Training Course

Amazon Web Service

Course Overview

- Deploying, administering, and monitoring AWS system and network resources in an automatable and reusable manner
- Prerequisites
  - ✓ Some Linux or Windows system administration experience
  - ✓ Basic familiarity with Linux command line or Windows PowerShell
  - ✓ Knowledge of popular development and scripting languages (e.g., Python) a plus, but not required

Course Overview

- Module 1: System Operations on AWS
  - ✓ **Goal:** Get started with the tools you need to administer resources on AWS
  - ✓ Data Center vs. the Cloud; High Level Overview; Securing Your AWS Account; Command Line Basics
- Module 2: Computing on AWS
  - ✓ **Goal**: Understand how to deploy instances and maintain instance health
  - ✓ Creating Instances, Instance Security, Pricing, Troubleshooting
  - ✓ **Lab 1**: Launching and Troubleshooting Amazone EC2 Instances

Course Overview

- Module 3: Networking on AWS
  - ✓ **Goal**: Understand how to create your own custom virtual private cloud using the AWS Management Console
  - ✓ Common Amazon VPC Scenarios, Example Walkthrough, Amazon VPC Peering and Direct Connect, Amazon VPC Security, Troubleshooting
  - ✓ **Lab 2**: Creating a New VPC, Verifying the VPC Configuration

Course Overview

- Module 4: Storage and Archiving in the Cloud
  - ✓ **Goal**: Use the varios storage options in AWS to enable both short-term access and long-term storage of business data
  - ✓ Using Amazon Elastic Block Store, Amazon S3, AWS Import/Export, AWS Storage Gateway, Amazon Glacier, Storage Security, Troubleshooting, Storage Pricing Comparison
  - ✓ **Lab 3**: Using Storage in the Cloud, Synchronizing Files with Amazon S3

Course Overview

- Module 5: Monitoring in the Cloud
  - ✓ **Goal**: Perform basic monitoring with Amazon CloudWatch and Amazon CloudWatch Logs, and understand role of third party monitoring packages
  - ✓ Loggin Basics, Using CloudWatch and CloudWatch Logs, Using AWS CloudTrail, Security and Monitoring, Troubleshooting
  - ✓ **Lab 4**: Monitor EC2 System Status with CloudWatch; Auto-Stop Unused Instances

Course Overview

- Module 6: Managing Resource Comsumption in the Cloud
  - ✓ **Goal**: Learn how to monitor resource spend and how to control costs via scripting and automation
  - ✓ Automating Cost Reduction, Tagging, CloudWatch, Cost Explorer, Trusted Advisor
  - ✓ **Lab 5**: Managing Resources with Tagging; Indentifying and Terminating Non-Compliant Resources

Course Overview

- Module 7: Configuration Management in the Cloud
  - ✓ **Goal**: Cover the basics of using AMIs and Configuration Management to initialize new Amazon EC2 instances
  - ✓ Using and Creating New AMIs, Using Configuration Management, Troubleshooting CM

Course Overview

- Module 8: Creating Scalable Deployments in the Cloud
  - ✓ **Goal**: Use Elastic Load Balancing and Auto Scaling to scale systems out and in automatically
  - ✓ Common Deployment Scenarios, Redirecting Traffic with Elastic Load Balancing, Scaling to Demand with Auto Scaling, Routing with Amazon Route 53, Troubleshooting Scalable Deployments
  - ✓ **Lab 6**: Deploy an Auto Scaling Web Service

Course Schedule

Day	Presentations	Lab
Day 1	System Operations on AWS	
Day 2	Computing on AWS	X
Day 3	Networking on AWS	X
Day 4	Storage and Archiving in the Cloud	X
Day 5	Monitoring in the Cloud	X
Day 6	Managing Resource Consumption in the Cloud	X

Course Schedule

Day	Presentations	Lab
Day 7	Configuration Management in the Cloud Creating Scalable Deployment in the Cloud	X
Day 8, 9 & half of day 10	Assignment: + Introduce the assignment (purpose, requrements, …) + Let student practice the assignment + Assessment, check and test practice + Summary content of course	X
Half of day 10	Test: multi choice quiz	

Course Schedule

Day	Presentations	Lab
Day 1	System Operations on AWS	
Day 2	Computing on AWS	X
Day 3	Networking on AWS	X
Day 4	Storage and Archiving in the Cloud	X
Day 5	Monitoring in the Cloud	X
Day 6	Managing Resource Consumption in the Cloud	X

Module 1:

Understanding System Operations on AWS

Module 1: Understand System Operations in AWS

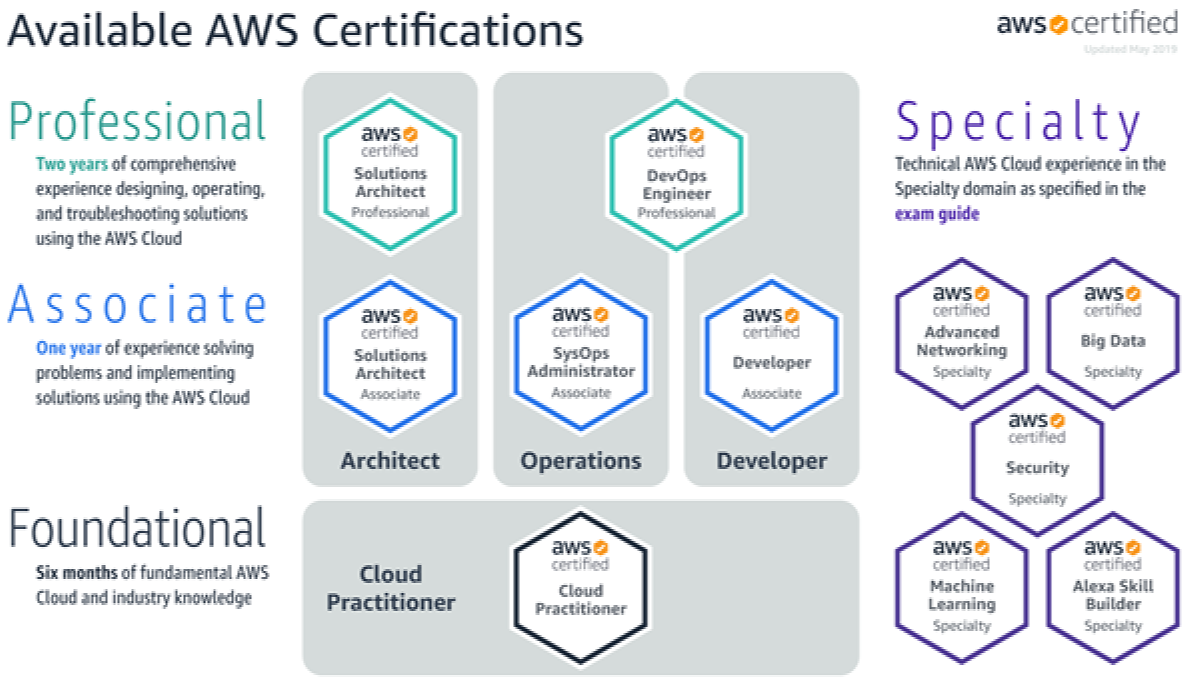
- **Goal**: Get started with the tools you need to administer resources on AWS
  - ✓ AWS Training and Certification
  - ✓ Comparing Data Center and the Cloud
  - ✓ Securing Your AWS Account

Module 1: Understand System Operations in AWS

- **Goal**: Get started with the tools you need to administer resources on AWS
  - ✓ **AWS Training and Certification**
  - ✓ Comparing Data Center and the Cloud
  - ✓ Securing Your AWS Account

Module 1: Understand System Operations in AWS

AWS certification process



Available AWS Certifications

aws certified

Updated May 2019

Professional

Two years of comprehensive experience designing, operating, and troubleshooting solutions using the AWS Cloud

Associate

One year of experience solving problems and implementing solutions using the AWS Cloud

Foundational

Six months of fundamental AWS Cloud and industry knowledge

Specialty

Technical AWS Cloud experience in the Specialty domain as specified in the exam guide

aws certified Solutions Architect Professional
aws certified DevOps Engineer Professional
aws certified Solutions Architect Associate
aws certified SysOps Administrator Associate
aws certified Developer Associate
Architect
Operations
Developer
Cloud Practitioner
aws certified Cloud Practitioner
aws certified Advanced Networking Specialty
aws certified Big Data Specialty
aws certified Security Specialty
aws certified Machine Learning Specialty
aws certified Alexa Skill Builder Specialty

Module 1: Understand System Operations in AWS

AWS Document and References

https://docs.aws.amazon.com/index.html
https://viblo.asia/newest
https://cafedev.vn/
https://udemy.com
https://acloudguru.com

Module 1: Understand System Operations in AWS

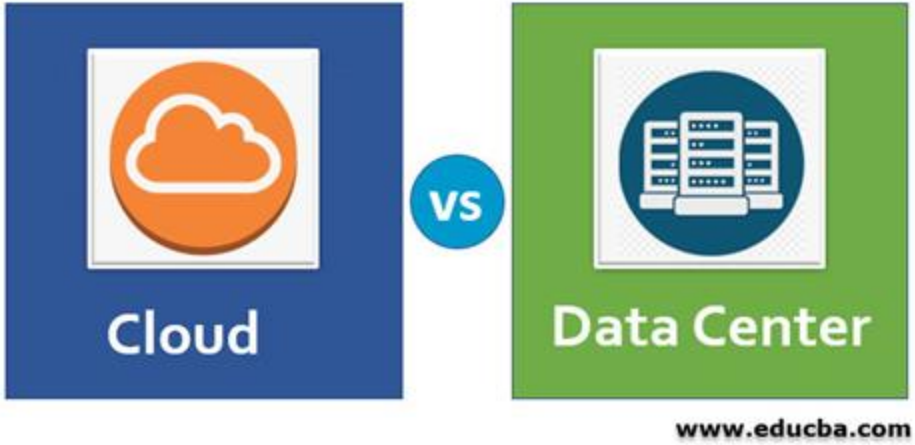
- **Goal**: Get started with the tools you need to administer resources on AWS
  - ✓ AWS Training and Certification
  - ✓ **Comparing Data Center and the Cloud**
  - ✓ High Level Overview
  - ✓ Securing Your AWS Account

What is System Operations?

