

AWS Academy Cloud Foundations

# Course Introduction

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Module overview



### Topics

- Course objectives and overview
- AWS certification exam information
- AWS Documentation

### Activities

- AWS Documentation scavenger hunt

# Module objectives

After completing this module, you should be able to:

- Recognize the purpose of the AWS Academy Cloud Foundations course
- Recognize the course structure
- Recognize the AWS certification process
- Navigate the AWS Documentation website

## Course Introduction

### Section 1: Course objectives and overview

# Course prerequisites

- General Required Knowledge
  - IT technical knowledge
  - IT business knowledge
- Preferred Knowledge
  - Familiarity with cloud computing concepts
  - Working knowledge of distributed systems
  - Familiarity with general networking concepts



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

5

# Course objectives

After completing this course, you should be able to:

- Define the AWS Cloud.
- Explain the AWS pricing philosophy.
- Identify the global infrastructure components of AWS.
- Describe security and compliance measures of the AWS Cloud including AWS Identity and Access Management (IAM).
- Create an AWS Virtual Private Cloud (Amazon VPC).
- Demonstrate when to use Amazon Elastic Compute Cloud (EC2), AWS Lambda and AWS Elastic Beanstalk.
- Differentiate between Amazon S3, Amazon EBS, Amazon EFS and Amazon S3 Glacier.
- Demonstrate when to use AWS Database services including Amazon Relational Database Service (RDS), Amazon DynamoDB, Amazon Redshift, and Amazon Aurora.
- Explain AWS Cloud architectural principles.
- Explore key concepts related to Elastic Load Balancing (ELB), Amazon CloudWatch, and Auto Scaling.



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

6

# Course outline



- Module 1: Cloud Concepts Overview
- Module 2: Cloud Economics and Billing
- Module 3: AWS Global Infrastructure Overview
- Module 4: AWS Cloud Security
- Module 5: Networking and Content Delivery
- Module 6: Compute
- Module 7: Storage
- Module 8: Databases
- Module 9: Cloud Architecture
- Module 10: Automatic Scaling and Monitoring



7

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Module 1: Cloud Concepts Overview

### Module sections:

- Introduction to cloud computing
- Advantages of cloud computing
- Introduction to Amazon Web Services (AWS)
- Moving to the AWS Cloud – The AWS Cloud Adoption Framework (AWS CAF)



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

8

# Module 2: Cloud Economics and Billing

## Module sections:

- Fundamentals of pricing
- Total Cost of Ownership
- AWS Organizations
- AWS Billing and Cost Management
- Technical support



# Module 3: AWS Global Infrastructure Overview

## Module sections:

- AWS Global Infrastructure
- AWS services and service category overview



# Module 4: AWS Cloud Security

## Module sections:

- AWS shared responsibility model
- AWS Identity and Access Management (IAM)
- Securing a new AWS account
- Securing accounts
- Securing data on AWS
- Working to ensure compliance



# Module 5: Networking and Content Delivery

## Module sections:

- Networking basics
- Amazon VPC
- VPC networking
- VPC security
- Amazon Route 53
- Amazon CloudFront



# Module 6: Compute

## Module sections:

- Compute services overview
- Amazon EC2
- Amazon EC2 cost optimization
- Container services
- Introduction to AWS Lambda
- Introduction to AWS Elastic Beanstalk



# Module 7: Storage

## Module sections:

- Amazon Elastic Block Store (Amazon EBS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Elastic File System (Amazon EFS)
- Amazon Simple Storage Service Glacier



## Module 8: Databases

### Module sections:

- Amazon Relational Database Service (Amazon RDS)
- Amazon DynamoDB
- Amazon Redshift
- Amazon Aurora



## Module 9: Cloud Architecture

### Module sections:

- AWS Well-Architected Framework
- Reliability and availability
- AWS Trusted Advisor



## Module 10: Automatic Scaling and Monitoring

### Module sections:

- Elastic Load Balancing
- Amazon CloudWatch
- Amazon EC2 Auto Scaling



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

17

Course Introduction

## Section 2: AWS certification exam information



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

# AWS certification exams



aws certified  
Updated May 2019

## Available AWS Certifications

*This course helps prepare you for the AWS Cloud Practitioner certification exam*

### 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



Architect

Operations

Developer

### 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](#)



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

19

## AWS Certified Cloud Practitioner exam

- Details about the exam—including how to register for it—are at <https://aws.amazon.com/certification/certified-cloud-practitioner/>
  - Download and carefully read the [AWS Certified Cloud Practitioner Exam Guide](#)
  - Download the [sample exam questions](#)
- See the recommended path to attain the certification at <https://aws.amazon.com/training/path-cloudpractitioner/>
  - AWS Academy Cloud Foundations covers much of the same material found in the Cloud Practitioner Essentials course, but in greater depth.
  - There is additional free digital training available at [aws.training](https://aws.training)



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

20

## Course Introduction

# Section 3: AWS Documentation

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## AWS Documentation

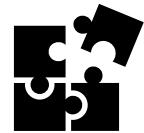
- Find user guides, developer guides, API references, tutorials, and more.
  - <https://docs.aws.amazon.com/>
- **Whitepapers** are also available at <https://aws.amazon.com/whitepapers/>, including these which are recommended reading for the AWS Cloud Practitioner exam:
  - [Overview of Amazon Web Services](#)
  - [Architecting for the Cloud: AWS Best Practices](#)
  - [How AWS Pricing Works](#)
  - [The Total Cost of \(Non\) Ownership of Web Applications in the Cloud](#)

# Activity - AWS Documentation Scavenger Hunt

23



- Navigate the AWS Documentation website
- Start from the main page at <https://docs.aws.amazon.com>
- Five challenge questions for the class appear in the following slides



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## AWS Documentation Scavenger Hunt – Question 1

24



- Question #1: What guides and references exist for the Amazon EC2 service?
- Answer:
  - User Guides for Linux and Windows
  - API Reference
  - AWS CLI Reference
  - EC2 Instance Connect Reference
  - User Guide for Auto Scaling
  - VM Import/Export User Guide

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## AWS Documentation Scavenger Hunt – Question 2

25

- Question #2: Can you find the documentation that describes how to create an Amazon S3 bucket?

- Answer:

- From <https://docs.aws.amazon.com/> click **S3**
- Click the **Getting Started Guide**
- Click **Create a Bucket**

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## AWS Documentation Scavenger Hunt – Question 3

26

- Question #3: Can you find a one-sentence summary of the AWS Cloud9 service?

- Answer:

- AWS Cloud9 is a cloud-based integrated development environment (IDE) that you use to write, run, and debug code.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## AWS Documentation Scavenger Hunt – Question 4

27

- Question #4: Which programming languages does the AWS Lambda service API support?

- Answer:

- From the main AWS Documentation page, click the **AWS Lambda** link
- Click the **API Reference** link
- Click **Getting Started > Tools** to find a table that lists the following languages: **Node.js, Java, C#, Python, Ruby, Go, and PowerShell**

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## AWS Documentation Scavenger Hunt – Question 5

28

- Question #5: Find the tutorial that describes how to run a serverless Hello World application, then scroll through the documented steps. What two AWS services does the tutorial have you use?

- Answer:

- From the main AWS Documentation page, click **Tutorials and Projects**
- In the **Websites & Web Apps** area, click the tutorial.
- The tutorial has you use **AWS Lambda** and **Amazon CloudWatch**.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Course Introduction

### Module wrap-up

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Module summary

In summary, in this module, you learned how to:

- Recognize the purpose of the AWS Academy Cloud Foundations course
- Recognize the course structure
- Recognize the AWS certification process
- Navigate the AWS Documentation website

# Additional resources

- [AWS Certification](#)
- [AWS Certified Cloud Practitioner](#)
- [AWS Documentation](#)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

31

Thank you

© 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. Corrections or feedback on the course, please email us at: [aws-course-feedback@amazon.com](mailto:aws-course-feedback@amazon.com). For all other questions, contact us at: <https://aws.amazon.com/contact-us/aws-training/>. All trademarks are the property of their owners.



AWS Academy Cloud Foundations

# Module 1: Cloud Concepts Overview

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Module overview

### Topics

- Introduction to cloud computing
- Advantages of cloud computing
- Introduction to Amazon Web Services (AWS)
- AWS Cloud Adoption Framework (AWS CAF)



### Knowledge check

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

34

# Module objectives

After completing this module, you should be able to:

- Define different types of cloud computing models
- Describe six advantages of cloud computing
- Recognize the main AWS service categories and core services
- Review the AWS Cloud Adoption Framework (AWS CAF)

## Module 1: Cloud Concepts Overview

### Section 1: Introduction to cloud computing

# What is cloud computing?



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

37

## Cloud computing defined

**Cloud computing** is the **on-demand** delivery of compute power, database, storage, applications, and other IT resources **via the internet** with **pay-as-you-go** pricing

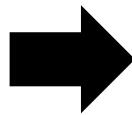


© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

38

# Infrastructure as software

Cloud computing enables you to **stop thinking of your infrastructure as hardware**, and instead **think of (and use) it as software**.



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

39

## Traditional computing model

- Infrastructure as hardware
  - Hardware solutions:
    - Require space, staff, physical security, planning, capital expenditure
    - Have a long hardware procurement cycle
    - Require you to provision capacity by guessing theoretical maximum peaks

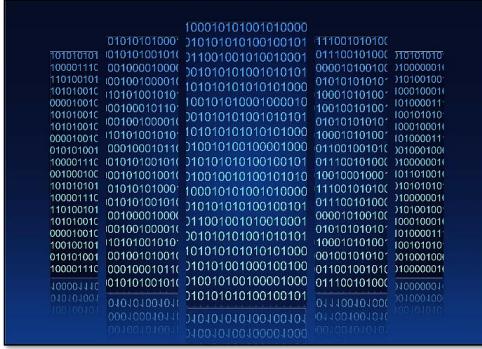


© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

40

# Cloud computing model

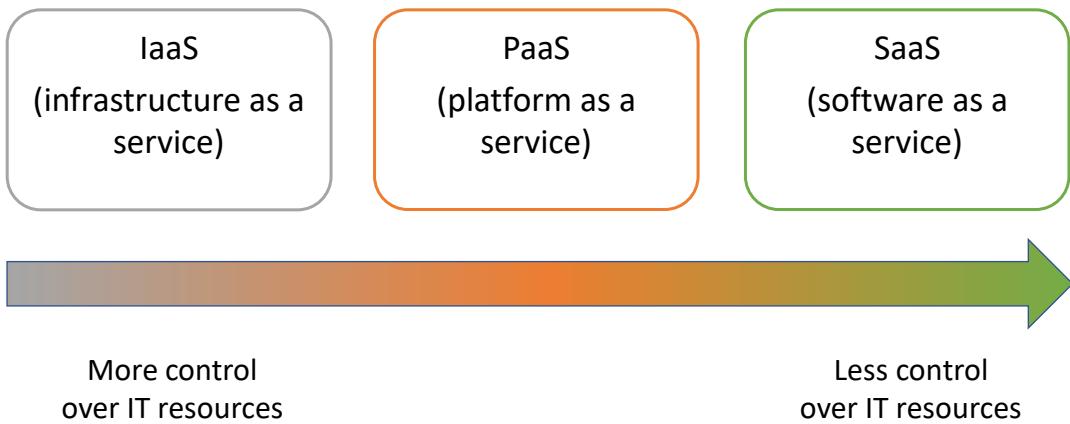
- Infrastructure as software
- Software solutions:
  - Are flexible
  - Can change more quickly, easily, and cost-effectively than hardware solutions
  - Eliminate the undifferentiated heavy-lifting tasks



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

41

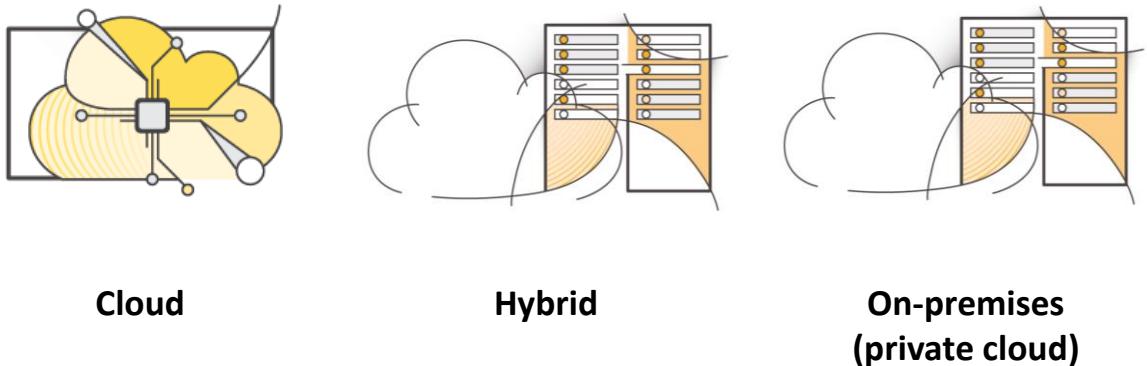
## C service models



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

42

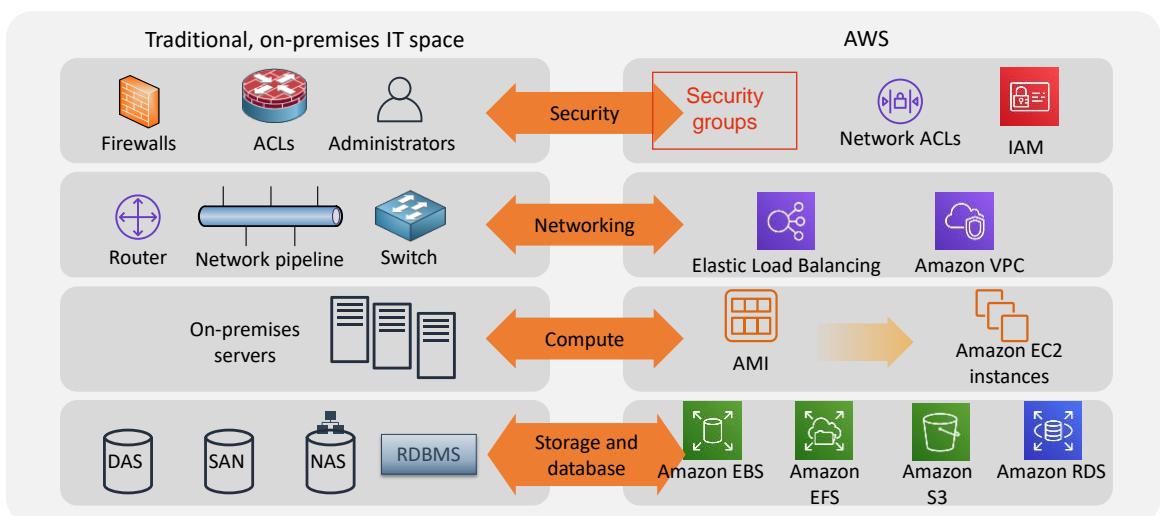
# Cloud computing deployment models



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

43

## Similarities between AWS and traditional IT



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

44

## Section 1 key takeaways



45



- Cloud computing is the on-demand delivery of IT resources via the internet with pay-as-you-go pricing.
- Cloud computing enables you to think of (and use) your infrastructure as software.
- There are three cloud service models: IaaS, PaaS, and SaaS.
- There are three cloud deployment models: cloud, hybrid, and on-premises or private cloud.
- Almost anything you can implement with traditional IT can also be implemented as an AWS cloud computing service.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Module 1: Cloud Concepts Overview

## Section 2: Advantages of cloud computing

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Trade capital expense for variable expense



Data center investment  
based on forecast



Pay only for the amount  
you consume

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

47

## Massive economies of scale

Because of aggregate usage from all customers, AWS can achieve higher economies of scale and pass savings on to customers.



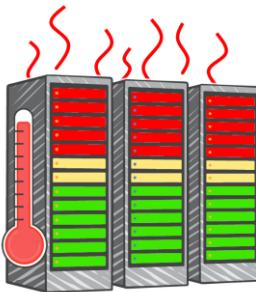
© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

48

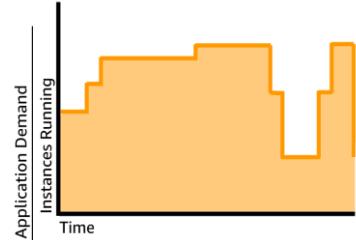
## Stop guessing capacity



Overestimated server capacity



Underestimated server capacity



Scaling on demand

## Increase speed and agility

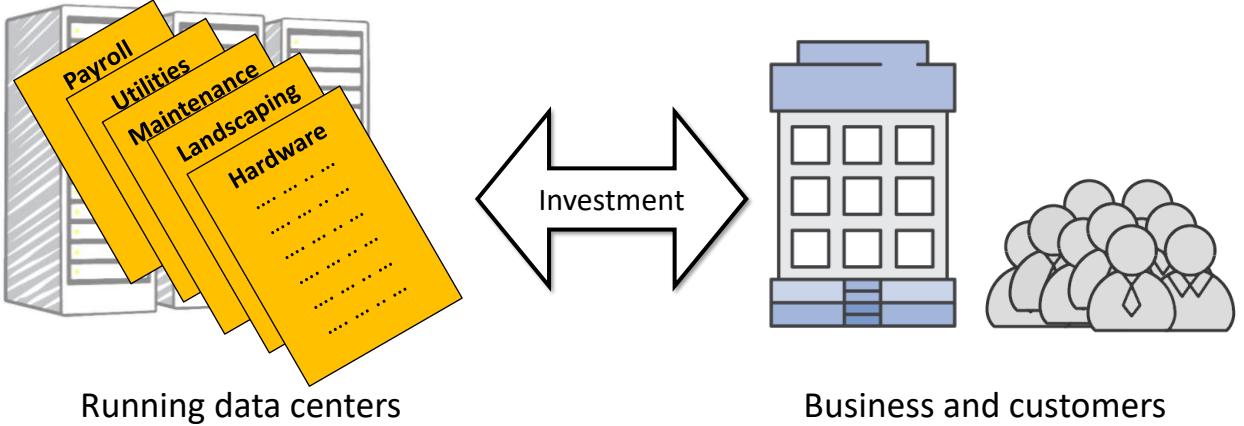


*Weeks* between wanting resources and having resources



*Minutes* between wanting resources and having resources

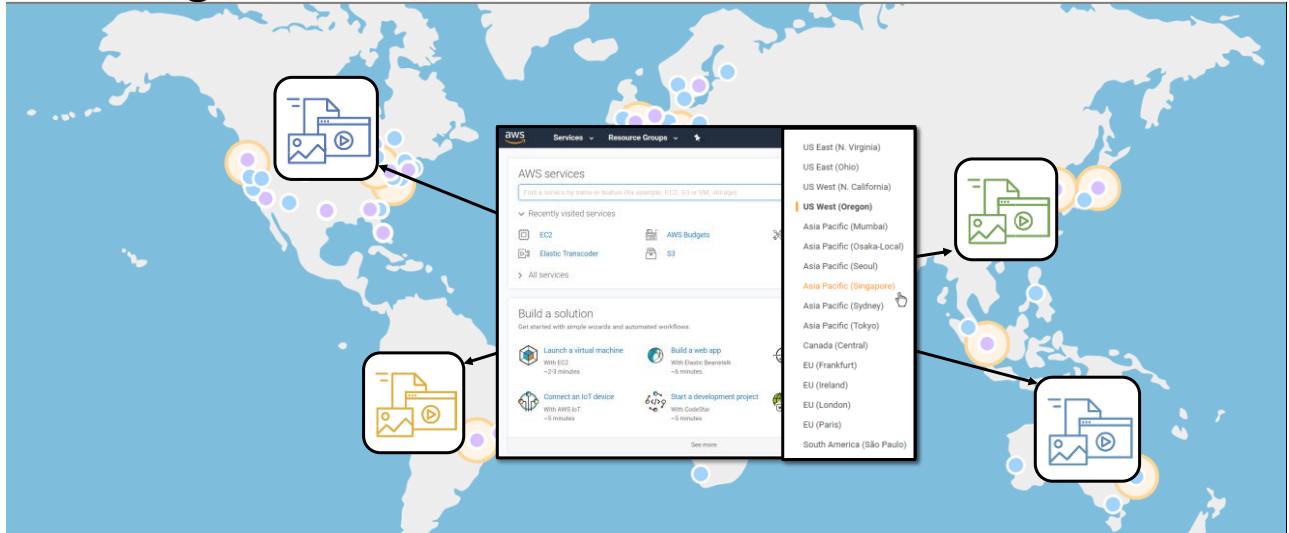
# Stop spending money on running and maintaining data centers



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

51

## Go global in minutes



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

52



## Section 2 key takeaways



53

- Trade capital expense for variable expense
- Benefit from massive economies of scale
- Stop guessing capacity
- Increase speed and agility
- Stop spending money on running and maintaining data centers
- Go global in minutes

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Module 1: Cloud Concepts Overview

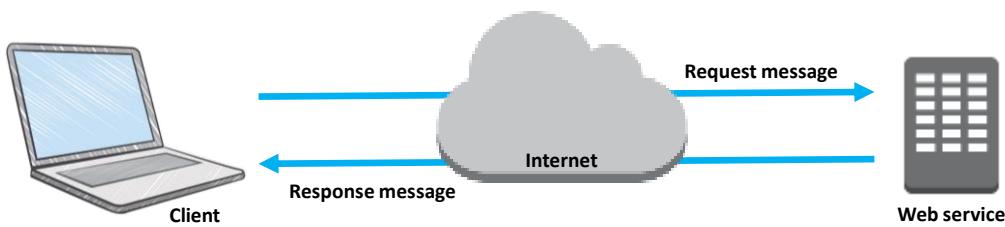
## Section 3: Introduction to Amazon Web Services (AWS)



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

# What are web services?

A **web service** is any piece of software that makes itself available over the internet and uses a **standardized format**—such as Extensible Markup Language (XML) or JavaScript Object Notation (JSON)—for the request and the response of an **application programming interface (API) interaction**.



