Day 2: IAM Basics

Topic: Identity and Access Management (IAM)

Understanding IAM (Identity and Access Management)

IAM stands for **Identity and Access Management**. IAM helps you decide **who** is allowed to do **what** in your AWS account. That means IAM helps you control **who** can access your **AWS resources**.

Example:

1. Imagine a school: some people are **students**, some are **teachers**, and not everyone can go into every room.
2. Think of it like giving **keys** to your digital house – you decide **who** gets a key and **what rooms** they can enter.

   Just like in real life, you don't want everyone to have access to everything. IAM is the tool that lets you **organize** and **protect** your AWS environment.

Why IAM is Important

Imagine your AWS account is a **house**. Would you give every visitor a **master key** to every room? Probably not!

IAM helps you:

- **Control** access to your resources.
- **Give the right permissions** to the right people.
- **Track** who is doing what.
- Helps you keep everything **safe and sound**.

Example: You might want your **developer** to access only **EC2** (virtual servers), but not **billing information**. IAM makes this possible.

Users, Groups, and Roles

- **User**: A person or application that needs access to AWS.
  Example: Alice, a developer.
- **Group**: A collection of users with similar permissions.
  Example: All developers in the **DevTeam** group.

- **Role**: A set of permissions that can be **temporarily assumed** by users or services.
  Example: An app running on **EC2** that needs to access **S3**.

Policies and JSON Structure

Policies – The Rules of IAM:
Policies are like **permission slips**. They are written in **JSON** and define what **actions** are allowed or denied.

Each policy contains:

- **Version**: Always use '2012-10-17' for modern policies.
- **Statement**: What is allowed or denied.
- **Effect**: 'Allow' or 'Deny'.
- **Action**: What the user can do (e.g., 's3:*' = all actions on S3).
- **Resource**: What the actions apply to (e.g., a specific **bucket**).

