

Amazon Web Services

objective: complement/reinforce lectures with hands-on using Amazon Cloud

handouts: overview + step-by-step lab exercises

- AWS01: Amazon Web Services
- AWS02: AWS Core Services
- AWS03: Cloud Service Models: IaaS, PaaS, SaaS, FaaS
- AWS04: AWS MapReduce

2 Lab assignments (20%)

AWS01: Amazon Web Services



Outline

- Regions and Availability Zones
- AWS Login and Identity and Access Management (IAM)
- Access and Manage AWS Services
 - AWS Management Console
 - AWS Command Line Interface (CLI)
- Summary
- Videos & References

Amazon Web Services

“Amazon Web Services (AWS), a subsidiary of Amazon.com, offers a suite of cloud-computing services that make up an on-demand computing platform. These services operate from multiple geographical regions across the world.”



Amazon Web Services (AWS)

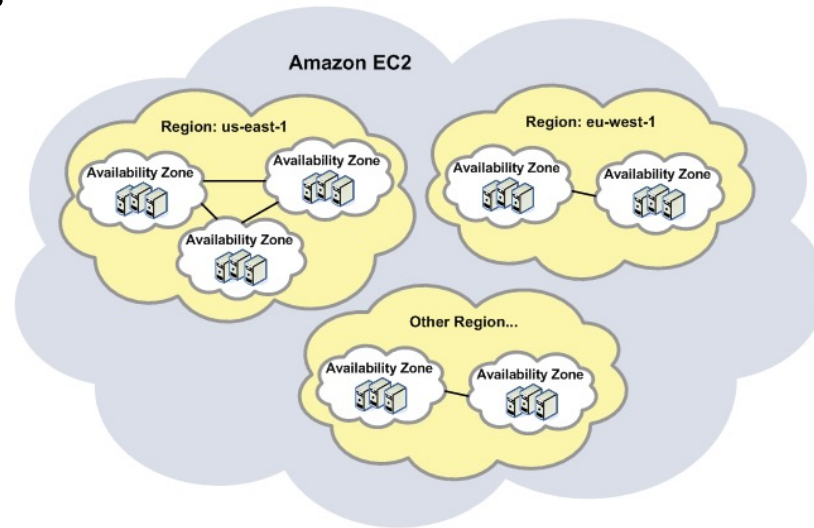
- a collection of **remote computing services** (> 175 services) that together make up a cloud computing platform
- Some basic services: [covered in AWS02]
 - Compute: EC2 (Elastic Computing Cloud)
 - Storage: S3 (Simple Storage Service)
 - Database: RDS (Relational Database Service)
 - Network: VPC (Virtual Private Cloud)
 - Scaling: Auto-scaling
 - Load balancing: Elastic Load Balancing
 - Monitoring services: Cloudwatch



How Services are Organized?

Regions and Availability Zones

- offers cloud services through a network of datacenters organized as:
 - **Regions:** distributed across **different geographical areas** and communicate through **Internet** but **do not share resources**
 - application can be closer to specific customers or to meet (data) legal requirements



- **Availability zones:** each region is divided into availability zones interconnected by **high-speed networks**
 - a data center consisting of a large number of servers
 - distinct locations within a region
 - protect applications from **failure** of a single location