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

55

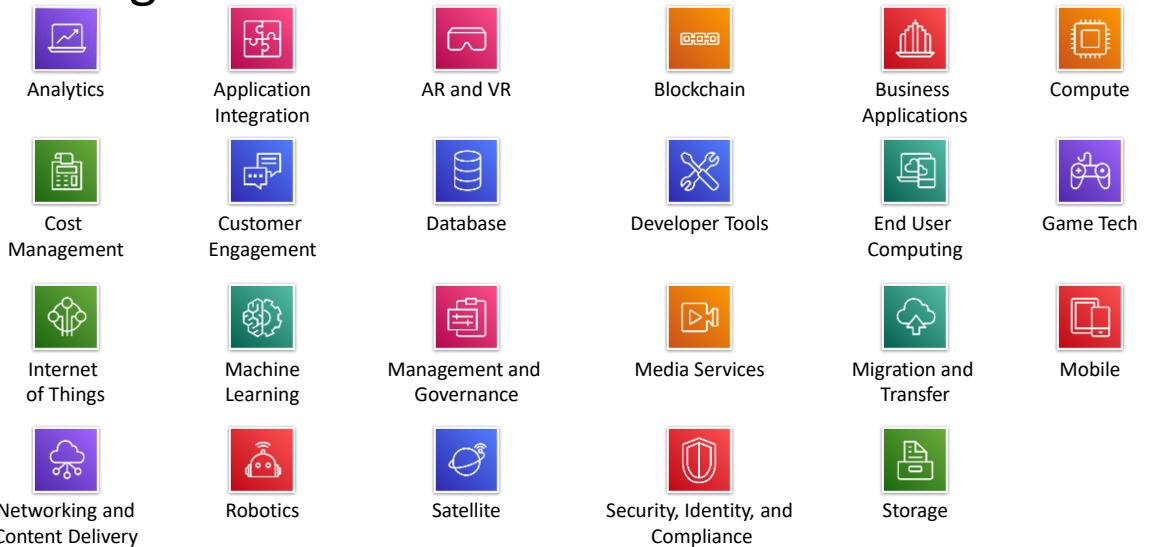
# What is AWS?

- AWS is a **secure cloud platform** that offers a **broad set of global cloud-based products**.
- AWS provides you with **on-demand access** to compute, storage, network, database, and other IT resources and management tools.
- AWS offers **flexibility**.
- You **pay only for the individual services you need**, for as long as you **use them**.
- AWS services **work together** like building blocks.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

56

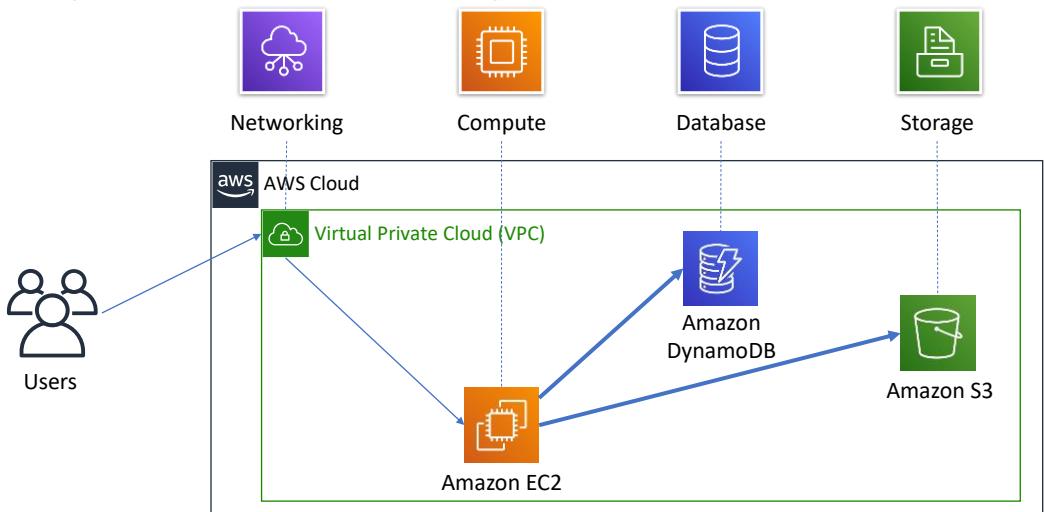
# Categories of AWS services



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

57

# Simple solution example

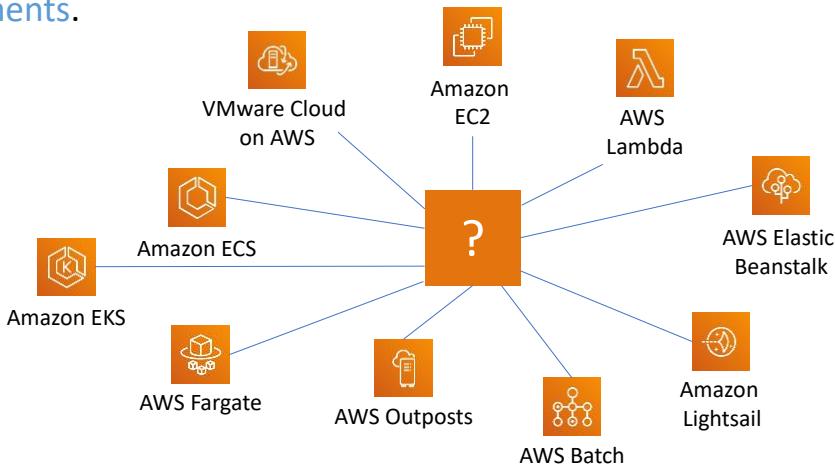


© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

58

# Choosing a service

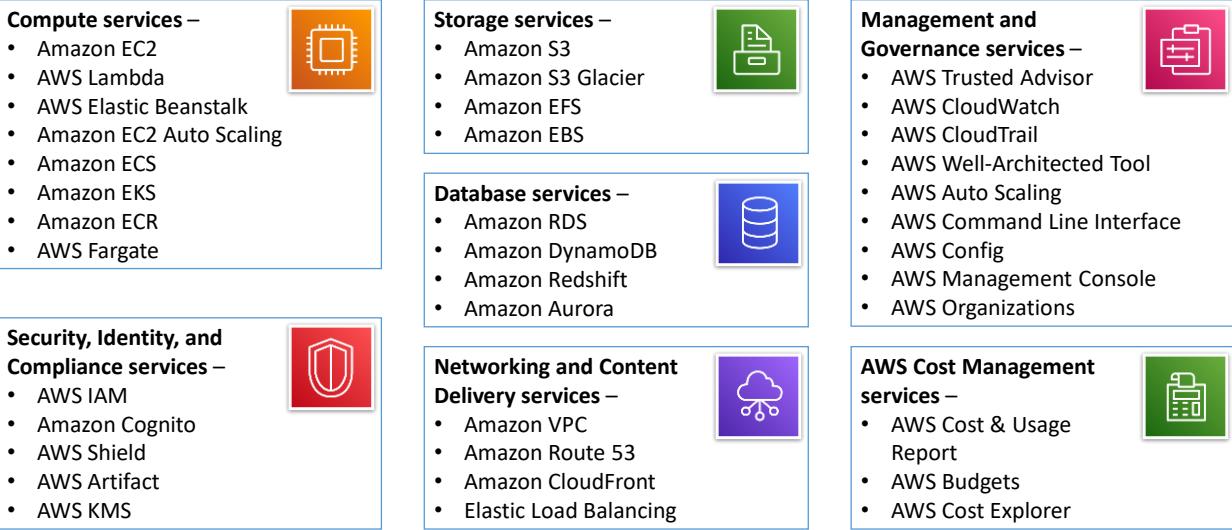
The service you select depends on your business goals and technology requirements.



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

59

# Services covered in this course



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

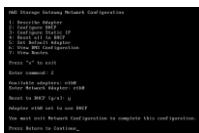
60

# Three ways to interact with AWS



## AWS Management Console

Easy-to-use graphical interface



## Command Line Interface (AWS CLI)

Access to services by discrete commands or scripts



## Software Development Kits (SDKs)

Access services directly from your code (such as Java, Python, and others)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

61



## Section 3 key takeaways



- AWS is a secure cloud platform that offers a broad set of global cloud-based products called services that are designed to work together.
- There are many categories of AWS services, and each category has many services to choose from.
- Choose a service based on your business goals and technology requirements.
- There are three ways to interact with AWS services.

## Module 1: Cloud Concepts Overview

# Section 4: Moving to the AWS Cloud – The AWS Cloud Adoption Framework (AWS CAF)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## AWS Cloud Adoption Framework (AWS CAF)



 BUSINESS	 PLATFORM
 PEOPLE	 SECURITY
 GOVERNANCE	 OPERATIONS

AWS CAF perspectives

- AWS CAF provides guidance and best practices to help organizations build a comprehensive approach to cloud computing across the organization and throughout the IT lifecycle to accelerate successful cloud adoption.

- AWS CAF is organized into six perspectives.
- Perspectives consist of sets of capabilities.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

# Six core perspectives

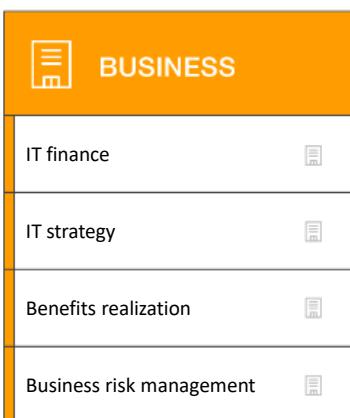


Focus on **business**  
capabilities



Focus on **technical**  
capabilities

## Business perspective



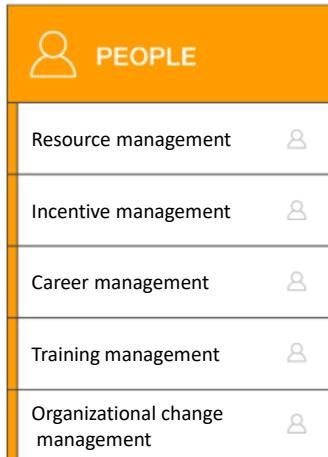
**Business perspective capabilities**

We must ensure that **IT is aligned with business needs**, and that IT investments can be traced to demonstrable business results.



Business managers, finance  
managers, budget owners,  
and strategy stakeholders

# People perspective



People perspective capabilities

We must prioritize **training, staffing, and organizational changes** to build an agile organization.



Human resources, staffing, and people managers

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

67

# Governance perspective



Governance perspective capabilities

We must ensure that **skills and processes align IT strategy and goals with business strategy and goals** so the organization can maximize the business value of its IT investment and minimize business risks.

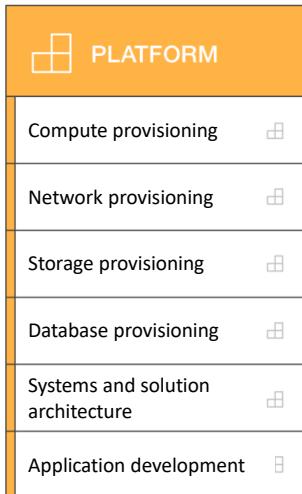


CIO, program managers, enterprise architects, business analysts, and portfolio managers

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

68

# Platform perspective



We must understand and communicate the nature of IT systems and their relationships. We must be able to describe the architecture of the target state environment in detail.



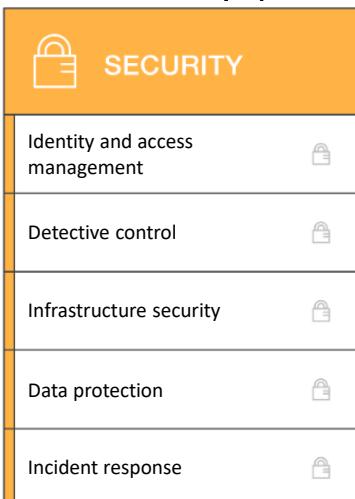
CTO, IT managers, and solutions architects

## Platform perspective capabilities

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

69

# Security perspective



We must ensure that the organization meets its security objectives.



CISO, IT security managers, and IT security analysts

## Security perspective capabilities

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

70

# Operations perspective

OPERATIONS	
Service monitoring	⚙️
Application performance monitoring	⚙️
Resource inventory management	⚙️
Release management/ change management	⚙️
Reporting and analytics	⚙️
Business continuity/ Disaster recovery	⚙️
IT service catalog	⚙️

Operations perspective capabilities

We align with and support the operations of the business, and **define how day-to-day, quarter-to-quarter, and year-to-year business will be conducted.**



IT operations managers and  
IT support managers

71



## Section 4 key takeaways



72

- Cloud adoption is not instantaneous for most organizations and requires a thoughtful, deliberate strategy and alignment across the whole organization.
- The AWS CAF was created to help organizations develop efficient and effective plans for their cloud adoption journey.
- The AWS CAF organizes guidance into six areas of focus, called perspectives.
- Perspectives consist of sets of business or technology capabilities that are the responsibility of key stakeholders.

## Module 1: Cloud Concepts Overview

### Module wrap-up

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Module summary

In summary, in this module you learned how to:

- Define different types of cloud computing models
- Describe six advantages of cloud computing
- Recognize the main AWS service categories and core services
- Review the AWS Cloud Adoption Framework

## Complete the knowledge check



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

75

## Sample exam question

Why is AWS more economical than traditional data centers for applications with varying compute workloads?

- A. Amazon Elastic Compute Cloud (Amazon EC2) costs are billed on a monthly basis.
- B. Customers retain full administrative access to their Amazon EC2 instances.
- C. Amazon EC2 instances can be launched on-demand when needed.
- D. Customers can permanently run enough instances to handle peak workloads.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

76

# Additional resources

- [What is AWS?](#) YouTube video
- [Cloud computing with AWS](#) website
- [Overview of Amazon Web Services](#) whitepaper
- [An Overview of the AWS Cloud Adoption Framework](#) whitepaper
- [6 Strategies for Migrating Applications to the Cloud](#) AWS Cloud Enterprise Strategy blog post

Thank You

AWS Academy Cloud Foundations

## Module 2: Cloud Economics and Billing

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Module overview



### Topics

- Fundamentals of pricing
- Total Cost of Ownership
- AWS Organizations
- AWS Billing and Cost Management
- Technical Support

### Activities

- AWS Pricing Calculator
- Support plans scavenger hunt

### Demo

- Overview of the Billing Dashboard



### Knowledge check

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

80

# Module objectives

After completing this module, you should be able to:

- Explain the AWS pricing philosophy
- Recognize fundamental pricing characteristics
- Indicate the elements of total cost of ownership
- Discuss the results of the AWS Pricing Calculator
- Identify how to set up an organizational structure that simplifies billing and account visibility to review cost data.
- Identify the functionality in the AWS Billing Dashboard
- Describe how to use AWS Bills, AWS Cost Explorer, AWS Budgets, and AWS Cost and Usage Reports
- Identify the various AWS technical support plans and features

## Module 2: Cloud Economics and Billing

### Section 1: Fundamentals of pricing

# AWS pricing model

## Three fundamental drivers of cost with AWS

### Compute

- Charged per hour/second\*
- Varies by instance type

\*Linux only

### Storage

- Charged typically per GB

### Data transfer

- Outbound is aggregated and charged
- Inbound has no charge (with some exceptions)
- Charged typically per GB

## How do you pay for AWS?

### Pay for what you use



### Pay less when you reserve

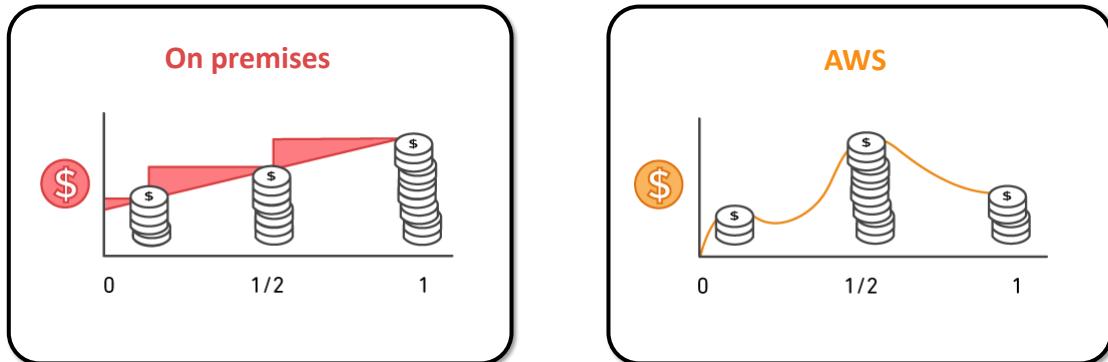


### Pay less when you use more and as AWS grows



## Pay for what you use

Pay only for the services that you consume, with no large upfront expenses.



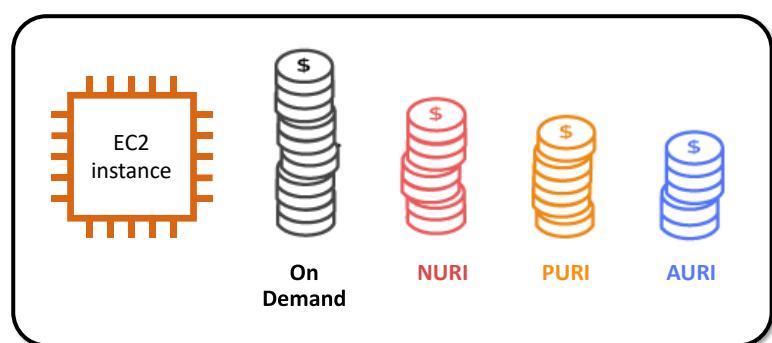
© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

85

## Pay less when you reserve

Invest in Reserved Instances (RIs):

- Save up to 75 percent
- Options:
  - All Upfront Reserved Instance (**AURI**) → largest discount
  - Partial Upfront Reserved Instance (**PURI**) → lower discounts
  - No Upfront Payments Reserved Instance (**NURI**) → smaller discount



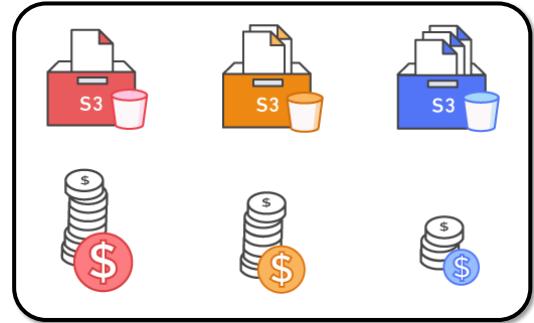
© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

86

## Pay less by using more

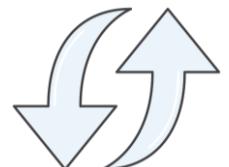
Realize volume-based discounts:

- **Savings** as usage increases.
- **Tiered pricing** for services like Amazon Simple Storage Service (Amazon S3), Amazon Elastic Block Store (Amazon EBS), or Amazon Elastic File System (Amazon EFS) → the more you use, the less you pay per GB.
- Multiple storage services deliver **lower** storage costs based on needs.



## Pay even less as AWS grows

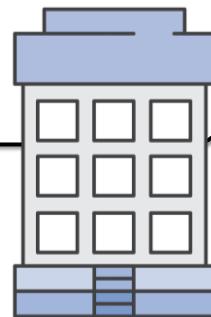
As AWS grows:



- AWS focuses on lowering cost of doing business.
- This practice results in AWS passing savings from economies of scale to you.
- Since 2006, AWS has **lowered pricing 75 times** (as of September 2019).
- Future higher-performing resources replace current resources for no extra charge.

## Custom pricing

- Meet varying needs through custom pricing.
- Available for high-volume projects with unique requirements.

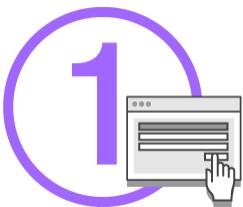


© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

89

## AWS Free Tier

Enables you to gain free hands-on experience with the AWS platform, products, and services. Free for 1 year for new customers.



**Sign up for an AWS account**



**Learn with 10-minute tutorials**



**Start building with AWS**

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

90

# Services with no charge



**\*\*Note:** There might be charges associated with other AWS services that are used with these services.

91

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Key takeaways



- There is no charge for:
  - Inbound data transfer.
  - Data transfer between services within the same AWS Region.
- Pay for what you use.
- Start and stop anytime.
- No long-term contracts are required.
- Some services are free, but the other AWS services that they provision might not be free.

92

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

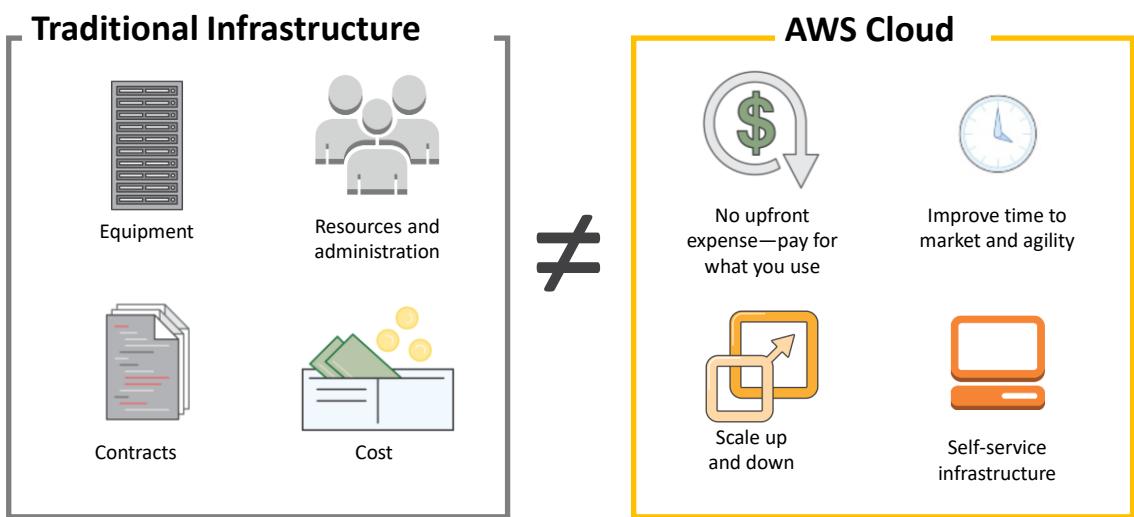
## Module 2: Cloud Economics and Billing

### Section 2: Total Cost of Ownership

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## On-premises versus cloud



# What is Total Cost of Ownership (TCO)?

**Total Cost of Ownership (TCO)** is the financial estimate to help identify direct and indirect costs of a system.

## Why use TCO?

- To compare the costs of running an **entire infrastructure environment or specific workload** on-premises versus on AWS
- To budget and **build the business case** for moving to the cloud



## TCO considerations

1	Server Costs	Hardware: Server, rack chassis power distribution units (PDUs), top-of-rack (TOR) switches (and maintenance)	Software: Operating system (OS), virtualization licenses (and maintenance)	Facilities cost
2	Storage Costs	Hardware: Storage disks, storage area network (SAN) or Fibre Channel (FC) switches	Storage administration costs	Facilities cost
3	Network Costs	Network hardware: Local area network (LAN) switches, load balancer bandwidth costs	Network administration costs	Facilities cost
4	IT Labor Costs		Server administration costs	

# On-premises versus all-in-cloud



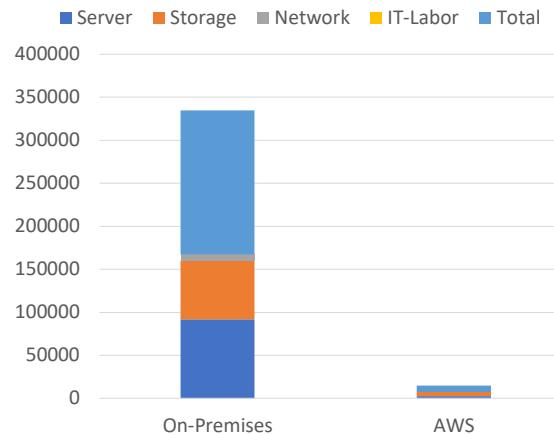
You could save up to **96 percent** a year by moving your infrastructure to AWS.