Example Policy:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "s3:*",
 "Resource": "*"
 }
]
}
```

This means: Allow everything (all actions) in S3 for this user.

Challenge Task – Let's Practice!

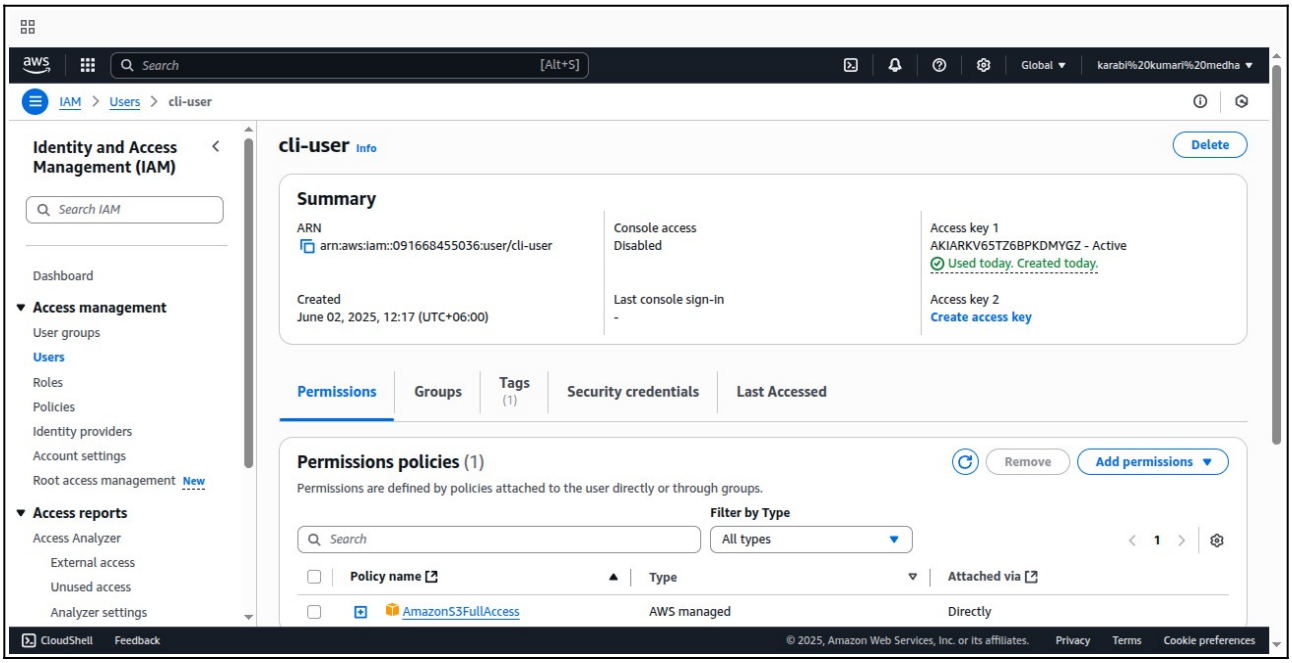
Your task is to create an **IAM user** with the following steps:

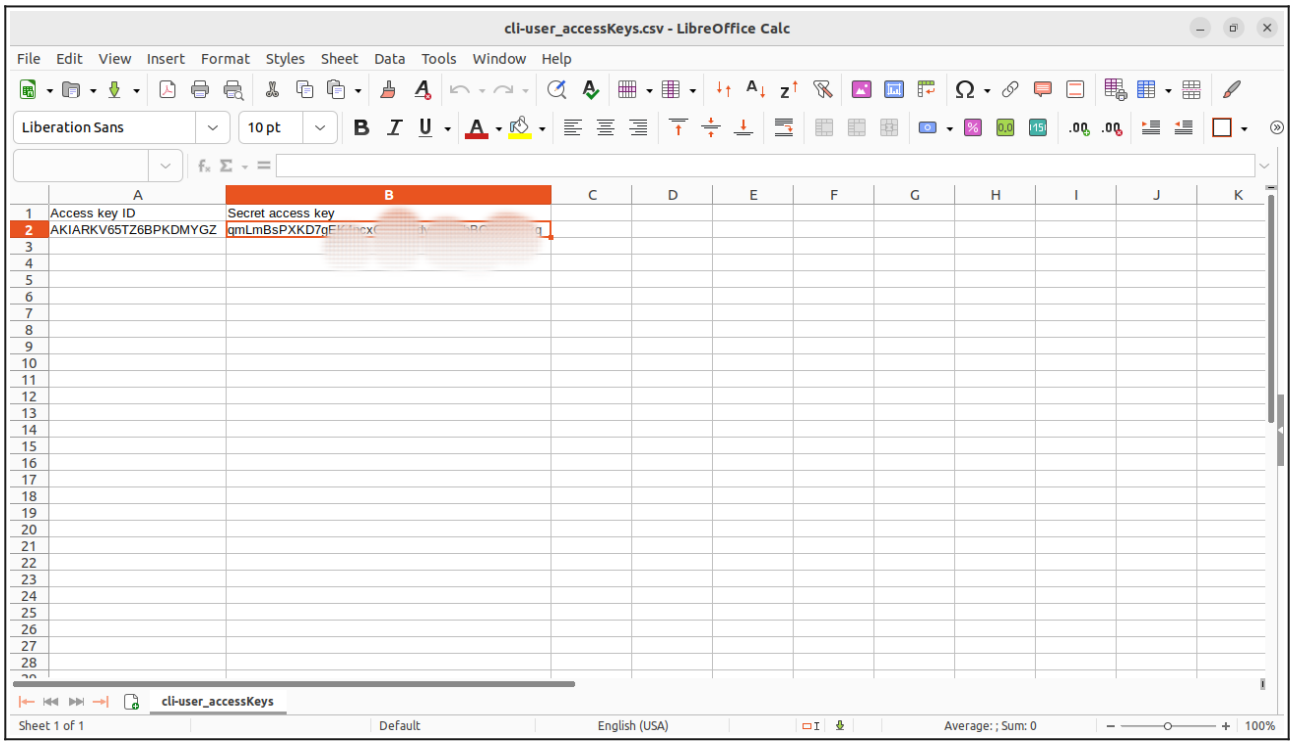
1. Go to the **IAM** section in **AWS**.
2. Click '**Add user**'.
3. Enter a name like '**s3-access-user**'.
4. Enable '**Programmatic access**' to use the AWS CLI.
5. On the **permissions** page, attach the policy called '**AmazonS3FullAccess**'.
6. Finish creating the user and note down the **Access Key ID** and **Secret**.

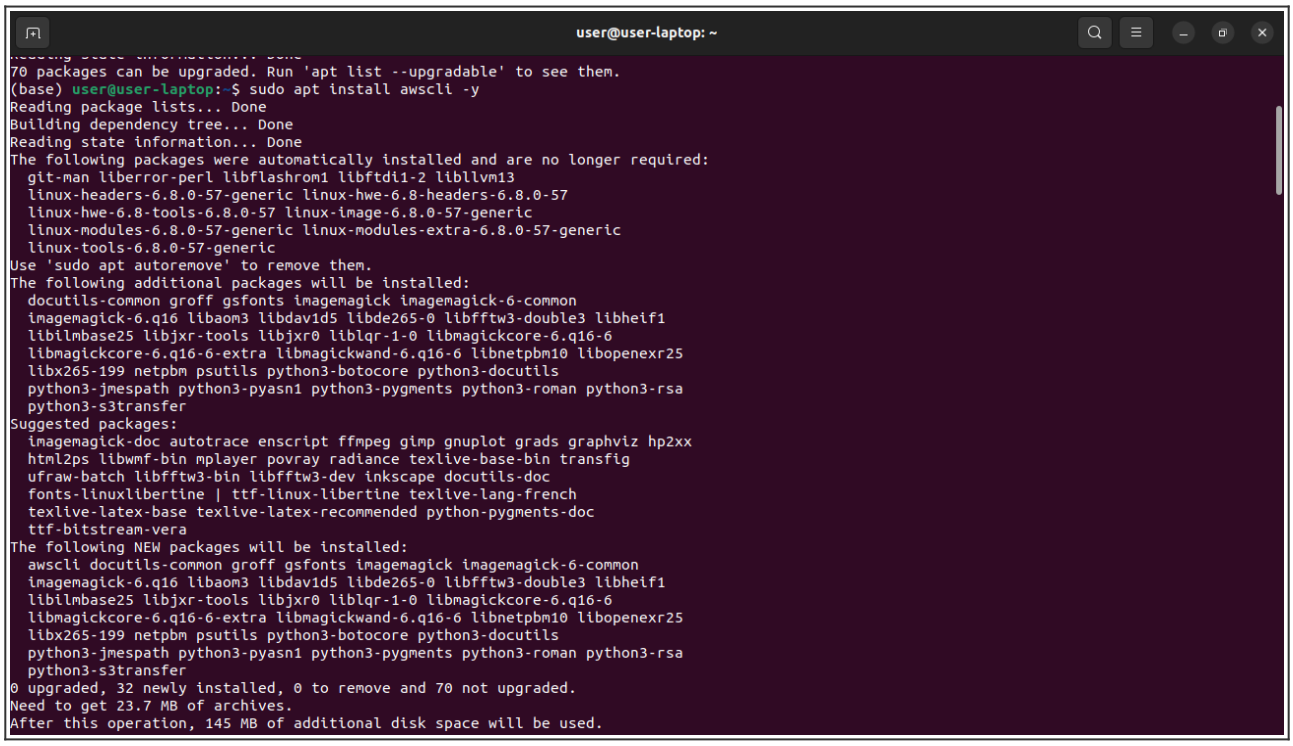
Now this user can use tools like the **AWS CLI** to work with **S3 buckets** (create, delete, upload files, etc.).

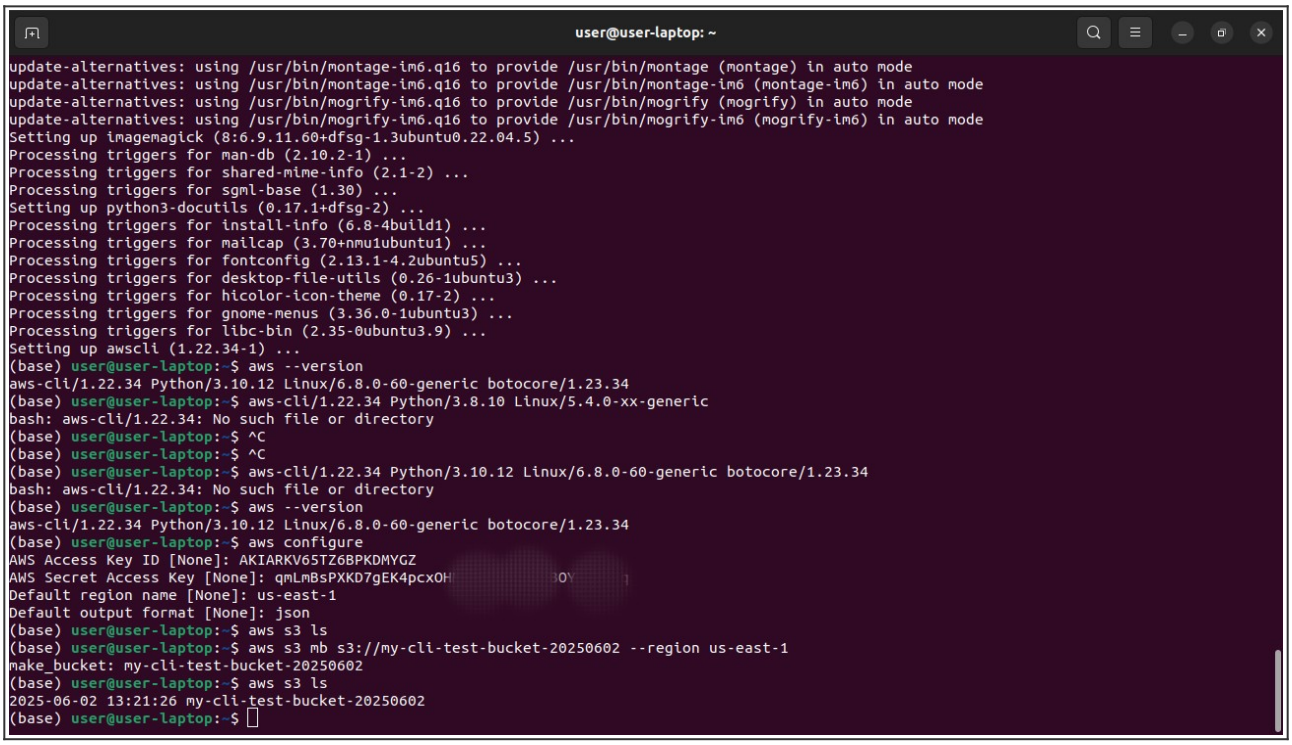
Tip: Always give only the **permissions that are truly needed**.

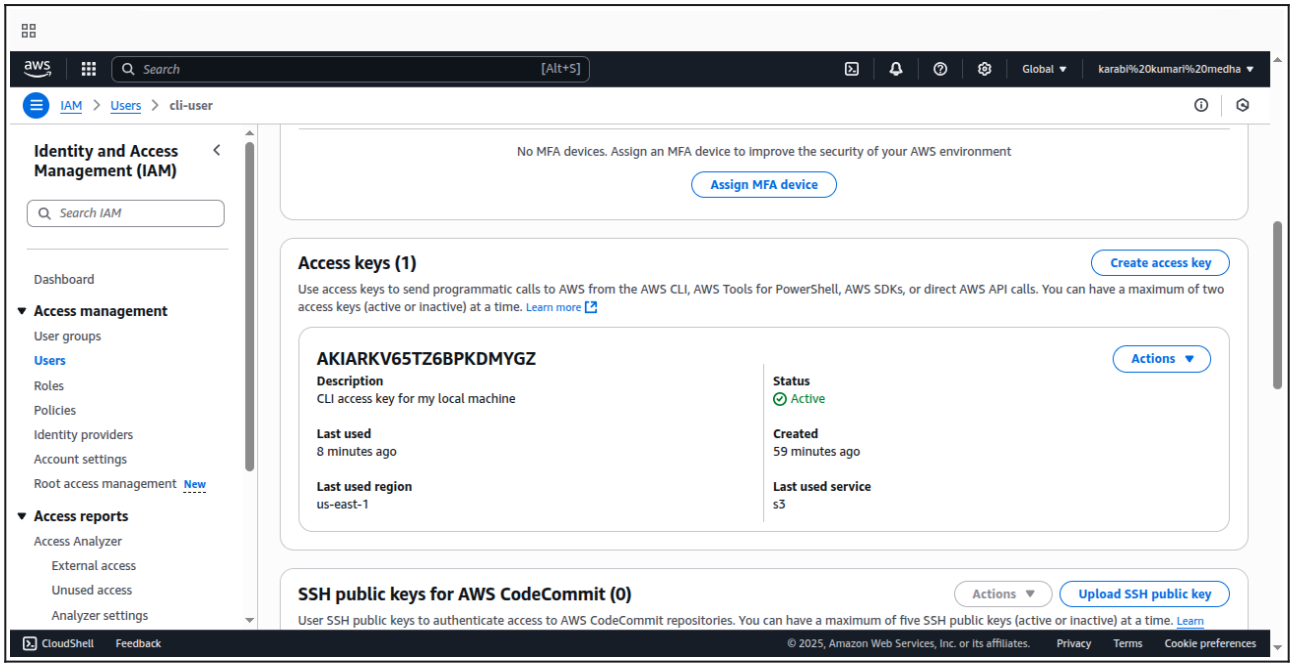
Work in Action

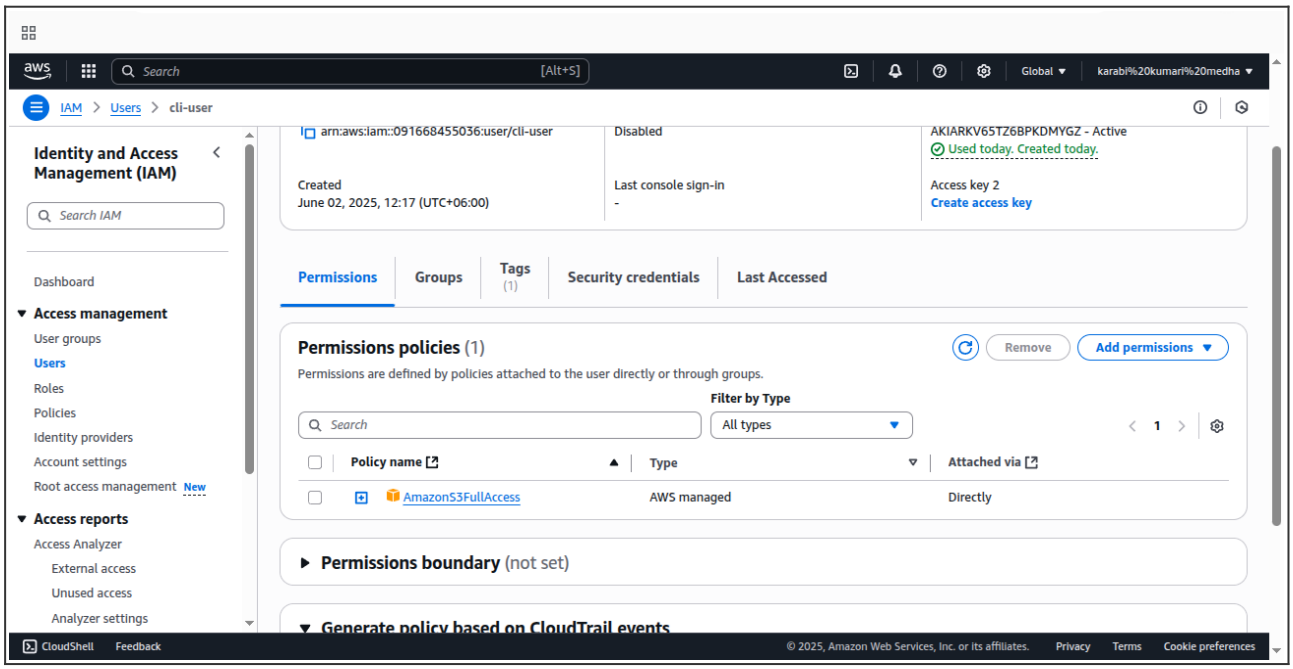



cli-user_accessKeys.csv - LibreOffice Calc
File Edit View Insert Format Styles Sheet Data Tools Window Help
