Module 2 - IAM

Saxena, Piyush

IAM (Identity and Access Management).

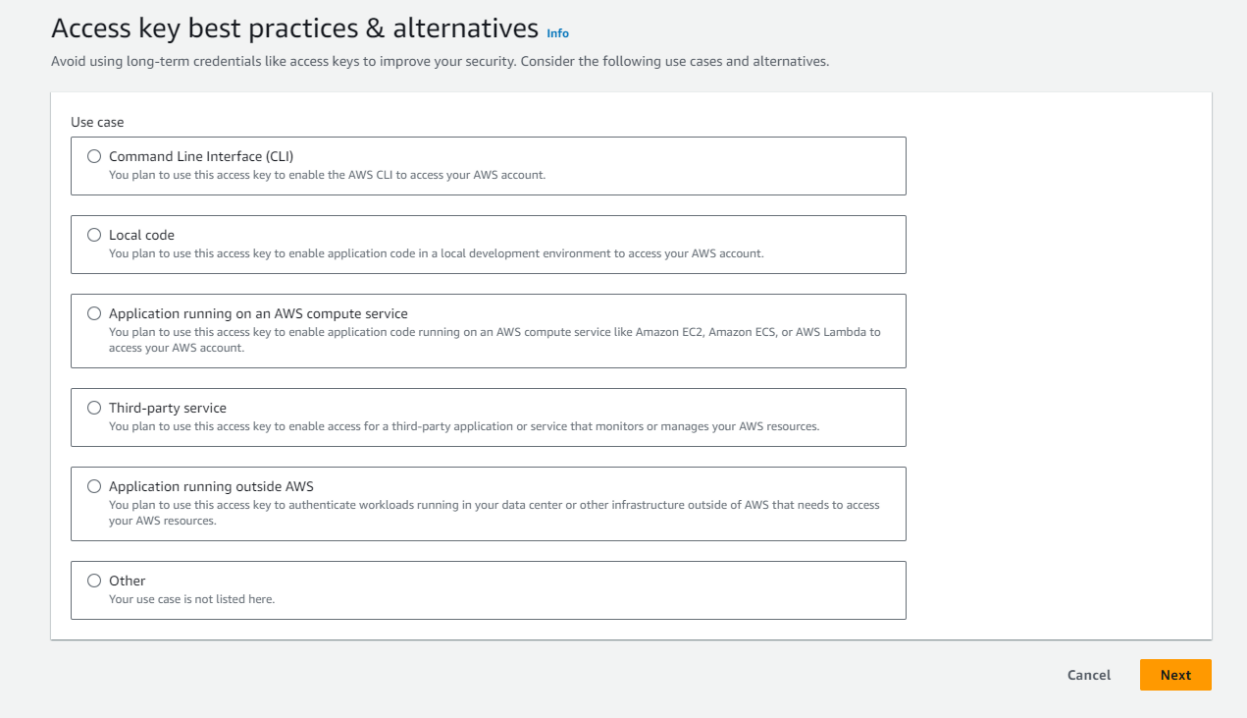
- IAM allows you to create and manage users, groups, roles, and policies.
- Users represent individual people who need access to your AWS resources.
- Groups are collections of users with similar access requirements.
- Roles are used to grant temporary access to external entities or services.
- Policies are written in JSON format and specify what actions are allowed or denied on specific AWS resources. These policies can be attached to IAM entities (users, groups, or roles) to grant or restrict access to AWS services and resources.

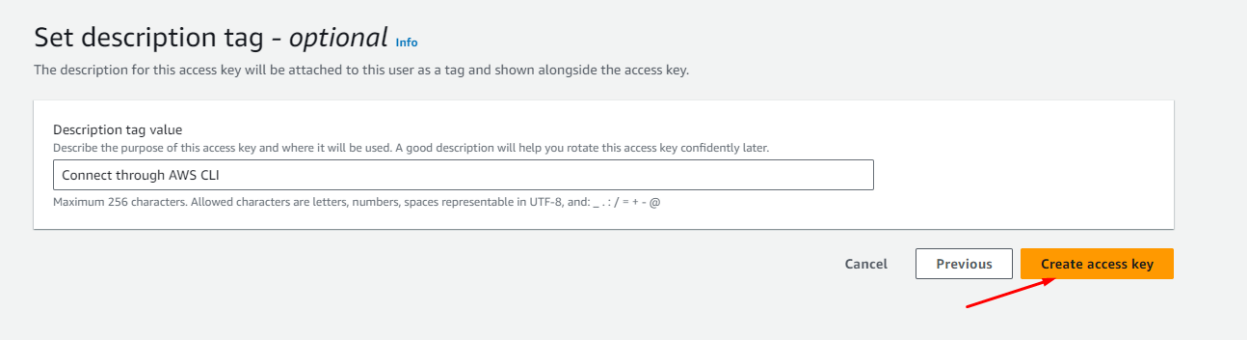
How to create user and their access keys.

- Go to the IAM services and click on Create User.
- Enter the username that you want to create and then select on AWS management console. This will help the user to use the console / AWS Portal.
- Click on Next, Now assigns the permissions that we want this user to have. Let's provide user with Admin permission.
- Click on Next and then click on create user.

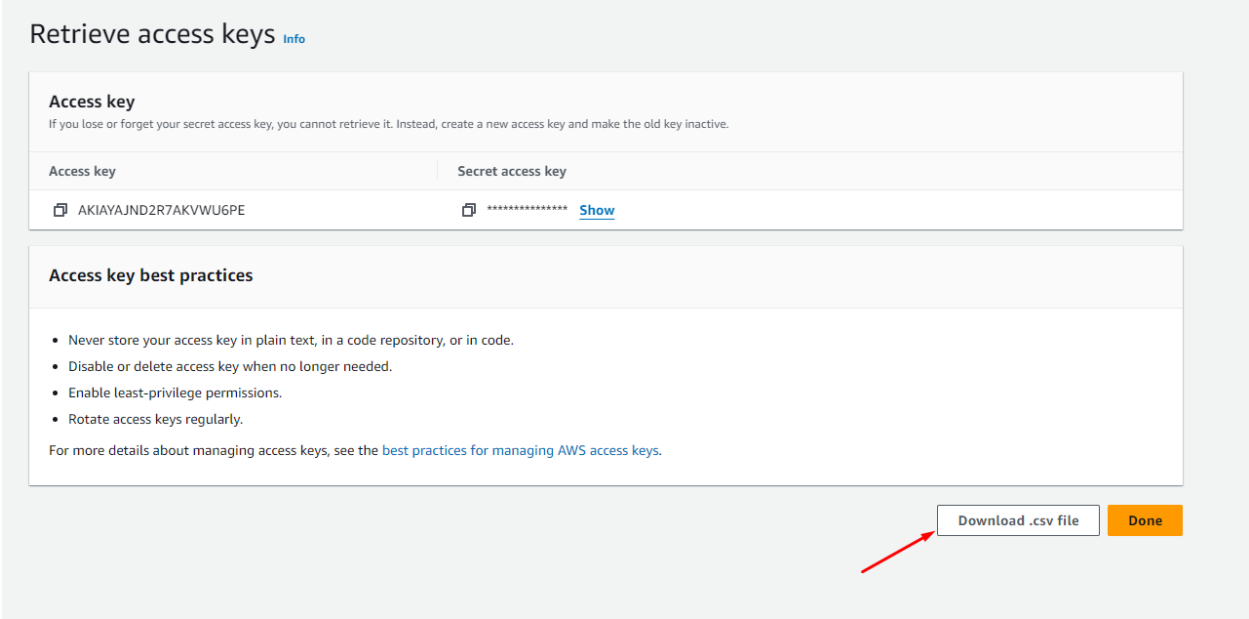
Access keys.

- click on Security credentials → create access key.





Download the .csv file for the future reference.



AWS CLI installation.

Go to https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html and select the operating system where we want to install.

Linux –
Run the below command. OS – RedHat

curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"

```
[ec2-user@ip-10-230-253-50 ~]$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
```

unzip awscliv2.zip

```
[ec2-user@ip-10-230-253-50 ~]$ unzip awscliv2.zip
```

sudo ./aws/install

```
[ec2-user@ip-10-230-253-50 ~]$ sudo ./aws/install
```

aws --version

```
[ec2-user@ip-10-230-253-50 ~]$ aws --version
aws-cli/2.15.0 Python/3.11.6 Linux/5.14.0-362.8.1.el9_3.x86_64 exe/x86_64.rhel.9 prompt/off
[ec2-user@ip-10-230-253-50 ~]$
```

Windows –
Download the msi package
https://awscli.amazonaws.com/AWSCLIV2.msi
double click on the file and install it.
Once its installed, open cmd to verify.

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.20348.2113]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>aws --version
aws-cli/2.15.0 Python/3.11.6 Windows/10 exec-env/EC2 exe/AMD64 prompt/off

C:\Users\Administrator>
```

How to create Roles and Policies.

We will be using below policy. This Policy will restrict the user to use any services apart from the services in **US-EAST-1**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "*",
      "Effect": "Deny",
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}
```

What is Inline Policy - An inline policy is a policy created for a single IAM identity (a user, group, or role). Inline policies maintain a strict one-to-one relationship between a policy and an identity. They are deleted when you delete the identity.

Role.

- Click on Create Role.
- Select entity as AWS Services and use cases as EC2 and then click Next.
- Here we are going to assign what Permission we are going to provide the users. In this case we are going to select SSM permission and later we will use this role to attach to EC2 instance.
- So, select below two permission –
    - **AmazonEC2RoleforSSM**
    - **AmazonSSMManagedEC2InstanceDefaultPolicy**
- Click on Next
- Specify the role name and give the Description.