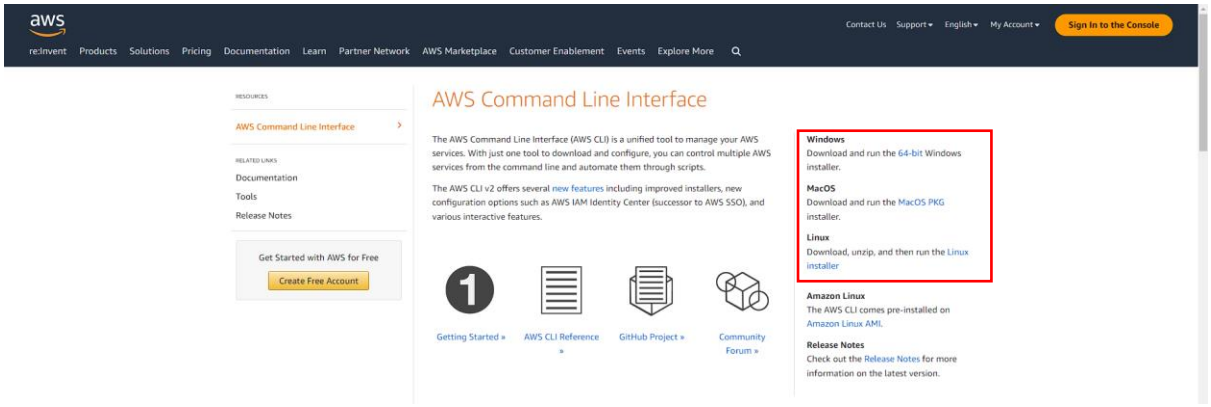
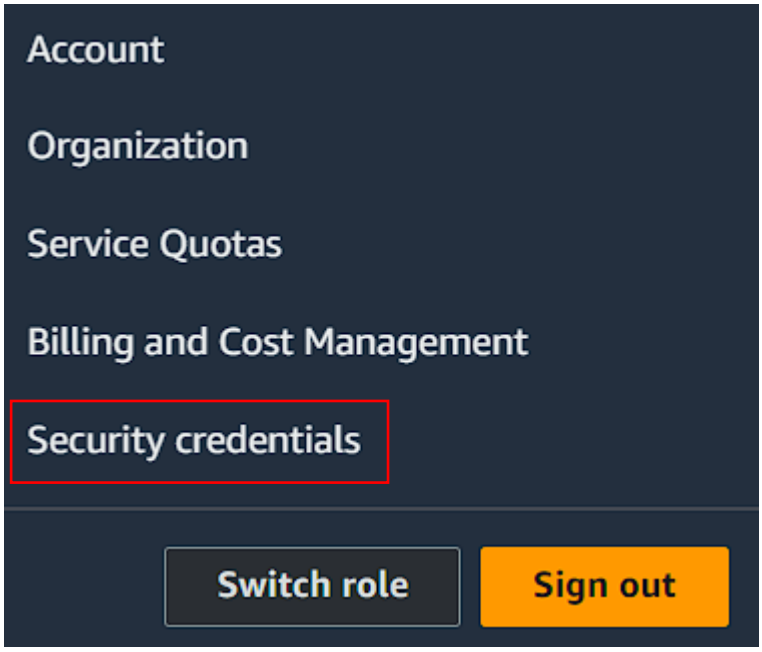
😊 AWS COMMAND LINE INTERFACE