Liberation Sans
10 pt
Access key ID
Secret access key
AKIARKV65TZ6BPKDMYGZ
cli-user_accessKeys
Sheet 1 of 1
Default
English (USA)
Average: ; Sum: 0
100%


user@user-laptop: ~
70 packages can be upgraded. Run 'apt list --upgradable' to see them.
(base) user@user-laptop:~$ sudo apt install awscli -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
git-man liberror-perl libflashrom1 libftdi1-2 libllvm13
linux-headers-6.8.0-57-generic linux-hwe-6.8-headers-6.8.0-57
linux-hwe-6.8-tools-6.8.0-57 linux-image-6.8.0-57-generic
linux-modules-6.8.0-57-generic linux-modules-extra-6.8.0-57-generic
linux-tools-6.8.0-57-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
docutils-common groff gsfonts imagemagick imagemagick-6-common
imagemagick-6.q16 libaom3 libdav1d5 libde265-0 libfftw3-double3 libheif1
libilmbase25 libjxr-tools libjxr0 liblqr-1-0 libmagickcore-6.q16-6
libmagickcore-6.q16-6-extra libmagickwand-6.q16-6 libnetpbm10 libopenexr25
libx265-199 netpbm psutils python3-botocore python3-docutils
python3-jmespath python3-pyasn1 python3-pygments python3-roman python3-rsa
python3-s3transfer
Suggested packages:
