



## Accessing AWS Services using CLI

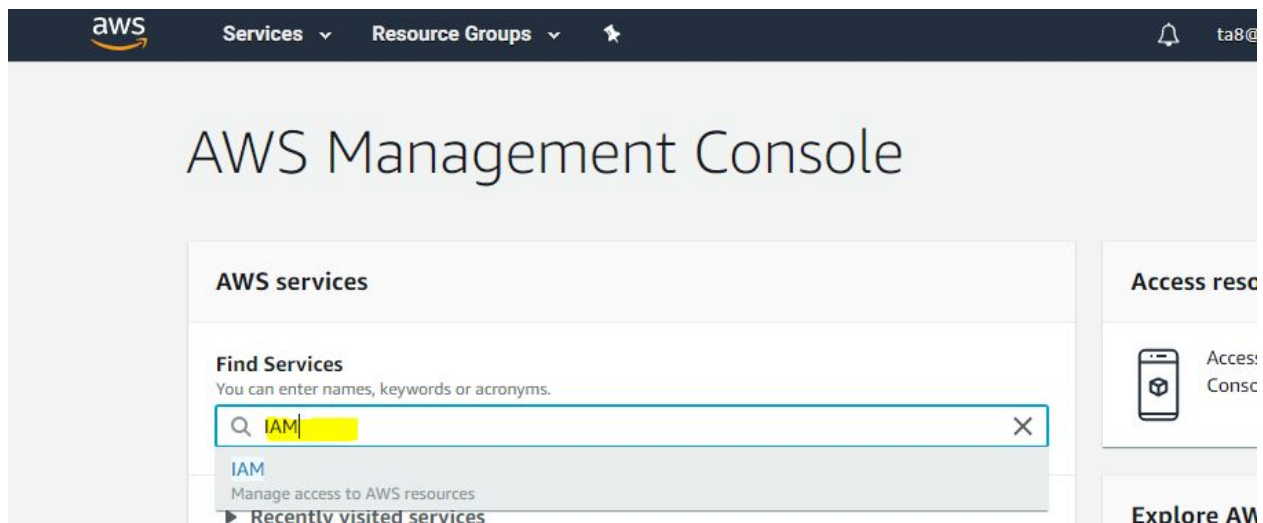
### Section 1: Creating Access Key Pair

To access AWS CLI from your local terminal, you need the Access key pair. The access key pair acts as the credentials for you to login to the AWS CLI through the local terminal. There are two components associated with it:

- Access key ID (user ID)
- Security access key (password)

Therefore, first, you must create the Access key pair to access AWS through AWS Console. You can follow the steps provided to generate the same:

1. Login to an AWS account and try to access the IAM service using the Search bar.





- After clicking on the service, you will land at the IAM Dashboard. There, click on the **Users** tab. You will be able to see your username on the page. Click on the username to get the details of the user.

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, the 'Users' tab is selected under the 'Access management' section. The main area displays a table of users. The first user, 'ta8@upgrad.com', is highlighted. Above the table, there are buttons for 'Add user' and 'Delete user', and a search bar labeled 'Find users by username or access key'. The table has columns for 'User name', 'Groups', 'Access key age', and 'Password age'. The user 'ta8@upgrad.com' is associated with the groups 'NL\_DND\_SSO', 'NL\_DND\_Upgrad\_Policy\_SDP', and 1 more. The 'Access key age' is 152 days, and the 'Password age' is also 152 days.

- Move to the “Security credentials” section and click on “Create access key” button.

The screenshot shows the AWS IAM console for the user 'ta8@upgrad.com'. The 'Security credentials' tab is selected. The page displays the user's ARN, path, and creation time. Below this, there are tabs for 'Permissions', 'Groups (3)', 'Tags', 'Security credentials', and 'Access Advisor'. The 'Security credentials' tab is active, showing 'Sign-in credentials' and 'Access keys'. Under 'Sign-in credentials', there is a 'Summary' section with a console sign-in link, a 'Console password' section (enabled, never signed in), an 'Assigned MFA device' section (not assigned), and a 'Signing certificates' section (none). Under 'Access keys', there is a 'Create access key' button. A note at the bottom states: 'Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret access key with anyone. As a best practice, we recommend frequent key rotation. Learn more'.

AWS will return with an Access key ID and the Secret Access Key in a dialogue box.



## Create access key



### Success

This is the **only** time that the secret access keys can be viewed or downloaded. You cannot recover them later. However, you can create new access keys at any time.



Download .csv file

Access key ID	Secret access key
AKIAxTRU3JEJDxFSQGwK	Xq0ihNxvmyrptfM3ycevCGefynynWi5DcNdR8P+8 Hide

- Click on Download .csv file to download the credentials. These credentials must be safely stored in your system and must not be shared, as they give complete control of your AWS account through the CLI.



## Section 2: Accessing AWS Services

Now, let us see how to use these credentials to run AWS CLI on your local machine. To do that:

1. Open to Command prompt on your laptop. You can search for **cmd** after pressing the Windows key.
2. On the command prompt, you can run the following command:

```
aws configure
```

3. AWS will ask you to provide the details. You can use the .csv file that you downloaded using the steps mentioned above to fill the required fields.

AWS Access Key ID [None]: \*\*\*\*\*QGWK

AWS Secret Access Key [None]: \*\*\*\*\*GefynynWi5D

4. Next, AWS will ask you for the default region and output format for the queries that you will implement using AWS CLI. Here, you are expected to provide the following details:

Default region name [None]: **us-east-1**

Default output format [None]: **json**



C:\WINDOWS\system32\cmd.exe

```
C:\Users\avdhesh.kumar>
C:\Users\avdhesh.kumar>
C:\Users\avdhesh.kumar>aws --version
aws-cli/1.17.9 Python/3.6.0 Windows/10 botocore/1.14.9

C:\Users\avdhesh.kumar>aws configure
AWS Access Key ID [None]: AKIAxTRU3JEJDXFSQGWK
AWS Secret Access Key [None]: Xq0ihNxvmYrptfM3ycevCGefynynWi5DcNdR8P+8
Default region name [None]: us-east-1
Default output format [None]: json

C:\Users\avdhesh.kumar>
```

Remember that you can change the output format, but the region must not be changed. It must be kept the same.

Let us now verify if you can access AWS services using CLI.

`aws s3 ls`

```
C:\Users\avdhesh.kumar>aws s3 ls
2020-01-23 11:38:10 test-agaw
2020-04-08 11:30:58 upgrad-123
2020-04-14 00:44:40 vasnotech.in

C:\Users\avdhesh.kumar>
```

As you can see, you can access the S3 buckets associated with this IAM user using AWS CLI.

---