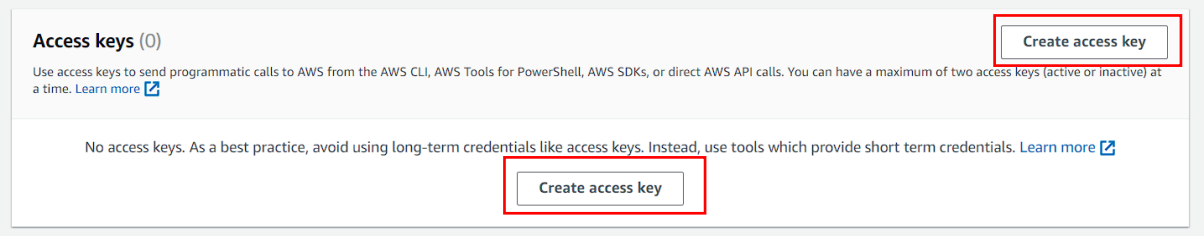
1. In this lab you are going to learn, how to use AWS CLI (Command Line Interface).
2. For that first you need to install AWS CLI.
3. Now you need to search AWS CLI on any of your browser. Then open the first site that is for official AWS. Or you can simply go to this website listed below and download CLI from there.
   https://aws.amazon.com/cli/
4. On the website you will see that you have different version of AWS CLI to install for.
5. Choose which ever OS you have either it is Windows, MacOS or Linux.



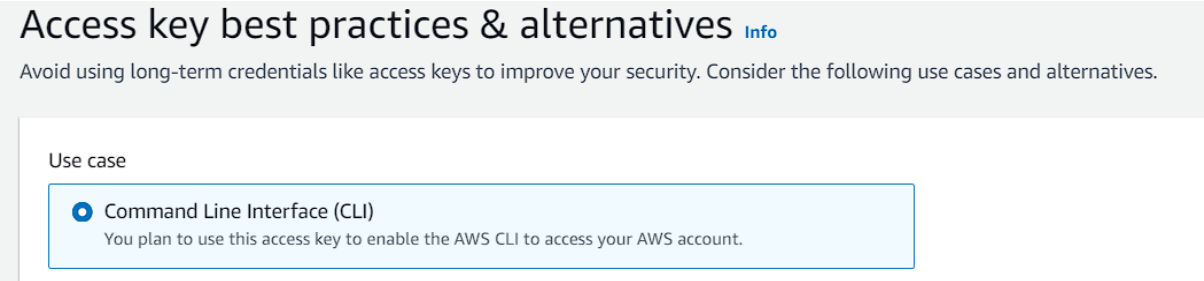
6. Just Download CLI and install it on your local machine.
7. After the installation you need to go back to AWS Console for your root user.
8. There you need to create Access keys for your root user.
9. For that you need to look at the top right of your screen there you will see your user's name, click on it.
10. There you have multiple option to choose from, but you need click on Security Credentials and open it.



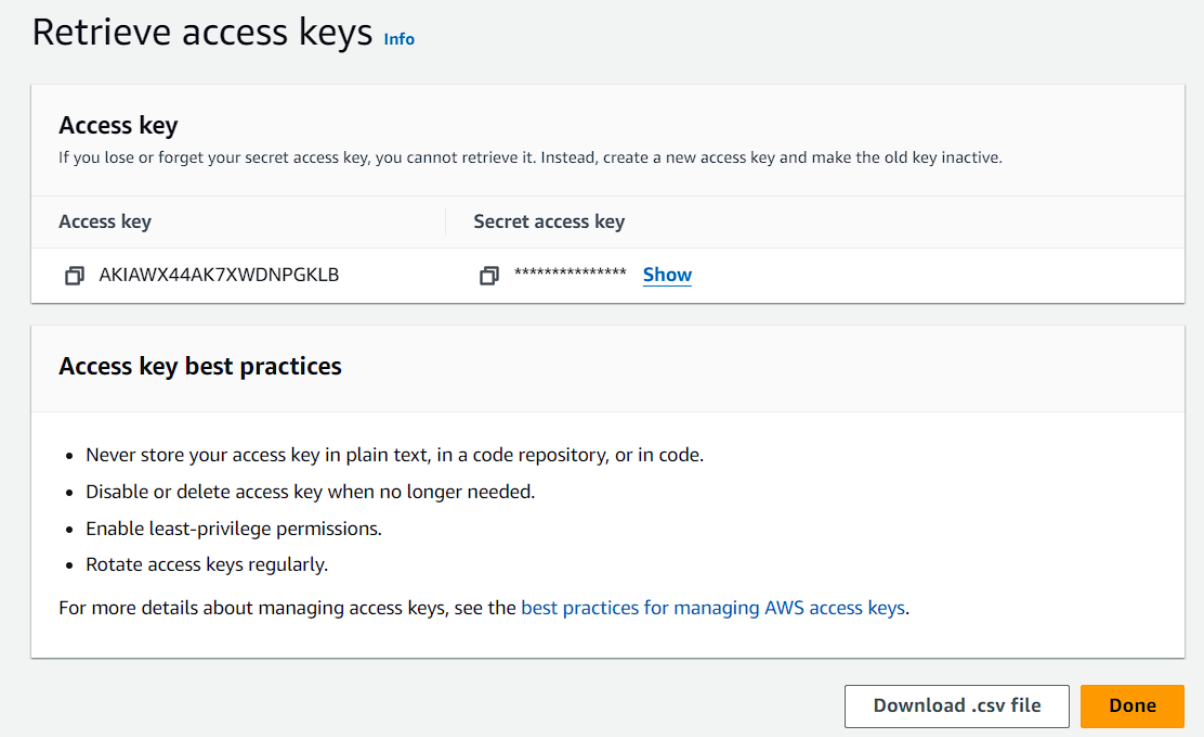
11. On the security credentials page if you scroll down a little, you will see your access keys option.
12. Here you need to click on Create access key.