imagemagick-doc autotrace enscript ffmpeg gimp gnuplot grads graphviz hp2xx
html2ps libwmf-bin mplayer povray radiance texlive-base-bin transfig
ufraw-batch libfftw3-bin libfftw3-dev inkscape docutils-doc
fonts-linuxlibertine | ttf-linux-libertine texlive-lang-french
texlive-latex-base texlive-latex-recommended python-pygments-doc
ttf-bitstream-vera
The following NEW packages will be installed:
awscli docutils-common groff gsfonts imagemagick imagemagick-6-common
imagemagick-6.q16 libaom3 libdav1d5 libde265-0 libfftw3-double3 libheif1
libilmbase25 libjxr-tools libjxr0 liblqr-1-0 libmagickcore-6.q16-6
libmagickcore-6.q16-6-extra libmagickwand-6.q16-6 libnetpbm10 libopenexr25
libx265-199 netpbm psutils python3-botocore python3-docutils
python3-jmespath python3-pyasn1 python3-pygments python3-roman python3-rsa
python3-s3transfer
0 upgraded, 32 newly installed, 0 to remove and 70 not upgraded.
Need to get 23.7 MB of archives.
After this operation, 145 MB of additional disk space will be used.


user@user-laptop: ~
update-alternatives: using /usr/bin/montage-im6.q16 to provide /usr/bin/montage (montage) in auto mode