Your 3-year total savings would be **\$159,913**.

3-Year Total Cost of Ownership		
	On-Premises	AWS
Server	\$91,922	\$2,547
Storage	\$67,840	\$4,963
Network	\$7,660	\$-----
IT – Labor	\$ ----- --	\$-----
Total	\$167,422	\$7,509

AWS cost includes business-level support and  
a 3-year PURI EC2 instance

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



97

## AWS Pricing Calculator

Use the [AWS Pricing Calculator](#) to:

- Estimate monthly costs
- Identify opportunities to reduce monthly costs
- Model your solutions before building them
- Explore price points and calculations behind your estimate
- Find the available instance types and contract terms that meet your needs
- Name your estimate and create and name **groups** of services

Access the [AWS Pricing Calculator](#)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

98

# Reading an estimate

Your estimate is broken into: first 12 months total, total upfront, and total monthly.

The screenshot shows the AWS Pricing Calculator interface. At the top, there are buttons for 'Add service', 'Add support', 'Add group', 'Clear estimate', 'Action ▾', and 'Save and share'. Below this, the estimate summary is displayed:

First 12 months total	Total upfront	Total monthly
886.92 USD	0.00 USD	73.51 USD

Below the summary, the 'Services (2)' section is shown:

- Amazon Simple Storage Service (S3)**  
Region: US East (Ohio)  
S3 Standard storage (100 GB per month)  
Monthly: 2.37 USD
- Amazon EC2**  
Region: US East (Ohio)  
Quick estimate  
Operating system (Linux), Quantity (1), Pricing strategy (EC2 Instance Savings Plans 1 Year No Upfront), Storage for each EC2 instance (General Purpose SSD (gp2)), Storage amount (100 GB), Instance type (t4g.xlarge)  
Monthly: 71.54 USD

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

99

## Activity: AWS Pricing Calculator activity

- Break up into groups of four or five and use the [AWS Pricing Calculator](#) and specifications provided to develop a cost estimate.
- Be prepared to report your findings back to the class.

The screenshot shows the AWS Pricing Calculator website. On the left, a box titled 'Create an estimate' contains the text: 'Start your estimate with no commitment, and explore AWS services and pricing for your architecture needs.' with a 'Create estimate' button. An arrow points from this box to the 'Select service' step on the right.

The 'Select service' step shows the following interface:

- Step 1: Select service**
- AWS services (63)** (with a search bar and 'Configure' button)
- Amazon API Gateway**: A fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the front door for applications to access data, business logic, or functionality from your backend services.
- Amazon Aurora PostgreSQL-Compatible DB**: Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud, that combines the performance and
- Amazon Athena**: Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3, so there is no infrastructure to manage.
- Amazon Carrier IP**: A Carrier IP address is used to interface with external networks.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

100

# Additional benefit considerations



## Hard benefits

- Reduced spending on compute, storage, networking, security
- Reductions in hardware and software purchases (capex)
- Reductions in operational costs, backup, and disaster recovery
- Reduction in operations personnel



## Soft Benefits

- Reuse of service and applications that enable you to define (and redefine solutions) by using the same cloud service
- Increased developer productivity
- Improved customer satisfaction
- Agile business processes that can quickly respond to new and emerging opportunities
- Increase in global reach

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

101

# Case study: Total Cost Of Ownership



## Background:

- Growing global company with over 200 locations
- 500 million customers, \$3 billion annual revenue

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

102

# Case study: Total Cost of Ownership


**Background:**

- Growing global company with over 200 locations
- 500 million customers, \$3 billion annual revenue

**Challenge:**

- Meet demand to rapidly deploy new solutions
- Constantly upgrade aging equipment

# Case study: Total Cost of Ownership


**Background:**

- Growing global company with over 200 locations
- 500 million customers, \$3 billion annual revenue

**Challenge:**

- Meet demand to rapidly deploy new solutions
- Constantly upgrade aging equipment

**Criteria:**

- Broad solution to handle all workloads
- Ability to modify processes to improve efficiency and lower costs
- Eliminate busy work (such as patching software)
- Achieve a positive return on investment (ROI)

# Case study: Total Cost of Ownership



- Background:**
- Is a growing global company with over 200 locations
  - Have 500 million customers, \$3 billion (USD) annual revenue
- Challenge:**
- Meet demand to rapidly deploy new solutions
  - Constantly upgrade aging equipment
- Criteria:**
- Have a broad solution to handle all workloads
  - Be able to modify processes to improve efficiency and lower costs
  - Eliminate busy work (such as patching software)
  - Achieve a positive return on investment (ROI)
- Solution:**
- Moved their on-premises data center to AWS
    - Eliminated 205 servers (90 percent)
    - Moved nearly all applications to AWS
  - Used 3-year Amazon EC2 Reserved Instances

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

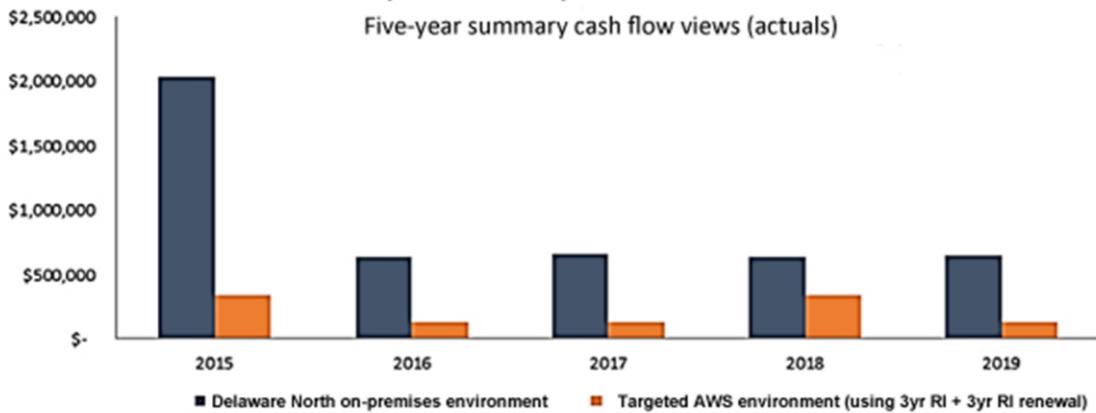
105

# Case study: Total Cost of Ownership



**Cost comparison: On-premises data center vs. AWS**

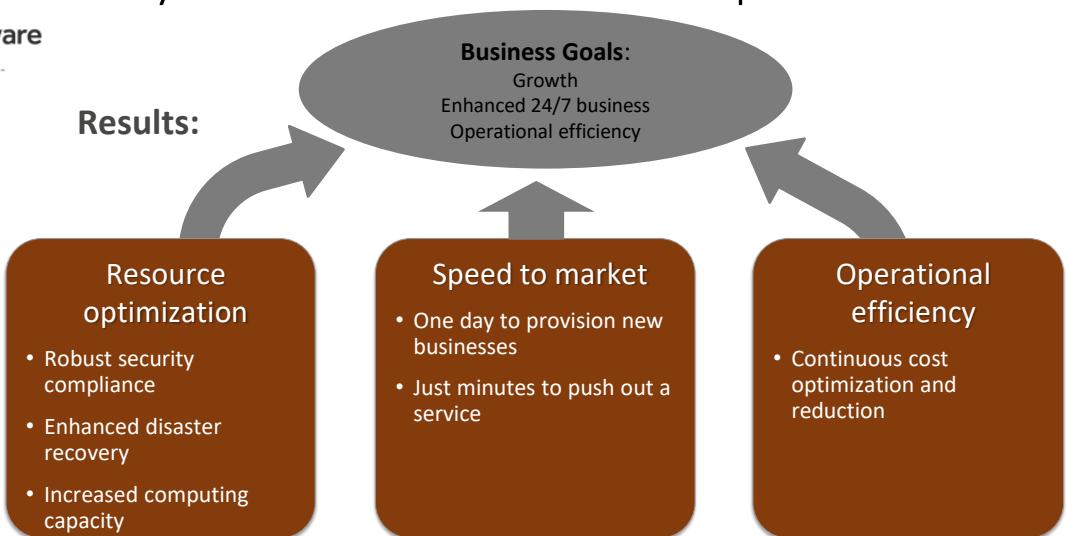
Five-year summary cash flow views (actuals)



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

106

# Case study: Total Cost of Ownership



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

107

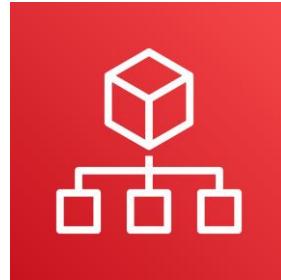
Module 2: Cloud Economics and Billing

## Section 3: AWS Organizations

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



# Introduction to AWS Organizations

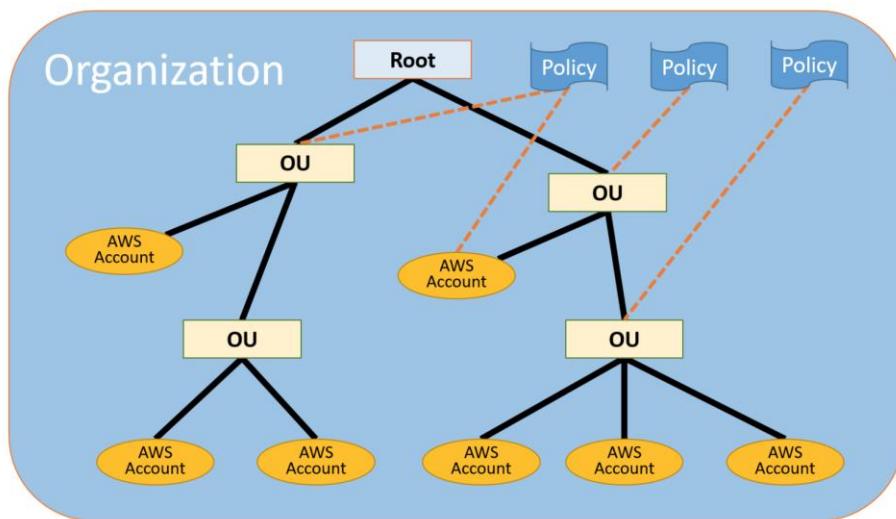


AWS Organizations

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

109

## AWS Organizations terminology

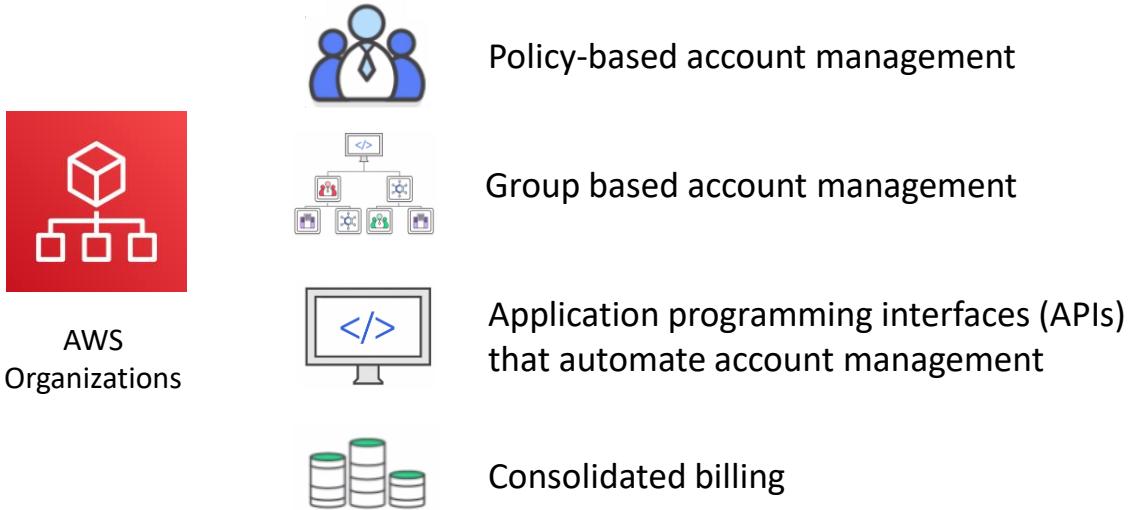


© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

\*Organizational Units (OUs)

110

# Key features and benefits



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

111

## Security with AWS Organizations

Control access with AWS Identity and Access Management (IAM).



IAM policies enable you to allow or deny access to AWS services for users, groups, and roles.

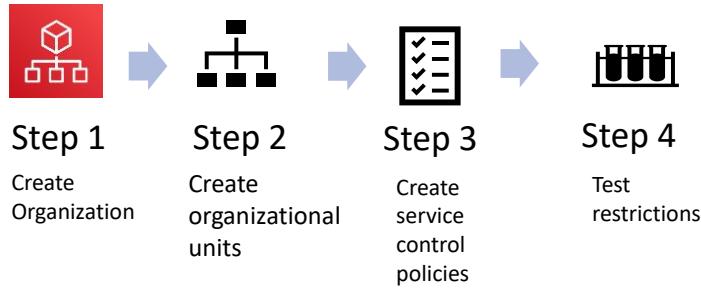


Service control policies (SCPs) enable you to allow or deny access to AWS services for individuals or group accounts in an organizational unit (OU).

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

112

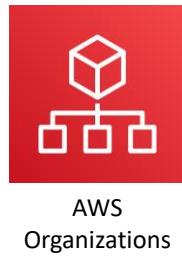
# Organizations setup



## Limits of AWS Organizations

Limits		
Limits on Names	Names must be composed of Unicode characters. Names must not exceed 250 characters in length.	
Maximum and Minimum Values	Number of AWS accounts	Varies. Note: An invitation sent to an account counts against this limit.
	Number of roots	1
	Number of OUs	1,000
	Number of policies	1,000
	Maximum size of a service control policy document	5,120 bytes
	Maximum nesting of OUs in a root	5 levels of OUs under a root
	Invitations sent per day	20
	Number of member accounts you can create concurrently	Only five can be in progress at one time
	Number of entities to which you can attach a policy	Unlimited

# Accessing AWS Organizations



AWS Management Console



AWS Command Line Interface (AWS CLI) tools



Software development kits (SDKs)



HTTPS Query application programming interfaces (API)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

115

Module 2: Cloud Economics and Billing

## Section 4: AWS Billing and Cost Management

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

**aws** academy

# Introducing AWS Billing and Cost Management



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

117

## AWS Billing Dashboard

### Billing & Cost Management Dashboard

#### Spend Summary

Welcome to the AWS Account Billing console. Your last month, month-to-date, and month-end forecasted costs appear below.

*Current month-to-date balance for October 2017*

**\$7,453.41**



#### Cost Explorer

#### Monthly-to-Date Spend by Service

The chart below shows the proportion of costs spent for each service you use.



EC2	\$3,700.71
RDS	\$1,876.36
ElastiCache	\$938.18
DynamoDB	\$625.44
Other Services	\$312.57
Tax	\$0.16

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

118

# Tools



AWS Budgets



AWS Cost and Usage Report



AWS Cost Explorer

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

119

## Monthly bills

[BILLS](#) | [COST EXPLORER](#) | [BUDGETS](#) | [REPORTS](#)

Total	\$7,453.41 USD
<b>AWS Marketplace Charges</b>	<b>\$15.00</b>
▼ Usage Charges and Recurring Fees	\$15.00
Invoice 32342548 – AWS Service Charges: Usage charge for this statement period	2017-10-10
	\$15.00
<b>AWS Service Charges</b>	<b>\$7,438.41</b>
▼ Usage Charges and Recurring Fees	\$7,414.41
Invoice 32342513 – AWS Service Charges: Usage charge for this statement period	2017-10-10
	\$7,414.41
▼ Usage Charges and Recurring Fees	\$24.00
Invoice 32342507 – AWS Service Charges: Subscription charge	2017-10-10
	\$24.00

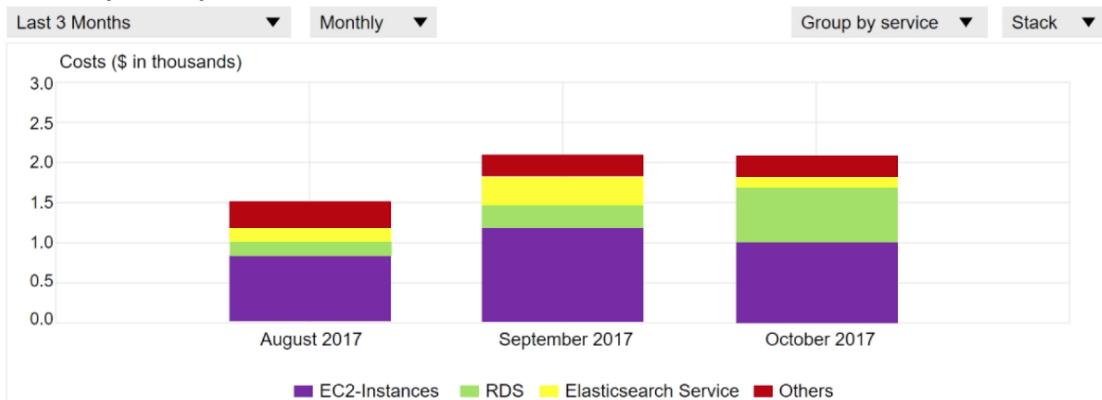
© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

120

# Cost Explorer

BILLS | COST EXPLORER | BUDGETS | REPORTS

## Monthly costs by service



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

121

# Forecast and track costs

BILLS | COST EXPLORER | BUDGETS | REPORTS

Create budget		Copy	Edit	Delete	<a href="#">Download CSV</a>		<a href="#">...</a>
<input type="button" value="Filter by budget name"/>							
	Budget name	Current	Forecasted	Budgeted	Current vs. budgeted	Forecasted vs. budgeted	
<input type="checkbox"/>	▶ Total Monthly Cost	\$760.27	\$787.44	\$1,000.00			
<input type="checkbox"/>	▼ S3 Usage Bucket	2978.00 Req	3650.16 Req	3000.00 Req			

**Budget details**

**Start date** 10/01/17  
**End date** -  
**Budget Period** Monthly

**Variance analysis**

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

122

# Cost and usage reporting

BILLS | COST EXPLORER | BUDGETS | REPORTS

Product Code	Usage Type	Operation	Availability Zone	Usage Amount	Currency Code	Line Item Description
Amazon S3	Requests – Tier 1	ListAllMyBuckets		2	USD	\$0.00 per request – PUT, COPY, POST, LIST under the global free tier
Amazon EC2	USW2-Boxusage:t2.micro	Runinstances:0002	us-west-2a	1	USD	\$0.00 per Windows t2.micro instance-hour under monthly free tier
Amazon S3	Requests – Tier 1	ListAllMyBuckets		2	USD	\$0.00 per request – PUT, COPY, POST, LIST under the global free tier
Amazon EC2	USW2-Boxusage:t2.micro	Runinstances:0002	us-west-2a	1	USD	\$0.00 per Windows t2.micro instance-hour under monthly free tier
Amazon S3	Requests – Tier 1	ListAllMyBuckets		2	USD	\$0.00 per request – PUT, COPY, POST, LIST under the global free tier
Amazon S3	Requests – Tier 1	ListAllMyBuckets		2	USD	\$0.00 per request – PUT, COPY, POST, LIST under the global free tier

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

123

Recorded demo:  
Amazon Billing  
dashboard

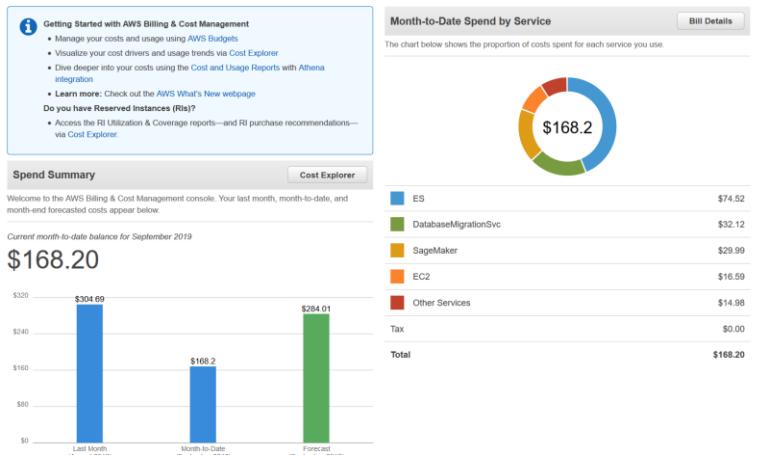
124



Amazon Billing  
dashboard demo

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

# Billing dashboard demonstration



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

125

## Module 2: Cloud Economics and Billing

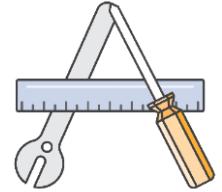
### Section 5: Technical support

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



# AWS support

- Provide unique combination of tools and expertise:
  - AWS Support
  - AWS Support Plans
- Support is provided for:
  - Experimenting with AWS
  - Production use of AWS
  - Business-critical use of AWS



## AWS support



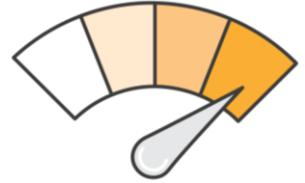
- Proactive guidance :
  - Technical Account Manager (TAM)
- Best practices :
  - AWS Trusted Advisor
- Account assistance :
  - AWS Support Concierge



# Support plans

AWS Support offers four support plans:

- **Basic Support** – Resource Center access, Service Health Dashboard, product FAQs, discussion forums, and support for health checks
- **Developer Support**: Support for early development on AWS
- **Business Support**: Customers that run production workloads
- **Enterprise Support**: Customers that run business and mission-critical workloads



## Case severity and response times

	Critical	Urgent	High	Normal	Low
Basic			No Case Support		
Developer Plan (Business hours)				12 hours or less	24 hours or less
Business Plan (24/7)		1 hour or less	4 hours or less	12 hours or less	24 hours or less
Enterprise Plan (24/7)	15 minutes or less	1 hour or less	4 hours or less	12 hours or less	24 hours or less

## Activity: Support plan scavenger hunt

- Break up into groups of four or five and develop a recommendation for the best support plan for one of the business cases that are provided.
- Be prepared to report your findings back to the class.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

131

Module 2: Cloud Economics and Billing

## Module wrap-up

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



# Module summary

- Explored the fundamental of AWS pricing
- Reviewed TCO concepts
- Reviewed an AWS Pricing Calculator estimate
- Reviewed the Billing dashboard
- Reviewed Technical Support options and costs

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

133

## Complete the knowledge check



```
<header>
  <div id="content">
    <div id="topnav">
      <nav>
        <ul>
          <li class="active"><a href="#">Home</a></li>
          <li><a href="#">Our Service</a></li>
          <li><a href="#">Our Product</a></li>
          <li><a href="#">Portfolio</a></li>
          <li><a href="#">Products</a></li>
          <li><a href="#">Portfolio</a></li>
          <li><a href="#">Test</a></li>
          <li><a href="#">Contact</a></li>
        </ul>
      </nav>
    </div>
  </div>
</header>
<div class="logo">
  

```

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

134

## Sample exam question

Which AWS service provides infrastructure security optimization recommendations?