13. Now in there you need to select command line interface.



14. Then move to next page. On the next page leave as it is.
15. Then click on create access keys.
16. Here you can see your access keys. You can also download them if you want to use them further. Because once you are off this page you won't get your secret access keys again. So, it is better recommended to paste it somewhere or download the .csv file of it.



17. Now you need to open **Command Prompt** on your local machine.

18. There you need to write **AWS configure** it will configure CLI for you and ask you to enter access key and secret access key.
19. You can see that once your access and secret access keys are entered it will ask your region.
20. Now you need to enter the region where most of the resources are. Type it and hit enter.
21. Then you leave default output format as it is.

```
C:\Users\      >aws configure
AWS Access Key ID [None]: AKIAZ37XJK363PISC47H
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]:
```

22. There are some commands which you need to run to view your AWS Resources.
23. First command is to check your buckets.
    Aws s3 ls
24. After typing this command hit enter and you will be able to see all your buckets.

```
C:\Users\      >aws s3 ls
2023-08-20 18:06:23 appbucket8000
2023-08-21 12:09:29 appbucket9000

C:\Users\      >
```

25. The next command is to list the objects that you have in your bucket.
    Aws s3 ls s3://appbucket9000

```
C:\Users\      >aws s3 ls s3://appbucket9000
                           PRE scripts/
2023-08-20 18:07:31        253 01.sql
2023-08-20 18:07:31        477 02.sql
2023-08-21 12:16:05        290 03.sql

C:\Users\      >
```

26. Now if you want to see the folders that are in your bucket then you can use this command
    Aws s3 ls s3://appbucket9000 --recursive

```
C:\Users\alash>aws s3 ls s3://appbucket9000 --recursive
2023-08-20 18:07:31        253 01.sql
2023-08-20 18:07:31        477 02.sql
2023-08-21 12:16:05        290 03.sql
2023-08-20 18:07:46          0 scripts/
2023-08-20 18:07:57        290 scripts/03.sql
2023-08-20 18:07:58        385 scripts/04.sql
2023-08-20 18:07:59        567 scripts/05.sql
```

27. There are some more commands if you want to try those you can also do that.

// The following command is used to list all EC2 Instances

aws ec2 describe-instances

// The following command is used to list an EC2 Instance based on the instance id

aws ec2 describe-instances --instance-ids i-0c5c3a771ff6d29bf

// The following command is used to start an EC2 Instance based on the instance id

aws ec2 start-instances --instance-ids i-0c5c3a771ff6d29bf

// The following command is used to stop an EC2 Instance based on the instance id

aws ec2 stop-instances --instance-ids i-0c5c3a771ff6d29bf

IT IS ALSO A BEST CHOICE TO GO AN DELETE YOUR ACCESS KEYS ONCE THEY HAVE SERVE THEIR PURPOSE.

GO BACK TO SECURITY CREDENTIALS AND FIRST DEACTIVATE YOUR ACCESS KEYS THEN DELETE IT.