- Configuration, deployment, and maintenance of system infrastructure
  - Network configuration and management
  - Server configuration and deployment
  - Application deployment and management
  - Storage, backup, and archive
  - Monitoring
  - Security

Cloud or Data Center?

Brain Storming!!



System Operations in Data Center and The Cloud

Data Center

- Upfront capital expense
- Provision hardware and staff for normal operations and disaster recovery (DR)
- Limited experimentation and reusability

The Cloud

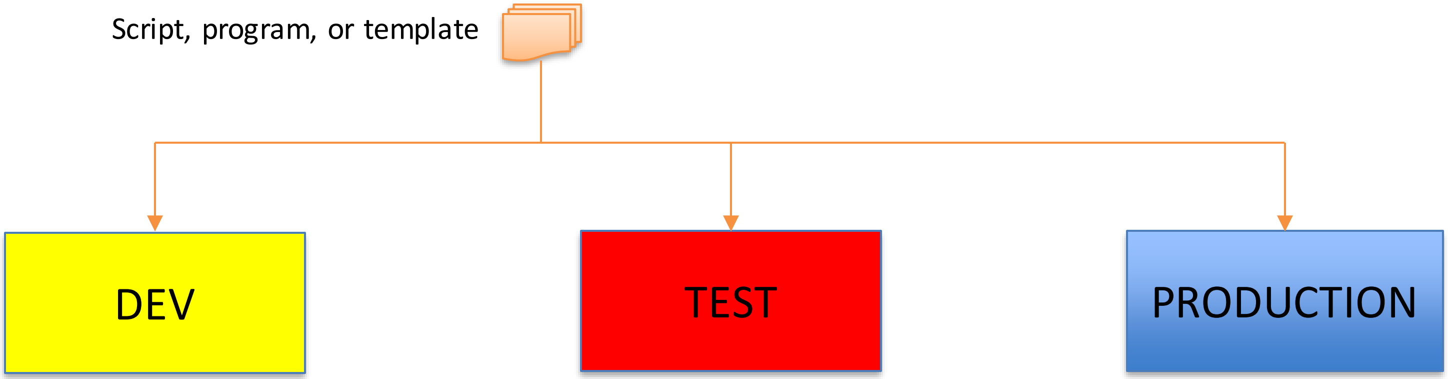
- Available when needed
- Build up, tear down and reuse with ease
- Reduced cost and planning for DR, storage redundancy
- More independence innovation within the company

Hybrid Model

- Connect data center and cloud resources

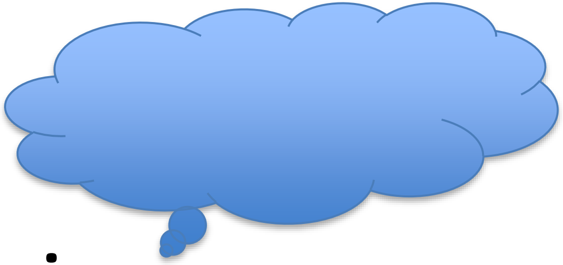
System Operations in the Cloud

- Cloud computing enables automated and repeatable deployment of infrastructure on demand.
- Systems can become self-describing.



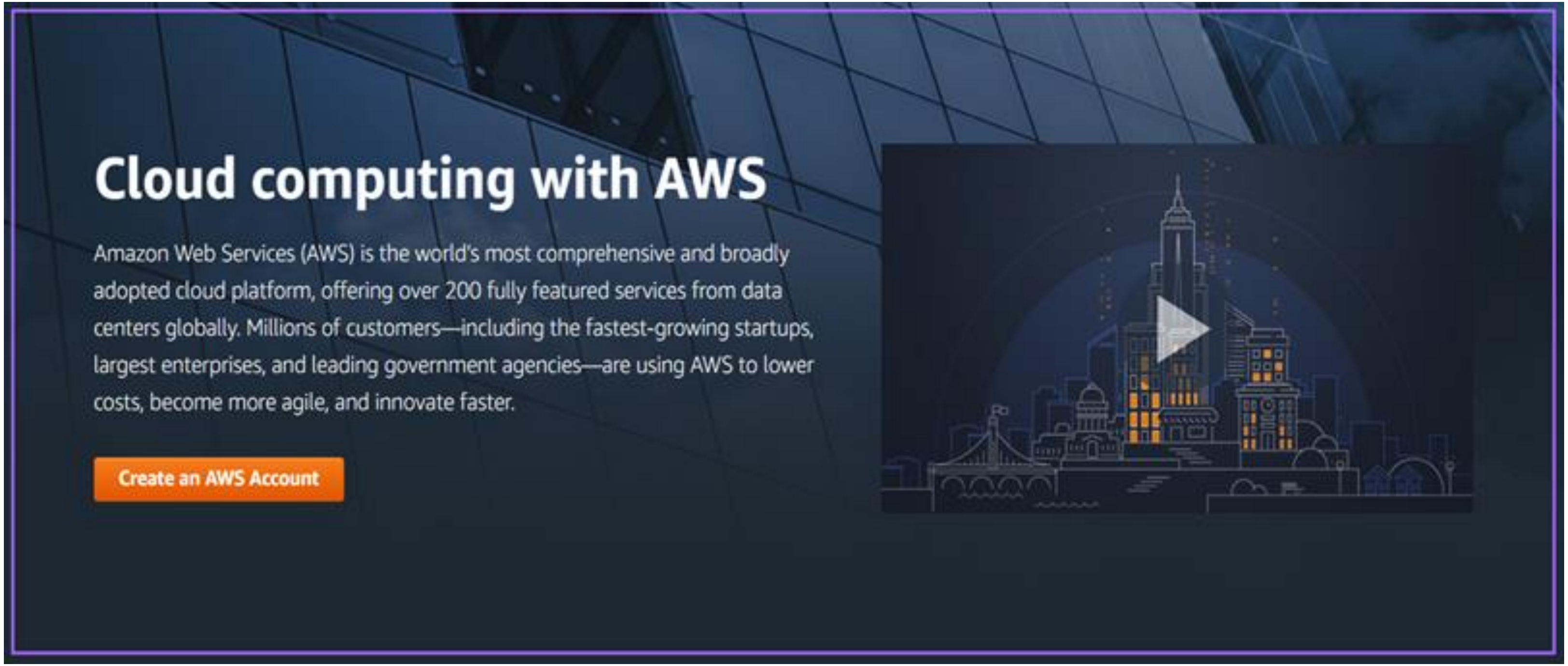
System Operations Scenarios in the Cloud

Operation Area	Tasks
Create	Configure instances, store data, create reusable infrastructure, domains and routing
Deploy	Green field deployment, create dev/test environments, replicate across regions
Monitor	Log and monitor, capture log data, analyze, troubleshoot, scale to demand
Change	Deploy new version (e.g., “blue/green” deployment), maintain and patch instances reclaim resources



AWS Overview

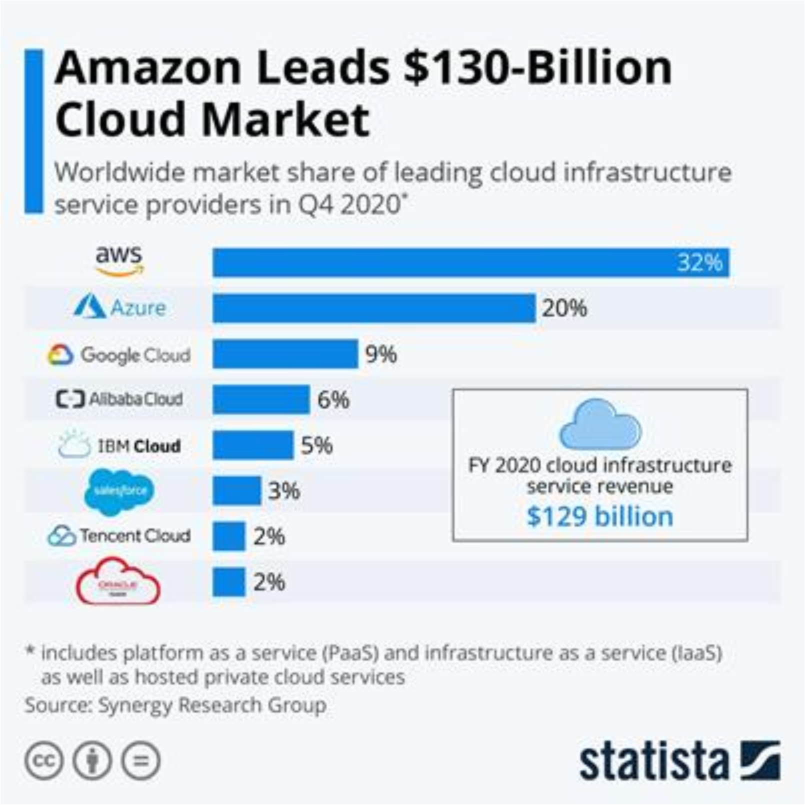
What is AWS?



Cloud computing with AWS

Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted cloud platform, offering over 200 fully featured services from data centers globally. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—are using AWS to lower costs, become more agile, and innovate faster.