- A. AWS Price List Application Programming Interface (API)
- B. Reserved Instances
- C. AWS Trusted Advisor
- D. Amazon Elastic Compute Cloud (Amazon EC2) Spot Fleet

## Additional resources

- AWS Economics Center: <http://aws.amazon.com/economics/>
- AWS Pricing Calculator: <https://calculator.aws/#/>
- Case studies and research: <http://aws.amazon.com/economics/>
- Additional pricing exercises: <https://dx1572sre29wk.cloudfront.net/cost/>

# Thank you

© 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. Corrections or feedback on the course, please email us at: [aws-course-feedback@amazon.com](mailto:aws-course-feedback@amazon.com). For all other questions, contact us at: <https://aws.amazon.com/contact-us/aws-training/>. All trademarks are the property of their owners.



AWS Academy Cloud Foundations

## Module 3: AWS Global Infrastructure Overview



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

# Module overview



## Topics

- AWS Global Infrastructure
- AWS service and service category overview

## Demo

- AWS Global Infrastructure

## Activities

- AWS Management Console clickthrough



## Knowledge check

# Module objectives

After completing this module, you should be able to:

- Identify the difference between AWS Regions, Availability Zones, and edge locations
- Identify AWS service and service categories

## Module 3: AWS Global Infrastructure Overview

# Section 1: AWS Global Infrastructure

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



# AWS Global Infrastructure

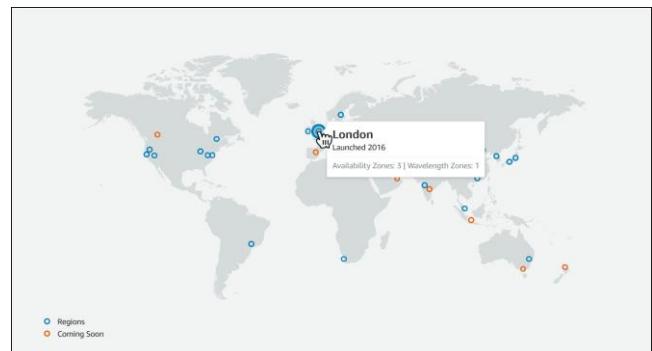
- The [AWS Global Infrastructure](#) is designed and built to deliver a **flexible, reliable, scalable**, and **secure** cloud computing environment with high-quality **global network performance**.
- AWS continually updates its global infrastructure footprint. Visit one of the following web pages for current infrastructure information:

- [\*\*AWS Global Infrastructure Map\*\*](#)

Choose a circle on the map to view summary information about the Region represented by the circle.

- [\*\*Regions and Availability Zones\*\*](#)

Choose a tab to view a map of the selected geography and a list of Regions, Edge locations, Local zones, and Regional Caches.



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

142



## Educator-Led Demo: AWS Global Infrastructure Details

143

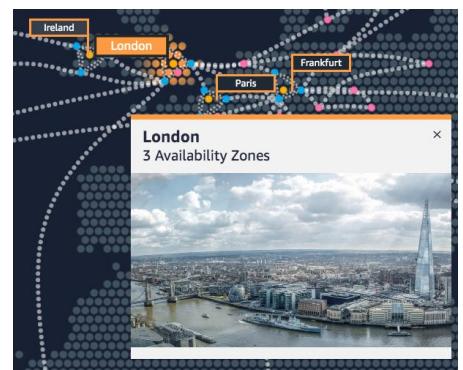


© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## AWS Regions



- An **AWS Region** is a geographical area.
  - **Data replication** across Regions is controlled by you.
  - **Communication** between Regions uses AWS backbone network infrastructure.
- Each Region provides full redundancy and connectivity to the network.
- A Region typically consists of two or more **Availability Zones**.



Example: London Region

# Selecting a Region

Determine the right Region for your services, applications, and data based on these factors



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

145

# Availability Zones

- Each **Region** has multiple Availability Zones.
- Each **Availability Zone** is a fully isolated partition of the AWS infrastructure.
  - Availability Zones consist of discrete **data centers**
  - They are designed for fault isolation
  - They are interconnected with other Availability Zones by using high-speed private networking
  - You choose your Availability Zones.
  - **AWS recommends replicating data and resources across Availability Zones** for resiliency.



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

146

# AWS data centers

- AWS data centers are **designed for security**.
- Data centers are where the data resides and data processing occurs.
- Each data center has redundant power, networking, and connectivity, and is housed in a separate facility.
- A data center typically has 50,000 to 80,000 physical servers.



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

147

## Points of Presence



- AWS provides a global network of **Points of Presence** locations
- Consists of **edge locations** and a much smaller number of **Regional edge caches**
- Used with Amazon CloudFront
  - A global Content Delivery Network (CDN), that delivers content to end users with **reduced latency**
- Regional edge caches used for content with infrequent access.

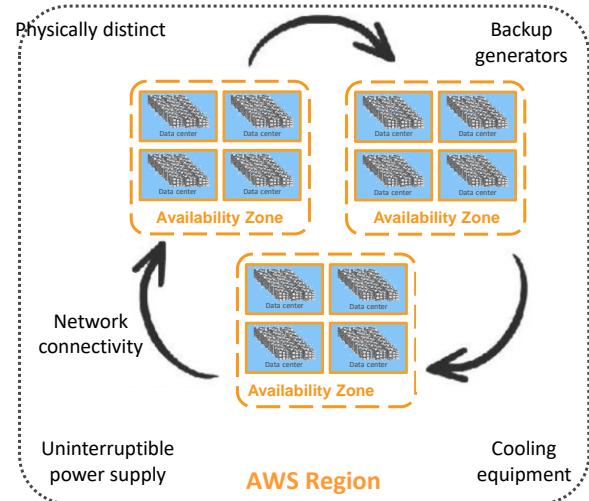


© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

148

# AWS infrastructure features

- Elasticity and scalability
  - Elastic infrastructure; dynamic adaption of capacity
  - Scalable infrastructure; adapts to accommodate growth
- Fault-tolerance
  - Continues operating properly in the presence of a failure
  - Built-in redundancy of components
- High availability
  - High level of operational performance
  - Minimized downtime
  - No human intervention



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

149

## Key takeaways



150



- The **AWS Global Infrastructure** consists of **Regions** and **Availability Zones**.
- Your choice of a **Region** is typically based on **compliance requirements** or to **reduce latency**.
- Each **Availability Zone** is physically separate from other Availability Zones and has redundant power, networking, and connectivity.
- **Edge locations**, and **Regional edge caches** improve performance by **caching** content closer to users.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

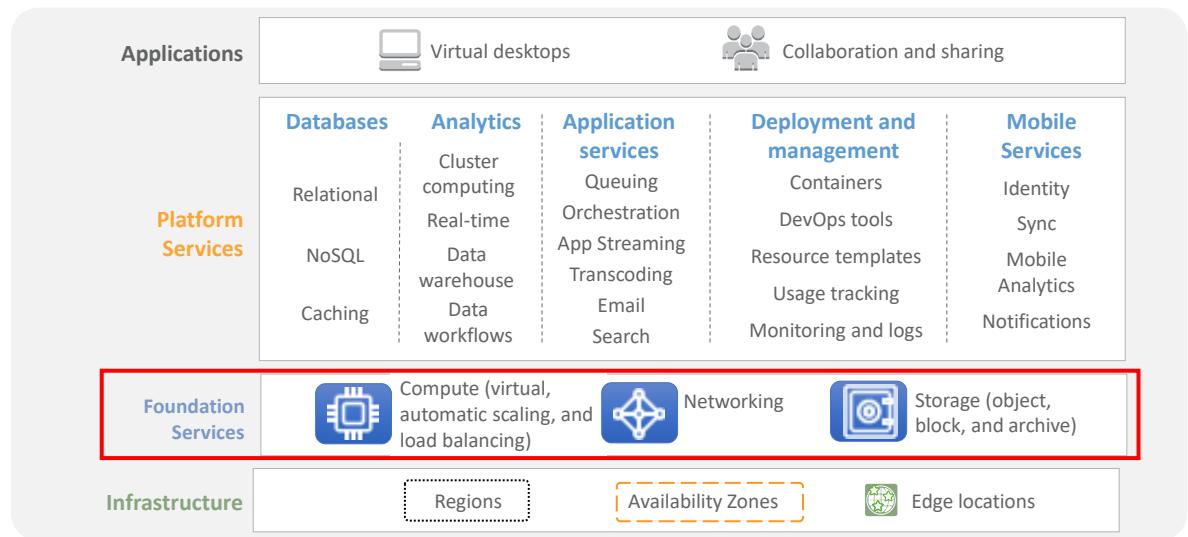
## Module 3: AWS Global Infrastructure Overview

### Section 2: AWS services and service category overview

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



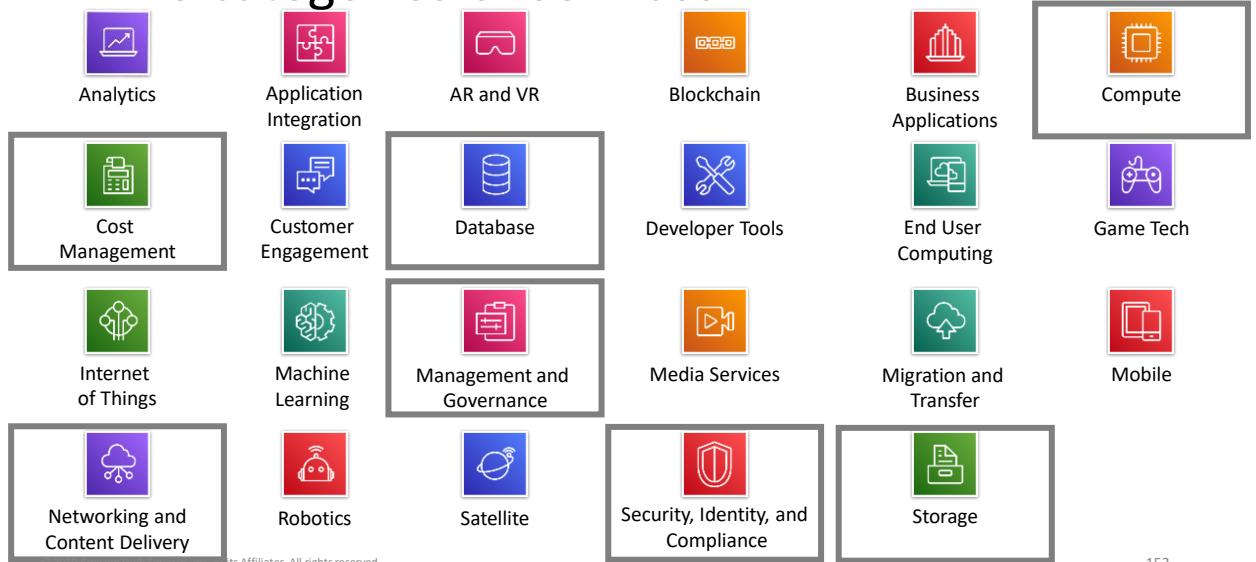
## AWS foundational services



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

152

# AWS categories of services



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

153

## Storage service category



Photo from <https://www.pexels.com/photo/black-and-grey-device-159282/>



**AWS storage** services



Amazon Simple Storage  
Service (Amazon S3)



Amazon Elastic  
Block Store (Amazon EBS)



Amazon Elastic  
File System  
(Amazon EFS)



Amazon Simple Storage  
Service  
Glacier

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

154

# Compute service category



Photo from <https://www.pexels.com/photo/technology-computer-lines-board-50711/>



**AWS Compute** services



Amazon EC2



Amazon EC2  
Auto Scaling



Amazon Elastic  
Container Service  
(Amazon ECS)



Amazon EC2  
Container Registry



AWS Elastic  
Beanstalk



AWS Lambda



Amazon Elastic  
Kubernetes Service  
(Amazon EKS)



AWS Fargate

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

155

# Database service category



Photo from <https://aws.amazon.com/compliance/data-center/data-centers/>



**AWS Database** services



Amazon Relational  
Database Service



Amazon Aurora



Amazon Redshift



Amazon  
DynamoDB

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

156

# Networking and content delivery service category



Photo by Umberto on Unsplash

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## AWS networking and content delivery services



Amazon VPC



Elastic Load Balancing



Amazon CloudFront



AWS Transit Gateway



Amazon Route 53



AWS Direct Connect



AWS VPN

11

# Security, identity, and compliance service category



Photo by Paweł Czerwiński on Unsplash



## AWS security, identity, and compliance services



AWS Identity and Access Management (IAM)



AWS Organizations



Amazon Cognito



AWS Artifact



AWS Key Management Service



AWS Shield

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

158

## AWS cost management service category



Photo by Alexander Mills on Unsplash



**AWS cost management services**



AWS Cost and Usage Report



AWS Budgets



AWS Cost Explorer

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

159

## Management and governance service category



Photo by Marta Branco from Pexels



**AWS management and governance services**



AWS Management Console



AWS Config



Amazon CloudWatch



AWS Auto Scaling



AWS Command Line Interface



AWS Trusted Advisor



AWS Well-Architected Tool



AWS CloudTrail

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

160



## Activity: AWS Management Console clickthrough

161



Photo by Pixabay from Pexels.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Hands-on activity: AWS Management Console clickthrough

1. Launch the [Sandbox](#) hands-on environment and connect to the [AWS Management Console](#).
2. Explore the AWS Management Console.
  - A. Click the **Services** menu.
  - B. Notice how services are grouped into service categories. For example, the **EC2** service appears in the **Compute** service category.
    - Question #1:** Under which service category does the **IAM** service appear?
    - Question #2:** Under which service category does the **Amazon VPC** service appear?
  - C. Click the **Amazon VPC** service. Notice that the dropdown menu in the top-right corner displays an AWS Region (for example, it might display *N. Virginia*).
  - D. Click the Region menu and switch to a different Region. For example, choose **EU (London)**.
  - E. Click **Subnets** (on the left side of the screen). The Region has three subnets in it. Click the box next to one of the subnets. Notice that the bottom half of the screen now displays details about this subnet.
    - Question #3:** Does the subnet you selected exist at the level of the Region or at the level of the Availability Zone?
  - F. Click **Your VPCs**. An existing VPC is already selected.
    - Question #4:** Does the VPC exist at the level of the Region or the level of the Availability Zone?
    - Question #5:** Which services are global instead of Regional? Check Amazon EC2, IAM, Lambda, and Route 53.

# Activity answer key

- Question #1: Under which service category does the **IAM** service appear?
  - Answer: [Security, Identity, & Compliance](#).
- Question #2: Under which service category does the **Amazon VPC** service appear?
  - Answer: [Networking & Content Delivery](#)
- Question #3: Does the subnet that you selected exist at the level of the Region or the level of the Availability Zone?
  - Answer: Subnets exist at the [level of the Availability Zone](#).
- Question #4: Does the VPC exist at the level of the Region or the level of the Availability Zone?
  - Answer: VPCs exist at the [Region level](#).
- Question #5: Which of the following services are global instead of Regional? Check Amazon EC2, IAM, Lambda, and Route 53.
  - Answer: [IAM and Route 53 are global](#). Amazon EC2 and Lambda are Regional.

Module 3: AWS Global Infrastructure Overview

## Module wrap-up

# Module summary

In summary, in this module you learned how to:

- Identify the difference between AWS Regions, Availability Zones, and edge locations
- Identify AWS service and service categories

Complete the knowledge check



## Sample exam question

Which component of AWS global infrastructure does Amazon CloudFront use to ensure low-latency delivery?

- A. AWS Regions
- B. AWS edge locations
- C. AWS Availability Zones
- D. Amazon Virtual Private Cloud (Amazon VPC)

## Additional resources

- [AWS Global Infrastructure](#)
- [AWS Regional Services List](#)
- [AWS Cloud Products](#)

# Thank you

© 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. Corrections or feedback on the course, please email us at: [aws-course-feedback@amazon.com](mailto:aws-course-feedback@amazon.com). For all other questions, contact us at: <https://aws.amazon.com/contact-us/aws-training/>. All trademarks are the property of their owners.



AWS Academy Cloud Foundations

## Module 4: AWS Cloud Security

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



# Module overview



## Topics

- AWS shared responsibility model
- AWS Identity and Access Management (IAM)
- Securing a new AWS account
- Securing accounts
- Securing data on AWS
- Working to ensure compliance

## Activities

- AWS shared responsibility model activity

## Demo

- Recorded demonstration of IAM

## Lab

- Introduction to AWS IAM



## Knowledge check

# Module objectives

After completing this module, you should be able to:

- Recognize the shared responsibility model
- Identify the responsibility of the customer and AWS
- Recognize IAM users, groups, and roles
- Describe different types of security credentials in IAM
- Identify the steps to securing a new AWS account
- Explore IAM users and groups
- Recognize how to secure AWS data
- Recognize AWS compliance programs

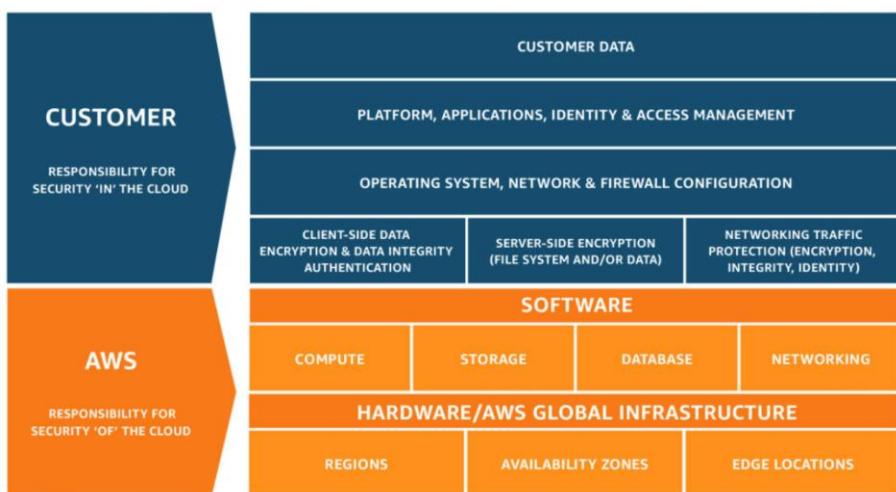
## Module 4: AWS Cloud Security

### Section 1: AWS shared responsibility model

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



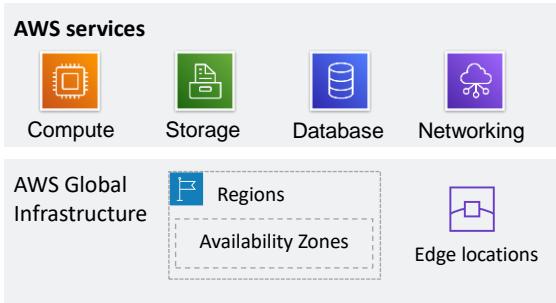
## AWS shared responsibility model



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

174

# AWS responsibility: Security *of* the cloud



## AWS responsibilities:

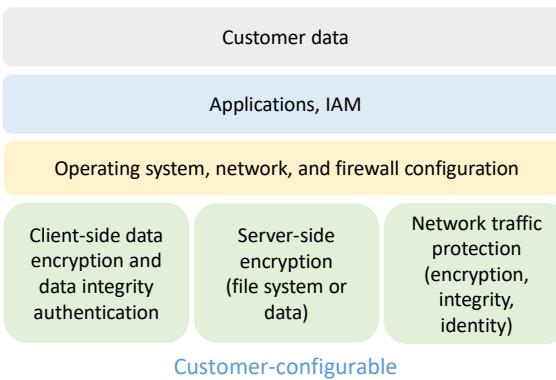
- Physical security of data centers
  - Controlled, need-based access
- Hardware and software infrastructure
  - Storage decommissioning, host operating system (OS) access logging, and auditing
- Network infrastructure
  - Intrusion detection
- Virtualization infrastructure
  - Instance isolation



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

175

# Customer responsibility: Security *in* the cloud



## Customer responsibilities:

- Amazon Elastic Compute Cloud (Amazon EC2) instance **operating system**
  - Including patching, maintenance
- Applications**
  - Passwords, role-based access, etc.
- Security group** configuration
- OS or host-based **firewalls**
  - Including intrusion detection or prevention systems
- Network** configurations
- Account management
  - Login and permission settings for each user

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

176

# Service characteristics and security responsibility



## Example services managed by the customer



Amazon EC2



Amazon Elastic Block Store (Amazon EBS)



Amazon Virtual Private Cloud (Amazon VPC)

## Example services managed by AWS



AWS Lambda



Amazon Relational Database Service (Amazon RDS)



AWS Elastic Beanstalk

## Infrastructure as a service (IaaS)

- Customer has more flexibility over configuring networking and storage settings
- Customer is responsible for managing more aspects of the security
- Customer configures the access controls

## Platform as a service (PaaS)

- Customer does not need to manage the underlying infrastructure
- AWS handles the operating system, database patching, firewall configuration, and disaster recovery
- Customer can focus on managing code or data

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

177

# Service characteristics and security responsibility (continued)



## SaaS examples



AWS Trusted Advisor



AWS Shield



Amazon Chime

## Software as a service (SaaS)

- Software is centrally hosted
- Licensed on a subscription model or pay-as-you-go basis.
- Services are typically accessed via web browser, mobile app, or application programming interface (API)
- Customers do not need to manage the infrastructure that supports the service

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

178



## Activity: AWS shared responsibility model

179

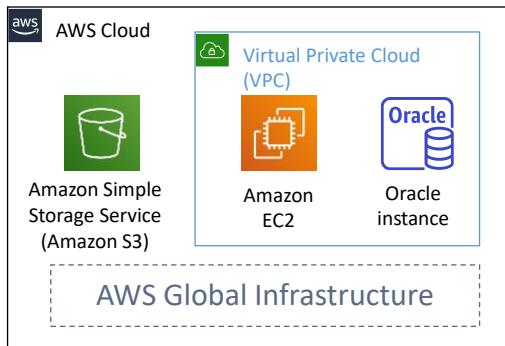


Photo by Pixabay from Pexels.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Activity: Scenario 1 of 2

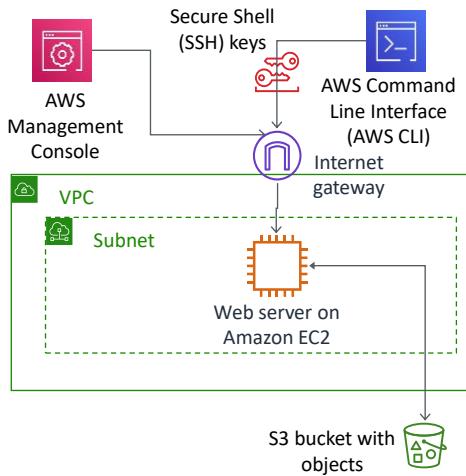
**Consider this deployment. Who is responsible – AWS or the customer?**



1. Upgrades and patches to the operating system on the EC2 instance?  
• **ANSWER: The customer**
2. Physical security of the data center?  
• **ANSWER: AWS**
3. Virtualization infrastructure?  
• **ANSWER: AWS**
4. EC2 security group settings?  
• **ANSWER: The customer**
5. Configuration of applications that run on the EC2 instance?  
• **ANSWER: The customer**
6. Oracle upgrades or patches If the Oracle instance runs as an Amazon RDS instance?  
• **ANSWER: AWS**
7. Oracle upgrades or patches If Oracle runs on an EC2 instance?  
• **ANSWER: The customer**
8. S3 bucket access configuration?  
• **ANSWER: The customer**

## Activity: Scenario 2 of 2

Consider this deployment. Who is responsible – AWS or the customer?



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

181

1. Ensuring that the AWS Management Console is not hacked?  
• **ANSWER:** AWS
2. Configuring the subnet?  
• **ANSWER:** The customer
3. Configuring the VPC?  
• **ANSWER:** The customer
4. Protecting against network outages in AWS Regions?  
• **ANSWER:** AWS
5. Securing the SSH keys  
• **ANSWER:** The customer
6. Ensuring network isolation between AWS customers' data?  
• **ANSWER:** AWS
7. Ensuring low-latency network connection between the web server and the S3 bucket?  
• **ANSWER:** AWS
8. Enforcing multi-factor authentication for all user logins?  
• **ANSWER:** The customer

## Section 1 key takeaways



182



- AWS and the customer share security responsibilities:
  - AWS is responsible for security **of** the cloud
  - Customer is responsible for security **in** the cloud
- **AWS is responsible for protecting the infrastructure**—including hardware, software, networking, and facilities—that run AWS Cloud services
- For services that are categorized as infrastructure as a service (IaaS), the **customer is responsible for performing necessary security configuration and management tasks**
  - For example, guest OS updates and security patches, firewall, security group configurations

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Module 4: AWS Cloud Security

### Section 2: AWS Identity and Access Management (IAM)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## AWS Identity and Access Management (IAM)

- Use **IAM** to manage access to **AWS resources** –
  - A resource is an entity in an AWS account that you can work with
  - Example resources; An Amazon EC2 instance or an Amazon S3 bucket
- *Example* – Control who can terminate Amazon EC2 instances
- Define fine-grained access rights –
  - **Who** can access the resource
  - **Which** resources can be accessed and what can the user do to the resource
  - **How** resources can be accessed
- IAM is a no-cost AWS account feature



AWS Identity and Access Management (IAM)

# IAM: Essential components



IAM user

A **person or application** that can authenticate with an AWS account.



IAM group

A **collection of IAM users** that are granted identical authorization.



IAM policy

The document that defines **which resources can be accessed** and the **level of access** to each resource.



IAM role

Useful mechanism to grant a set of permissions for making AWS service requests.

## Authenticate as an IAM user to gain access

When you define an **IAM user**, you select what **types of access** the user is permitted to use.

### Programmatic access

- Authenticate using:
  - Access key ID
  - Secret access key
- Provides AWS CLI and AWS SDK access



AWS CLI

AWS Tools  
and SDKs

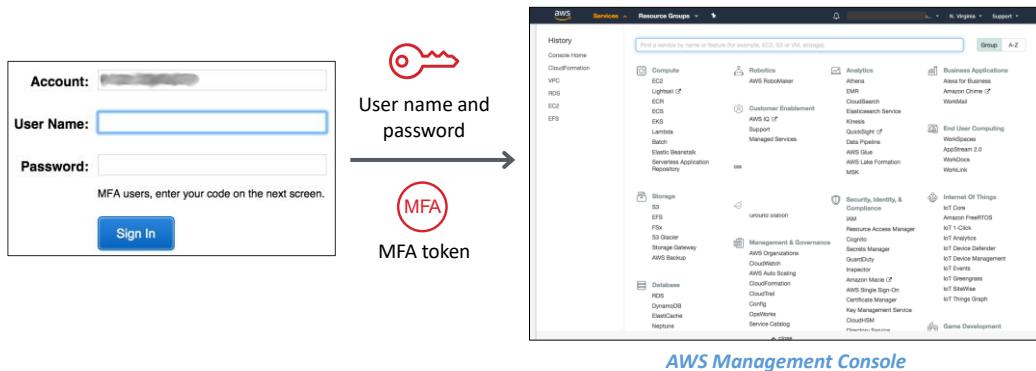
### AWS Management Console access

- Authenticate using:
  - 12-digit Account ID *or* alias
  - IAM user name
  - IAM password
- If enabled, **multi-factor authentication (MFA)** prompts for an authentication code.

AWS Management  
Console

# IAM MFA

- MFA provides increased security.
- In addition to **user name** and **password**, MFA requires a unique **authentication code** to access AWS services.

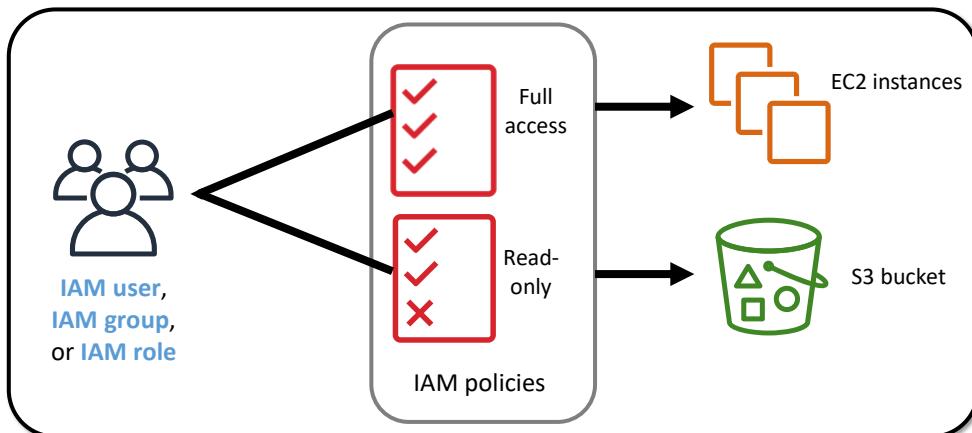


© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

187

## Authorization: What actions are permitted

*After the user or application is connected to the AWS account, what are they allowed to do?*



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

188

# IAM: Authorization

- Assign permissions by creating an IAM policy.
- Permissions determine **which resources and operations** are allowed:
  - All permissions are implicitly denied by default.
  - If something is explicitly denied, it is never allowed.

**Best practice:** Follow the **principle of least privilege**.

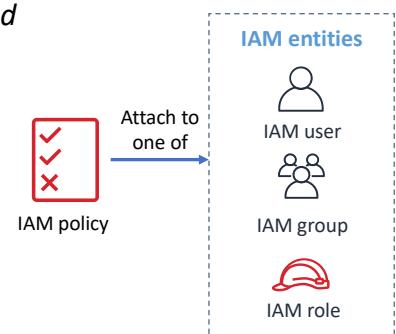


IAM  
permissions

Note: The scope of IAM service configurations is **global**. Settings apply across all AWS Regions.

# IAM policies

- An IAM policy is a document that defines permissions**
  - Enables fine-grained access control
- Two types of policies – *identity-based* and *resource-based*
- Identity-based** policies –
  - Attach a policy to any IAM entity
  - An IAM user, an IAM group, or an IAM role
- Policies specify:
  - Actions that *may* be performed by the entity
  - Actions that *may not* be performed by the entity
- A single *policy* can be attached to multiple *entities*
- A single *entity* can have multiple *policies* attached to it
- Resource-based** policies
  - Attached to a resource (such as an S3 bucket)



