



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.

The screenshot shows the AWS Command Line Interface (CLI) landing page. At the top, there's a navigation bar with links like 'Products', 'Documentation', 'Learn', 'AWS Marketplace', 'Events', and 'Explore More'. Below the navigation, there's a sidebar with 'AWS Command Line Interface' and 'RELATED LINKS' sections. The main content area is titled 'AWS Command Line Interface' and contains a brief introduction. It features several download links for different operating systems: 'Windows', 'MacOS', 'Linux', and 'Amazon Linux'. A large red box highlights the 'Windows' section, which includes a link to the '64-bit Windows installer'. Below the download links, there are 'Getting Started', 'AWS CLI Reference', 'GitHub Project', and 'Community Forum' links. On the right side, there's a 'Release Notes' section with a link to 'Release Notes'.

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.

The screenshot shows the AWS IAM 'Security credentials' page. At the top, there are links for 'Account', 'Organization', 'Service Quotas', and 'Billing and Cost Management'. Below these, there's a prominent red box around the 'Security credentials' link. At the bottom, there are two buttons: 'Switch role' (in a grey box) and 'Sign out' (in an orange box). The 'Switch role' button is also highlighted with a red box.

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.

Access keys (0)
Create access key

No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#)

Create access key

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

Access key best practices & alternatives [Info](#)

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

Command Line Interface (CLI)

You plan to use this access key to enable the AWS CLI to access your AWS account.

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.

Retrieve access keys [Info](#)

Access key

If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key

Secret access key

AKIAWX44AK7XWDNPGKLB

***** [Show](#)

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

[Download .csv file](#)

[Done](#)

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 AND DELETE YOUR ACCESS KEYS ONCE THEY HAVE SERVED THEIR PURPOSE.

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