

AWS CLI and IAM Users

1. AWS CLI (Command Line Interface)

The AWS Command Line Interface (CLI) is a tool that allows users to interact with AWS services using command-line commands. It provides an alternative to using the AWS Management Console and is useful for automation, scripting, and managing AWS resources efficiently.

Key Features of AWS CLI:

- Allows management of AWS services from a terminal or command prompt.
- Supports automation via shell scripting and other programming tools.
- Can be configured with different AWS credentials (profiles).
- Works across Windows, macOS, and Linux.
- Provides support for almost all AWS services.

Basic AWS CLI Commands:

- `aws configure` – Configures the AWS CLI with access key, secret key, region, and output format.
 - `aws s3 ls` – Lists S3 buckets.
 - `aws ec2 describe-instances` – Retrieves details of EC2 instances.
 - `aws iam list-users` – Lists IAM users in the AWS account.
-

2. AWS IAM (Identity and Access Management)

AWS IAM is a service that helps securely control access to AWS resources. It enables the creation and management of users, groups, roles, and policies.

IAM Users:

An IAM user is an entity that interacts with AWS. Users are created under an AWS account and can be assigned permissions using policies.

Key Concepts of IAM Users:

- **IAM User Credentials:** Each user can have an Access Key ID and Secret Access Key for programmatic access (CLI, SDK).
- **IAM Policies:** JSON-based rules that define permissions for users, groups, or roles.
- **IAM Groups:** A collection of users that share the same permissions.
- **IAM Roles:** Temporary access permissions assigned to users or services.

```
Command Prompt
Microsoft Windows [Version 10.0.22631.4751]
(c) Microsoft Corporation. All rights reserved.

C:\Users\eriga>aws --version
aws-cli/2.24.4 Python/3.12.6 Windows/11 exe/AMD64

C:\Users\eriga>
```

aws

Search

[Alt+S]

IAM

Users

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Access reports

Ready to streamline human access to AWS and cloud apps?

Identity Center is enabled. We recommend managing workforce users' access to AWS accounts and cloud applications in Identity Center.

Learn more Watch how it works

Users (2)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Search

	User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Acc
<input type="checkbox"/>	boto3-user	/	0	11 minutes ago	-	-	-	Act
<input type="checkbox"/>	cli-user	/	0	2 days ago	-	-	-	Act

aws

Search

[Alt+S]

IAM

Users

cli-user

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Access reports

cli-user

Delete

Summary

ARN: am:aws:iam::307946678032:user/cli-user

Console access: Disabled

Created: February 14, 2025, 23:36 (UTC-06:00)

Last console sign-in: -

Access key 1: AKIAUPMNM4IHDIETZNI - Active

Access key 2: Used 2 days ago. 2 days old.

Permissions

Groups

Tags (1)

Security credentials

Last Accessed

Console sign-in

Console sign-in link: https://307946678032.signin.aws.amazon.com/console

Console password: Not enabled

Enable console access

Multi-factor authentication (MFA) (0)

Remove

Resync

Assign MFA device

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Search

[Alt+S]

Global

Haritha

IAM > Users > cli-user > Create access key

Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys

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.

☐ **Local code**
You plan to use this access key to enable application code in a local development environment to access your AWS account.

☐ **Application running on an AWS compute service**
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

☐ **Third-party service**
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

☐ **Application running outside AWS**
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

☐ **Other**
Your use case is not listed here.

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Search

[Alt+S]

Global

Haritha

IAM > Users > cli-user > Create access key

Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys

Set description tag - optional [Info](#)

The description for this access key will be attached to this user as a tag and shown alongside the access key.

Description tag value
Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

cli-access

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . : / = + - @

Cancel

Previous

Create access key

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Command Prompt

Microsoft Windows [Version 10.0.22631.4751]
(c) Microsoft Corporation. All rights reserved.

C:\Users\eriga>aws --version
aws-cli/2.24.4 Python/3.12.6 Windows/11 exe/AMD64

C:\Users\eriga>aws configure
AWS Access Key ID [*****C2NM]: AKIAUPMYNM4IEQFJ5RPH
AWS Secret Access Key [*****wxdu]: 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
Default region name [us-east-1]: us-east-1
Default output format [json]:

C:\Users\eriga>

Amazon S3 (Simple Storage Service)

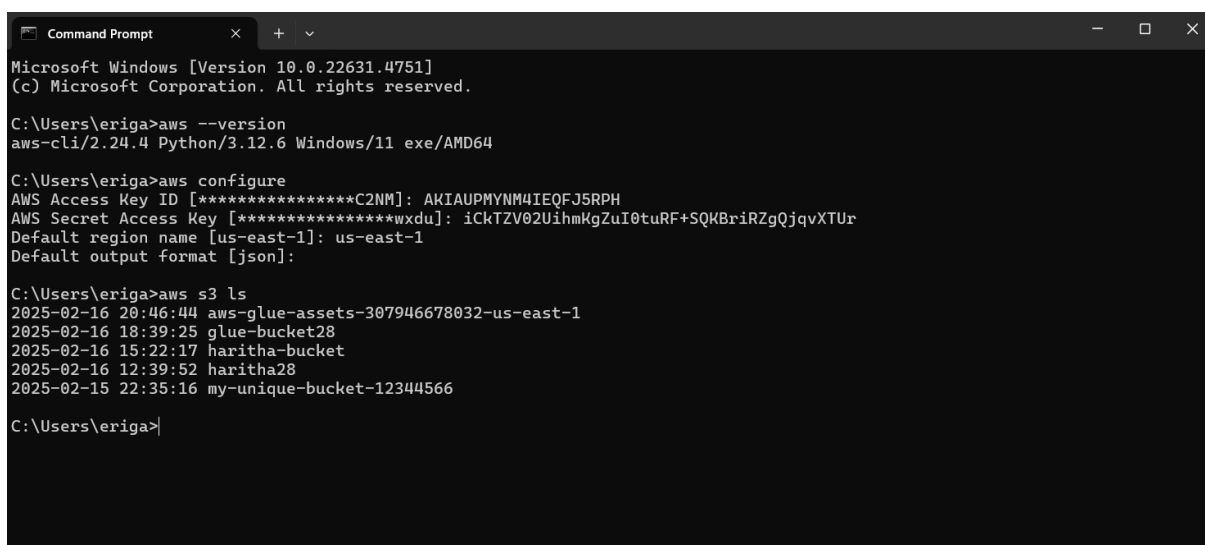
Amazon S3 is an object storage service that provides scalability, security, and durability for storing data.

Key Features of S3:

- **Scalability** – Stores unlimited data.
- **Durability** – 99.999999999% (11 9's) durability.
- **Security** – Supports IAM policies, encryption, and bucket policies.
- **Data Management** – Lifecycle rules, versioning, and replication.

S3 Storage Classes:

- **S3 Standard** – For frequently accessed data.
- **S3 Intelligent-Tiering** – Moves data between storage classes automatically.
- **S3 Standard-IA** – For infrequent access.
- **S3 Glacier** – Low-cost archival storage.



```
Microsoft Windows [Version 10.0.22631.4751]
(c) Microsoft Corporation. All rights reserved.

C:\Users\eriga>aws --version
aws-cli/2.24.4 Python/3.12.6 Windows/11 exe/AMD64

C:\Users\eriga>aws configure
AWS Access Key ID [*****C2NM]: AKIAUPMYNM4IEQFJ5RPH
AWS Secret Access Key [*****wxdu]: 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
Default region name [us-east-1]: us-east-1
Default output format [json]:

C:\Users\eriga>aws s3 ls
2025-02-16 20:46:44 aws-glue-assets-307946678032-us-east-1
2025-02-16 18:39:25 glue-bucket28
2025-02-16 15:22:17 haritha-bucket
2025-02-16 12:39:52 haritha28
2025-02-15 22:35:16 my-unique-bucket-12344566

C:\Users\eriga>
```