update-alternatives: using /usr/bin/montage-im6.q16 to provide /usr/bin/montage-im6 (montage-im6) in auto mode
update-alternatives: using /usr/bin/mogrify-im6.q16 to provide /usr/bin/mogrify (mogrify) in auto mode
update-alternatives: using /usr/bin/mogrify-im6.q16 to provide /usr/bin/mogrify-im6 (mogrify-im6) in auto mode
Setting up imagemagick (8:6.9.11.60+dfsg-1.3ubuntu0.22.04.5) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for shared-mime-info (2.1-2) ...
Processing triggers for sgml-base (1.30) ...
Setting up python3-docutils (0.17.1+dfsg-2) ...
Processing triggers for install-info (6.8-4build1) ...
Processing triggers for mailcap (3.70+nmu1ubuntu1) ...
Processing triggers for fontconfig (2.13.1-4.2ubuntu5) ...
Processing triggers for desktop-file-utils (0.26-1ubuntu3) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu3) ...
Processing triggers for libc-bin (2.35-0ubuntu3.9) ...
Setting up awscli (1.22.34-1) ...
(base) user@user-laptop:~$ aws --version
aws-cli/1.22.34 Python/3.10.12 Linux/6.8.0-60-generic botocore/1.23.34
(base) user@user-laptop:~$ aws-cli/1.22.34 Python/3.8.10 Linux/5.4.0-xx-generic