AWS Market Share



Amazon Leads $130-Billion Cloud Market

Worldwide market share of leading cloud infrastructure service providers in Q4 2020*

* includes platform as a service (PaaS) and infrastructure as a service (IaaS) as well as hosted private cloud services

Source: Synergy Research Group

Global Infrastructure: AWS Regions, AZs, and Edge Locations

AWS achieves this by supporting a secure, redundant, and global infrastructure, which devide into regions, Availability Zones, and edge locations.

- A **region** is a collection of two or more Availability Zones in a specific geographic area.
- An **Availability Zone** is an isolated collection of AWS resources. Availability Zones within a region are connected through low-latency links.
- An **edge location** is A site that CloudFront uses to cache copies of your content for faster delivery to users at any location.

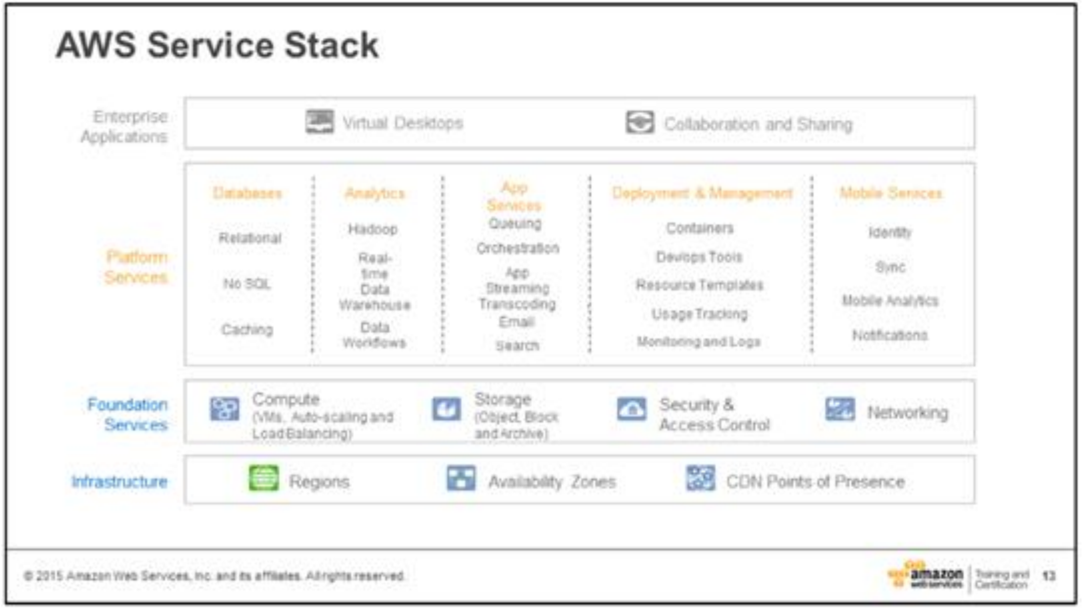
https://aws.amazon.com/about-aws/global-infrastructure/regions_az/?nc1=h_ls

Module 1: Understand System Operations in AWS

AWS Service Stack

AWS provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses all over the world.

At the core is the compute, storage and data services that are the heart of AWS's offering.



AWS Service Stack

Enterprise Applications: Virtual Desktops | Collaboration and Sharing

Platform Services:

- Databases: Relational, No SQL, Caching
- Analytics: Hadoop, Real-time Data Warehouse, Data Workflows
- App Services: Queuing, Orchestration, App Streaming, Transcoding, Email, Search
- Deployment & Management: Containers, Devops Tools, Resource Templates, Usage Tracking, Monitoring and Logs
- Mobile Services: Identity, Sync, Mobile Analytics, Notifications

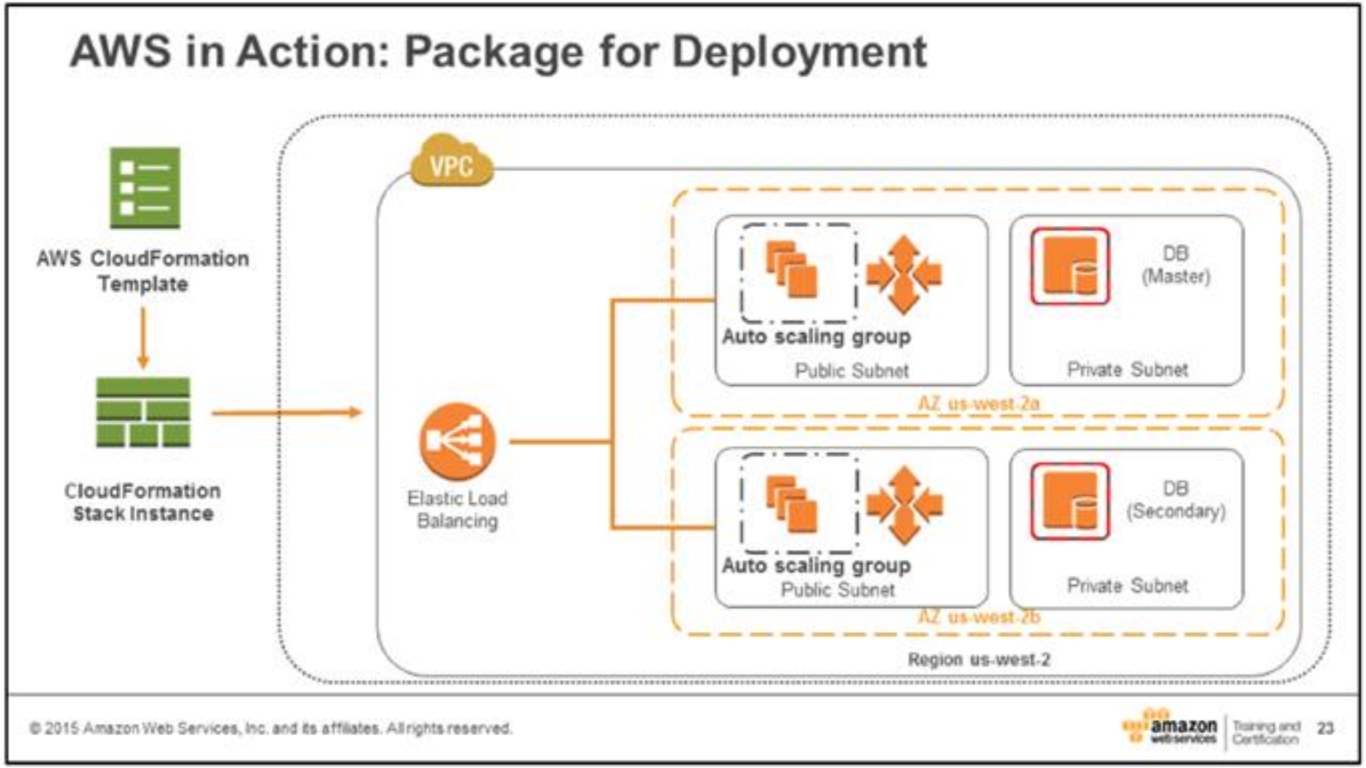
Foundation Services: Compute (VMs, Auto-scaling and Load Balancing) | Storage (Object, Block and Archive) | Security & Access Control | Networking

Infrastructure: Regions | Availability Zones | CDN Points of Presence

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

Module 1: Understand System Operations in AWS

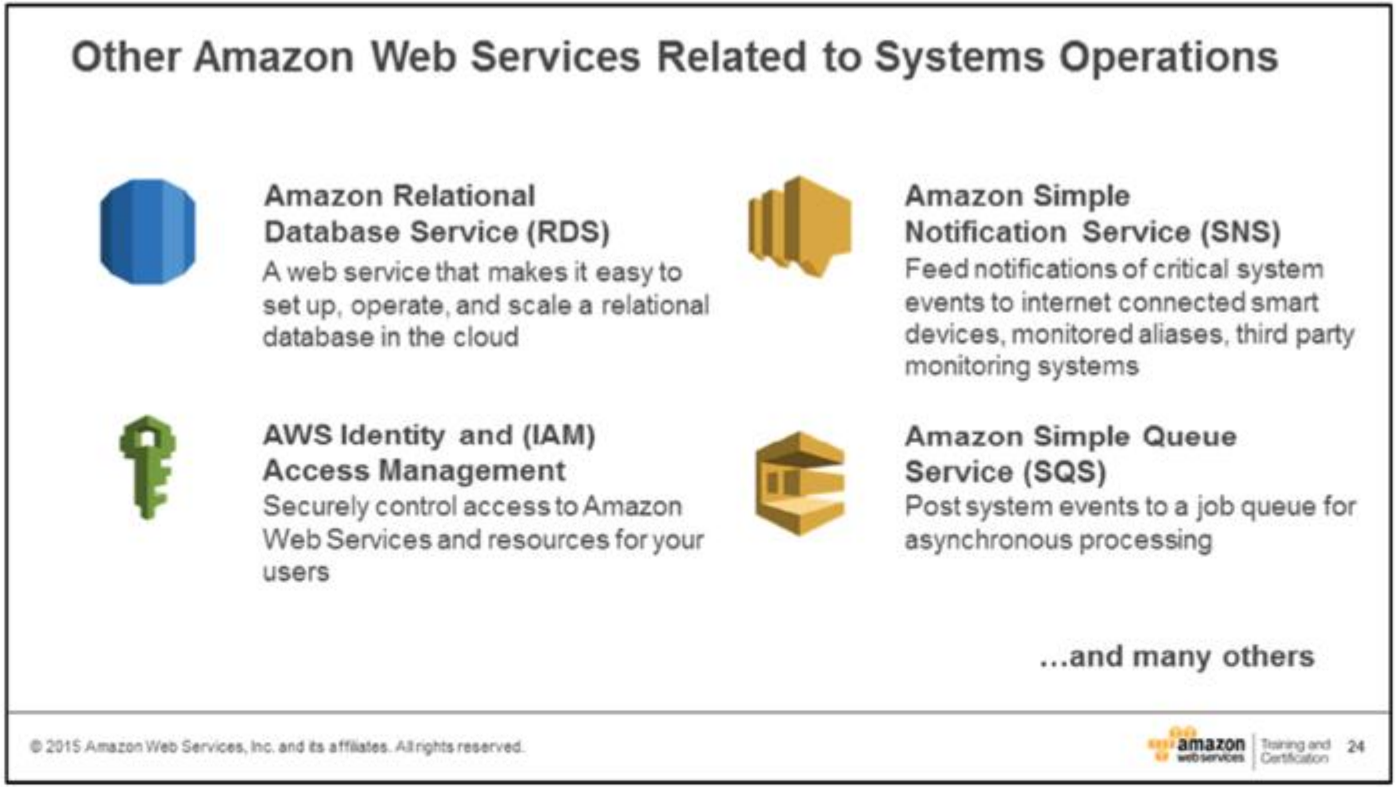
AWS in Action Example



AWS in Action: Package for Deployment

Module 1: Understand System Operations in AWS

AWS in Action Example



Other Amazon Web Services Related to Systems Operations

Amazon Relational Database Service (RDS)
A web service that makes it easy to set up, operate, and scale a relational database in the cloud