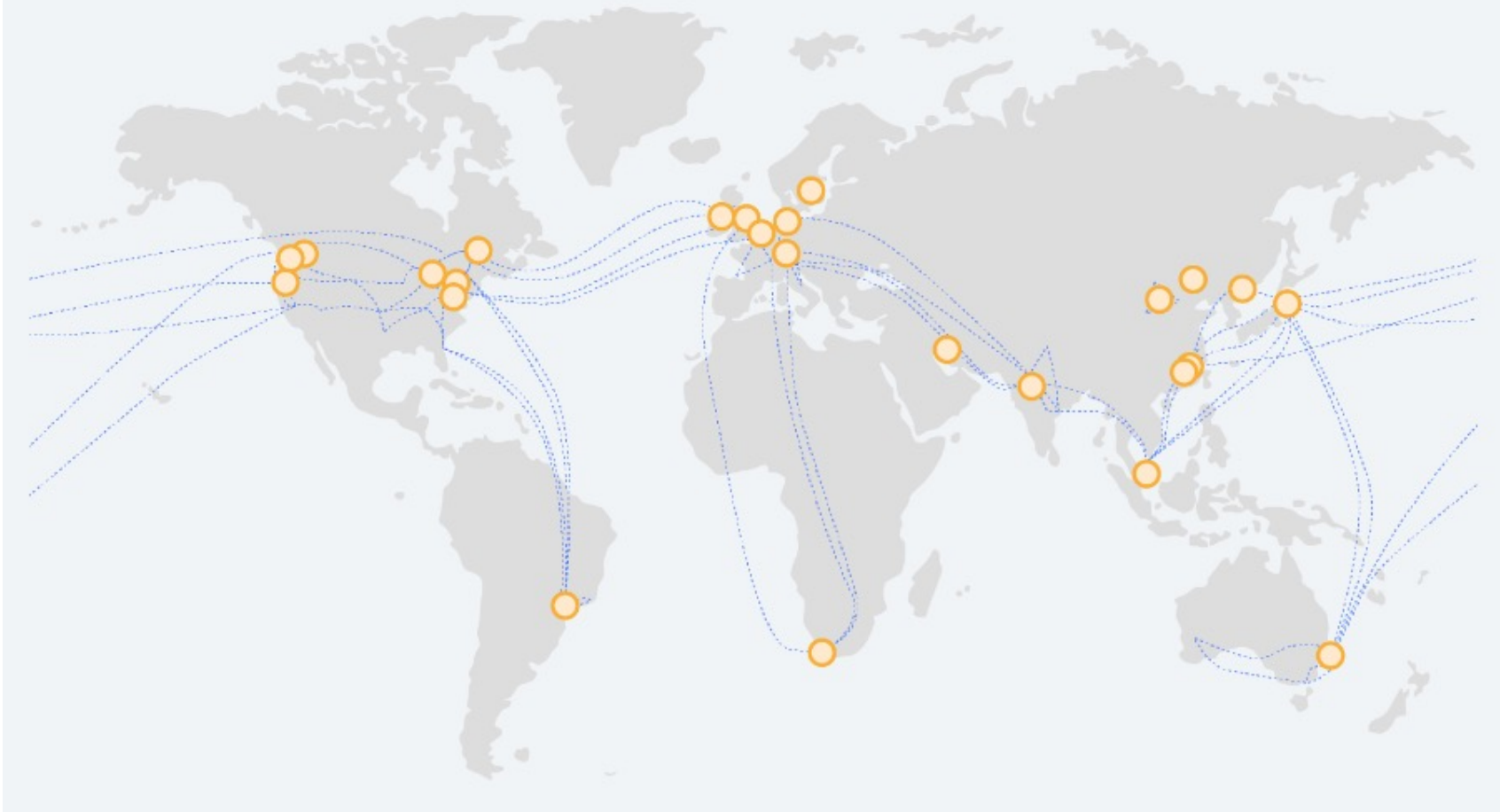
Example: Global Network of AWS Regions

The AWS Cloud spans 84 Availability Zones within 26 geographic regions around the world, with announced plans for 24 more Availability Zones and 8 more AWS Regions in Australia, Canada, India, Israel, New Zealand, Spain, Switzerland, and United Arab Emirates (UAE).

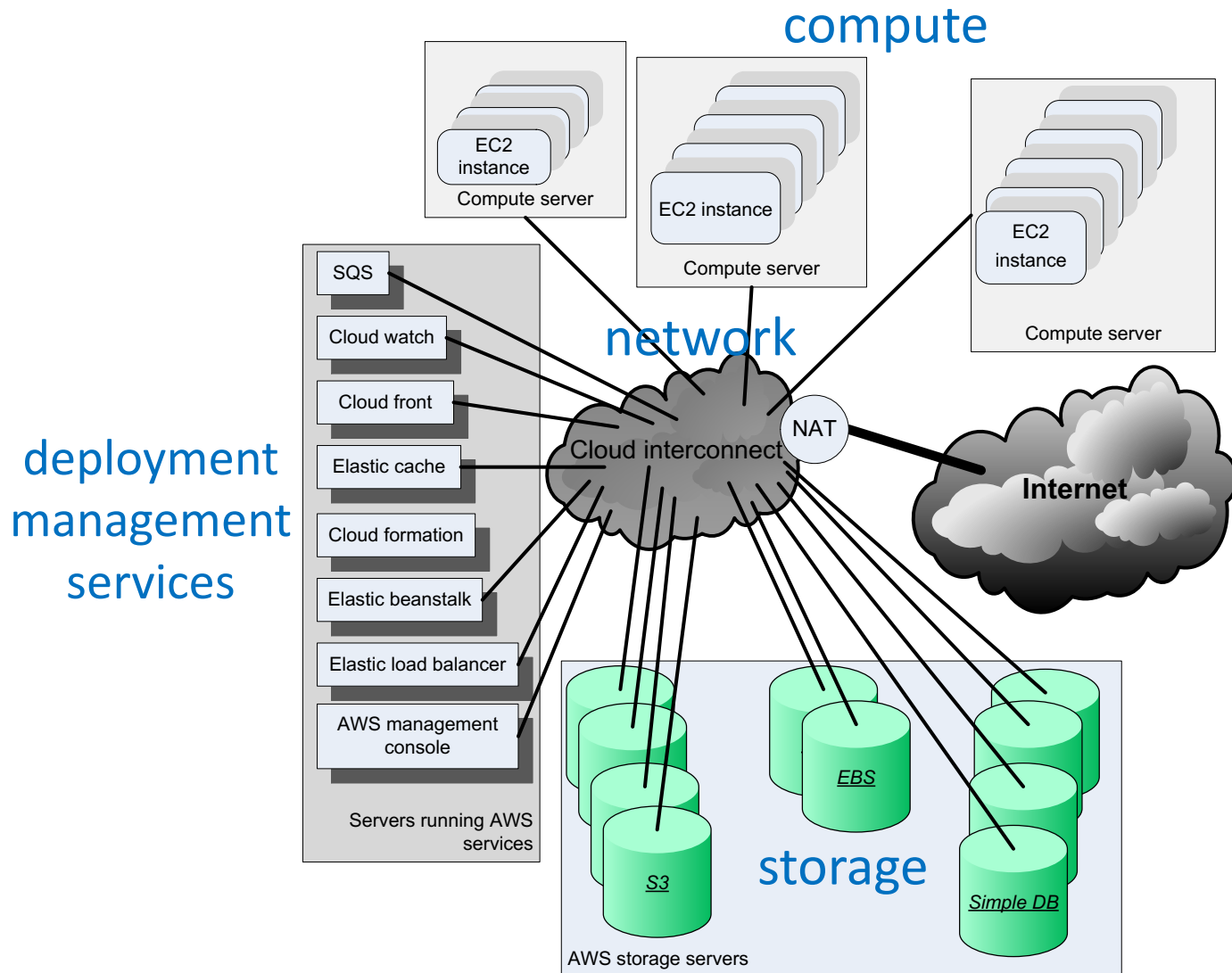


Example: Global Network of AWS Regions

Every data center, AZ, and AWS Region is interconnected via a purpose-built, highly available, and low-latency private global network infrastructure. The network is built on a global, fully redundant, parallel 100 GbE metro fiber network that is linked via trans-oceanic cables across the Atlantic, Pacific, and Indian Oceans, as well as the Mediterranean, Red Sea, and South China Seas.



Example: An Availability Zone Configuration



Amazon Web Services



Analytics



Application Integration



AWS Cost Management



Blockchain



Business Applications



Compute



Containers



Customer Engagement



Database



Developer Tools



End User Computing



Front-End Web & Mobile



Game Tech



Internet of Things



Machine Learning



Management & Governance



Media Services



Migration & Transfer



Networking & Content
Delivery



Quantum Technologies



Robotics



Satellite



Security, Identity &
Compliance



Serverless



Storage



VR & AR

AWS Catalog

The screenshot displays the AWS Catalog website. At the top, the AWS logo is on the left, and navigation links for 'Contact Sales', 'Support', 'English', and 'My Account' are on the right, alongside a 'Sign In to the Console' button. Below this is a horizontal menu with 'Products' (highlighted), 'Solutions', 'Pricing', 'Documentation', 'Learn', 'Partner Network', 'AWS Marketplace', and 'Explore More'. The main content area is divided into three columns. The left column, titled 'Featured Services', lists various AWS categories like Analytics, Application Integration, AR & VR, AWS Cost Management, Blockchain, Business Applications, Compute, Customer Engagement, Database, Developer Tools, End User Computing, Game Tech, Internet of Things, Machine Learning, Management & Governance, Media Services, Migration & Transfer, Mobile, Networking & Content Delivery, and Robotics. The middle column, also titled 'Featured Services', provides details for specific services: Amazon EC2 (Virtual servers in the cloud), Amazon Simple Storage Service (S3) (Scalable storage in the cloud), Amazon Aurora (High performance managed relational database), Amazon DynamoDB (Managed NoSQL database), Amazon RDS (Managed relational database service for MySQL, PostgreSQL, Oracle, SQL Server, and MariaDB), AWS Lambda (Run code without thinking about servers), Amazon VPC (Isolated cloud resources), and Amazon Lightsail (Launch and manage virtual private servers). The right column, titled 'Resources and Media', includes links to the AWS Blog, documentation, and getting started guides. Below this, the 'Training and Certification' section offers links to AWS Training and AWS Certification. A close button (X) is located in the top right corner of the right column.

aws

Contact Sales Support English My Account **Sign In to the Console**

Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Explore More

Featured Services

- Analytics
- Application Integration
- AR & VR
- AWS Cost Management
- Blockchain
- Business Applications
- Compute
- Customer Engagement
- Database
- Developer Tools
- End User Computing
- Game Tech
- Internet of Things
- Machine Learning
- Management & Governance
- Media Services
- Migration & Transfer
- Mobile
- Networking & Content Delivery
- Robotics

Featured Services

- Amazon EC2**
Virtual servers in the cloud
- Amazon Simple Storage Service (S3)**
Scalable storage in the cloud
- Amazon Aurora**
High performance managed relational database
- Amazon DynamoDB**
Managed NoSQL database
- Amazon RDS**
Managed relational database service for MySQL, PostgreSQL, Oracle, SQL Server, and MariaDB
- AWS Lambda**
Run code without thinking about servers
- Amazon VPC**
Isolated cloud resources
- Amazon Lightsail**
Launch and manage virtual private servers

Resources and Media

- Blog**
Read the latest AWS blogs
- Documentation**
Find documentation and resources for AWS services
- What's New on AWS**
See announcements for AWS services
- Getting Started**
Find tutorials for AWS services

Training and Certification

- AWS Training**
Build your technical skills with free digital training
- AWS Certification**
Validate your technical expertise by getting AWS Certified

Target Cloud Consumers

- Application Developers
 - Supports multiple languages
 - Auto-managed: version control, flexible capacity
- Businesses
 - Ease of deployment -> faster time-to-market
 - Lesser need for technical know-how
- Users
 - Needs are addressed fast
 - Feature updates made sooner
 - No need for special “going live mode” to update/release feature

Companies using AWS



Expedia is all in on AWS, with plans to migrate 80 percent of its mission-critical applications.



Using Amazon SageMaker, Intuit cuts the time to deploy machine-learning models by 90 percent.



General Electric (GE) is migrating more than 9,000 workloads to AWS.



Brooks Brothers runs key business-critical SAP applications on AWS.



Airbnb benefits from the scalability, agility, and reliability provided by AWS.



Mapbox can collect 100 million miles of telemetry data every day using AWS.



Lyft is going all in on AWS to deliver better customer experiences and focus on innovation.



Nextdoor has relied on AWS to support every component of its platform.



FINRA collects and analyzes billions of brokerage transactions daily using AWS.



By using AWS, Coursera can handle half a petabyte of traffic each month.