bash: aws-cli/1.22.34: No such file or directory
(base) user@user-laptop:~$ ^C
(base) user@user-laptop:~$ ^C
(base) user@user-laptop:~$ aws-cli/1.22.34 Python/3.10.12 Linux/6.8.0-60-generic botocore/1.23.34
bash: aws-cli/1.22.34: No such file or directory
(base) user@user-laptop:~$ aws --version
aws-cli/1.22.34 Python/3.10.12 Linux/6.8.0-60-generic botocore/1.23.34
(base) user@user-laptop:~$ aws configure
AWS Access Key ID [None]: AKIARKV65TZ6BPKDMYGZ
AWS Secret Access Key [None]: qmLmBsPXKD7gEK4pcxOH
Default region name [None]: us-east-1
Default output format [None]: json
(base) user@user-laptop:~$ aws s3 ls
(base) user@user-laptop:~$ aws s3 mb s3://my-cli-test-bucket-20250602 --region us-east-1
make_bucket: my-cli-test-bucket-20250602
(base) user@user-laptop:~$ aws s3 ls
2025-06-02 13:21:26 my-cli-test-bucket-20250602
(base) user@user-laptop:~$


Search
[Alt+S]
Global
karabi%20kumari%20medha
IAM > Users > cli-user
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
No MFA devices. Assign an MFA device to improve the security of your AWS environment
Assign MFA device
Access keys (1)
Create access key
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more
AKIARKV65TZ6BPKDMYGZ
Actions
Description
CLI access key for my local machine
Status
Active
Last used
8 minutes ago
Created
59 minutes ago
Last used region
us-east-1
Last used service
s3
SSH public keys for AWS CodeCommit (0)
Actions
Upload SSH public key
User SSH public keys to authenticate access to AWS CodeCommit repositories. You can have a maximum of five SSH public keys (active or inactive) at a time. Learn
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
Global
karabi%20kumari%20medha
IAM
Users
cli-user
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
arn:aws:iam::091668455036:user/cli-user
Disabled
AKIARKV65TZ6BPKDMYGZ - Active
Used today. Created today.
Created
June 02, 2025, 12:17 (UTC+06:00)
Last console sign-in
-
Access key 2
Create access key
Permissions
Groups
Tags (1)
Security credentials
Last Accessed
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
Search
All types
1
Policy name
Type
Attached via
AmazonS3FullAccess
AWS managed
Directly
Permissions boundary (not set)
Generate policy based on CloudTrail events
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences