

The background of the slide is a light gray gradient. It is decorated with several realistic water droplets of various sizes, some at the top left, some at the bottom right, and others scattered in the center. A faint, large circular pattern, resembling a ripple or a stylized 'O', is centered in the upper half of the image.

AWS - INTRODUCTION

BY

KESHAV KUMMARI

AWS – CERTIFICATION DETAILS



Certified
Cloud
Practitioner

Developer
Associate

Solutions
Architect
Associate

Sysops
Administrator
Associate

Security
Specialty

Big Data
Specialty

Advanced
Networking
Specialty

Devops Pro

Solutions
Architect
Professional

aws  CERTIFIED

Role-Based Certifications

Specialty Certifications

Professional

✓ AWS Certified
Solutions Architect
- Professional

✓ AWS Certified
DevOps Engineer
- Professional

✓ AWS Certified
DevOps Engineer
- Professional

Associate

✓ AWS Certified
Solutions Architect
- Associate

✓ AWS Certified
Developer
- Associate

✓ AWS Certified
SysOps Administrator
- Associate

Foundational

✓ AWS Certified
Cloud Practitioner

✓ AWS Certified
Cloud Practitioner
optional

✓ AWS Certified
Cloud Practitioner
optional

✓ AWS Certified
Cloud Practitioner
optional



Cloud Practitioner



Architect



Developer



Operations



✓ AWS Certified
**Advanced
Networking**
- Specialty



✓ AWS Certified
Big Data
- Specialty

Specialty certifications
require one active
role-based certification

OLD EXAM – IS ACTIVE NOW!

Objective	Weighting
Designing highly available, cost efficient, fault tolerant, scalable systems	60%
Implementing/Deploying	10%
Data Security	20%
Troubleshooting	10%

- 80 Minutes in Length
- 60 Questions (this can change)
- \$150 USD
- Multiple Choice
- Pass mass is based on a bell curve (it moves around)
- Aim for 70%
- Qualification is valid for 2 years
- Scenario based questions

NEW EXAM - DETAILS

Objective	Weighting
Design Resilient Architectures	34%
Define Performant Architectures	24%
Specify Secure Applications and Architectures	26%
Design Cost-Optimized Architectures	10%
Define Operationally-Excellent Architectures	6%

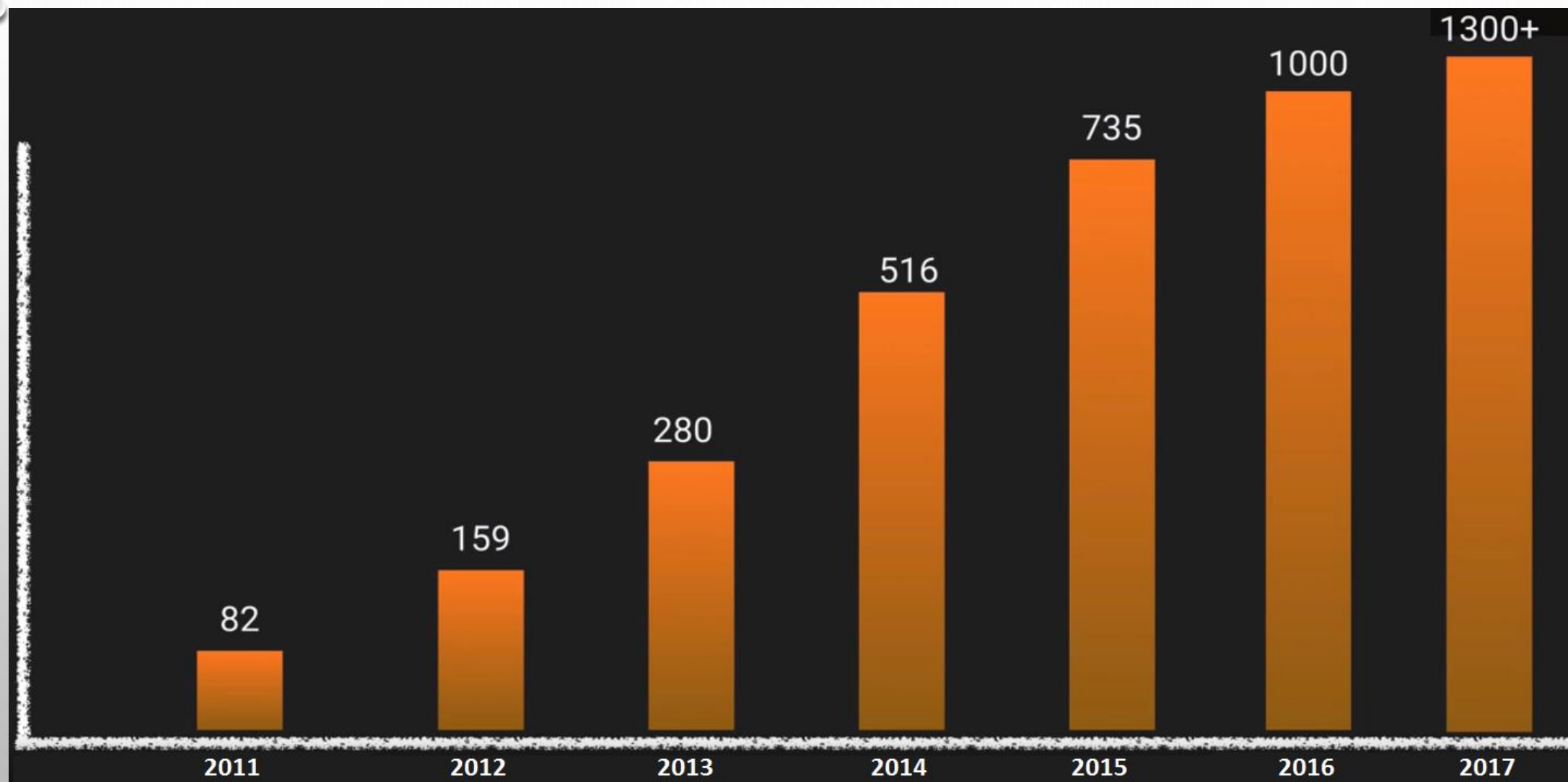
NEW EXAM - DETAILS

- <https://aws.amazon.com/certification/beta-exam/>
- 150 Minutes in Length
- 80 Questions
- Results within 3 months
- \$75 USD
- Multiple Choice
- Pass mass is based on a bell curve (it moves around)
- Aim for 70%
- Qualification is valid for 2 years
- Scenario based questions

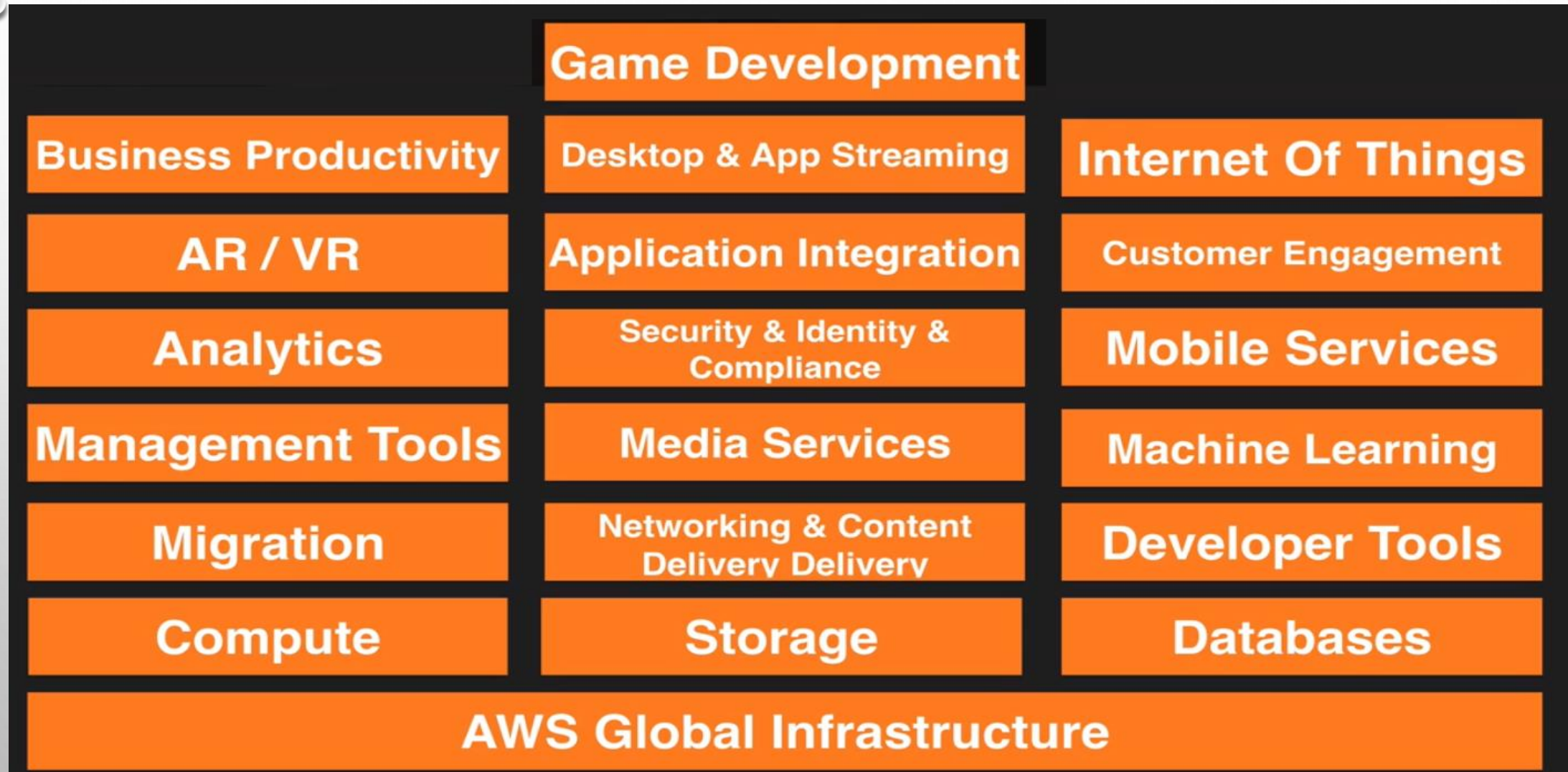
HISTORY OF AWS

- 2003 - Chris Pinkhan & Benjamin Black present a paper on what Amazon's own internal infrastructure should look like
- Suggested selling it as a service and prepared a business case.
- SQS officially launched in 2004
- AWS Officially launched in 2006
- 2007 over 180,000 developers on the platform
- 2010 all of amazon.com moved over
- 2012 First re:Invent Conference
- 2013 Certifications Launched
- 2014 Committed to achieve 100% renewable energy usage for its global footprint
- 2015 AWS breaks out its revenue: \$6 Billion USD per annum and growing close to 90% year on year
- 2016 Run rate of \$13 billion USD.
- 2017 AWS re:invent releases a host of Artificial Intelligent Services as well as Virtual Reality services.

SERVICES IN AWS



AWS – SERVICES



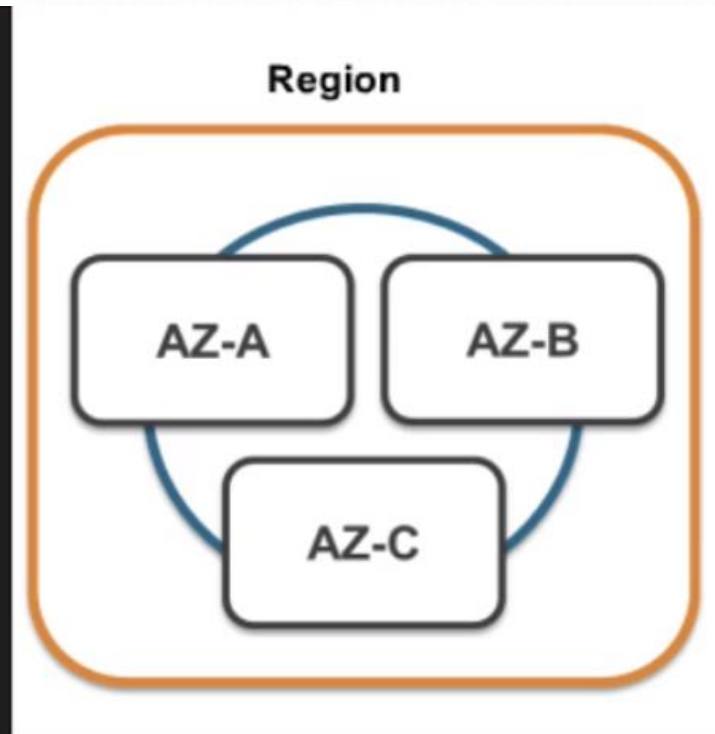
GLOBAL INFRASTRUCTURE

Global Infrastructure



16 Regions & 44 Availability Zones - December 2017
6 More Regions & 17 More AZ's for 2018

WHAT IS REGION & AVAILABILITY ZONE?