# IAM policy example

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["DynamoDB:*", "s3:*"],
      "Resource": [
        "arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
        "arn:aws:s3:::bucket-name",
        "arn:aws:s3:::bucket-name/*"
      ],
      "NotResource": [
        "arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
        "arn:aws:s3:::bucket-name",
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ]
}
```

**Explicit allow** gives users access to a specific DynamoDB table and...

...Amazon S3 buckets.

**Explicit deny** ensures that the users cannot use any other AWS actions or resources other than that table and those buckets.

An explicit deny statement **takes precedence** over an allow statement.

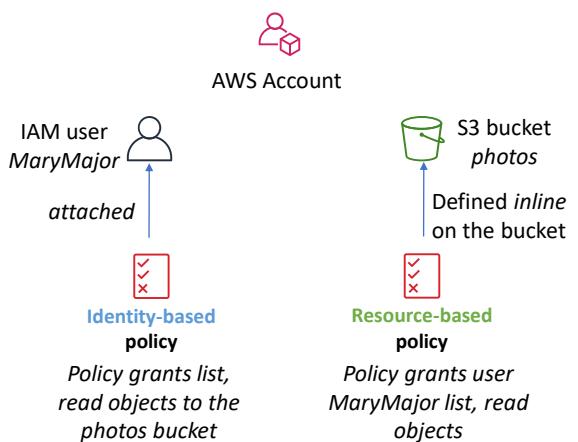
© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

191

## Resource-based policies



- Identity-based policies* are attached to a user, group, or role
- Resource-based policies** are attached to a resource (*not* to a user, group or role)
- Characteristics of resource-based policies –
  - Specifies who has access to the resource and what actions they can perform on it
  - The policies are *inline* only, not managed
- Resource-based policies are supported only by some AWS services

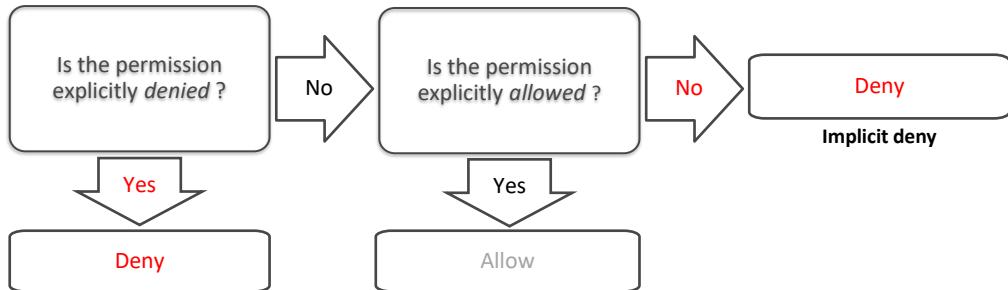


© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

192

# IAM permissions

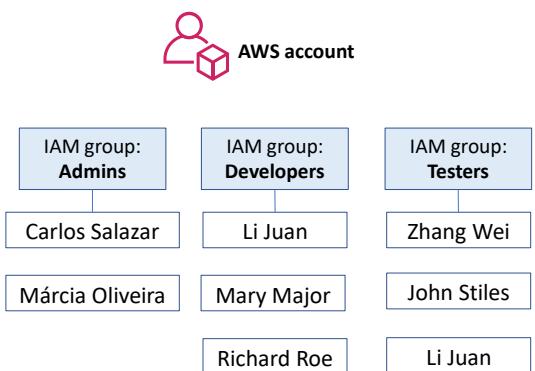
How IAM determines permissions:



## IAM groups



- An **IAM group** is a collection of IAM users
- A group is used to grant the same permissions to multiple users
  - Permissions granted by attaching IAM *policy* or policies to the group
- A user can belong to multiple groups
- There is no default group
- Groups cannot be nested



# IAM roles

- An **IAM role** is an IAM identity with specific permissions
- Similar to an IAM user
  - Attach permissions policies to it
- Different from an IAM user
  - Not uniquely associated with one person
  - Intended to be *assumable* by a **person, application, or service**
- Role provides **temporary** security credentials
- Examples of how IAM roles are used to **delegate** access –
  - Used by an IAM user in the same AWS account as the role
  - Used by an AWS service—such as Amazon EC2—in the same account as the role
  - Used by an IAM user in a different AWS account than the role



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

195

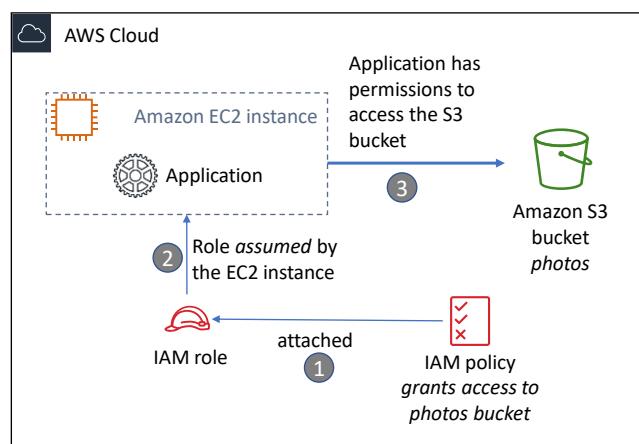
## Example use of an IAM role

### Scenario:

- An application that runs on an EC2 instance needs access to an S3 bucket

### Solution:

- Define an IAM policy that grants access to the S3 bucket.
- Attach the policy to a role
- Allow the EC2 instance to assume the role



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

196

## Section 2 key takeaways



197



- **IAM policies** are constructed with JavaScript Object Notation (JSON) and define permissions.
  - IAM policies can be attached to any **IAM entity**.
  - Entities are IAM users, IAM groups, and IAM roles.
- An **IAM user** provides a way for a person, application, or service to authenticate to AWS.
- An **IAM group** is a simple way to attach the same policies to multiple users.
- An **IAM role** can have permissions policies attached to it, and can be used to delegate temporary access to users or applications.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Recorded demo: IAM

198



### Set up demo

AWS Identity and Access Management (IAM)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

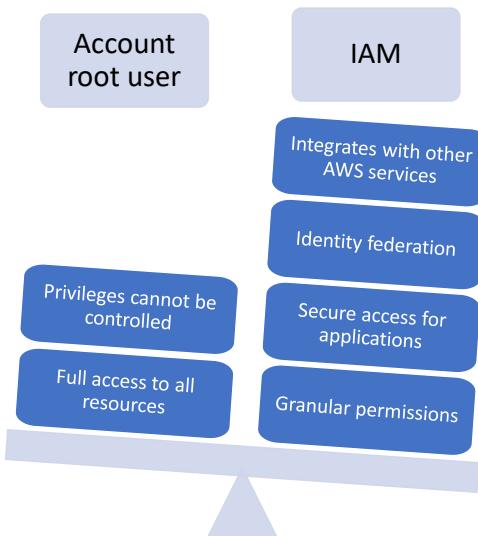
## Module 4: AWS Cloud Security

### Section 3: Securing a new AWS account

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## AWS account root user access versus IAM access



- **Best practice:** Do not use the AWS account root user except when necessary.
  - Access to the **account root user** requires logging in with the *email address* (and password) that you used to create the account.
- Example actions that can only be done with the account root user:
  - Update the account root user password
  - Change the AWS Support plan
  - Restore an IAM user's permissions
  - Change account settings (for example, contact information, allowed Regions)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

200

## Securing a new AWS account: Account root user

### Step 1: Stop using the account root user as soon as possible.

- The account root user has unrestricted access to all your resources.
- To stop using the account root user:
  1. While you are logged in as the account root user, [create an IAM user](#) for yourself. Save the access keys if needed.
  2. Create an IAM group, give it full administrator permissions, and add the IAM user to the group.
  3. Disable and [remove your account root user access keys](#), if they exist.
  4. [Enable a password policy](#) for users.
  5. Sign in with your new IAM user credentials.
  6. Store your account root user credentials in a secure place.

## Securing a new AWS account: MFA

### Step 2: Enable multi-factor authentication (MFA).

- Require MFA for your [account root user](#) and for [all IAM users](#).
- You can also use MFA to control access to AWS service APIs.
- Options for retrieving the MFA token –
  - Virtual MFA-compliant applications:
    - Google Authenticator.
    - Authy Authenticator (Windows phone app).
  - U2F security key devices:
    - For example, YubiKey.
  - Hardware MFA options:
    - Key fob or display card offered by [Gemalto](#).



MFA token

## Securing a new AWS account: AWS CloudTrail

### Step 3: Use AWS CloudTrail.

- CloudTrail tracks user activity on your account.
  - Logs all API requests to resources in all supported services your account.
  - Basic AWS CloudTrail event history is enabled by default and is free.
  - It contains all management event data on latest 90 days of account activity.
- To access CloudTrail –
  1. Log in to the **AWS Management Console** and choose the **CloudTrail** service.
  2. Click **Event history** to view, filter, and search the last 90 days of events.
- **To enable logs beyond 90 days and enable specified event alerting, create a trail.**
  1. From the CloudTrail Console trails page, click **Create trail**.
  2. Give it a name, apply it to all Regions, and create a new Amazon S3 bucket for log storage.
  3. Configure access restrictions on the S3 bucket (for example, only admin users should have access).

## Securing a new AWS account: Billing reports

### Step 4: Enable a billing report, such as the AWS Cost and Usage Report.

- Billing reports provide information about your use of AWS resources and estimated costs for that use.
- AWS delivers the reports to an Amazon S3 bucket that you specify.
  - Report is updated at least once per day.
- The **AWS Cost and Usage Report** tracks your AWS usage and provides estimated charges associated with your AWS account, either by the hour or by the day.

## Section 3 key takeaways



219



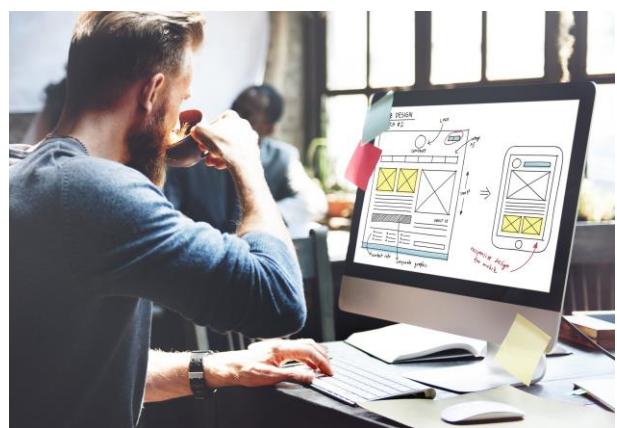
Best practices to secure an AWS account:

- **Secure** logins with multi-factor authentication (MFA).
- **Delete** account root user access keys.
- **Create** individual **IAM users** and grant permissions according to the principle of least privilege.
- **Use groups** to assign permissions to IAM users.
- **Configure** a **strong password policy**.
- **Delegate** using **roles** instead of sharing credentials.
- **Monitor** account activity by using AWS CloudTrail.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Lab 1: Introduction to IAM

220



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

# Lab 1: Tasks



- Task 1: Explore the Users and Groups.

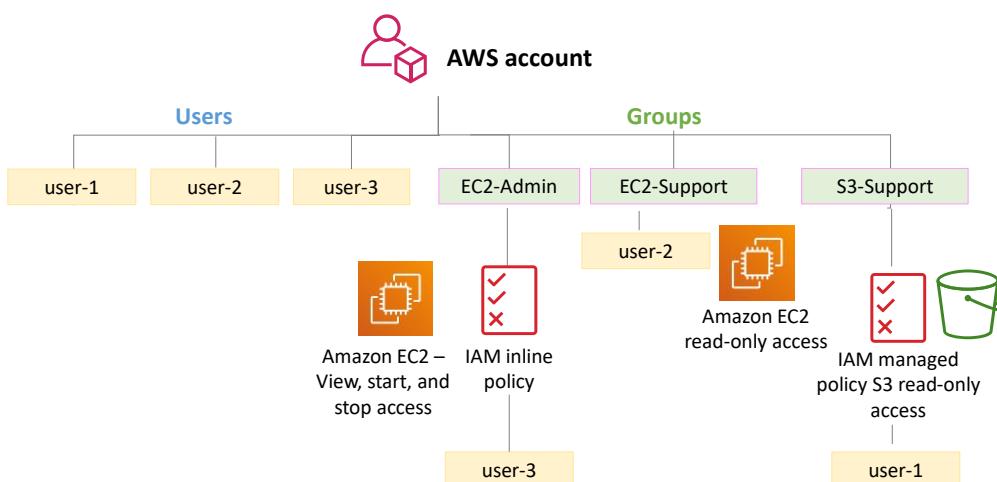


- Task 2: Add Users to Groups.

AWS Identity and Access Management (IAM)

- Task 3: Sign-In and Test Users.

# Lab 1: Final product



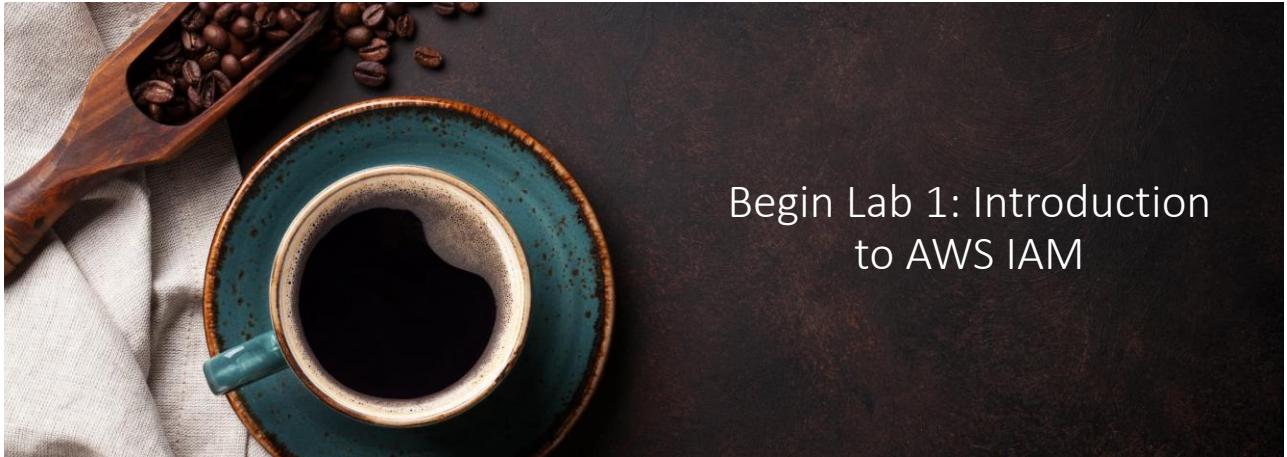


~ 40 minutes



Begin Lab 1: Introduction to AWS IAM

## Begin Lab 1: Introduction to AWS IAM



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

223



## Lab debrief: Key takeaways



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

224

## Module 4: AWS Cloud Security

### Section 4: Securing accounts

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## AWS Organizations

- **AWS Organizations** enables you to consolidate multiple AWS accounts so that you centrally manage them.



AWS Organizations

- **Security features** of AWS Organizations:

- **Group AWS accounts into organizational units (OUs)** and attach different access policies to each OU.

- Integration and support for IAM**

- Permissions to a user are the intersection of what is allowed by AWS Organizations and what is granted by IAM in that account.

- Use service control policies** to establish control over the AWS services and API actions that each AWS account can access

## AWS Organizations: Service control policies

- **Service control policies (SCPs)** offer centralized control over accounts.
  - Limit permissions that are available in an account that is part of an organization.
- Ensures that accounts comply with access control guidelines.
- SCPs are *similar* to IAM permissions policies –
  - They use similar syntax.
  - However, an SCP never grants permissions.
  - Instead, SCPs **specify the maximum permissions** for an organization.

## AWS Key Management Service (AWS KMS)

### **AWS Key Management Service (AWS KMS) features:**

- Enables you to **create and manage encryption keys**
- Enables you to control the use of encryption across AWS services and in your applications.
- Integrates with AWS CloudTrail to log all key usage.
- Uses hardware security modules (HSMs) that are validated by Federal Information Processing Standards (FIPS) 140-2 to protect keys



AWS Key Management Service (AWS KMS)

# Amazon Cognito

## Amazon Cognito features:

- Adds user sign-up, sign-in, and access control to your web and mobile applications.
- Scales to millions of users.
- Supports sign-in with social identity providers, such as Facebook, Google, and Amazon; and enterprise identity providers, such as Microsoft Active Directory via Security Assertion Markup Language (SAML) 2.0.



Amazon Cognito

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

229

# AWS Shield

- AWS Shield features:
  - Is a managed distributed denial of service (DDoS) protection service
  - Safeguards applications running on AWS
  - Provides always-on detection and automatic inline mitigations
  - AWS Shield Standard enabled for at no additional cost. AWS Shield Advanced is an optional paid service.
- Use it to minimize application downtime and latency.



AWS Shield

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

230

## Module 4: AWS Cloud Security

### Section 5: Securing data on AWS

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Encryption of data *at rest*

- **Encryption** encodes data with a **secret key**, which makes it unreadable

- Only those who have the secret key can decode the data
  - **AWS KMS** can manage your secret keys



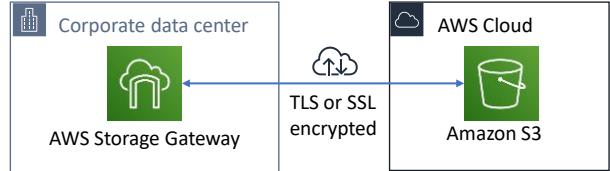
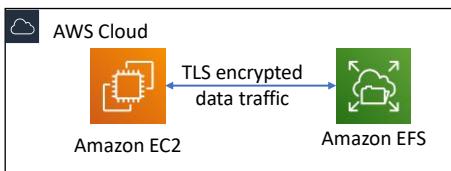
- AWS supports encryption of **data at rest**

- Data at rest = Data stored physically (on disk or on tape)
  - You can encrypt data stored in any service that is supported by AWS KMS, including:
    - Amazon S3
    - Amazon EBS
    - Amazon Elastic File System (Amazon EFS)
    - Amazon RDS managed databases



# Encryption of data *in transit*

- Encryption of **data in transit** (data moving across a network)
  - **Transport Layer Security (TLS)**—formerly SSL—is an open standard protocol
  - **AWS Certificate Manager** provides a way to manage, deploy, and renew TLS or SSL certificates
- Secure HTTP (HTTPS) creates a secure tunnel
  - Uses TLS or SSL for the bidirectional exchange of data
- **AWS services support data in transit encryption.**
  - Two examples:



233

## Securing Amazon S3 buckets and objects

- Newly created S3 buckets and objects are **private** and **protected** by default.
- When use cases require sharing data objects on Amazon S3 –
  - It is essential to manage and control the data access.
  - Follow the **permissions that follow the principle of least privilege** and consider using Amazon S3 encryption.
- Tools and options for controlling access to S3 data include –
  - [Amazon S3 Block Public Access](#) feature: Simple to use.
  - IAM policies: A good option when the user can authenticate using IAM.
  - [Bucket policies](#)
  - [Access control lists](#) (ACLs): A legacy access control mechanism.
  - [AWS Trusted Advisor](#) bucket permission check: A free feature.

## Module 4: AWS Cloud Security

# Section 6: Working to ensure compliance

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## AWS compliance programs

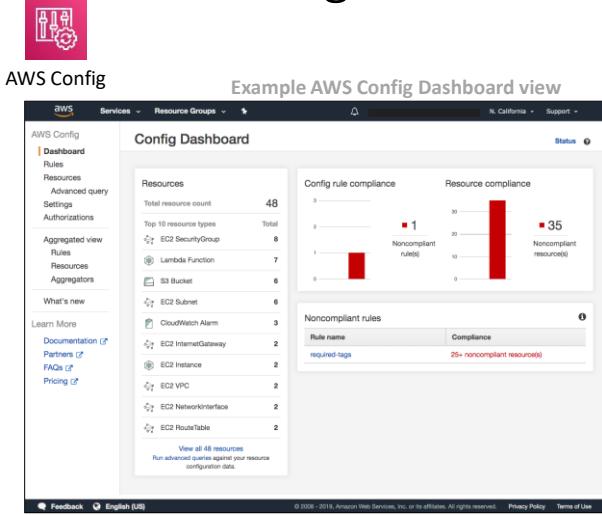
- Customers are subject to many different security and compliance regulations and requirements.
- AWS engages with certifying bodies and independent auditors to provide customers with detailed information about the policies, processes, and controls that are established and operated by AWS.
- Compliance programs can be broadly categorized –
  - **Certifications and attestations**
    - Assessed by a third-party, independent auditor
    - Examples: ISO 27001, 27017, 27018, and ISO/IEC 9001
  - **Laws, regulations, and privacy**
    - AWS provides security features and legal agreements to support compliance
    - Examples: EU General Data Protection Regulation (GDPR), HIPAA
  - **Alignments and frameworks**
    - Industry- or function-specific security or compliance requirements
    - Examples: Center for Internet Security (CIS), EU-US Privacy Shield certified



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

236

# AWS Config



The screenshot shows the AWS Config dashboard with the following details:

- Resources:** Total resource count: 48
- Config Rule Compliance:**
  - Total: 1 Noncompliant rule(s)
  - Total: 35 Noncompliant resource(s)
- Noncompliant rules:**

Rule name	Compliance
required-tags	25+ noncompliant resources

- **Assess, audit, and evaluate the configurations of AWS resources.**
- Use for continuous monitoring of configurations.
- Automatically evaluate *recorded* configurations versus *desired* configurations.
- Review configuration changes.
- View detailed configuration histories.
- **Simplify compliance auditing and security analysis.**

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

237

# AWS Artifact



AWS Artifact

- **Is a resource for compliance-related information**
- Provide access to security and compliance reports, and select online agreements
- Can access example downloads:
  - AWS ISO certifications
  - Payment Card Industry (PCI) and Service Organization Control (SOC) reports
- Access AWS Artifact directly from the AWS Management Console
  - Under **Security, Identify & Compliance**, click **Artifact**.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

238



## Section 6 key takeaways



239

- **AWS security compliance programs** provide information about the policies, processes, and controls that are established and operated by AWS.
- **AWS Config** is used to assess, audit, and evaluate the configurations of AWS resources.
- **AWS Artifact** provides access to security and compliance reports.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Module 4: AWS Cloud Security

## Module wrap-up

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



# Module summary

In summary, in this module you learned how to:

- Recognize the shared responsibility model
- Identify the responsibility of the customer and AWS
- Recognize IAM users, groups, and roles
- Describe different types of security credentials in IAM
- Identify the steps to securing a new AWS account
- Explore IAM users and groups
- Recognize how to secure AWS data
- Recognize AWS compliance programs

## Complete the knowledge check



## Sample exam question

Which of the following is AWS's responsibility under the AWS shared responsibility model?

- A. Configuring third party applications
- B. Maintaining physical hardware
- C. Securing application access and data
- D. Managing custom Amazon Machine Images (AMIs)

## Additional resources

- [AWS Cloud Security](#) home page
- [AWS Security Resources](#)
- [AWS Security Blog](#)
- [Security Bulletins](#)
- [Vulnerability and Penetration testing](#)
- AWS Well-Architected Framework – [Security pillar](#)
- AWS documentation - [IAM Best Practices](#)

# Thank you

© 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. Corrections or feedback on the course, please email us at: [aws-course-feedback@amazon.com](mailto:aws-course-feedback@amazon.com). For all other questions, contact us at: <https://aws.amazon.com/contact-us/aws-training/>. All trademarks are the property of their owners.



AWS Academy Cloud Foundations

## Module 5: Networking and Content Delivery



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved

# Module overview



## Topics

- Networking basics
- Amazon VPC
- VPC networking
- VPC security
- Amazon Route 53
- Amazon CloudFront

## Activities

- Label a network diagram
- Design a basic VPC architecture

## Demo

- VPC demonstration

## Lab

- Build your VPC and launch a web server



## Knowledge check

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

250

# Module objectives

After completing this module, you should be able to:

- Recognize the basics of networking
- Describe virtual networking in the cloud with Amazon VPC
- Label a network diagram
- Design a basic VPC architecture
- Indicate the steps to build a VPC
- Identify security groups
- Create your own VPC and add additional components to it to produce a customized network
- Identify the fundamentals of Amazon Route 53
- Recognize the benefits of Amazon CloudFront

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

251

## Module 5: Networking and Content Delivery

### Section 1: Networking basics

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Networks

### Number System

### Protocol

### IP Addressing

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

253

# Networks

## Number System :-

- Decimal
- Roman
- Binary
- Octal
- HexaDecimal

# Networks

0 1 2 3 4 5 6 7 8 9 A B C D E F - Hexadecimal

0 1 - Binary

0	10	100	0	0	10	10	20	20	90	100
1	11	101	1	1	11	11	21	21	91	101
			2	2	12	12	2	12	92	102
			3	3	13	13	3	13	93	103
			4	4	14	14	4	14	94	104
			5	5	15	15	5	15	95	4
		110	6	6	16	16	6	16	96	5
		111	7	7	17	17	7	27	97	6
			8		18		8		98	7
			9		19		29		99	8
										109

# Networks

Conversion of Number from one number system to another

Decimal to Binary

Binary to Decimal

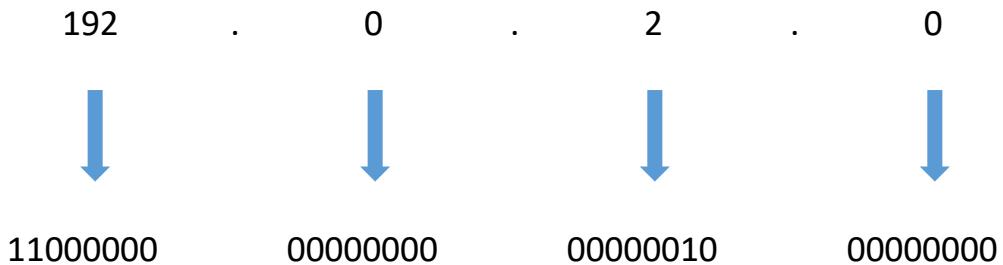
# Networks

## Protocol

### Network protocols:

- TCP/IP - DOD
- IPX/SPX - Novell
- AppleTalk - Apple
- NetBIOS - Microsoft
- OSI – ISO

## IP addresses



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

258

## IP addresses

### Range of IP Address

#### RANGE OF IPv4 ADDRESS

Taking example as all 0's and all 1's

0 0 0 0 0 0 0 = 0

0 0 0 0 0 0 1 = 1

0 0 0 0 0 1 0 = 2

0 0 0 0 0 1 1 = 3

0 0 0 0 1 0 0 = 4

1 1 1 1 1 1 1 1 = 255

Total IP Address Range: 0.0.0.0 to 255.255.255.255

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

259

# IPv4 and IPv6 addresses

**IPv4 (32-bit) address:** 192.0.2.0

**IPv6 (128-bit) address:** 2600:1f18:22ba:8c00:ba86:a05e:a5ba:00FF

# IP Address Classification

## IP ADDRESS CLASSIFICATION

IP ADDRESS are divided into 5 classes

CLASS A 0 - 127

CLASS B 128 - 191

CLASS C 192 - 223

CLASS D 224 – 239

CLASS E 240 – 255

CLAS A, B, C used in LAN & WAN

CLASS D reserved for multicasting

CLASS E reserved for research & development and for future use

# Public IP address And Private IP Address



- Public IP Address

- External (global) reach
- Used for communicating outside your private network, over the internet
- A unique numeric code never reused by other devices
- Found by Googling: "What is my IP address?"
- Assigned and controlled by your internet service provider
- Not free

- Private IP Address

- Internal (local) reach
- Used for communicating within your private network, with other devices in your home or office
- A non-unique numeric code that may be reused by other devices in other private networks
- Found via your device's internal settings
- Assigned to your specific device within a private network

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

262

## Public IP address types



### Public IPv4 address

- Manually assigned through an Elastic IP address
- Automatically assigned through the auto-assign public IP address settings at the subnet level

### Elastic IP address

- Associated with an AWS account
- Can be allocated and remapped anytime
- Additional costs might apply

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

263

## Private IP address Class



# NETWORK AND HOST PORTIONS

IP Address is divided into Network & Host Portion.

**CLASS A** N.H.H.H

**CLASS B** N.N.H.H

**CLASS C** N.N.N.H

Host: specific a device in the network.

Network: set of devices

## Private IP address Class



# PRIVATE IP ADDRESS

There are certain addresses in each class of IP address that are reserved for Private Networks. These addresses are called private addresses.

### CLASS A

10.0.0.0 to 10.255.255.255 (10.X.X.X)

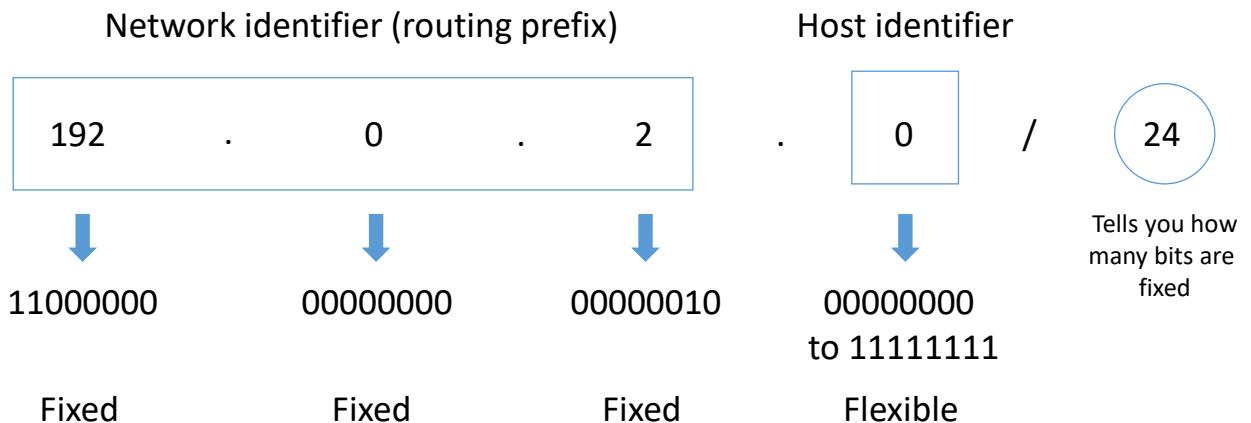
### CLASS B

172.16.0.0 to 172.31.255.255

### CLASS C

192.168.0.0 to 192.168.255.255 (192.168.X.X)

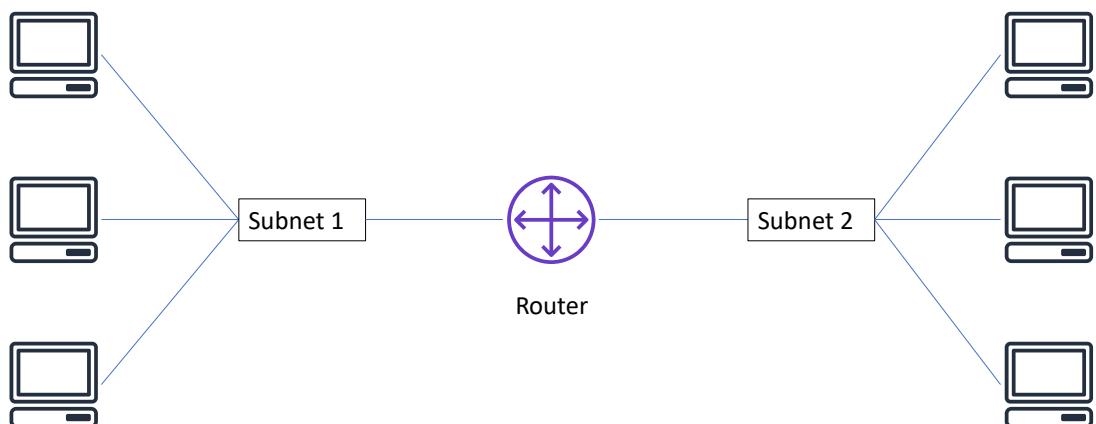
# Classless Inter-Domain Routing (CIDR)



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

266

# Networks



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

267

## Open Systems Interconnection (OSI) model

Layer	Number	Function	Protocol/Address
Application	7	Means for an application to access a computer network	HTTP(S), FTP, DHCP, LDAP
Presentation	6	<ul style="list-style-type: none"> <li>Ensures that the application layer can read the data</li> <li>Encryption</li> </ul>	ASCI, ICA
Session	5	Enables orderly exchange of data	NetBIOS, RPC
Transport	4	Provides protocols to support host-to-host communication	TCP, UDP
Network	3	Routing and packet forwarding (routers)	IP
Data link	2	Transfer data in the same LAN network (hubs and switches)	MAC
Physical	1	Transmission and reception of raw bitstreams over a physical medium	Signals (1s and 0s)

### Module 5: Networking and Content Delivery

## Section 2: Amazon VPC

# Amazon VPC



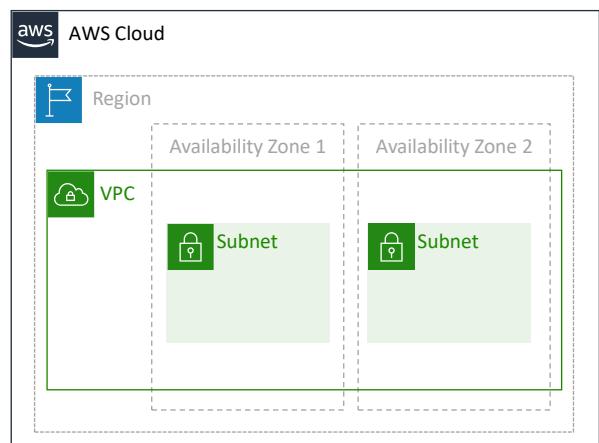
Amazon  
VPC

- Enables you to provision a **logically isolated** section of the AWS Cloud where you can launch AWS resources in a virtual network that you define
- Gives you **control over your virtual networking resources**, including:
  - Selection of IP address range
  - Creation of subnets
  - Configuration of route tables and network gateways
- Enables you to **customize the network configuration** for your VPC
- Enables you to use **multiple layers of security**

## VPCs and subnets



- VPCs:
  - **Logically isolated** from other VPCs
  - **Dedicated** to your AWS account
  - Belong to a single **AWS Region** and can span multiple Availability Zones
- Subnets:
  - **Range of IP addresses** that divide a VPC
  - Belong to a single **Availability Zone**
  - Classified as **public** or **private**



# IP addressing



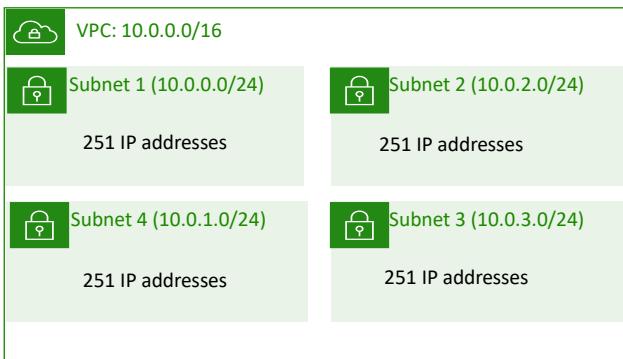
- When you create a VPC, you assign it to an IPv4 **CIDR block** (range of **private** IPv4 addresses).
- You **cannot change the address range** after you create the VPC.
- The **largest** IPv4 CIDR block size is **/16**.
- The **smallest** IPv4 CIDR block size is **/28**.
- IPv6 is also supported (with a different block size limit).
- CIDR blocks of subnets **cannot overlap**.



x.x.x.x/16 or 65,536 addresses (max)  
to  
x.x.x.x/28 or 16 addresses (min)

## Reserved IP addresses

**Example:** A VPC with an IPv4 CIDR block of 10.0.0.0/16 has 65,536 total IP addresses. The VPC has four equal-sized subnets. Only 251 IP addresses are available for use by each subnet.



IP Addresses for CIDR block 10.0.0.0/24	Reserved for
10.0.0.0	Network address
10.0.0.1	Internal communication
10.0.0.2	Domain Name System (DNS) resolution
10.0.0.3	Future use
10.0.0.255	Network broadcast address

# Elastic network interface

- An elastic network interface is a **virtual network interface** that you can:
  - Attach to an instance.
  - Detach from the instance, and attach to another instance to redirect network traffic.
- Its **attributes follow** when it is reattached to a new instance.
- Each instance in your VPC has a **default network interface** that is assigned a private IPv4



address range of your VPC.

## Route tables and routes



- A **route table** contains a set of rules (or routes) that **you can configure** to direct network traffic from your subnet.
- Each **route** specifies a destination and a target.
- By default, every route table contains a **local route** for communication within the VPC.
- Each **subnet must be associated with a route table** (at most one).

Main (Default) Route Table

Destination	Target
10.0.0.0/16	local

VPC CIDR block

## Section 2 key takeaways



276



- A VPC is a logically isolated section of the AWS Cloud.
- A VPC belongs to one Region and requires a CIDR block.
- A VPC is subdivided into subnets.
- A subnet belongs to one Availability Zone and requires a CIDR block.
- Route tables control traffic for a subnet.
- Route tables have a built-in local route.
- You add additional routes to the table.
- The local route cannot be deleted.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

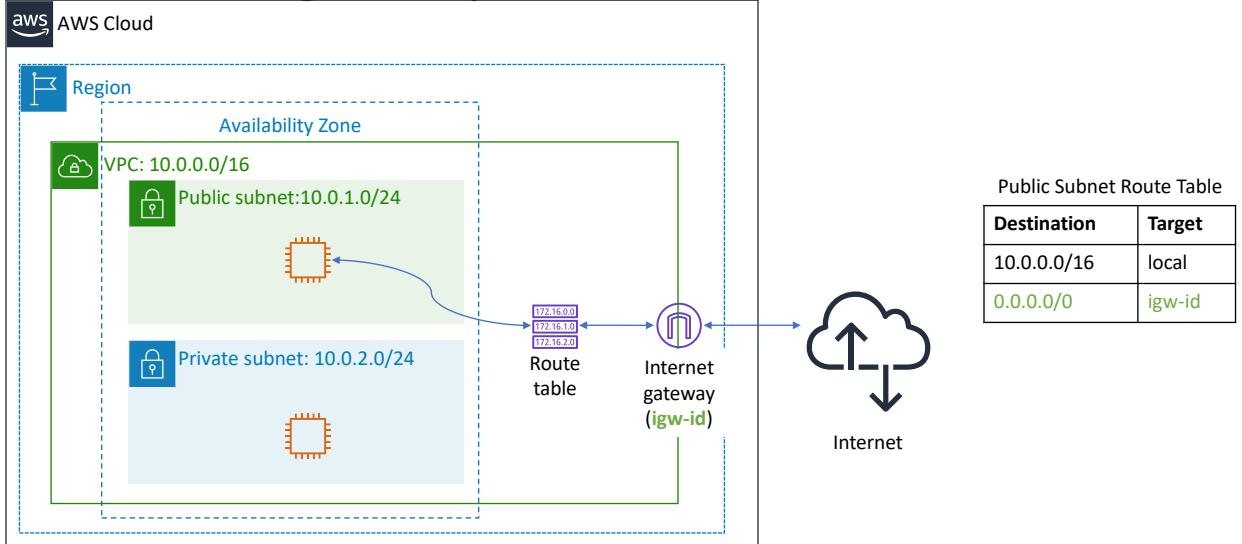
### Module 5: Networking and Content Delivery

## Section 3: VPC networking

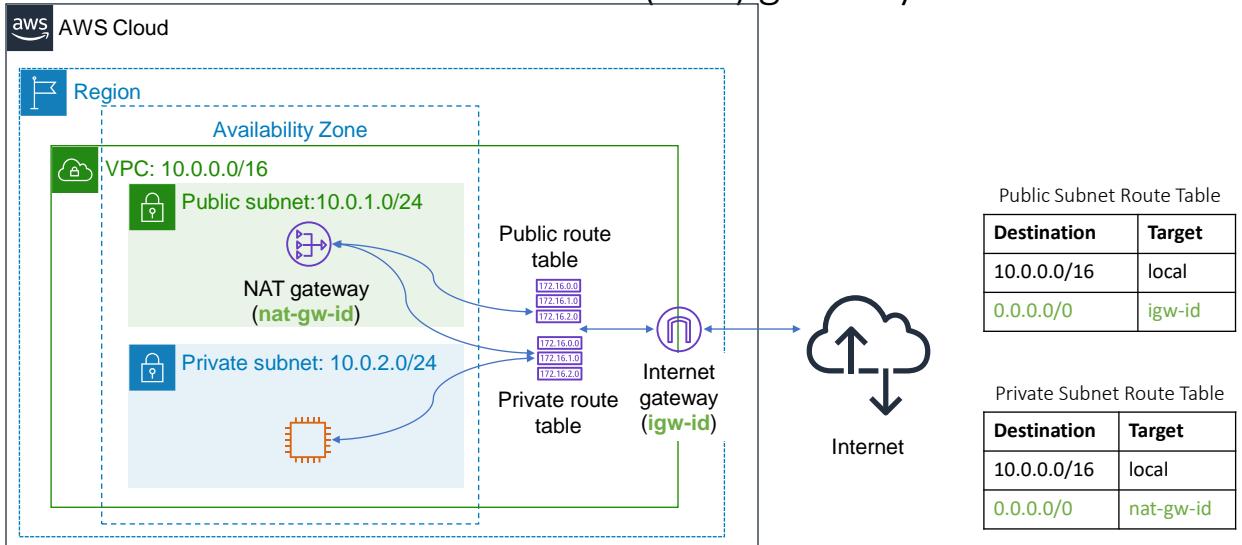
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



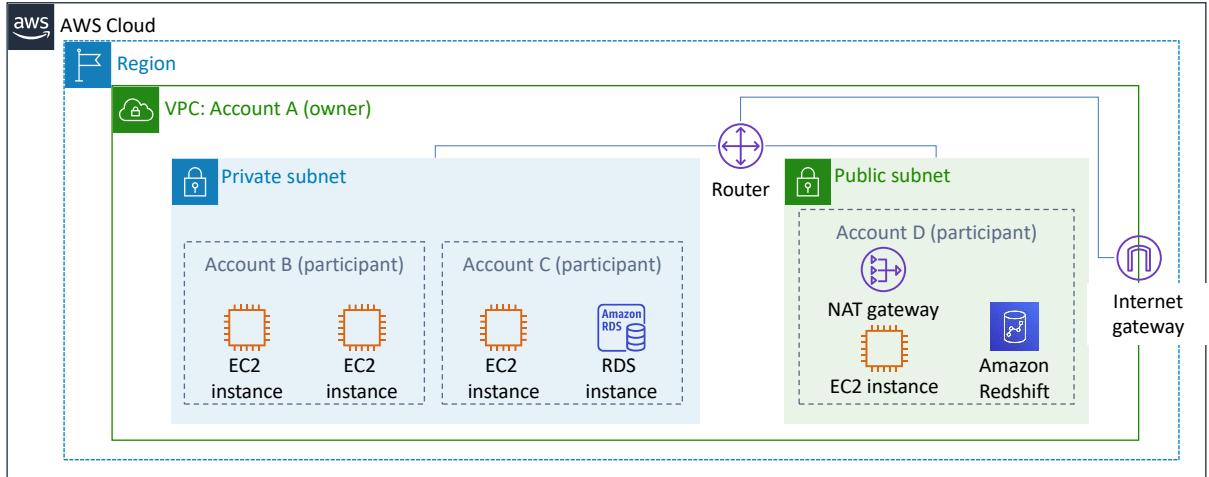
# Internet gateway



# Network address translation (NAT) gateway



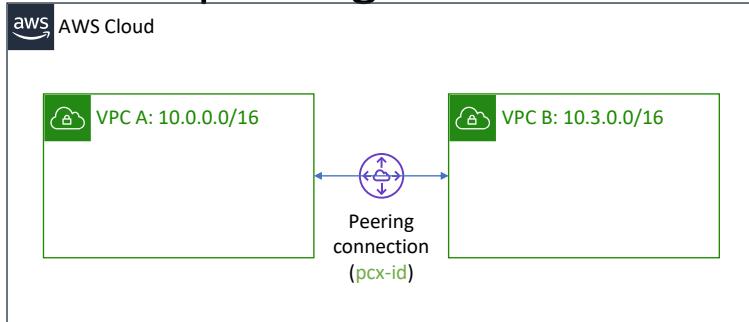
# VPC sharing



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

280

# VPC peering



You can connect VPCs in your own AWS account, between AWS accounts, or between AWS Regions.

#### Restrictions:

- IP spaces cannot overlap.
- Transitive peering is not supported.
- You can only have one peering resource between the same two VPCs.

Route Table for VPC A

Destination	Target
10.0.0.0/16	local
10.3.0.0/16	pcx-id

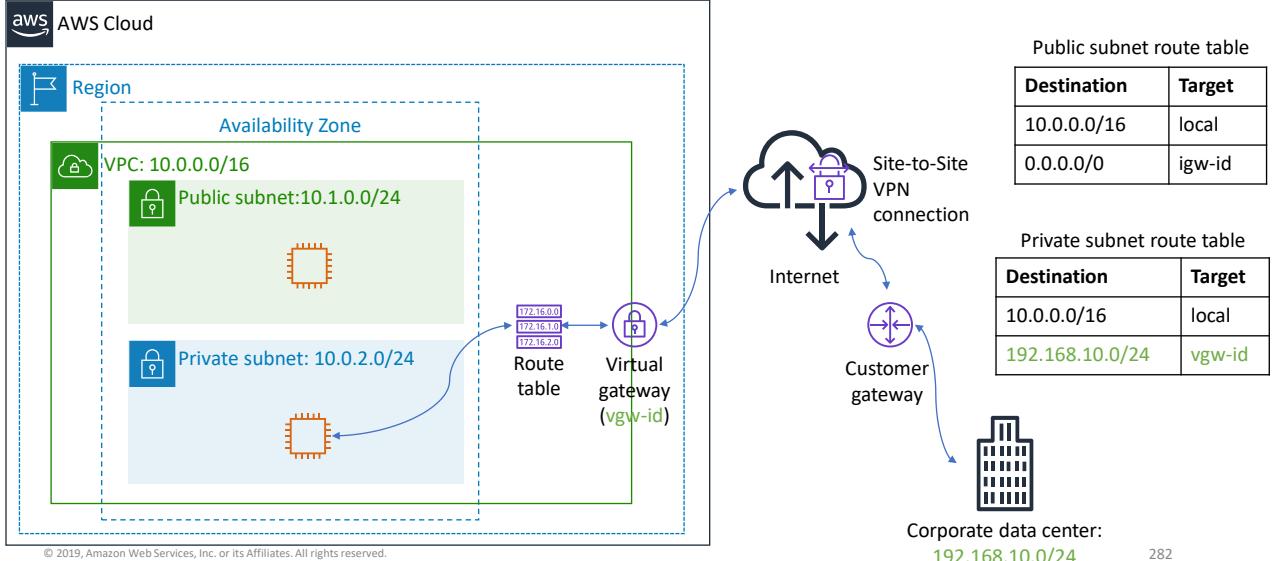
Route Table for VPC B

Destination	Target
10.3.0.0/16	local
10.0.0.0/16	pcx-id

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

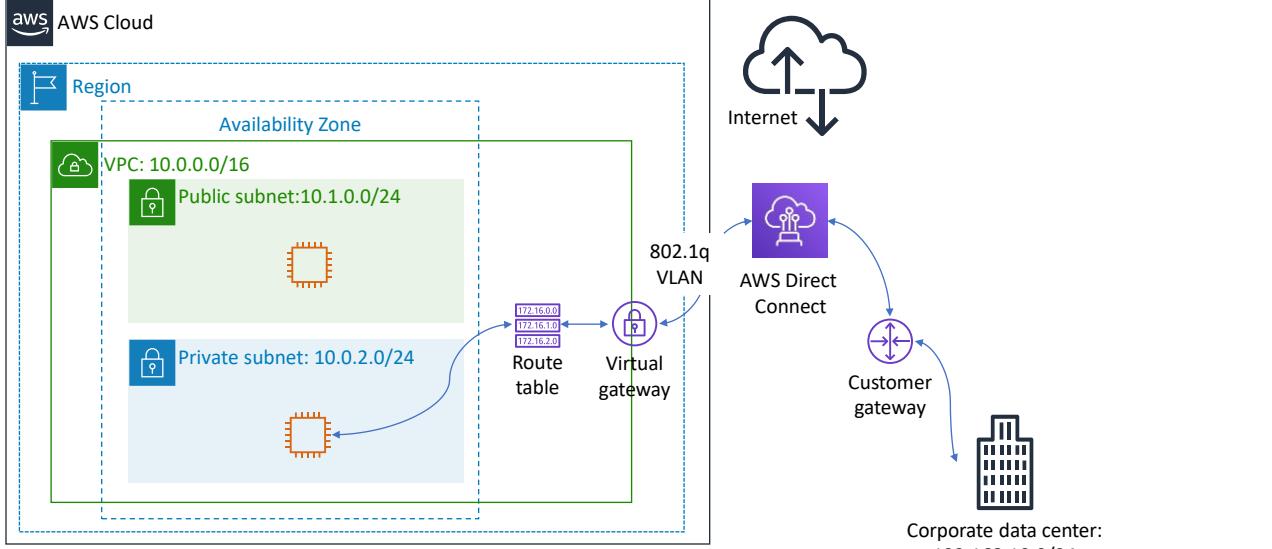
281

# AWS Site-to-Site VPN



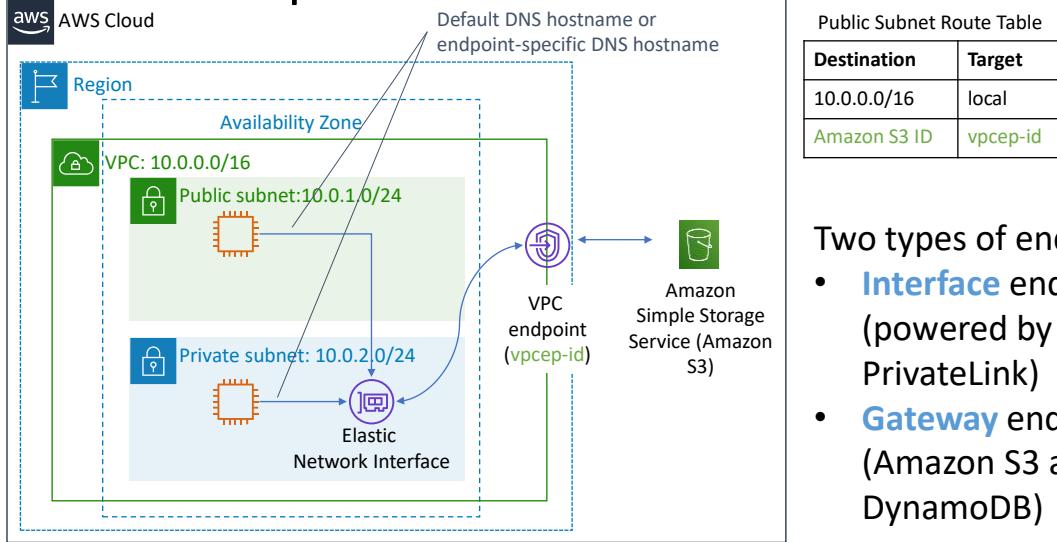
282

# AWS Direct Connect



283

# VPC endpoints



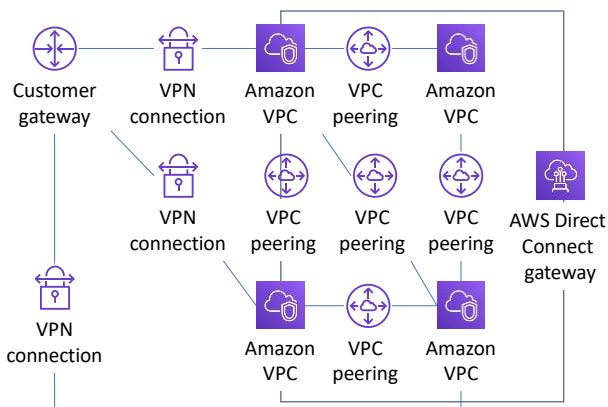
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

284

Two types of endpoints:

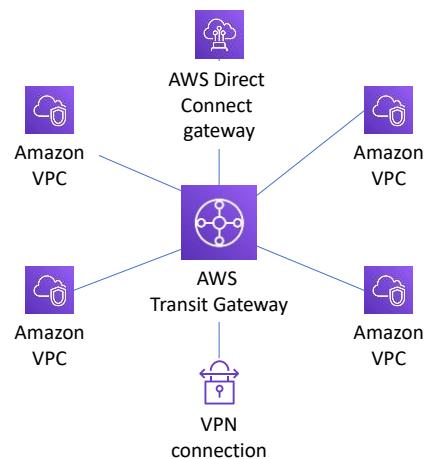
- **Interface endpoints** (powered by AWS PrivateLink)
- **Gateway endpoints** (Amazon S3 and Amazon DynamoDB)

From this...



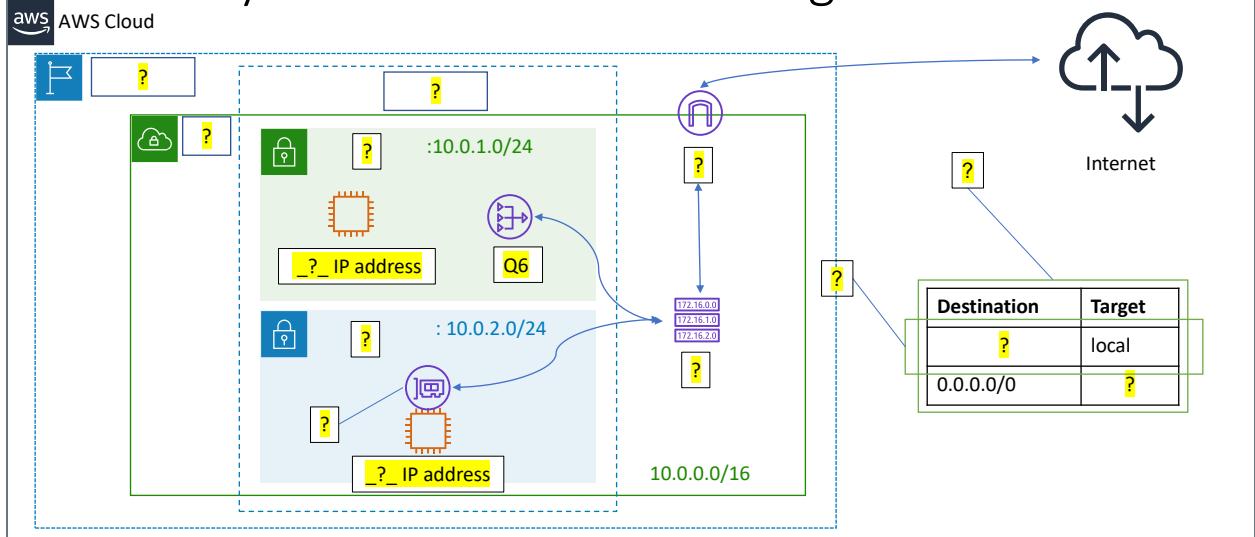
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

To this...

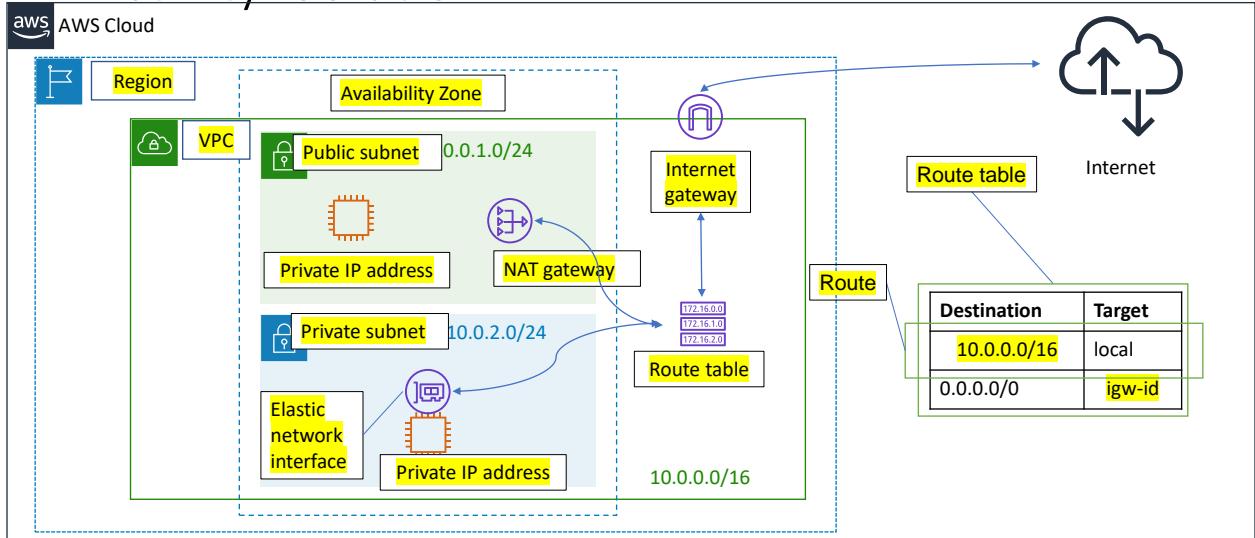


285

## Activity: Label this network diagram



## Activity: Solution



# Recorded Amazon VPC demonstration



**Set up demo**  
Amazon Virtual Private Cloud (VPC)

288

## Section 3 key takeaways

289



- There are several VPC networking options, which include:
  - Internet gateway
  - NAT gateway
  - VPC endpoint
  - VPC peering
  - VPC sharing
  - AWS Site-to-Site VPN
  - AWS Direct Connect
  - AWS Transit Gateway
- You can use the VPC Wizard to implement your design.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

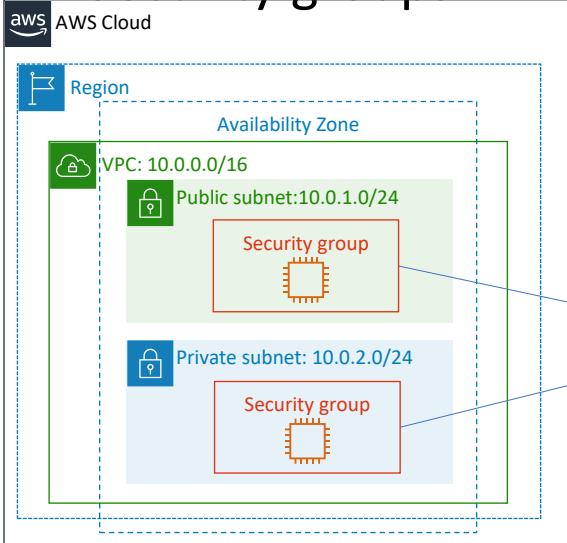
## Module 5: Networking and Content Delivery

### Section 4: VPC security

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Security groups



Security groups act at  
the **instance level**.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

291

# Security groups

- Security groups have **rules** that control inbound and outbound instance traffic.
- Default security groups **deny all inbound** traffic and **allow all outbound** traffic.
- Security groups are **stateful**.

Inbound			
Source	Protocol	Port Range	Description
sg-xxxxxxxx	All	All	Allow inbound traffic from network interfaces assigned to the same security group.

Outbound			
Destination	Protocol	Port Range	Description
0.0.0.0/0	All	All	Allow all outbound IPv4 traffic.
::/0	All	All	Allow all outbound IPv6 traffic.

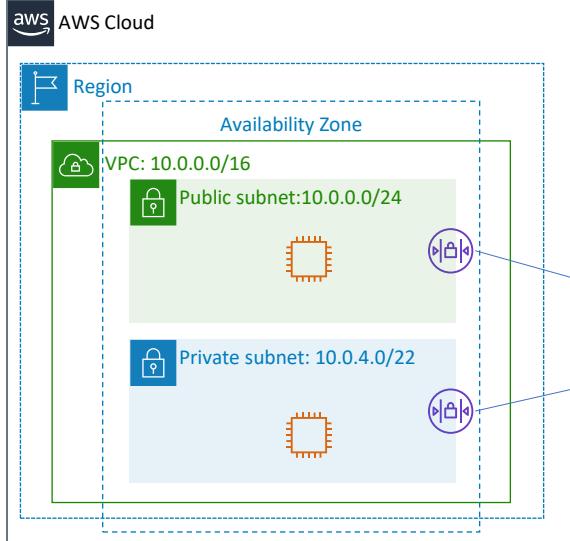
# Custom security group examples

- You can **specify allow** rules, but not deny rules.
- **All rules are evaluated** before the decision to allow traffic.

Inbound			
Source	Protocol	Port Range	Description
0.0.0.0/0	TCP	80	Allow inbound HTTP access from all IPv4 addresses
