ListAccountAliases",
                "iam:ListUsers",
                "iam:GetAccountSummary"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUserToUpdateCredentials",
            "Effect": "Allow",
            "Action": [
                "iam:ChangePassword",
                "iam:CreateAccessKey",
                "iam:CreateLoginProfile",
                "iam:DeleteAccessKey",
                "iam:DeleteLoginProfile",
                "iam:GetAccountPasswordPolicy",
                "iam:GetLoginProfile",
                "iam:ListAccessKeys",
                "iam:UpdateAccessKey",
                "iam:UpdateLoginProfile",
                "iam:ListSigningCertificates",
                "iam:DeleteSigningCertificate",
                "iam:UpdateSigningCertificate",
                "iam:UploadSigningCertificate",
                "iam:ListSSHPublicKeys",
                "iam:GetSSHPublicKey",
                "iam:DeleteSSHPublicKey",
                "iam:UpdateSSHPublicKey",
                "iam:UploadSSHPublicKey"],
            "Resource": "arn:aws:iam::123456789123:user/${aws:username}"
        }]}
```

Step 7: Enter a unique name to the policy (ignore the summary) and click on **Create Policy**



Review policy

Name* Rotate-credential-policy

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

Description policy to change password

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

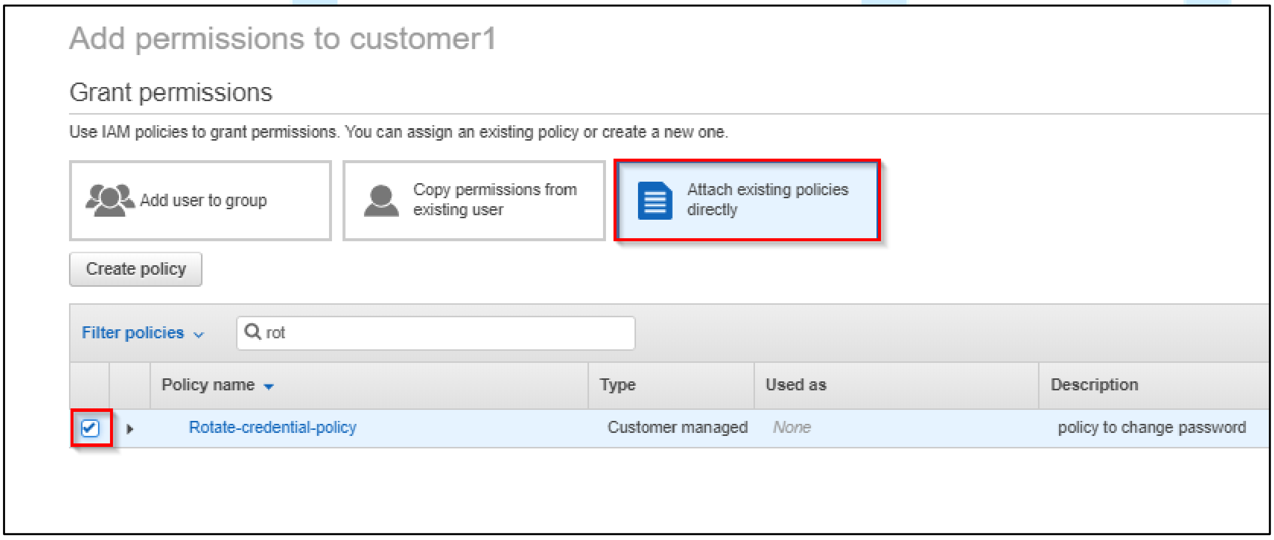
Summary

This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that applicable resource or condition. For details, choose **Show remaining.** Learn more

Filter

Service	Access level	Resource	Request condition
Allow (1 of 144 services) Show remaining 143			
IAM	Limited: List, Read, Write	Multiple	None

Step 8: Attach the policy to the user and click on **Add Permissions.**



Add permissions to customer1

Grant permissions

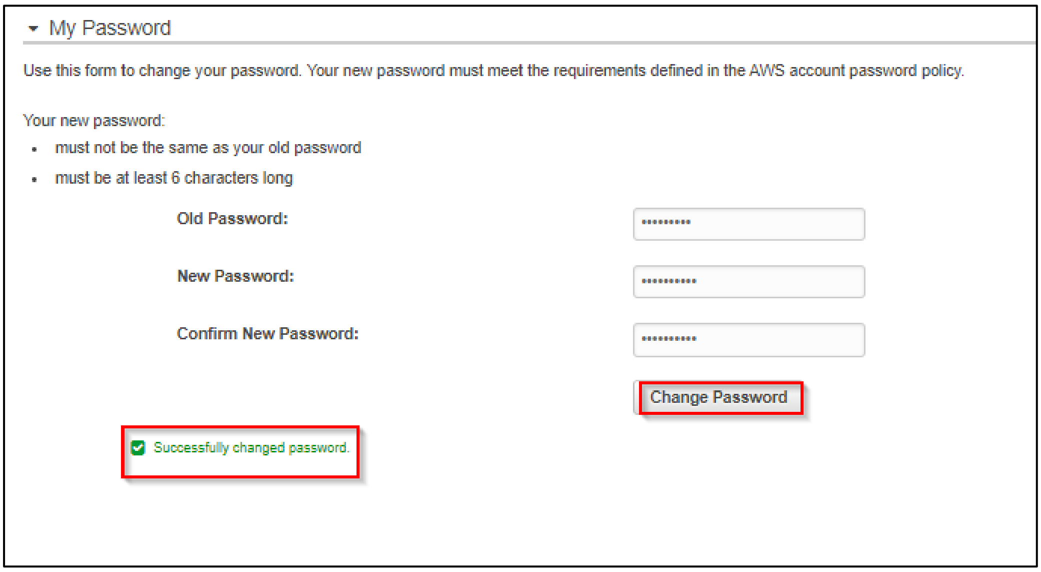
Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Add user to group
Copy permissions from existing user
Attach existing policies directly
Create policy
Filter policies

rot

☑		Policy name	Type	Used as	Description
☑	▸	Rotate-credential-policy	Customer managed	*None*	policy to change password

Step 9: Sign out from the root account and go back to the user account and try changing the password. This time it should be done.



My Password

Use this form to change your password. Your new password must meet the requirements defined in the AWS account password policy.

Your new password:

- must not be the same as your old password
- must be at least 6 characters long

Old Password: ••••••••••

New Password: •••••••••••

Confirm New Password: •••••••••••

✓ Successfully changed password.

Conclusion:

We have successfully created the **Rotate credentials policy** and attached it to the user so that the user can change the password anytime.