A Region is a geographical area. Each Region consists of 2 (or more) Availability Zones.

An Availability Zone (AZ) is simply a Data Center.

WHAT IS AN EDGE LOCATION?



Edge Locations are endpoints for AWS which are used for caching content. Typically this consists of CloudFront, Amazon's Content Delivery Network (CDN)

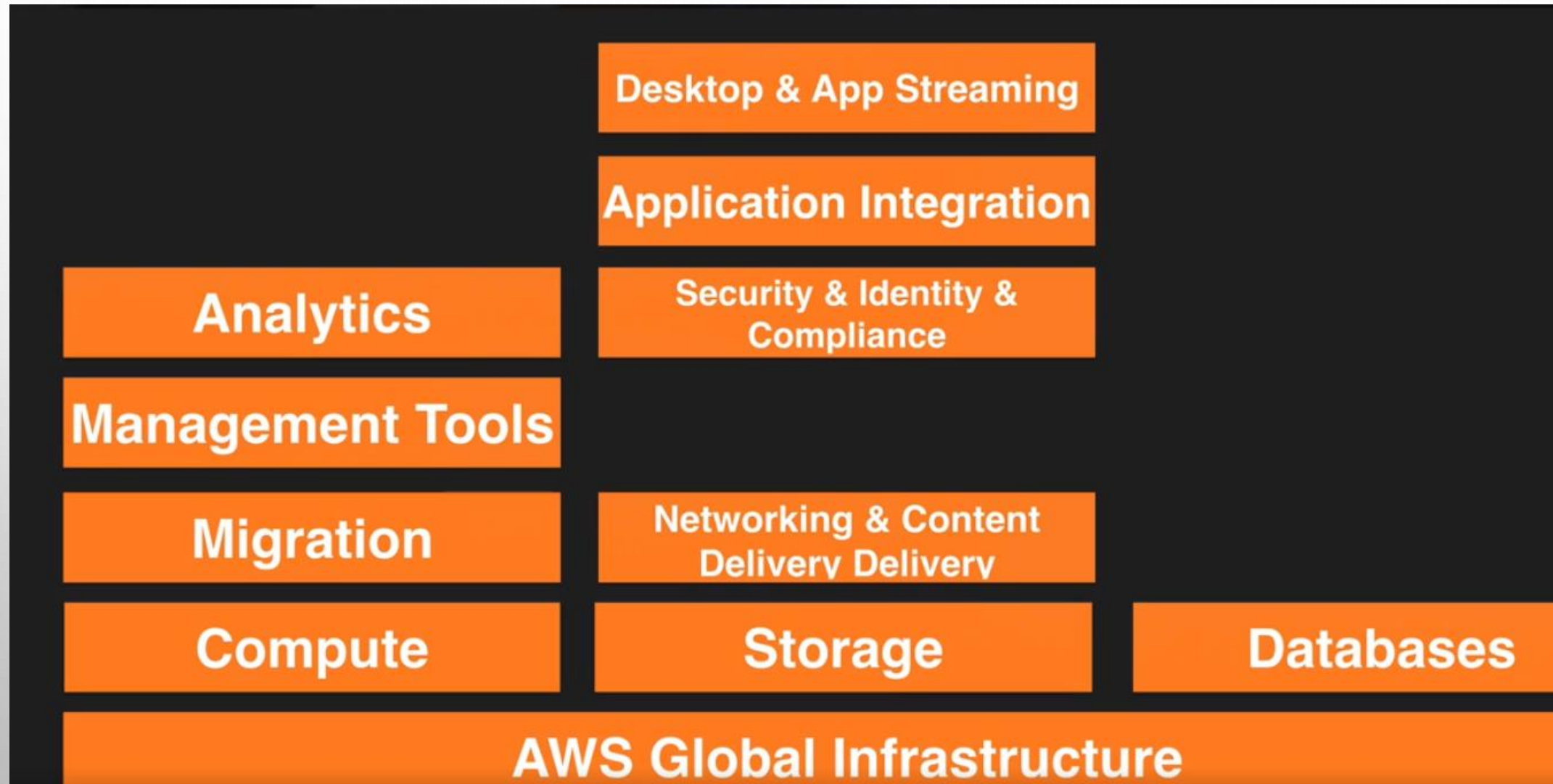
There are many more Edge Locations than Regions.
Currently there are over 96 Edge Locations.

EXAM - TIPS

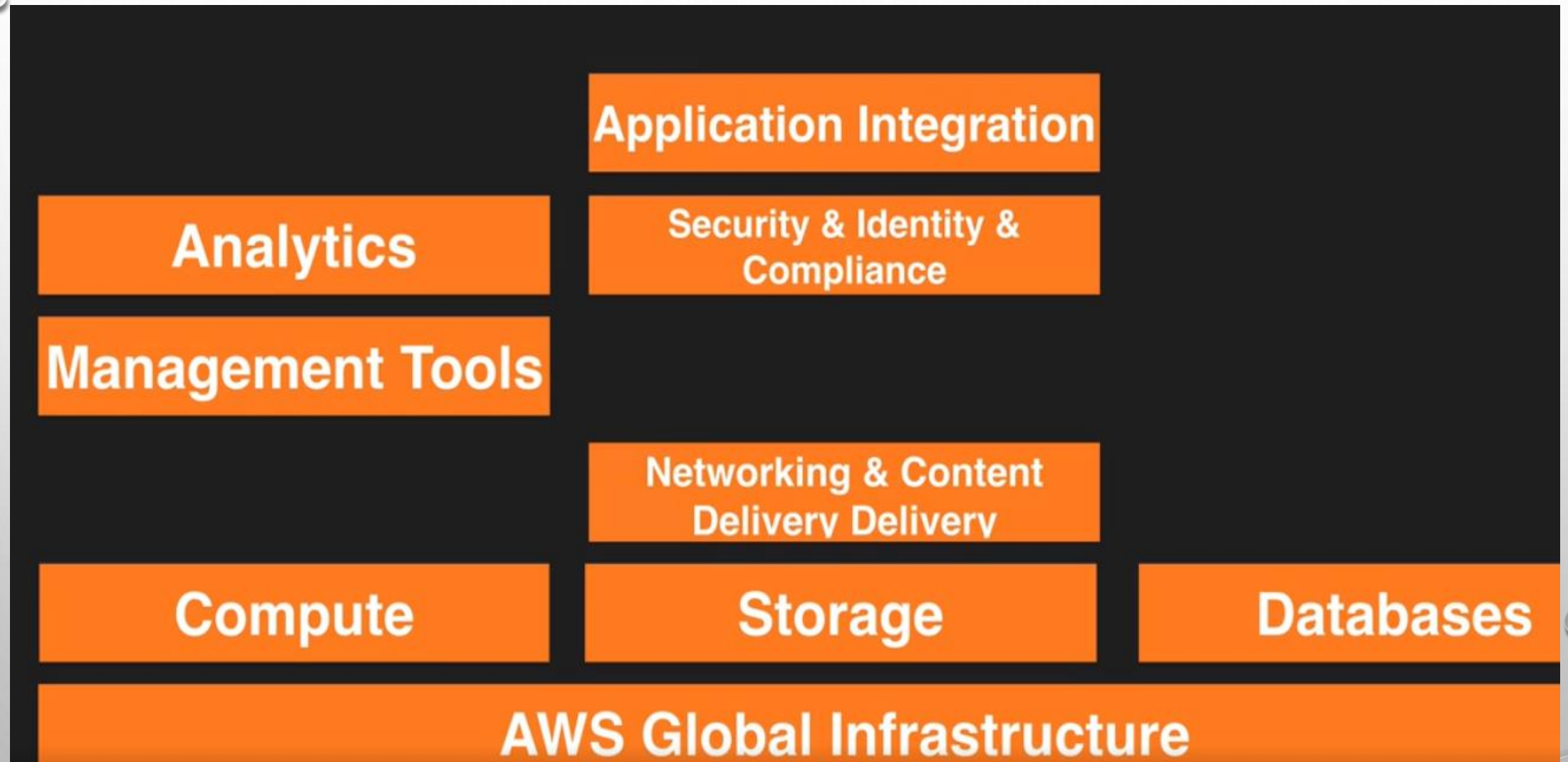
Understand the difference between a region, an Availability Zone (AZ) and an Edge Location.

- A Region is a physical location in the world which consists of two or more Availability Zones (AZ's).
- An AZ is one or more discrete data centers, each with redundant power, networking and connectivity, housed in separate facilities.
- Edge Locations are endpoints for AWS which are used for caching content. Typically this consists of CloudFront, Amazon's Content Delivery Network (CDN)

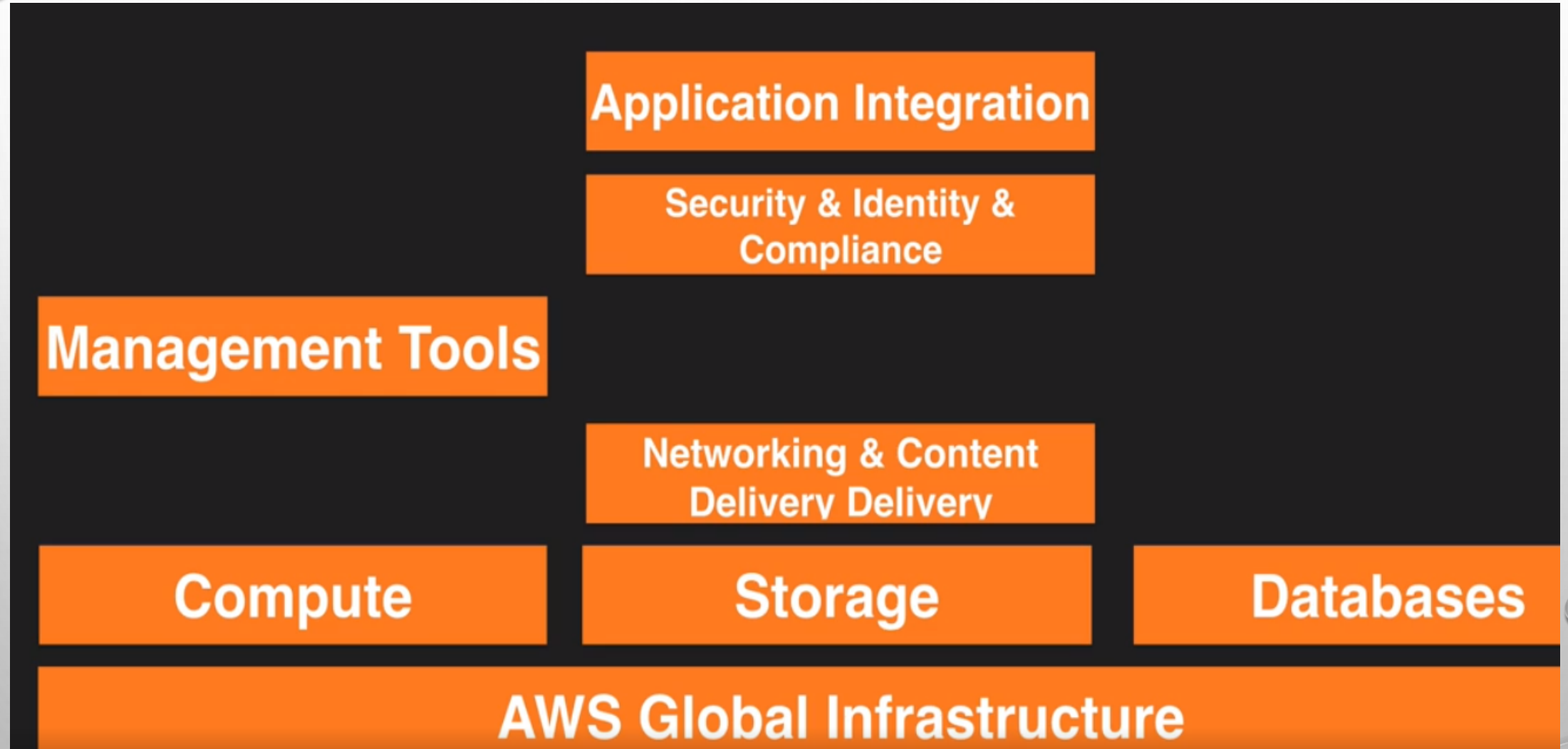
AWS – SOLUTION A ASSOCIATE



AWS – DEVELOPER ASSOCIATE



AWS - SYSOPS ADMINISTRATOR ASSOCIATE



IAM - IDENTITY ACCESS MANAGEMENT



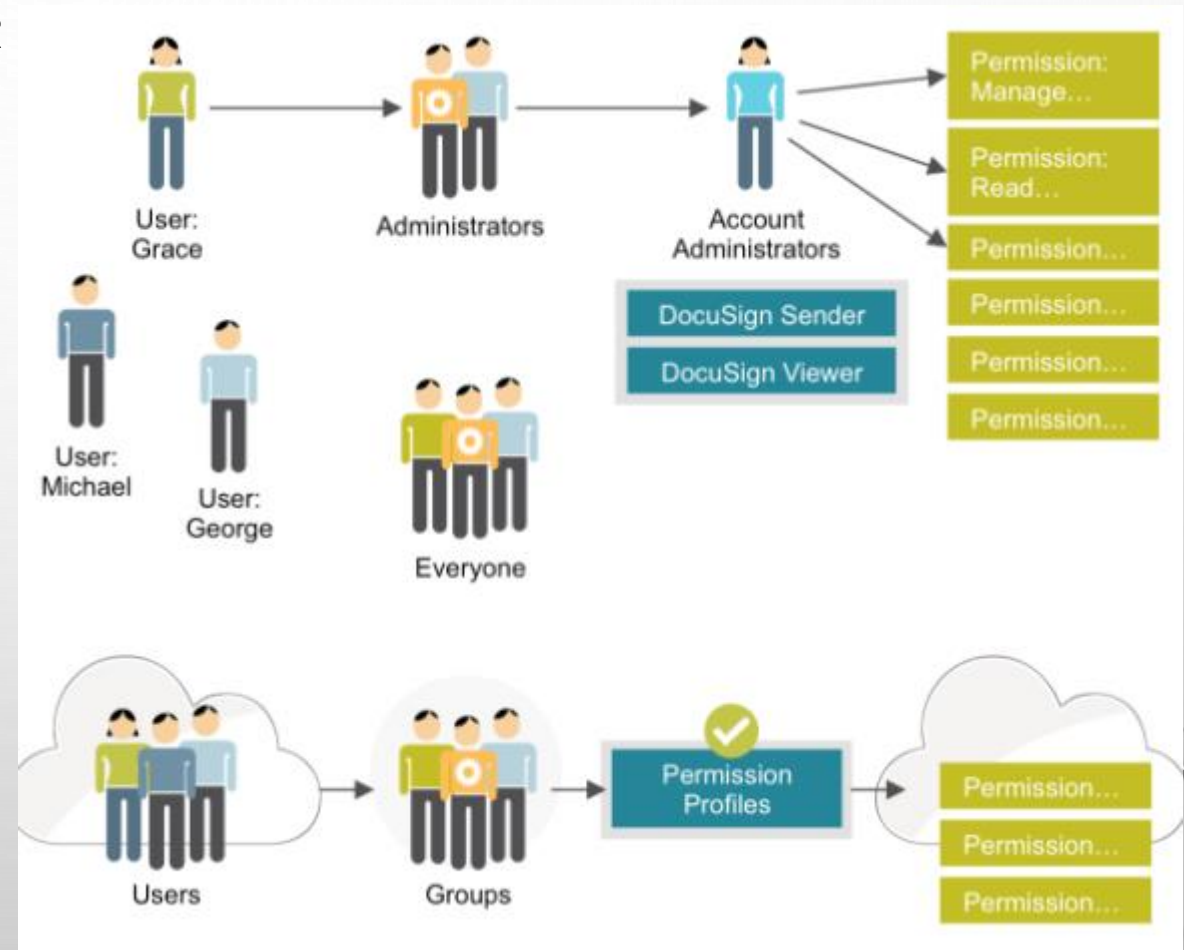
Essentially, IAM allows you to manage users and their level of access to the AWS Console. It is important to understand IAM and how it works, both for the exam and for administering a company's AWS account in real life.

WHAT IAM GIVE YOU?

- Centralised **control of your AWS** account
- **Shared Access** to your AWS account
- Granular **Permissions**
- Identity Federation (including **Active Directory**, Facebook, LinkedIn etc)
- **Multifactor Authentication**
- Provide **temporary access** for users/devices and services where necessary
- Allows you to set up your own **password rotation policy**
- Integrates with many different AWS services
- Supports PCI DSS Compliance

IAM

- USERS - END USERS
- GROUPS - A COLLECTION OF USERS UNDER
- ROLES - YOU CREATE ROLES AND CAN THEN ASSIGN THEM TO AWS RESOURCES
- POLICIES - A DOCUMENT THAT DEFINES ONE(OR MORE PERMISSIONS)



IAM - LAB

g | <https://ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1>

Services ^ **Resource Groups** v

ckk v **Mumbai** v

Group

Amazon Redshift

Migration

- AWS Migration Hub
- Application Discovery Service
- Database Migration Service
- Server Migration Service
- Snowball

Networking & Content Delivery

- VPC
- CloudFront
- Route 53
- API Gateway

Managed Services

Media Services

- Elastic Transcoder
- Kinesis Video Streams
- MediaConvert
- MediaLive
- MediaPackage
- MediaStore
- MediaTailor

AWS Glue

Security, Identity & Compliance

- IAM**
- Cognito
- GuardDuty
- Inspector
- Amazon Macie
- AWS Single Sign-On
- Certificate Manager
- CloudHSM
- Directory Service
- WAF & Shield
- Artifact

Amazon Chime

WorkDocs

WorkMail

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Internet Of Things

- AWS IoT
- IoT Analytics
- IoT Device Management
- Amazon FreeRTOS
- AWS Greengrass

CUSTOMIZE IAM USERS SIGN-IN LINK

The screenshot displays the AWS IAM console interface. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information. The left sidebar contains navigation links: 'Search IAM', 'Dashboard' (highlighted), 'Groups', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Credential report', and 'Encryption keys'. The main content area is titled 'Welcome to Identity and Access Management' and shows the 'IAM users sign-in link' as `https://726584800293.signin.aws.amazon.com/console`. A 'Customize' button is located next to the link. Below this, the 'IAM Resources' section shows counts for Users (2), Roles (12), Groups (2), and Identity Providers (0). The 'Security Status' section lists several recommendations, some with checkmarks and others with warning icons. A modal dialog titled 'Create Account Alias' is open in the foreground, with the 'Account Alias' field containing the text 'jessi-joel' and the 'Yes, Create' button highlighted in blue.

aws Services Resource Groups

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Welcome to Identity and Access Management

IAM users sign-in link:

`https://726584800293.signin.aws.amazon.com/console` Customize Copy Link

IAM Resources

Users: 2 Roles: 12

Groups: 2 Identity Providers: 0

Customer Managed Policies: 7

Security Status

- ✓ Delete your root access keys
- ⚠ Activate MFA on your root account
- ✓ Create individual IAM users
- ✓ Use groups to assign permissions
- ⚠ Apply an IAM password policy

Create Account Alias

Account Alias jessi-joel

Cancel Yes, Create

Feature Spotlight

Introduction to AWS IAM

Additional Information

- IAM best practices
- IAM documentation
- Web Identity Federation Playground
- Policy Simulator
- Videos, IAM release history and additional resources

ACTIVATE MFA

The screenshot shows the AWS IAM console interface. The top navigation bar includes the AWS logo, 'Services', and 'Resource Groups'. The left sidebar contains a search bar and a list of navigation items: Dashboard, Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area is titled 'Welcome to Identity and Access Management' and displays IAM user sign-in link, IAM Resources (Users: 2, Groups: 2, Customer Managed Policies: 7), and a Security Status section. A modal window titled 'Manage MFA device' is open, prompting the user to select the type of MFA device to activate. The modal has a close button (X) in the top right corner. The 'Next Step' button is highlighted in blue.

aws Services Resource Groups

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Welcome to Identity and Access Management

IAM users sign-in link:
<https://jessi-joe1.signin.aws.amazon.com/console> [Customize](#) | [Copy Link](#)

IAM Resources

Users: 2 Roles: 12

Groups: 2

Customer Managed Policies: 7

Security Status

- ✓ Delete your root access key
- ⚠ **Activate MFA on your root account**

Activate multi-factor authentication on your root account to keep your account secure. [Learn More](#)

Manage MFA

Manage MFA device

Select the type of MFA device to activate:

- ☒ A virtual MFA device
- ☐ A hardware MFA device

For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#).

[Cancel](#) [Next Step](#)

- ✓ Create individual IAM users
- ✓ Use groups to assign permissions
- ⚠ Apply an IAM password policy

MFS – GOOGLE AUTHENTICATOR



AWS re:Invent

Products ▾

Solutions

Pricing

Software

Support

Customers

More ▾

English ▾

My Account ▾

Sign in

Device	See table below.	Purchase.	Purchase.	Use your mobile device.
Physical Form Factor	Use your existing smartphone or tablet running any application that supports the open TOTP standard.	Tamper-evident hardware key fob device provided by Gemalto, a third-party provider.	Tamper-evident hardware display card device provided by Gemalto, a third-party provider.	Any mobile device that can receive Short Message Service (SMS) messages.
Price	Free	\$12.99	\$19.99	SMS or data charges may apply.
Features	Support for multiple tokens on a single device.	The same type of device used by many financial services and enterprise IT organizations.	Similar to key fob devices, but in a convenient form factor that fits in your wallet like a credit card.	Familiar option with low setup costs.
Compatibility with Root Account	✓	✓	✓	
Compatibility with IAM User	✓	✓	✓	✓

Virtual MFA Applications

Applications for your smartphone can be installed from the application store that is specific to your phone type. The following table lists some applications for different smartphone types.

Android

[Google Authenticator](#); [Authy 2-Factor Authentication](#)

iPhone

[Google Authenticator](#)

Windows Phone

[Authenticator](#)

Blackberry

[Google Authenticator](#)

IAM – MFA - II

Welcome to Identity and Access Management

IAM users sign-in link:
[https://\[redacted\].amazonaws.com/signin](https://[redacted].amazonaws.com/signin)

IAM Resources

- Users: 0
- Groups: 0
- Customer Managed Policies: 0

Security Status

- ✓ Delete your root account
- ⚠ Activate MFA on your root account


Activate multi-factor authentication for your root account
[Learn More](#)

Manage MFA

- ⚠ Create individual IAM users
- ⚠ Use groups to assign permissions
- ⚠ Apply an IAM password policy

Manage MFA Device

If your virtual MFA application supports scanning QR codes, scan the following image with your smartphone's camera.



▶ [Show secret key for manual configuration](#)

After the application is configured, enter two consecutive authentication codes in the boxes below and click **Activate Virtual MFA**.

Authentication Code 1

Authentication Code 2

[Cancel](#) [Previous](#) [Activate Virtual MFA](#)

Search 9:41 AM 100%


Authenticator

603 251
root-account-mfa-device

Amazon Web Services

841 294
root-account-mfa-device

CREATE A USER



Services ▾ Resource Groups ▾

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Welcome to Identity and Access Management

IAM users sign-in link:
<https://jessi-joeel.signin.aws.amazon.com/console> [Customize](#) | [Copy Link](#)

IAM Resources

Users: 2

Groups: 2

Customer Managed Policies: 7

Roles: 12

Identity Providers: 0

Security Status 3 out of 5 complete.

✓	Delete your root access keys	▼
⚠	Activate MFA on your root account	▼
✓	Create individual IAM users	▲
<p>Create IAM users and give them only the permissions they need. Do not use your AWS root account for day-to-day interaction with AWS, because the root account provides unrestricted access to your AWS resources. Learn More</p> <div>Manage Users</div>		
✓	Use groups to assign permissions	▼
⚠	Apply an IAM password policy	▼

CREATING A USER - JOEL

Add user



Details



Permissions



Review



Complete

Set user details

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

User name* joel

[+ 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.

Console password* ☐ Autogenerated password

☒ **Custom password**

.....

☐ Show password

Require password reset ☒ User must create a new password at next sign-in

Users automatically get the **IAMUserChangePassword** policy to allow them to change their own password.

IAM – CREATING A GROUP

1 2 3 4

Create group

Group name PythonDevelopers

Create policy Refresh

Filter: Policy type Search Showing 320 results

	Policy name	Type	Attachments	Description
	AdministratorAccess	Job function	2	Provides full access to AWS services and resources.

AdministratorAccess
Provides full access to AWS services and resources.

Policy summary JSON

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4
```

Cancel Create group

IAM – ADDING A USER TO A GROUP WHILE CREATING AN USER

Add user



Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	joel
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	PythonDevelopers
Managed policy	IAMUserChangePassword

USER BELOW DETAILS TO LOGIN TO AWS ACCOUNT VIA BROWSER & TERMINAL

- USERNAME : JOEL
- ACCESS KEY ID : AKIAJN6NOWKFYNZLFMGQ
- SECRET ACCESS KEY : JENK3DO9VQLLOWIDEKIFYWTKNFFOLVH/KYBUR2MBB

Add user

1

2

3

4

DetailsPermissionsReviewComplete

✓ 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://jessi-joel.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key	Email login instructions
▶	✓ joel	AKIAJN6NOWKFYNZLFMGQ	***** Show	Send email

Close

LOGIN AND CHANGE THE PASSWORD

Amazon Web Services S × +

← → ↻ | 🔒 us-east-1.signin.aws.amazon.com/oauth?SignatureVersion=4&X-Amz-Algo



Account ID or alias

jessi-joel

IAM user name

joel

Password

•••••

Sign In

[Sign-in using root account credentials](#)

← → ↻ | 🔒 us-east-1.signin.aws.amazon.com/oauth



You must change your password to continue

AWS account jessi-joel

IAM user name joel

Old password

New password

Retype new password

Confirm password change

[Sign-in using root account credentials](#)

IAM – LOGIN AS JOEL

The screenshot shows the AWS Management Console interface. The browser tab is labeled "AWS Management Console". The address bar shows the URL "ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1". The AWS logo is in the top left, and the top navigation bar includes "Services", "Resource Groups", and a user profile dropdown for "joel @ jessi-joel" in the "Mumbai" region. The main content area is divided into two columns. The left column has a section titled "AWS services" with a search bar and links to "Recently visited services" and "All services". Below this is a section titled "Build a solution" with the subtitle "Get started with simple wizards and automated workflows." and three quick-start options: "Launch a virtual machine" (With EC2 or Lightsail, ~1-2 minutes), "Build a web app" (With Elastic Beanstalk, ~6 minutes), and "Host a static website" (With S3, CloudFront, Route 53, ~5 minutes). The right column has a section titled "Helpful tips" with two items: "Manage your costs" (Get real-time billing alerts based on your cost and usage budgets. [Start now](#)) and "Create an organization" (Use AWS Organizations for policy-based management of multiple AWS accounts. [Start now](#)). At the bottom right, there is a section titled "Explore AWS".

AWS Management Console

ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1

aws Services Resource Groups

joel @ jessi-joel Mumbai

AWS services


Find a service by name or feature (for example, EC2, S3 or VM, storage).


Recently visited services


All services

Build a solution


Get started with simple wizards and automated workflows.


**Launch a virtual machine**
With EC2 or Lightsail
~1-2 minutes

**Build a web app**
With Elastic Beanstalk
~6 minutes

**Host a static website**
With S3, CloudFront, Route 53
~5 minutes

Helpful tips

**Manage your costs**
Get real-time billing alerts based on your cost and usage budgets. [Start now](#)

**Create an organization**
Use AWS Organizations for policy-based management of multiple AWS accounts. [Start now](#)

Explore AWS

IAM – ADDING SPECIFIC PERMISSIONS TO A USER - JOEL

Add permissions to joel

1

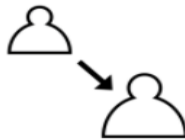
Permissions

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.



Add user to group



Copy permissions from
existing user





Attach existing policies
directly

Attach one or more existing policies directly to the users or create a new policy. [Learn more](#)

Create policy

Refresh

Filter: Policy type

	Policy name	Type	Attachments	Description
<input type="checkbox"/>	 AmazonDMSRedshiftS3Role	AWS managed	0	Provides access to manage S3 settings for Redshift endpoints for DMS.
<input type="checkbox"/>	 AmazonS3FullAccess	AWS managed	1	Provides full access to all buckets via the AWS Management Console.
<input checked="" type="checkbox"/>	 AmazonS3ReadOnlyAccess	AWS managed	0	Provides read only access to all buckets via the AWS Management Console.

IAM – CHECK THE USER DETAILS

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Users > joel

Summary

User ARN

arn:aws:iam::726584800293:user/joel

Path

/

Creation time

2018-02-18 19:58 UTC+0100

Permissions

Groups (1)

Security credentials

Access Advisor

Add permissions

Attached policies: 3

Policy name	Policy type	
Attached directly		
▶ AmazonS3ReadOnlyAccess	AWS managed policy	✕
▶ IAMUserChangePassword	AWS managed policy	✕
Attached from group		
▶ AdministratorAccess	AWS managed policy from group PythonDevelopers	✕

+ Add inline policy

IAM – ACTIVE OR INACTIVE A USER

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

User ARNarn:aws:iam::726584800293:user/joel

Path/

Creation time2018-02-18 19:58 UTC+0100

PermissionsGroups (1)Security credentialsAccess Advisor

Sign-in credentials

Console passwordEnabledManage password

Console login linkhttps://jessi-joel.signin.aws.amazon.com/console

Last login2018-02-18 20:04 UTC+0100

Assigned MFA deviceNo

Signing certificatesNone

Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. [Learn more](#)

Create access key

Access key ID	Created	Last used	Status
AKIAJN6NOWKFFYNZLFMGQ	2018-02-18 19:58 UTC+0100	N/A	ActiveMake inactive

IAM – USER HAS BEEN INACTIVE & NOW, HE CAN NOT LOGIN FROM AWS CLI

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

User ARNarn:aws:iam::726584800293:user/joel

Path/

Creation time2018-02-18 19:58 UTC+0100

PermissionsGroups (1)Security credentialsAccess Advisor

Sign-in credentials

Console passwordEnabledManage password

Console login linkhttps://jessi-joel.signin.aws.amazon.com/console

Last login2018-02-18 20:04 UTC+0100

Assigned MFA deviceNo

Signing certificatesNone

Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. [Learn more](#)

Create access key

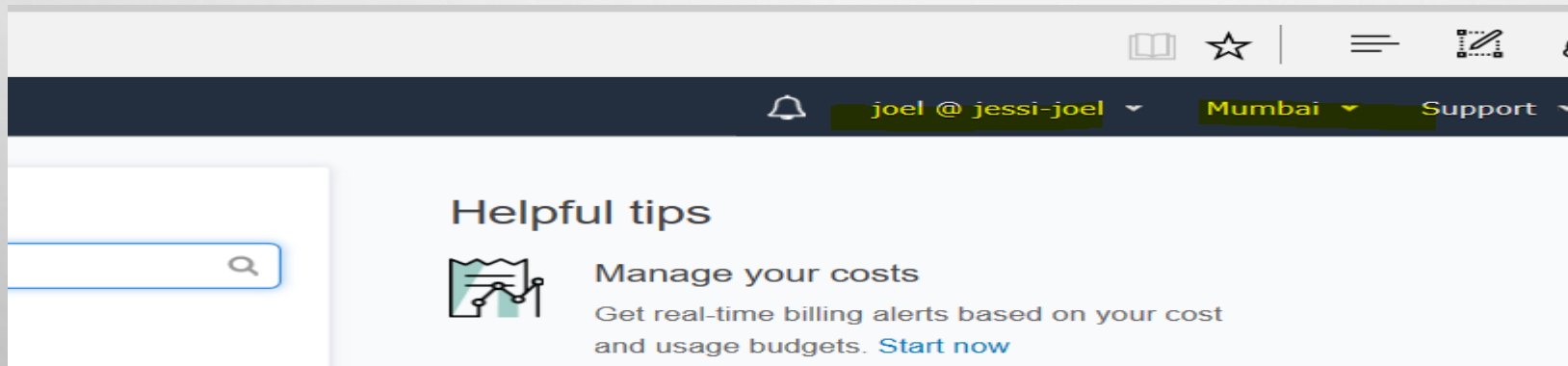
Access key ID	Created	Last used	Status
AKIAJN6NOWKFYNZLFMGQ	2018-02-18 19:58 UTC+0100	N/A	Inactive Make active

IAM – LOGIN FROM AWS CLI & BROWSER AND TEST

- LOGIN FROM AWS CLI FROM WINDOWS(CMD) OR MACOS(TERMINAL) :

```
λ aws configure
AWS Access Key ID [*****GQPQ]: AKIAJN6NOWKFYNZLFMGQ
AWS Secret Access Key [*****C+bm]: jENK3D09vqLLOwIDekFYWtKnFfoLVh/KYbur
2mbb
Default region name [ap-south-1]: ap-south-1
Default output format [None]:
```

- NOTE: AUTHENTICATION WAS NOT SUCCESSFUL.
- LOGIN FROM THE BROWSER AND CHECK :



- NOTE: IT'S SUCCESSFUL!

IAM – MAKE THE USER ACTIVE

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

User ARNarn:aws:iam::726584800293:user/joel

Path /

Creation time2018-02-18 19:58 UTC+0100

PermissionsGroups (1)Security credentialsAccess Advisor

Sign-in credentials

Console passwordEnabledManage password

Console login linkhttps://jessi-joel.signin.aws.amazon.com/console

Last login2018-02-18 20:04 UTC+0100

Assigned MFA deviceNo

Signing certificatesNone

Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. [Learn more](#)

Create access key

Access key ID	Created	Last used	Status
AKIAJN6NOWKFYNZLFMGQ	2018-02-18 19:58 UTC+0100	N/A	Active Make inactive

IAM – APPLY AN IAM PASSWORD POLICY

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Welcome to Identity and Access Management

IAM users sign-in link:
<https://jessi-joel.signin.aws.amazon.com/console> [Customize](#) | [Copy Link](#)

IAM Resources

Users: 3

Groups: 3

Customer Managed Policies: 7

Roles: 12

Identity Providers: 0

Security Status 3 out of 5 complete.

✓	Delete your root access keys	▼
⚠	Activate MFA on your root account	▼
✓	Create individual IAM users	▼
✓	Use groups to assign permissions	▼
⚠	Apply an IAM password policy	▲

Use a password policy to require your IAM users to create strong passwords and to rotate their passwords regularly. [Learn More](#)

Manage Password Policy

IAM – PASSWORD POLICY

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

▼ Password Policy

A password policy is a set of rules that define the type of password an IAM user can set. For more information about password policies, go to [Managing Passwords](#) in Using IAM.

Currently, this AWS account does not have a password policy. Specify a password policy below.

Minimum password length:

6

☐ Require at least one uppercase letter ⓘ

☐ Require at least one lowercase letter ⓘ

☐ Require at least one number ⓘ

☐ Require at least one non-alphanumeric character ⓘ

☒ Allow users to change their own password ⓘ

☐ Enable password expiration ⓘ

Password expiration period (in days):

☐ Prevent password reuse ⓘ

Number of passwords to remember:

☐ Password expiration requires administrator reset ⓘ

Apply password policy

Delete password policy

▼ Security Token Service Regions

IAM - SUMMARY

- IAM consists of the following;
 - **Users**
 - **Groups** (A way to group our users and apply policies to them collectively)
 - **Roles**
 - **Policy Documents.**

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

IAM - SUMMARY

- IAM is universal. It does not apply to regions at this time.
- The “root account” is simply the account created when first setup your AWS account. It has complete Admin access.
- New Users have NO permissions when first created.
- New Users are assigned **Access Key ID & Secret Access Keys** when first created.
- These are not the same as a password, and you cannot use the Access key ID & Secret Access Key to Login in to the console. You can use this to access AWS via the APIs and Command Line however.
- You only get to view these once. If you lose them, you have to regenerate them. So save them in a secure location.

- ALWAYS SETUP MULTIFACTOR AUTHENTICATION ON YOUR ROOT ACCOUNT.
- YOU CAN CREATE AND CUSTOMISE YOUR OWN PASSWORD ROTATION POLICIES.