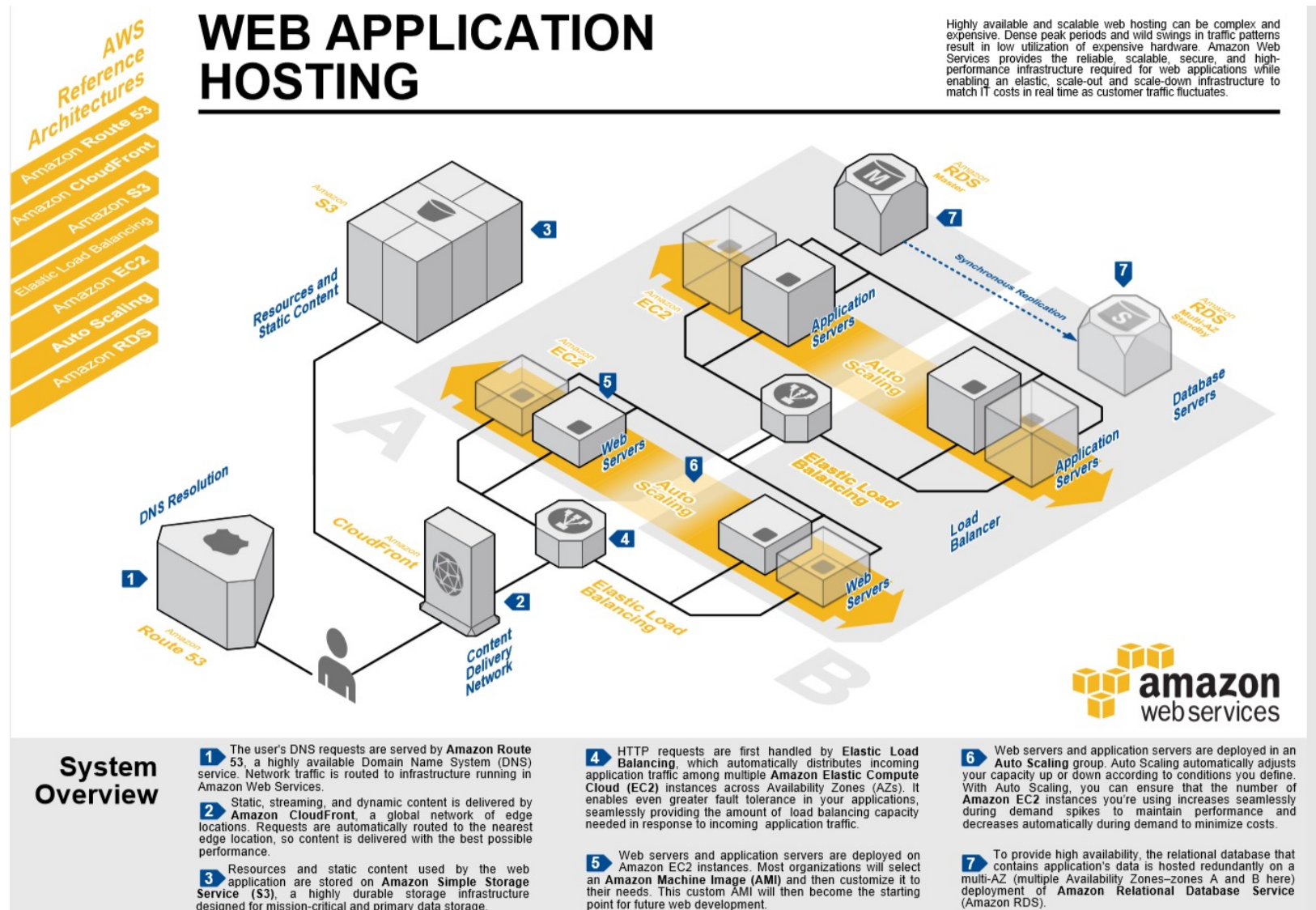


DigitalGlobe is all in on AWS and uses Amazon SageMaker to handle machine learning at scale.

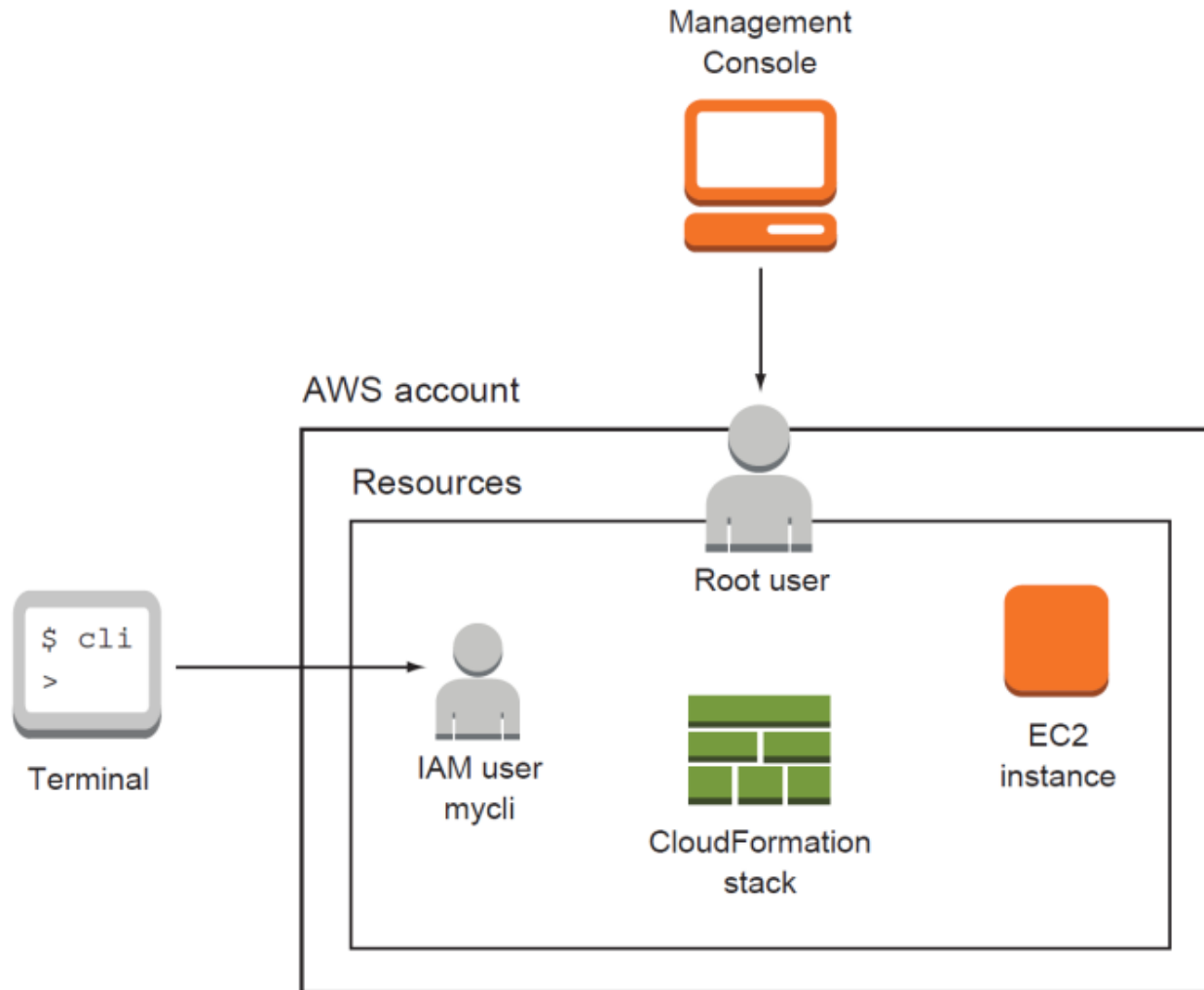


The Food and Drug Administration (FDA) uses AWS to deliver cost-effective, innovative new programs.