Amazon Simple Notification Service (SNS)
Feed notifications of critical system events to internet connected smart devices, monitored aliases, third party monitoring systems

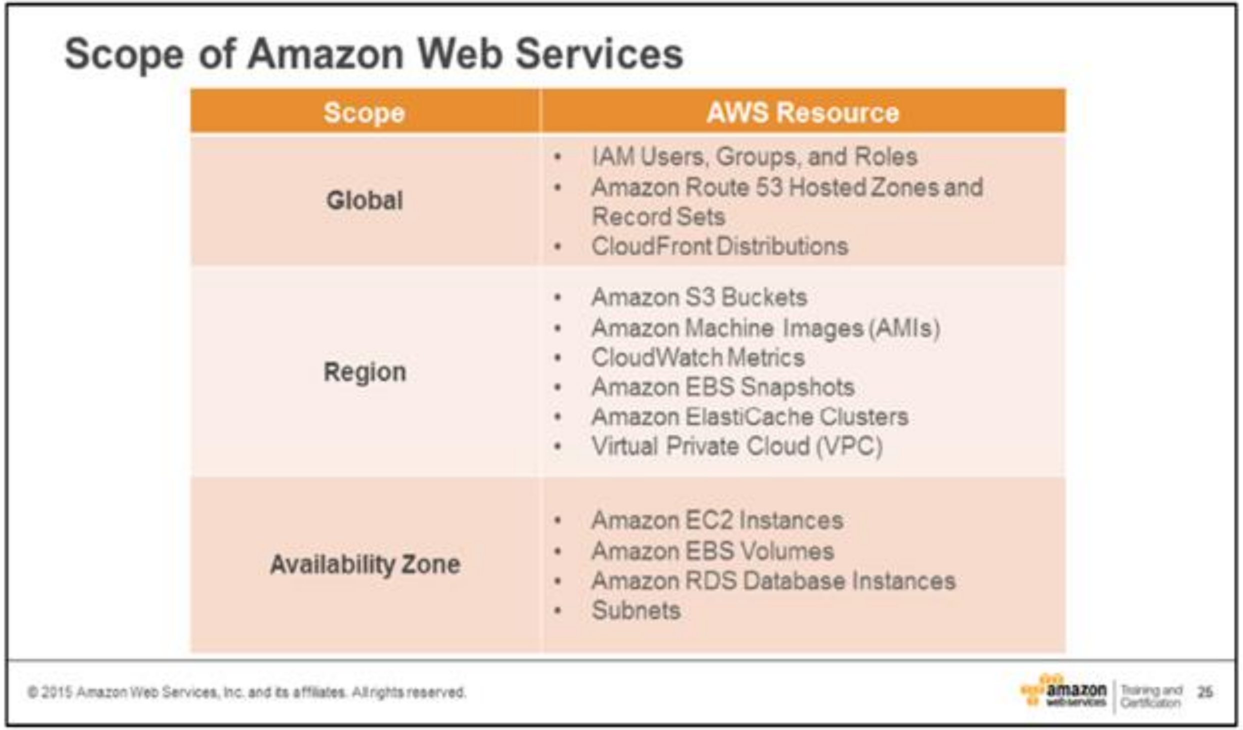
AWS Identity and (IAM) Access Management
Securely control access to Amazon Web Services and resources for your users

Amazon Simple Queue Service (SQS)
Post system events to a job queue for asynchronous processing

...and many others

Module 1: Understand System Operations in AWS

When create AWS resources, those resources exist at a scope which varies depending on the service – either global, region, or Availability Zone. Resources with global and regional scope are automatically distributed across multiple Availability Zones by AWS.



Scope of Amazon Web Services

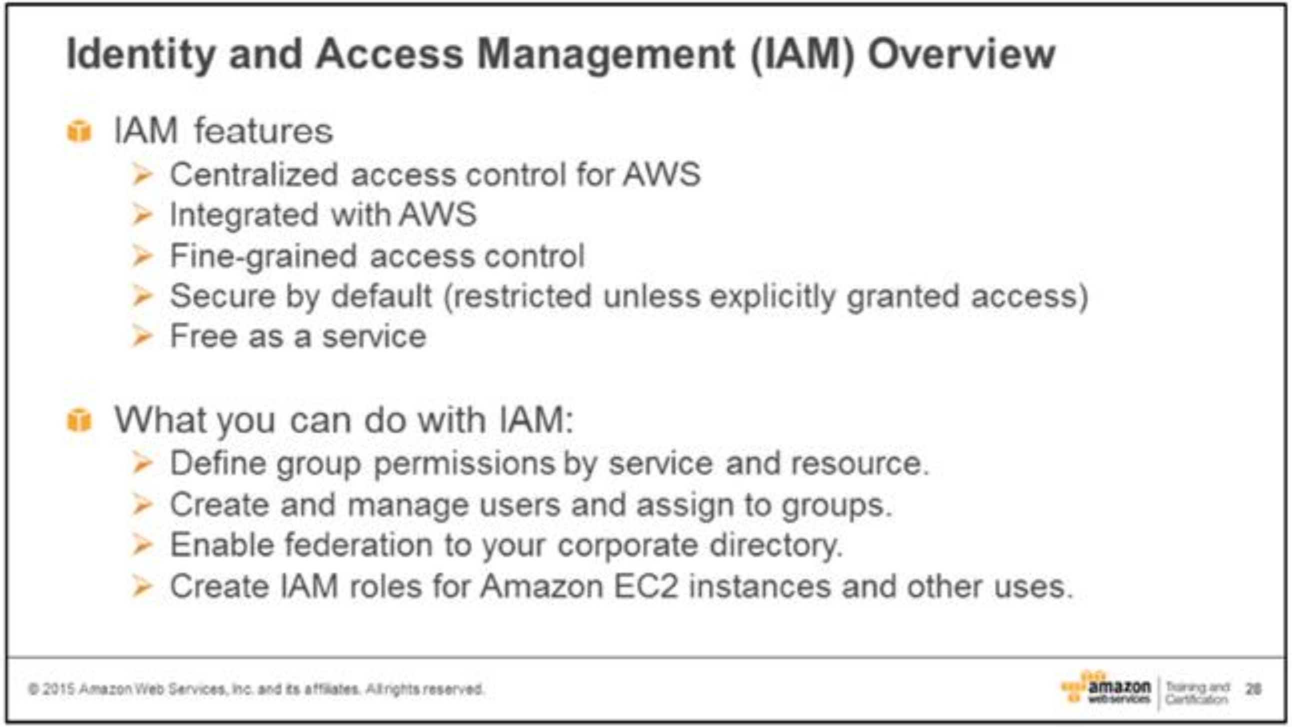
Scope	AWS Resource
Global	- IAM Users, Groups, and Roles - Amazon Route 53 Hosted Zones and Record Sets - CloudFront Distributions
Region	- Amazon S3 Buckets - Amazon Machine Images (AMIs) - CloudWatch Metrics - Amazon EBS Snapshots - Amazon ElastiCache Clusters - Virtual Private Cloud (VPC)
Availability Zone	- Amazon EC2 Instances - Amazon EBS Volumes - Amazon RDS Database Instances - Subnets

Module 1: Understand System Operations in AWS

- **Goal**: Get started with the tools you need to administer resources on AWS
  - ✓ AWS Training and Certification
  - ✓ Comparing Data Center and the Cloud
  - ✓ High Level Overview
  - ✓ **Securing Your AWS Account**

Module 1: Understand System Operations in AWS

AWS Identity and Access Management (IAM) provides a centralized environment in which to administer users, groups, roles and permissions.

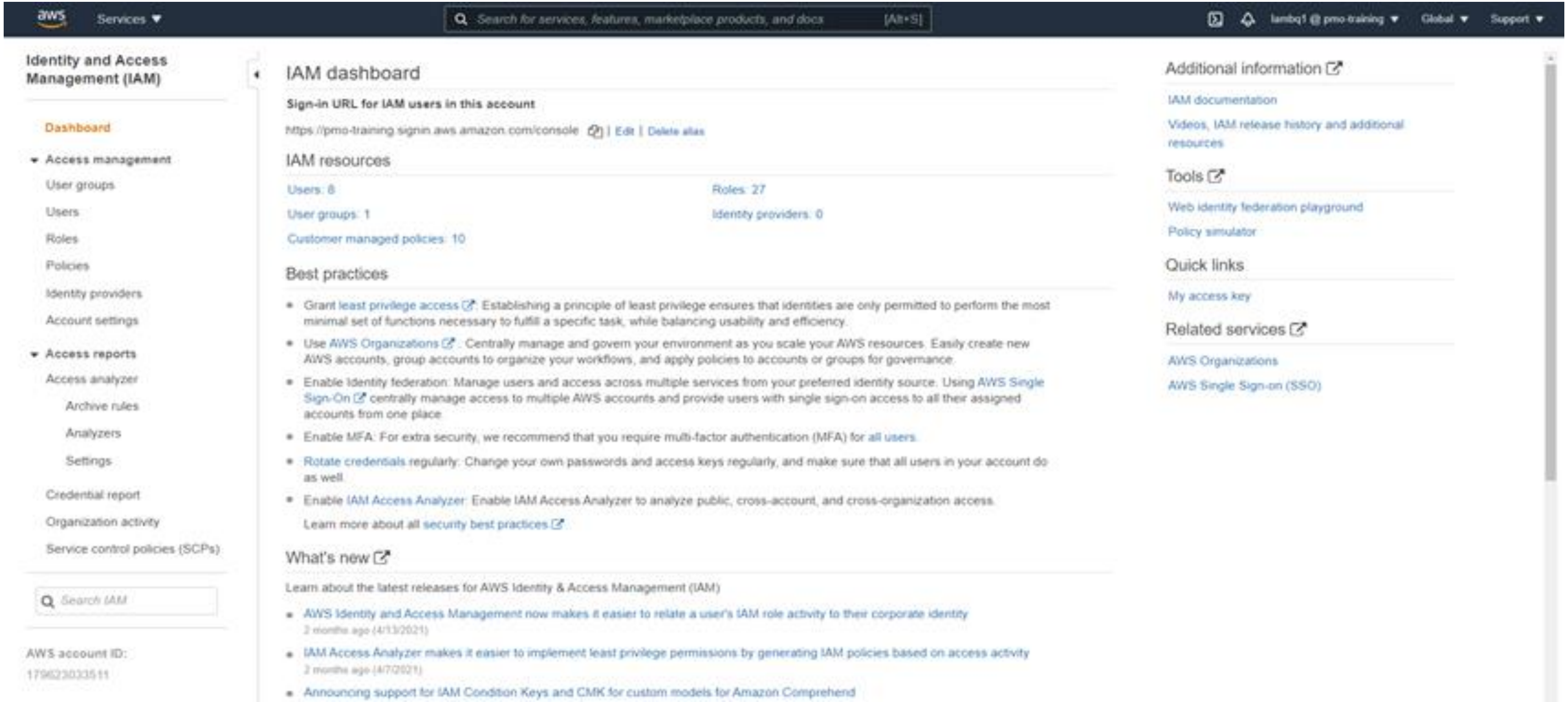


Identity and Access Management (IAM) Overview

- IAM features
  - Centralized access control for AWS
  - Integrated with AWS
  - Fine-grained access control
  - Secure by default (restricted unless explicitly granted access)
  - Free as a service
- What you can do with IAM:
  - Define group permissions by service and resource.
  - Create and manage users and assign to groups.
  - Enable federation to your corporate directory.
  - Create IAM roles for Amazon EC2 instances and other uses.

Module 1: Understand System Operations in AWS

Access to IAM services > Login AWS account >> Service > IAM (Manage access to AWS resources)


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
lambq1 @ pmo-training ▼
Global ▼
Support ▼

Identity and Access Management (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)

Search IAM

AWS account ID:
179623033511

IAM dashboard

Sign-in URL for IAM users in this account

https://pmo-training.signin.aws.amazon.com/console | Edit | Delete alias

IAM resources

Users: 8	Roles: 27
User groups: 1	Identity providers: 0
Customer managed policies: 10	

Best practices

- Grant least privilege access: Establishing a principle of least privilege ensures that identities are only permitted to perform the most minimal set of functions necessary to fulfill a specific task, while balancing usability and efficiency.
- Use AWS Organizations: Centrally manage and govern your environment as you scale your AWS resources. Easily create new AWS accounts, group accounts to organize your workflows, and apply policies to accounts or groups for governance.
- Enable Identity federation: Manage users and access across multiple services from your preferred identity source. Using AWS Single Sign-On centrally manage access to multiple AWS accounts and provide users with single sign-on access to all their assigned accounts from one place.
- Enable MFA: For extra security, we recommend that you require multi-factor authentication (MFA) for all users.
- Rotate credentials regularly: Change your own passwords and access keys regularly, and make sure that all users in your account do as well.
- Enable IAM Access Analyzer: Enable IAM Access Analyzer to analyze public, cross-account, and cross-organization access.

Learn more about all security best practices.

What's new

Learn about the latest releases for AWS Identity & Access Management (IAM)

- AWS Identity and Access Management now makes it easier to relate a user's IAM role activity to their corporate identity
  2 months ago (4/13/2021)
- IAM Access Analyzer makes it easier to implement least privilege permissions by generating IAM policies based on access activity
  2 months ago (4/7/2021)
- Announcing support for IAM Condition Keys and CMK for custom models for Amazon Comprehend

Additional information

- IAM documentation
- Videos, IAM release history and additional resources

Tools

- Web identity federation playground
- Policy simulator

Quick links

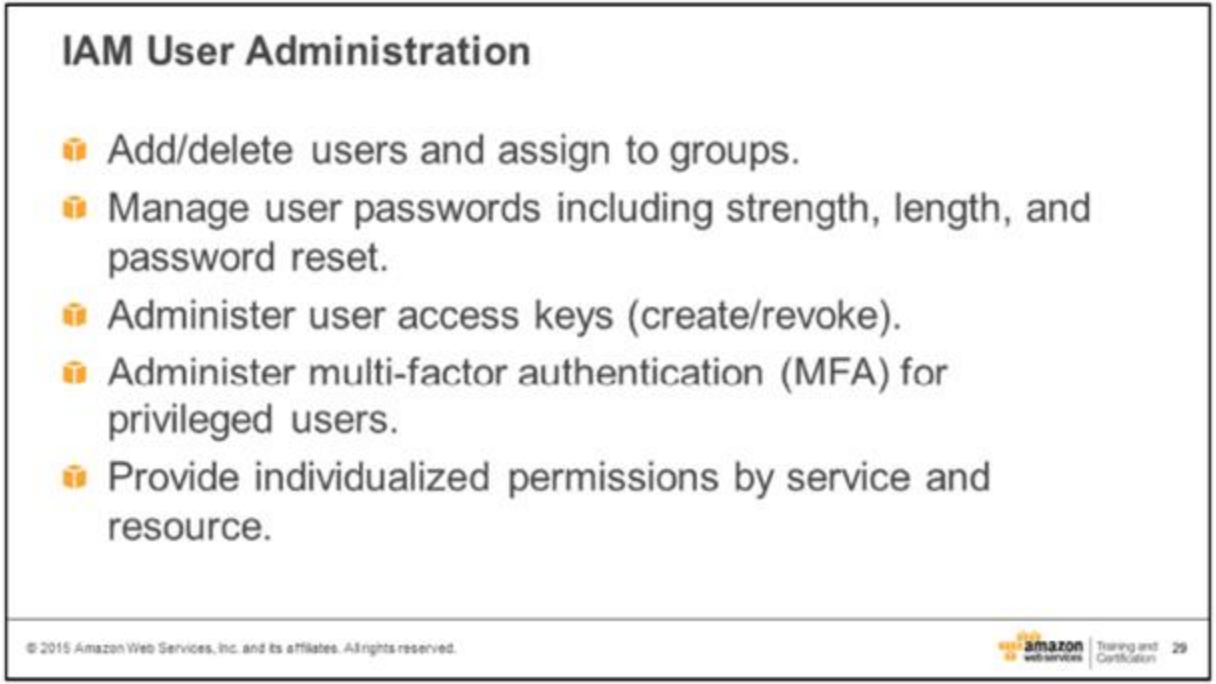
- My access key

Related services

- AWS Organizations
- AWS Single Sign-on (SSO)

Module 1: Understand System Operations in AWS

IAM enables a customer to create multiple users and manage the permissions for each of these users within their AWS account.



IAM User Administration

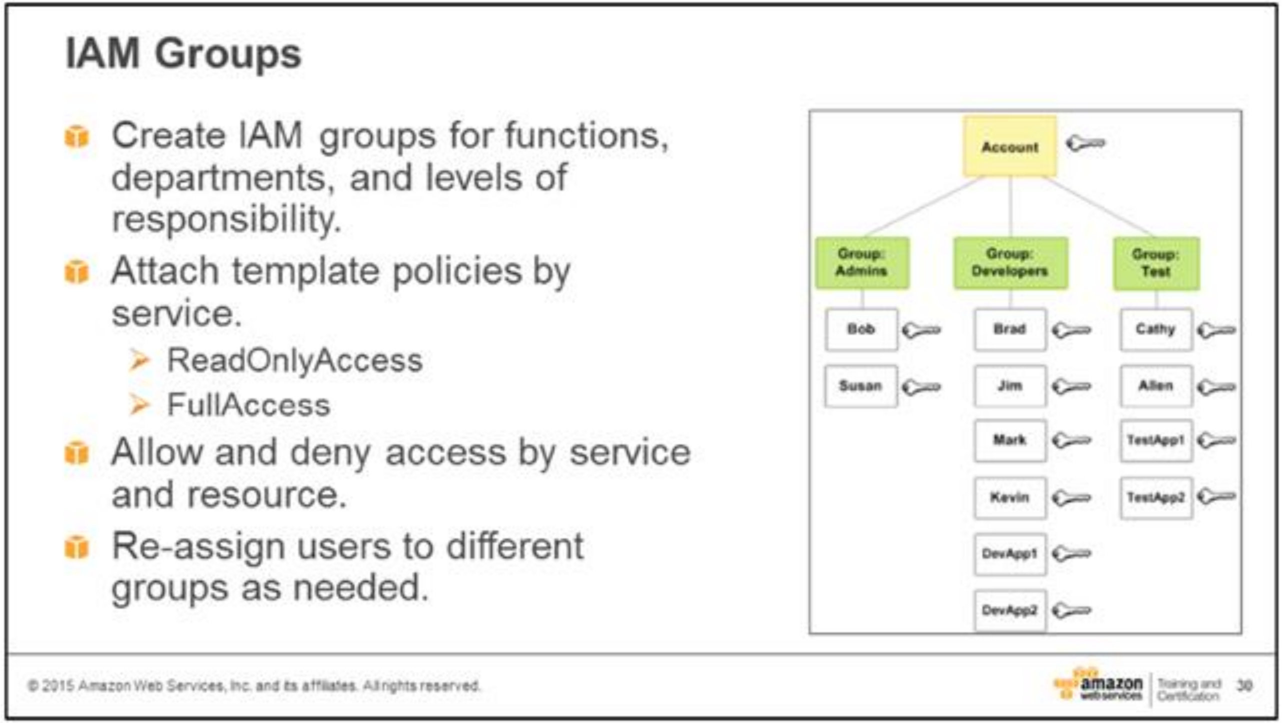
- Add/delete users and assign to groups.
- Manage user passwords including strength, length, and password reset.
- Administer user access keys (create/revoke).
- Administer multi-factor authentication (MFA) for privileged users.
- Provide individualized permissions by service and resource.

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

amazon web services Training and Certification 29

Module 1: Understand System Operations in AWS

To provide added security to AWS account, it is strongly encouraged that create a set of groups corresponding to the “least privilege” principle.

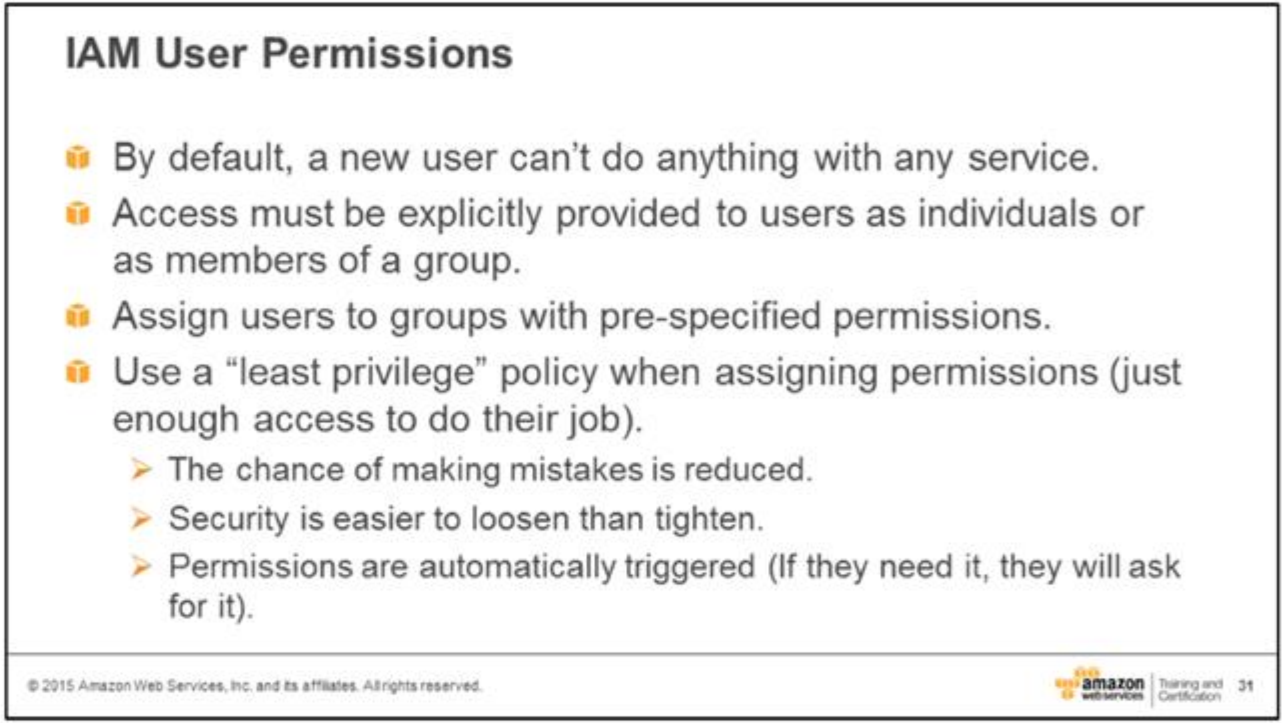


IAM Groups

- Create IAM groups for functions, departments, and levels of responsibility.
- Attach template policies by service.
  - ReadOnlyAccess
  - FullAccess
- Allow and deny access by service and resource.
- Re-assign users to different groups as needed.

Module 1: Understand System Operations in AWS

Using group simplifies the task of adding or removing permissions to a large number of users simultaneously.



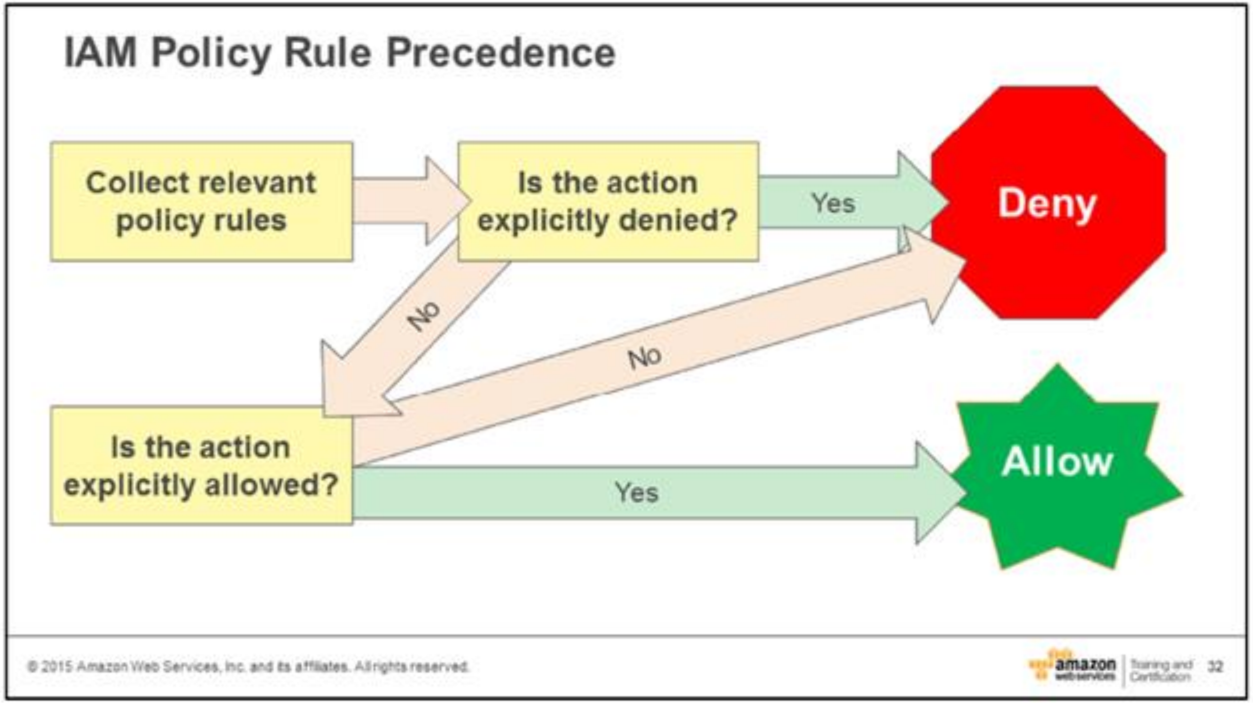
IAM User Permissions

- By default, a new user can’t do anything with any service.
- Access must be explicitly provided to users as individuals or as members of a group.
- Assign users to groups with pre-specified permissions.
- Use a “least privilege” policy when assigning permissions (just enough access to do their job).
  - The chance of making mistakes is reduced.
  - Security is easier to loosen than tighten.
  - Permissions are automatically triggered (If they need it, they will ask for it).

Module 1: Understand System Operations in AWS

To determine whether the request should be allowed or denied, these rules are followed:

- By default, all requests are denied
- An explicit allow overrides this default
- An explicit deny overrides any allows



IAM Policy Rule Precedence

Collect relevant policy rules

Is the action explicitly denied?

Yes

Deny

No

Is the action explicitly allowed?

No

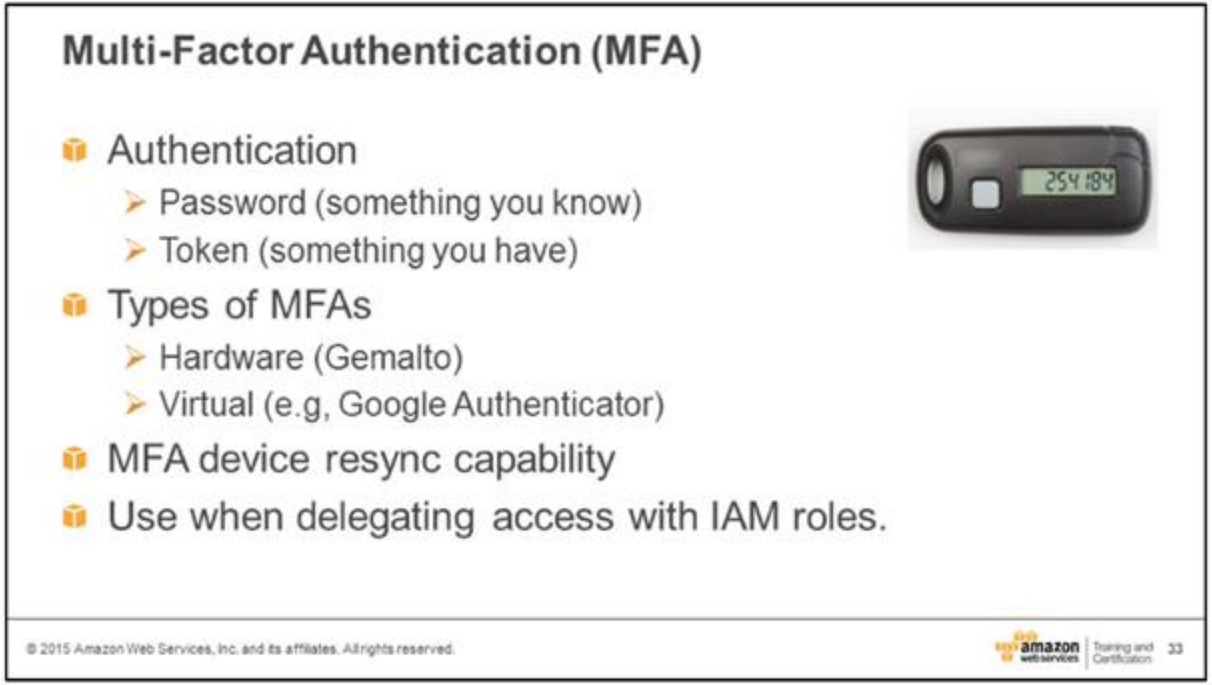
Yes

Allow

amazon web services | Training and Certification 32

Module 1: Understand System Operations in AWS

These days, password-only security is not enough. Should enable multi-factor authentication (MFA). With MFA, users must supply both a password and a one-time challenge/response token.



Multi-Factor Authentication (MFA)

- Authentication
  - Password (something you know)
  - Token (something you have)
- Types of MFAs
  - Hardware (Gemalto)
  - Virtual (e.g, Google Authenticator)
- MFA device resync capability
- Use when delegating access with IAM roles.

254 184

amazon web services
Training and Certification
33

Module 1: Understand System Operations in AWS

Securing your AWS Account

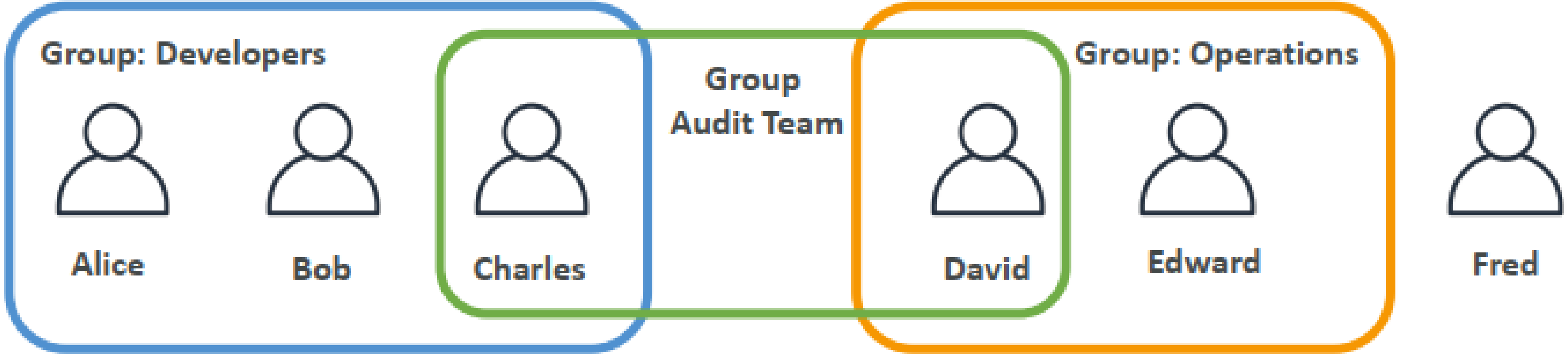
- ❑ Delegate system administration functions to least-privilege IAM admin groups
- ❑ Require multi-factor authentication for root-level access
- ❑ Physically secure hardware MFA devices in a secure place such as a vault
- ❑ Do not share root credentials with anyone other than the account holder
- ❑ Use IAM roles to provide cross-account access

IAM SECTION

IAM: User & Groups

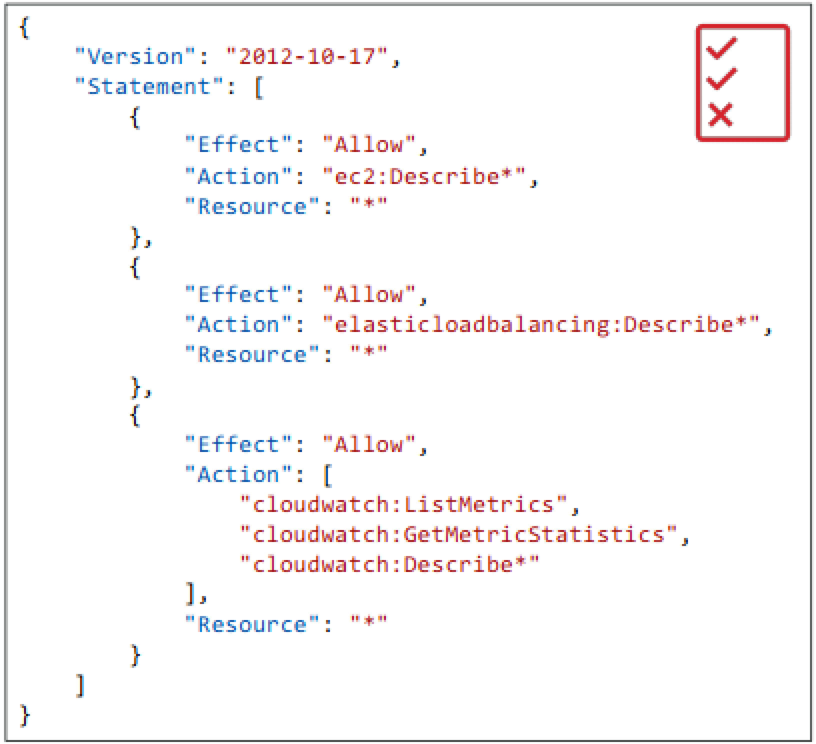
- IAM = Identity and Access Management, Global service
- Root account create by default, shouldn’t be used or shared
- User are people within your organization, and can be grouped
- Groups only contain users, not other groups
- User don’t have to belong to a group, and user can belong to multi group

IAM: User & Groups



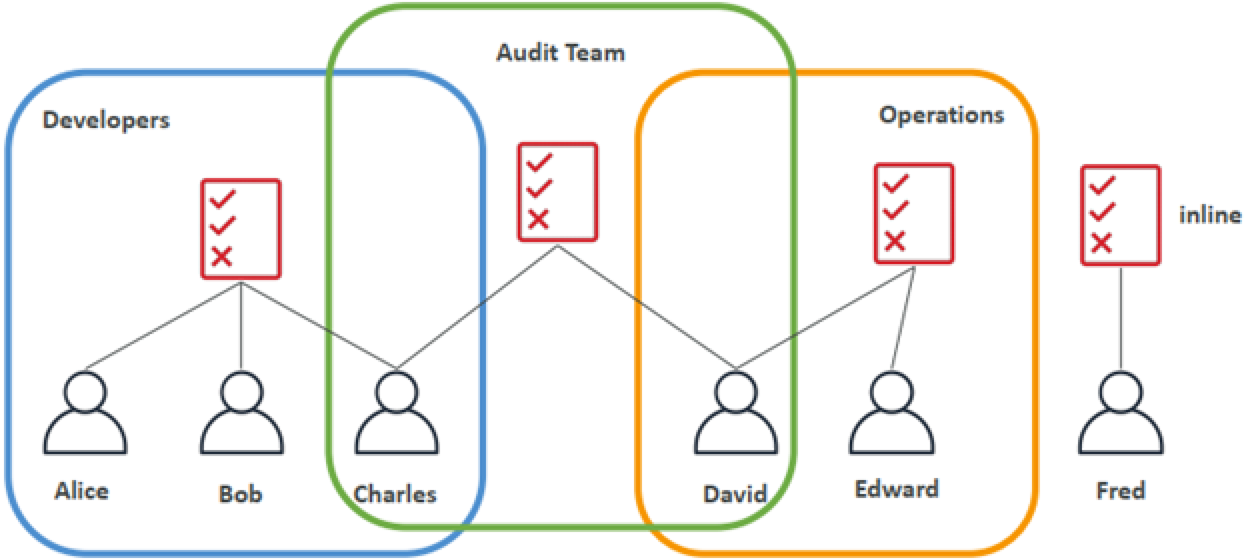
IAM: User & Groups

- Users or Groups can be assigned JSON documents called **policies**
- These **policies** define the permissions of the user
- In AWS you apply the **least privilege** principle: don't give more permission than user need



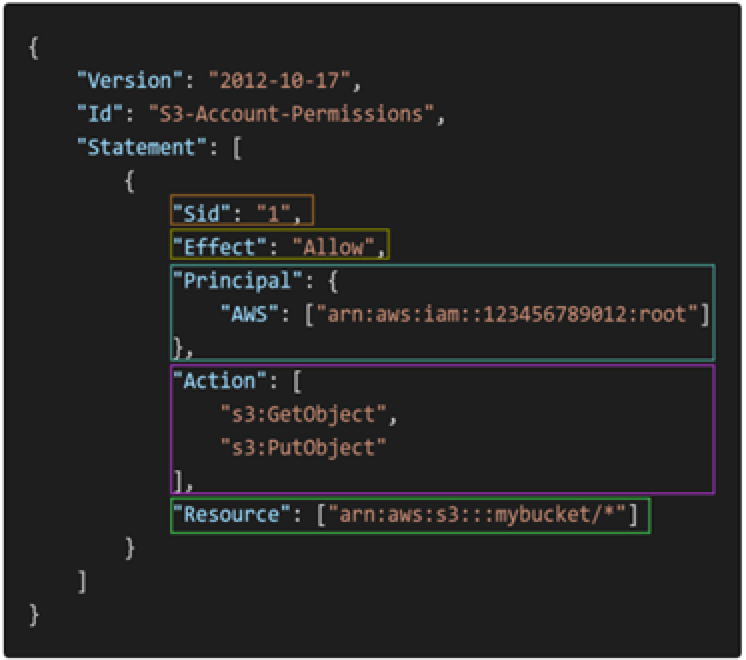
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:ListMetrics",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

IAM Policies inheritance



IAM Policies Structure

- Consist of
  - Version: policy language version, always include “2012-10-17”
  - Id: an indentifer for the policy (optional)
  - Statement: one or more individual statements (required)
- Statement consist of
  - Sid: an indentifer for the statement (optional)
  - Effect: whether the statement allows or denies access (allow, deny)
  - Principal: account/user/role which this policy applied to
  - Action: list of actions this policy allows or denies
  - Resource: list of resources to which the actions applied to
  - Condition: conditions for when this policy is in effect (optional)



```
{
    "Version": "2012-10-17",
    "Id": "S3-Account-Permissions",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Principal": {
                "AWS": ["arn:aws:iam::123456789012:root"]
            },
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": ["arn:aws:s3:::mybucket/*"]
        }
    ]
}
```

IAM – Password Policy

- Strong passwords = higher security for your account
- In AWS, you can setup a password policy
    - Set a minimum password lengh
    - Require specific character types
        - Including uppercase letters
        - Lowercase letters
        - Number
        - Non-alphanumeric characters
- Allow all IAM users to change their own passwords
- Require users to change their password after some time (password expiration)
- Prevent password re-use

Multi Factor Authentication - MFA

- Users have access to your account and can possibly change configurations or delete resources in your AWS account
- You want to protect your Root Accounts and IAM users
- MFA = password you know + security device you own
- Main benefit of MFA:
  - If a password is stolen or hacked, the account is not compromised

Alice
Password
+
MFA
=>
Successful login

MFA devices options in AWS

Virtual MFA device

571 208

222 104

140 359

364 218

Google Authenticator
(phone only)

204009

Authy
(multi-device)

Support for multiple tokens on a single device.

Universal 2nd Factor (U2F) Security Key

YubiKey by Yubico (3rd party)

Support for multiple root and IAM users using a single security key

MFA devices options in AWS

Hardware Key Fob MFA Device

Provided by Gemalto (3rd party)

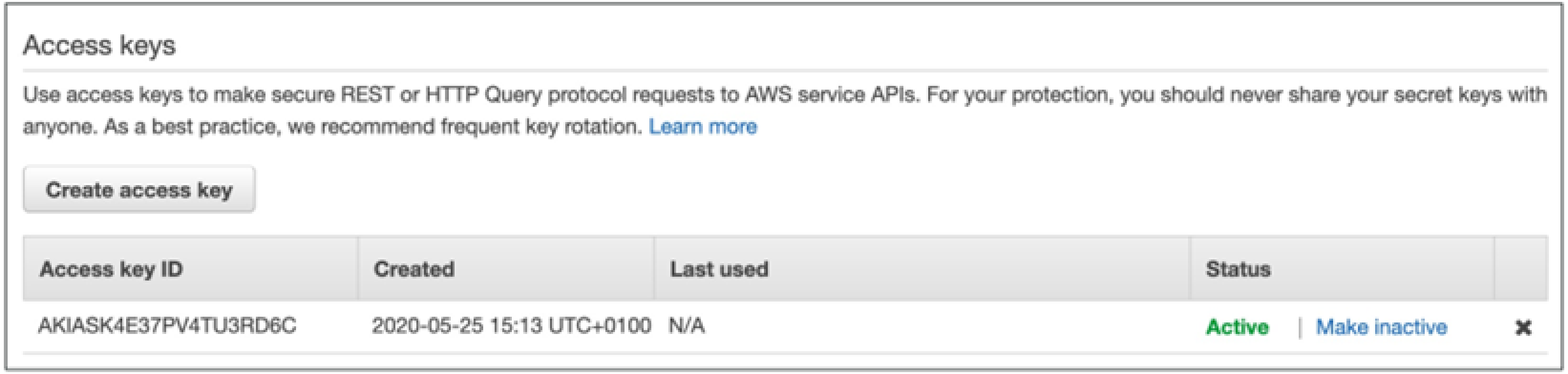
Hardware Key Fob MFA Device for AWS GovCloud (US)

Provided by SurePassID (3rd party)

How can users access AWS?

- To access AWS, you have three options:
    - AWS Management Console (protected by password + MFA)
    - AWS Command Line Interface (CLI): protect by access keys
    - AWS Software Developer Kit (SDK) – for code: protected by accese keys
- Access Keys are generated through the AWS Console
- Users manage their own access keys
- Access Keys are secret, just like a password. Don’t share them
- Access Key ID ~= username
- Secret Access Key ~= password

Example (Fake) Access Keys



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

Access key ID	Created	Last used	Status	
AKIASK4E37PV4TU3RD6C	2020-05-25 15:13 UTC+0100	N/A	Active | Make inactive	✖

- Access key ID: AKIASK4E37PV4983d6C
- Secret Access Key: AZPN3zojWozWCndljhB0Unh8239a1bzbzO5fqqkZq
- Remember: don't share your access keys

What’s the AWS CLI?

- A tool that enables you to interact with AWS services using commands in your command-line shell
- Direct access to the public APIs of AWS services
- You can develop scripts to manage your resources
- It’s open-source https://github.com/aws/aws-cli
- Alternative to using AWS Management Console

What’s the AWS SDK?

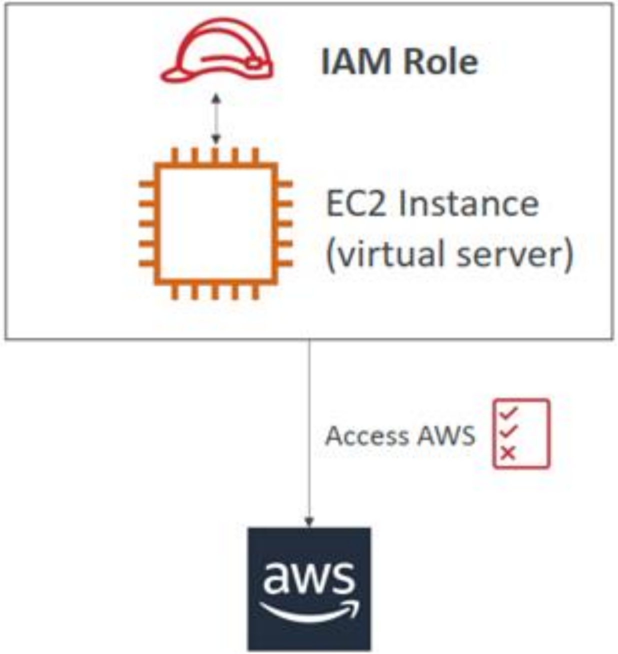
- AWS Software Development Kit (AWS SDK)
- Language-specific APIs (set of libraries)
- Enables you to access and manage AWS services programmatically
- Embedded within your application
- Supports
  - SDKs (JavaScript, Python, PHP, .NET. Ruby, Java, Go, Node.js, C++)
  - Mobile SDKs (Android, iOS, …)
  - IoT Device SDKs (Embedded C, Arduino, …)
- Example: AWS CLI is built on AWS SDK for Python

Your Application

Module 1: Understand System Operations in AWS

IAM Roles for Services

- Some AWS service will need to perform actions on your behalf
- To do so, we will assign permissions to **AWS services** with **IAM Roles**
- Common roles:
  - **EC2 Instance Roles**
  - Lambda Function Roles
  - Roles for CloudFormation



IAM Security Tools

- **IAM Credentials Report (account-level)**
  - A report that lists all your account’s users and the status of their various credential
- **IAM Access Advisor (user-level)**
  - Access advisor shows the service permission granted to a user and when those services were last accessed
  - You can use this information to revise your policies

IAM Guidelines & Best Practices

- Don’t use the root account except for AWS account setup
- One physical user = One AWS **user**
- **Assign users to groups** and assign permissions to groups
- Create a **strong password policy**
- Use and enforce the use of **Multi Factor Authentication (MFA)**
- Create and user **Roles** for giving permissions to AWS services
- Use Access Keys for Programmatic Access (CLI/SDK)
- Audit permissions of your account with the IAM Credentials Report
- <u>**Never share IAM users & Access Keys**</u>

IAM Section - Summary

- **Users:** mapped to a physical user, has a password for AWS Console
- **Groups:** contains users only
- **Policies:** JSON document that outlines permissions for users or groups
- **Roles:** for **EC2 instances** or AWS services
- **Security:** MFA + Password Policy
- **Access Keys:** access AWS using the CLI or SDK
- **Audit:** IAM Credential Reports & IAM Access Advisor

Thank you