AWS Architecture on Web Application Hosting



AWS Account



AWS Login



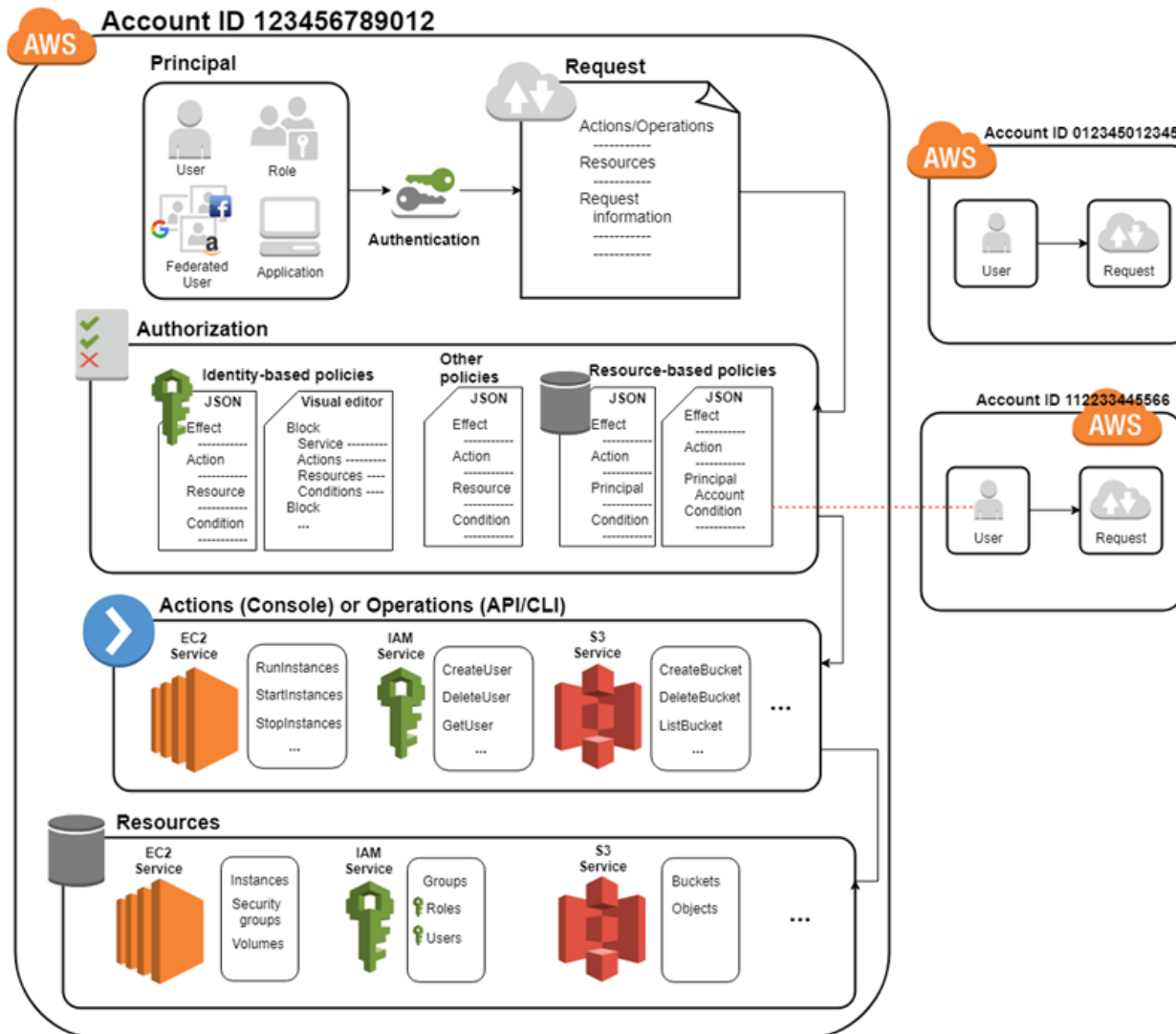
Sign in

☒ **Root user**
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☐ **IAM user**
User within an account that performs daily tasks. [Learn more](#)

- **Root user (AWS01)**
 - account you first created on AWS
 - complete access to all AWS services and resources
 - similar to UNIX root or Windows Administrator account
 - sign in with email address and password used to create the account
- **IAM (Identity & Access Management) user (AWS02-04)**
 - how can an organization set up accounts for its employees and manage and control accesses to AWS resources?
 - purpose: IAM gives control to people/applications that can access your AWS account (AWS resources); example: control who is authenticated (signed in) and authorized (has permissions) to use resources.
 - how: IAM user is created using the IAM service, a web service to control access to AWS resources
 - example: an organization subscribes to a pool of AWS resources and uses IAM to control employee's access to the AWS resource pool (allows resource pooling as discussed in L03: Cloud Architecture)

How IAM Works



Amazon Web Services

objective: complement/reinforce lectures with hands-on using Amazon Cloud

handouts: overview + step-by-step lab exercises

- AWS01: Amazon Web Services
- AWS02: AWS Core Services
- AWS03: Cloud Service Models: IaaS, PaaS, SaaS, FaaS
- AWS04: AWS MapReduce

2 Lab assignments (20%)

AWS Accounts in this CS5224

1. Personal Account (12-month free tier)
 - you need a root account to carry out AWS IAM experiments (AWS01 - Lab1)
2. IAM account, not root

CS5224 Classroom: IAM user accounts will be created using your NUS email addresses (you need to use this for Lab2, Lab3 and Lab4)

Access and Manage AWS Services

Two main interfaces:

1. AWS Management Console
2. AWS Command Line Interface

AWS Management Console

- a web interface to access and manage the AWS cloud
- login to management console using your AWS or IAM account credentials

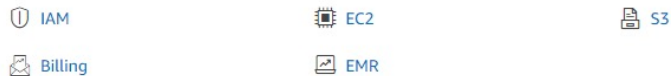
<https://console.aws.amazon.com/console/home>

AWS Management Console

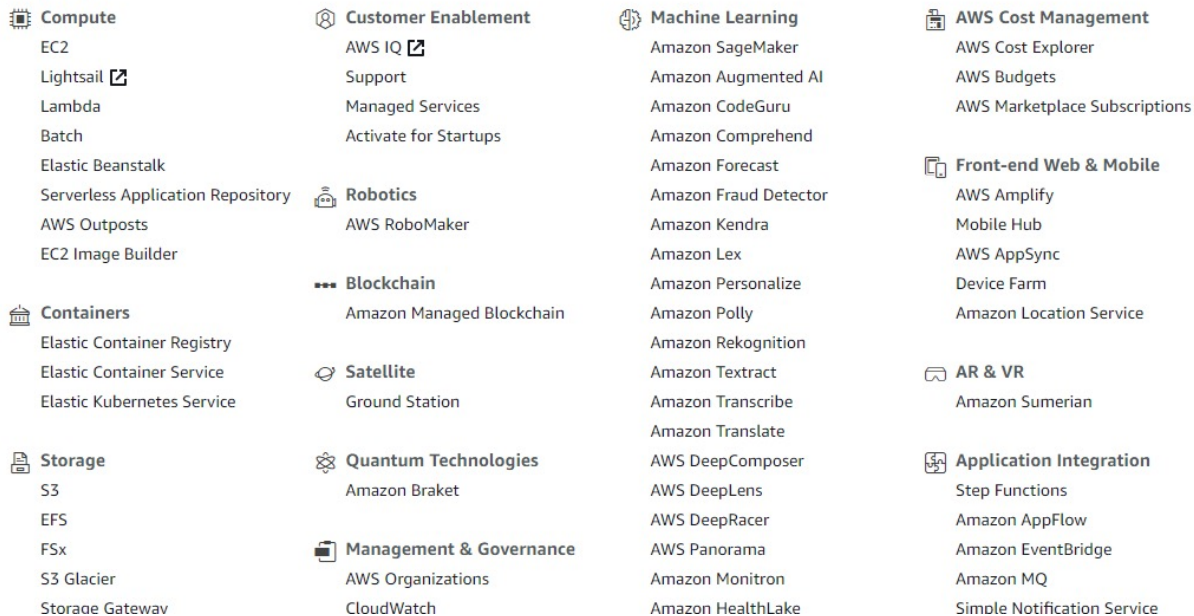
AWS Management Console

AWS services

▼ Recently visited services



▼ All services



Stay connected to your AWS resources on-the-go



Download the AWS Console Mobile App to your iOS or Android mobile device. [Learn more](#)

Explore AWS

Free Digital Training

Get access to 350+ self-paced online courses covering AWS products and services. [Learn more](#)

Amazon SageMaker Autopilot

Get hands-on with AutoML. [Learn more](#)

Amazon S3 on Outposts

You can now use S3 object storage in your on-premises environment. [Learn more](#)

AWS Certification

Explore the resources available to help you prepare for your AWS Certification. [Learn more](#)

Have feedback?

AWS Command Line Interface (CLI)

- enables interaction with AWS services using commands in command-line shell
 - With minimal configuration, the AWS CLI enables you to start running commands that implement functionality equivalent to that provided by the browser-based AWS Management Console from the command prompt in your terminal program
- All IaaS (infrastructure-as-a-service) AWS administration, management, and access functions in the AWS Management Console are available

Command Structure

AWS CLI command line:

```
$ aws <command> <subcommand>  
[options and parameters]
```

- base call to AWS program
- <command> - typically corresponds to an AWS service
- <subcommand> specifies operation to perform
- [options or parameters] required by the specified operation

Example: lists all your Amazon S3 buckets

```
$ aws s3 ls  
2018-12-11 17:08:50 my-bucket  
2018-12-14 14:55:44 my-bucket2
```


Summary

- How are cloud services organized?
- Login and IAM Access Control
- How to access and manage services?

Videos & References

Videos

- [What is AWS?](#) [2019, 3 min]
- [Introduction to AWS IAM - Identity and Access Management on AWS](#) [2014, 2 min]
- [Introduction to the AWS CLI v2](#) [2019, 46 min]
- [Deep Dive: AWS Command Line Interface](#) [2015, 64 min]

References

- <https://aws.amazon.com/>
- <https://aws.amazon.com/getting-started/fundamentals-overview/>
- <https://aws.amazon.com/console/>
- <https://aws.amazon.com/iam/>
- <https://aws.amazon.com/cli/>

HAPPY NEW YEAR
2022
YEAR OF THE TIGER



新
年
快
乐



AWS01: Amazon Web Services (Lab)



Outline

- Objectives
- Milestones
 - Create AWS IAM Group
 - Install AWS CLI
- Summary
- References

Objectives

- AWS Account
 - Create AWS account
- Management Console and IAM
 - Use AWS account (root user) to access to cloud services
 - Create IAM admin group to avoid using root user (for security)
- AWS CLI
 - Install CLI Environment

Outline

- Objective
- Milestone
 - Create AWS Account
 - Create AWS IAM Group
 - Install AWS CLI
- Summary
- Reference

Outline

- Objective
- Milestones
 - Create AWS Account
 - Create AWS IAM Group
 - Install AWS CLI
- Summary
- Reference

Create AWS IAM Group

Step 1: Login to AWS Management Console

Step 2: Enable IAM

Step 3: Add IAM User

Step 4: Create Group

Creating IAM Admin User and Groups

- As a best practice, do not use the AWS account root user for any task where it's not required. Instead, create a new IAM user for each person that requires administrator access.
- To try this, you have to apply for an AWS root account (Free but need to provide credit/debit card info)

Creating IAM Admin User and Groups

- Sign in to the IAM console as the account owner by choosing Root user and entering your AWS account email address.

<https://console.aws.amazon.com/iam/>

On the next page, enter your password.

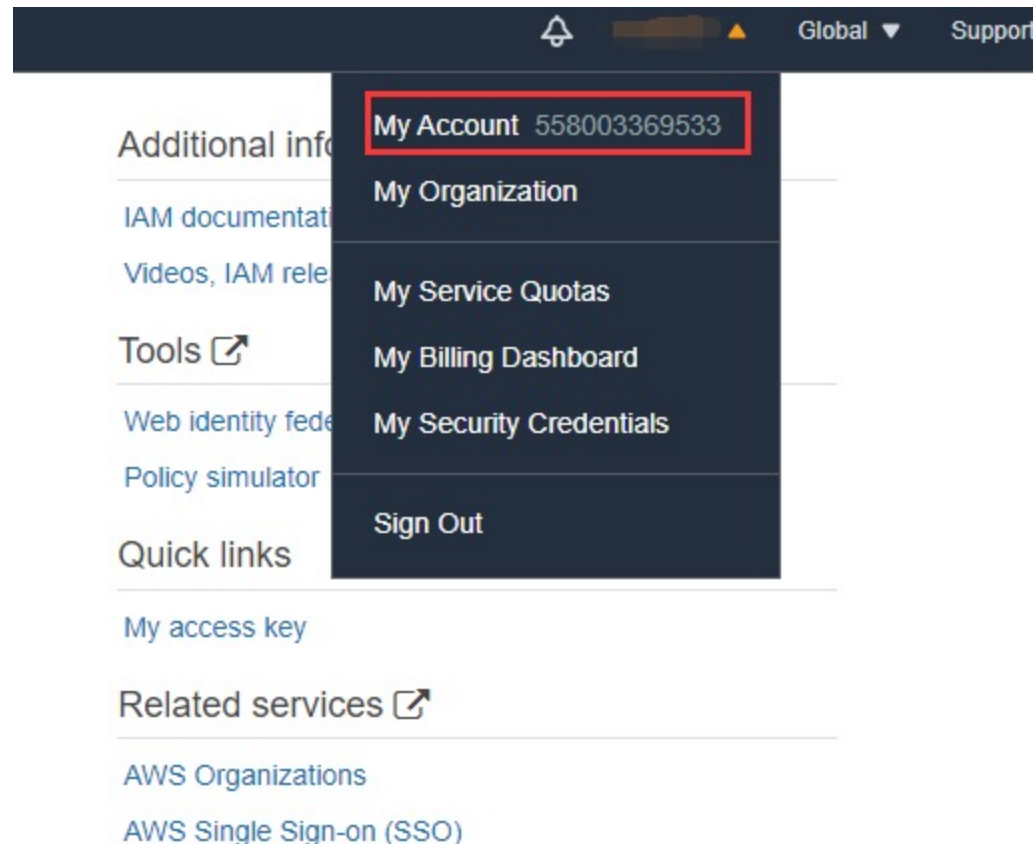
Step 1: Login to AWS Management Console (Personal account)

Enable access to billing data for the IAM admin user that you created as follows:

- On the navigation bar, choose your account name, and then choose **My Account**
- Next to **IAM User and Role Access to Billing Information**, choose **Edit**. You must be signed in as the **root user** for this section to be displayed on the account page
- Select the check box to **Activate IAM Access** and choose **Update**
- On the navigation bar, choose **Services** and then **IAM** to return to the IAM dashboard

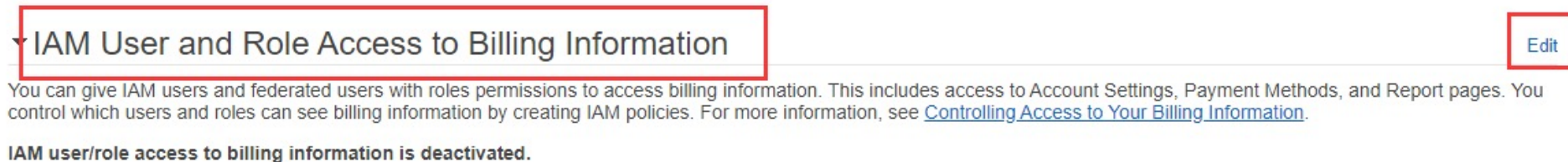
Step 1: Login to AWS Management Console

On the navigation bar, choose your account name, and then choose **My Account**



Step 2: Enable IAM

Next to **IAM User and Role Access to Billing Information**, choose **Edit**. You must be signed in as the **root user** for this section to be displayed on the account page.



▼ IAM User and Role Access to Billing Information Edit

You can give IAM users and federated users with roles permissions to access billing information. This includes access to Account Settings, Payment Methods, and Report pages. You control which users and roles can see billing information by creating IAM policies. For more information, see [Controlling Access to Your Billing Information](#).

IAM user/role access to billing information is deactivated.

Step 2: Enable IAM

Select the check box to **Activate IAM Access** and choose **Update**.

▼ IAM User and Role Access to Billing Information

You can give IAM users and federated users with roles permissions to access billing information. This includes access to Account Settings, Payment Methods, and Report pages. You can control which users and roles can see billing information by creating IAM policies. For more information, see [Controlling Access to Your Billing Information](#).



☒ **Activate IAM Access**

Update Cancel

Step 3: Add IAM User

On the navigation bar, choose **Services** and then **IAM** to return to the IAM dashboard



Step 3: Add IAM User

In the navigation pane, choose **Users** and then choose **Add users**

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ **Access management**

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

▼ **Access reports**

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Introducing the new Users list experience
We've redesigned the Users list experience to make it easier to use. [Let us know what you think.](#)

IAM > Users

Users (0) [Info](#)

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

Find users by username or access key

< 1 > ⚙

	User name	Groups	Last activity	MFA	Password age	Active key age
No resources to display						

Step 3: Add IAM User

For username, type Administrator

Add user



Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+ Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Access type***
- ☐ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
 - ☐ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Step 3: Add IAM User

- Select the check box for AWS Management Console access, select Custom password, and then type your new password in the text box.
- By default, AWS forces the new user to create a new password when first signing in. You can optionally clear the check box next to User must create a new password at next sign-in to allow the new user to reset their password after they sign in.
- Choose Next: Permissions


Step 4: Create Group


On the Permissions page, do the following:


- Choose **Add user to group**
- Choose **Create group**


Add user 1 2

▼ Set permissions

 Add user to group

 Copy permissions from existing user

 Attach existing policies directly

 **Get started with groups**

You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job function access, or your custom permissions. Get started by creating a group. [Learn more](#)

Create group

► Set permissions boundary

Step 4: Create Group

- In the Create group dialog box, for Group name type Administrators
- Select the check box for the AdministratorAccess policy

Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. [Learn more](#)

Group name

Administrators

Create policy

Refresh

Filter policies

Search

Showing 637 results

	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	AdministratorAccess	Job function	None	Provides full access to AWS services and resources.
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissions while explicitly allowing direct access to resources needed by Amplify applicat...
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and access to related AWS Services
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	None	Provide access to Lifesize AVS devices
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None	Provide access to Poly AVS devices
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForBusiness services
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Management Console.
<input type="checkbox"/>	AmazonAPIGatewayInvokeFullAccess	AWS managed	None	Provides full access to invoke APIs in Amazon API Gateway

Cancel

Create group

Step 4: Create Group

- Choose Create group
- Back on the page with the list of groups, select the check box for your new group. Choose Refresh if you don't see the new group in the list
- Choose Next: Tags
- Choose **Next: Review**
- Verify the group memberships to be added to the new user. When you are ready to proceed, choose **Create user**

Milestone: Create AWS IAM User and Group

If successful, you should see this on your screen. This is the last time these credentials will be available to download / view.

Add user




Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://558003369533.signin.aws.amazon.com/console>

 Download .csv

	User	Access key ID	Secret access key
▶  		AKIAYD24XWY6YFE5KRP5	***** Show

Outline

- Objective
- Milestones
 - Create AWS Educate Account
 - Create AWS IAM Group
 - Install AWS CLI
- Summary
- Reference

AWS CLI Installation

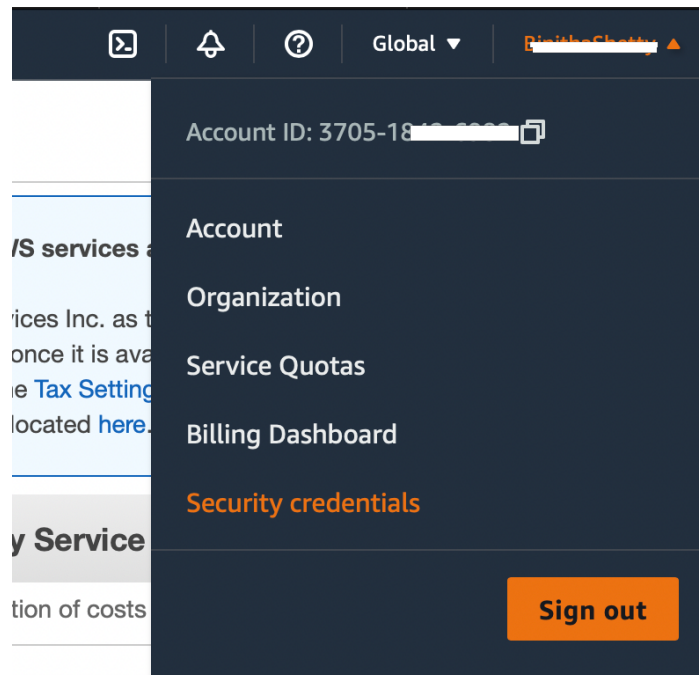
CLI depends on the OS you are using, please refer to the following document for CLI installation wrt to your OS:

<https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html>

We will leave this as an exercise for students that like to use CLI to access AWS services

Step 1: Login to AWS Management Console (personal account)

On the navigation bar, choose your account name, and then choose **Security Credentials**



Get AWS credentials

- Choose the **Access keys** section

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#).

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

▼ Password

You use an email address and password to sign in to secure pages on AWS, such as the AWS Management Console, AWS Forums, and AWS Support. For y create a password that contains many characters, including numbers and punctuation. Store your password securely, do not share it, and change it periodic

[Click here](#) to change the password, name, or email address for your root AWS account.

▲ Multi-factor authentication (MFA)

▲ **Access keys (access key ID and secret access key)**

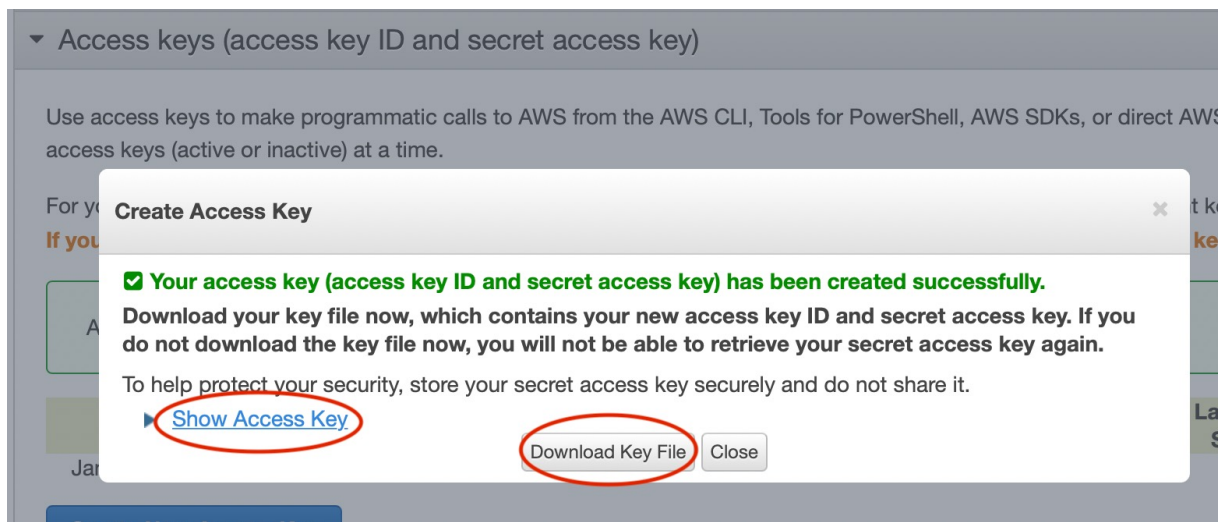
▲ CloudFront key pairs

▲ X.509 certificate

▲ Account identifiers

Get AWS credentials

- Choose **Create New Access Key** and retrieve the access key and secret key either by clicking on the **Show Access Key** or **Download Key File**.



Get AWS credentials

- Use '**aws configure**' command to set up your AWS CLI installation. Once you enter the command, type in the credentials (retrieved in the previous step) and other info.

```
(base) b[redacted] MacBook-Air cloudcomputing % aws configure
AWS Access Key ID [*****KBUU]: AKI/[redacted]CDU
AWS Secret Access Key [*****/1WG]: 4nk4[redacted]W
s0+fBM
Default region name [us-east-1]: us-east-1
Default output format [json]: json
```

Summary

- Management Console and IAM
 - Create AWS account (root user) to access to cloud services
 - Create IAM admin group to avoid using root user account
- AWS CLI
 - Install CLI Environment

References

- <https://aws.amazon.com/education/awseducate/apply/>
- https://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started_create-admin-group.html
- <https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html>