0.0.0.0/0	TCP	443	Allow inbound HTTPS access from all IPv4 addresses
Your network's public IPv4 address range	TCP	22	Allow inbound SSH access to Linux instances from IPv4 IP addresses in your network (over the internet gateway)

Outbound			
Destination	Protocol	Port Range	Description
The ID of the security group for your Microsoft SQL Server database servers	TCP	1433	Allow outbound Microsoft SQL Server access to instances in the specified security group

# Network access control lists (network ACLs)



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

294

## Network access control lists (network ACLs)

- A network ACL has **separate inbound and outbound rules**, and each rule can either **allow or deny traffic**.
- Default** network ACLs **allow** all inbound and outbound IPv4 traffic.
- Network ACLs are **stateless**.

Inbound					
Rule	Type	Protocol	Port Range	Source	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Outbound					
Rule	Type	Protocol	Port Range	Destination	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

295

## Custom network ACLs examples

- **Custom** network ACLs **deny** all inbound and outbound traffic until you add rules.
- You can specify **both allow and deny** rules.
- Rules are evaluated in number order, starting with the **lowest number**.

Inbound					
Rule	Type	Protocol	Port Range	Source	Allow/Deny
100	HTTPS	TCP	443	0.0.0.0/0	ALLOW
120	SSH	TCP	22	192.0.2.0/24	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Outbound					
Rule	Type	Protocol	Port Range	Destination	Allow/Deny
100	HTTPS	TCP	443	0.0.0.0/0	ALLOW
120	SSH	TCP	22	192.0.2.0/24	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

## Security groups versus network ACLs

Attribute	Security Groups	Network ACLs
Scope	Instance level	Subnet level
Supported Rules	Allow rules only	Allow and deny rules
State	Stateful (return traffic is automatically allowed, regardless of rules)	Stateless (return traffic must be explicitly allowed by rules)
Order of Rules	All rules are evaluated before decision to allow traffic	Rules are evaluated in number order before decision to allow traffic

# Activity: Design a VPC

**Scenario:** You have a small business with a website that is hosted on an Amazon Elastic Compute Cloud (Amazon EC2) instance. You have customer data that is stored on a backend database that you want to keep private. You want to use Amazon VPC to set up a VPC that meets the following requirements:

- Your web server and database server must be in separate subnets.
- The first address of your network must be 10.0.0.0. Each subnet must have 256 total IPv4 addresses.
- Your customers must always be able to access your web server.
- Your database server must be able to access the internet to make patch updates.
- Your architecture must be highly available and use at least one custom firewall layer.



## Section 4 key takeaways



- Build security into your VPC architecture:
  - Isolate subnets if possible.
  - Choose the appropriate gateway device or VPN connection for your needs.
  - Use firewalls.
- Security groups and network ACLs are firewall options that you can use to secure your VPC.

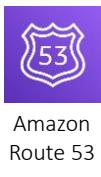
## Module 5: Networking and Content Delivery

### Section 5: Amazon Route 53

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



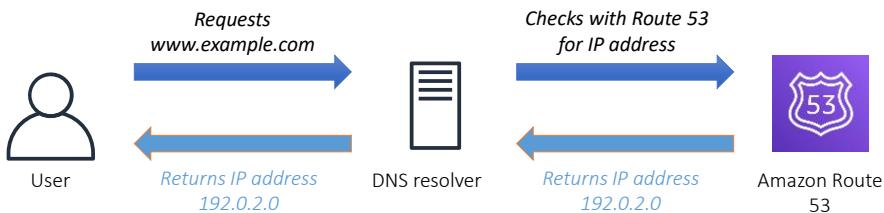
## Amazon Route 53



Amazon  
Route 53

- Is a highly available and scalable Domain Name System (DNS) web service
- Is used to route end users to internet applications by translating names (like [www.example.com](http://www.example.com)) into numeric IP addresses (like 192.0.2.1) that computers use to connect to each other
- Is fully compliant with IPv4 and IPv6
- Connects user requests to infrastructure running in AWS and also outside of AWS
- Is used to check the health of your resources
- Features traffic flow
- Enables you to register domain names

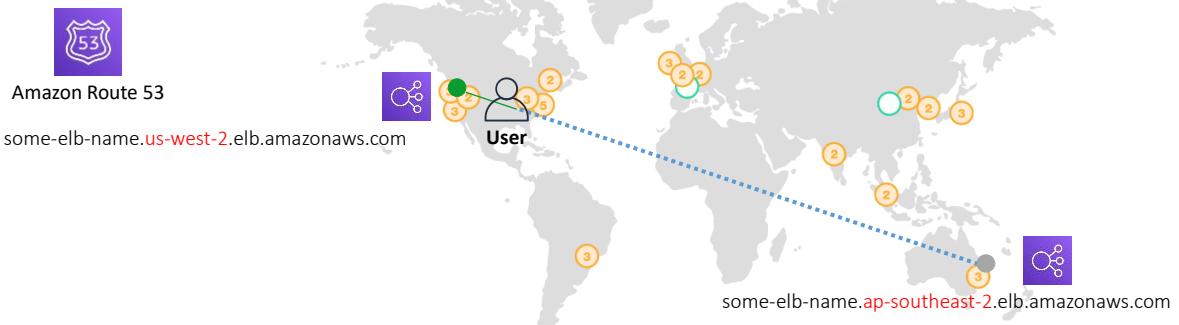
# Amazon Route 53 DNS resolution



# Amazon Route 53 supported routing

- **Simple routing** – Use in single-server environments
- **Weighted round robin routing** – Assign weights to resource record sets to specify the frequency
- **Latency routing** – Help improve your global applications
- **Geolocation routing** – Route traffic based on location of your users
- **Geoproximity routing** – Route traffic based on location of your resources
- **Failover routing** – Fail over to a backup site if your primary site becomes unreachable
- **Multivalue answer routing** – Respond to DNS queries with up to eight healthy records selected at random

# Use case: Multi-region deployment



Name	Type	Value
example.com	ALIAS	some-elb-name.us-west-2.elb.amazonaws.com
example.com	ALIAS	some-elb-name.ap-southeast-2.elb.amazonaws.com

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

304

## Amazon Route 53 DNS failover

Improve the availability of your applications that run on AWS by:

- Configuring backup and failover scenarios for your own applications
- Enabling highly available multi-region architectures on AWS
- Creating health checks

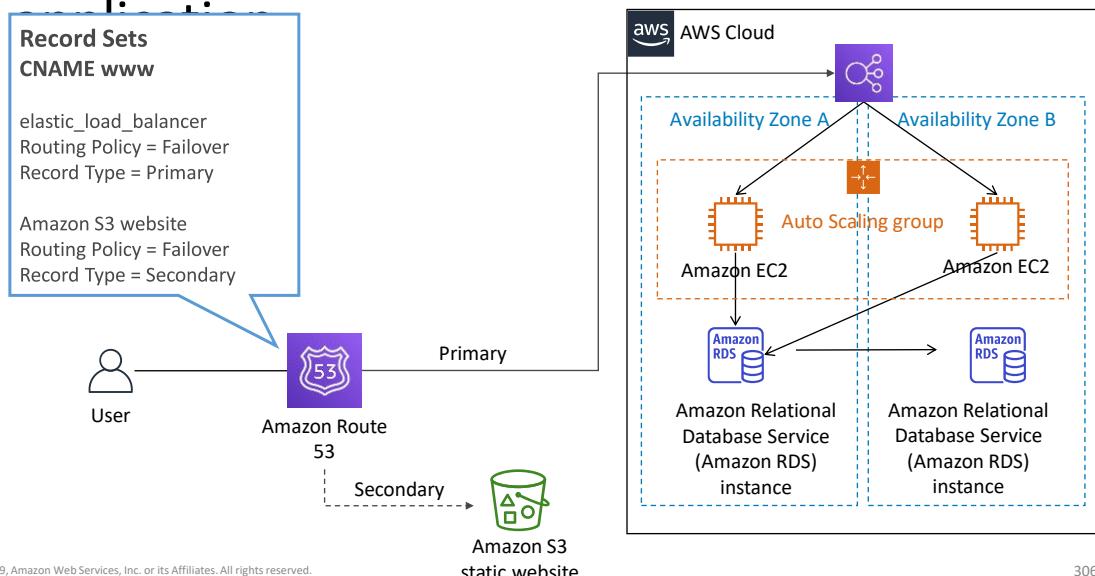
▼ Advanced configuration

Request interval	<input checked="" type="radio"/> Standard (30 seconds) <input type="radio"/> Fast (10 seconds)
Failure threshold *	<input type="text" value="3"/> <small>[min: 1, max: 10]</small>
String matching	<input checked="" type="radio"/> No <input type="radio"/> Yes <small>[optional]</small>
Latency graphs	<input checked="" type="checkbox"/> <small>[optional]</small>
Invert health check status	<input type="checkbox"/> <small>[optional]</small>

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

305

# DNS failover for a multi-tiered web



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

306

## Section 5 key takeaways



307



- Amazon Route 53 is a highly available and scalable cloud DNS web service that translates domain names into numeric IP addresses.
- Amazon Route 53 supports several types of routing policies.
- Multi-Region deployment improves your application's performance for a global audience.
- You can use Amazon Route 53 failover to improve the availability of your applications.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

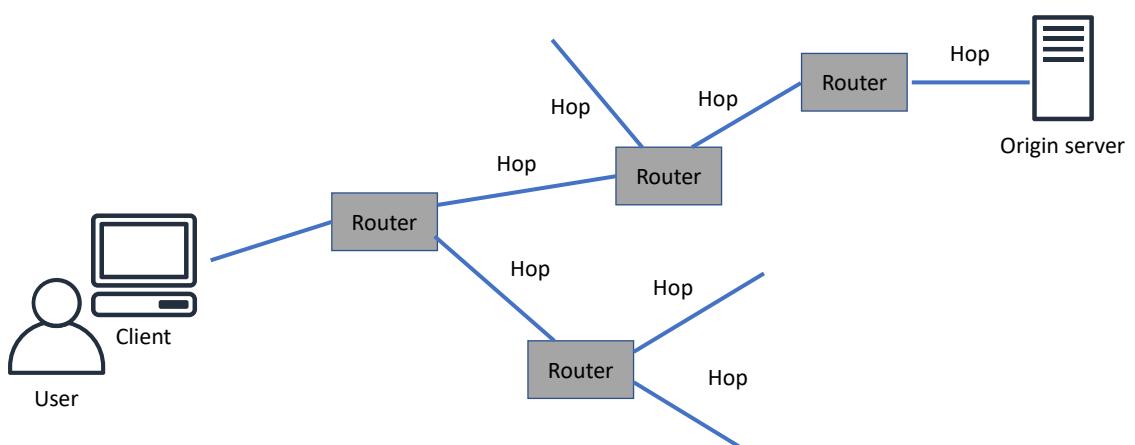
## Module 5: Networking and Content Delivery

### Section 6: Amazon CloudFront

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Content delivery and network latency



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

9

# Content delivery network (CDN)

- Is a globally distributed system of caching servers
- Caches copies of commonly requested files (static content)
- Delivers a local copy of the requested content from a nearby cache edge or Point of Presence
- Accelerates delivery of dynamic content
- Improves application performance and scaling

## Amazon CloudFront

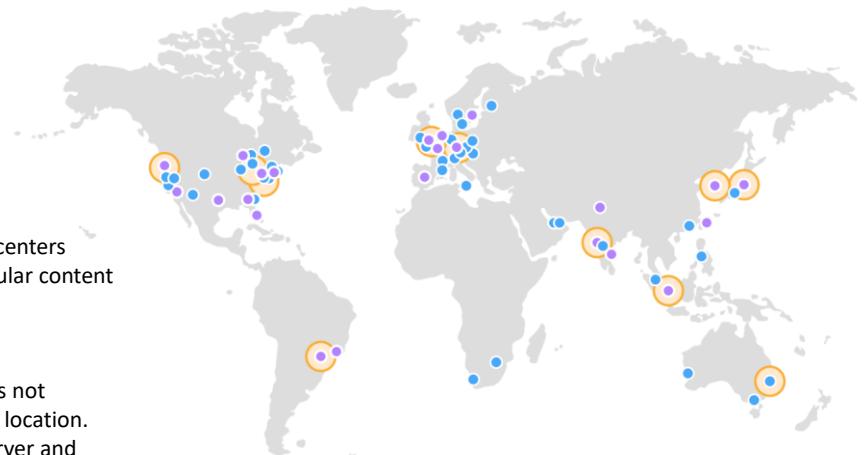


Amazon  
CloudFront

- Fast, global, and secure CDN service
- Global network of edge locations and Regional edge caches
- Self-service model
- Pay-as-you-go pricing

# Amazon CloudFront infrastructure

- Edge locations
- Multiple edge locations
- Regional edge caches



- **Edge locations** – Network of data centers that CloudFront uses to serve popular content quickly to customers.
- **Regional edge cache** – CloudFront location that caches content that is not popular enough to stay at an edge location. It is located between the origin server and the global edge location.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

312

# Amazon CloudFront benefits

- Fast and global
- Security at the edge
- Highly programmable
- Deeply integrated with AWS
- Cost-effective

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

313

# Amazon CloudFront pricing

## Data transfer out

- Charged for the volume of data transferred out from Amazon CloudFront edge location to the internet or to your origin.

## HTTP(S) requests

- Charged for number of HTTP(S) requests.

## Invalidation requests

- No additional charge for the first 1,000 paths that are requested for invalidation each month. Thereafter, \$0.005 per path that is requested for invalidation.

## Dedicated IP custom SSL

- \$600 per month for each custom SSL certificate that is associated with one or more CloudFront distributions that use the Dedicated IP version of custom SSL certificate support.



## Section 6 key takeaways



- A CDN is a globally distributed system of caching servers that accelerates delivery of content.
- Amazon CloudFront is a fast CDN service that securely delivers data, videos, applications, and APIs over a global infrastructure with low latency and high transfer speeds.
- Amazon CloudFront offers many benefits.

# Module summary

In summary, in this module you learned how to:

- Recognize the basics of networking
- Describe virtual networking in the cloud with Amazon VPC
- Label a network diagram
- Design a basic VPC architecture
- Indicate the steps to build a VPC
- Identify security groups
- Create your own VPC and added additional components to it to produce a customized network
- Identify the fundamentals of Amazon Route 53
- Recognize the benefits of Amazon CloudFront

## Complete the knowledge check



## Sample exam question

Which AWS networking service enables a company to create a virtual network within AWS?

- A. AWS Config
- B. Amazon Route 53
- C. AWS Direct Connect
- D. Amazon VPC

## Additional resources

- [Amazon VPC overview page](#)
- [Amazon Virtual Private Cloud Connectivity Options whitepaper](#)
- [One to Many: Evolving VPC Design](#) AWS Architecture blog post
- [Amazon VPC User Guide](#)
- [Amazon CloudFront overview page](#)

# Thank you

© 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. Corrections or feedback on the course, please email us at: [aws-course-feedback@amazon.com](mailto:aws-course-feedback@amazon.com). For all other questions, contact us at: <https://aws.amazon.com/contact-us/aws-training/>. All trademarks are the property of their owners.



AWS Academy Cloud Foundations

## Module 6: Compute

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



# Module overview



## Topics

- Compute services overview
- Amazon EC2
- Amazon EC2 cost optimization
- Container services
- Introduction to AWS Lambda
- Introduction to AWS Elastic Beanstalk

## Activities

- Amazon EC2 versus Managed Service
- Hands-on with AWS Lambda
- Hands-on with AWS Elastic Beanstalk

## Demo

- Recorded demonstration of Amazon EC2

## Lab

- Introduction to Amazon EC2



## Knowledge check

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

322

# Module objectives

After completing this module, you should be able to:

- Provide an overview of different AWS compute services in the cloud
- Demonstrate why to use Amazon Elastic Compute Cloud (Amazon EC2)
- Identify the functionality in the EC2 console
- Perform basic functions in Amazon EC2 to build a virtual computing environment
- Identify Amazon EC2 cost optimization elements
- Demonstrate when to use AWS Elastic Beanstalk
- Demonstrate when to use AWS Lambda
- Identify how to run containerized applications in a cluster of managed servers

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

323

## Module 6: Compute

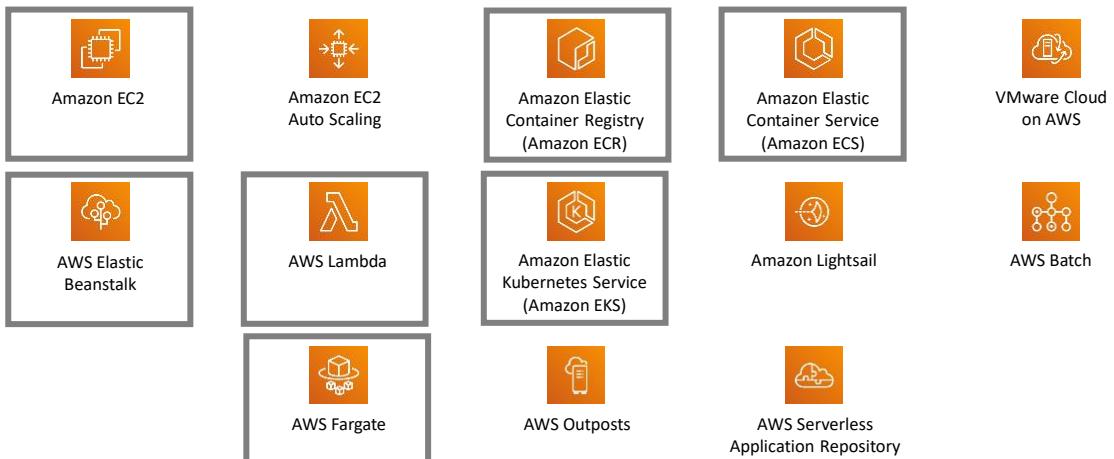
# Section 1: Compute services overview

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## AWS compute services

Amazon Web Services (AWS) offers many compute services. This module will discuss the highlighted services.



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

325

# Categorizing compute services



Services	Key Concepts	Characteristics	Ease of Use
• Amazon EC2	• Infrastructure as a service (IaaS) • Instance-based • <b>Virtual machines</b>	• Provision virtual machines that you can manage as you choose	A familiar concept to many IT professionals.
• AWS Lambda	• <b>Serverless</b> computing • Function-based • Low-cost	• Write and deploy code that runs on a schedule or that can be triggered by events • Use when possible (architect for the cloud)	A relatively new concept for many IT staff members, but easy to use after you learn how.
• Amazon ECS • Amazon EKS • AWS Fargate • Amazon ECR	• <b>Container-based</b> computing • Instance-based	• Spin up and run jobs more quickly	AWS Fargate reduces administrative overhead, but you can use options that give you more control.
• AWS Elastic Beanstalk	• Platform as a service (PaaS) • For <b>web applications</b>	• Focus on your code (building your application) • Can easily tie into other services—databases, Domain Name System (DNS), etc.	Fast and easy to get started.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

326

## Choosing the optimal compute service

- The optimal compute service or services that you use will depend on your use case
- Some aspects to consider –
  - What is your application design?
  - What are your usage patterns?
  - Which configuration settings will you want to manage?
- Selecting the wrong compute solution for an architecture can lead to lower performance efficiency
  - A good starting place—Understand the available compute options

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

327

## Module 6: Compute

### Section 2: Amazon EC2

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Amazon Elastic Compute Cloud (Amazon EC2)

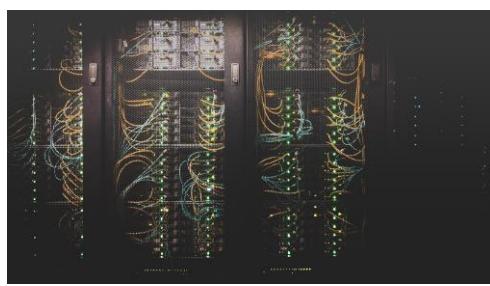
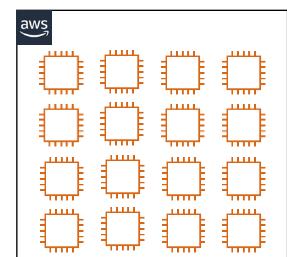


Photo by Taylor Vick on Unsplash

### On-premises servers

#### Example uses of Amazon EC2 instances

- ✓ Application server
- ✓ Web server
- ✓ Database server
- ✓ Game server
- ✓ Mail server
- ✓ Media server
- ✓ Catalog server
- ✓ File server
- ✓ Computing server
- ✓ Proxy server



### Amazon EC2 instances



Photo by panumas nikhomkhai from Pexels

329

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

# Amazon EC2 overview



Amazon  
EC2

- **Amazon Elastic Compute Cloud (Amazon EC2)**

- Provides **virtual machines**—referred to as **EC2 instances**—in the cloud.
- Gives you *full control* over the guest operating system (Windows or Linux) on each instance.
- You can launch instances of any size into an Availability Zone anywhere in the world.
  - Launch instances from **Amazon Machine Images (AMIs)**.
  - Launch instances with a few clicks or a line of code, and they are ready in minutes.
- You can control traffic to and from instances.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

330

## Launching an Amazon EC2 instance

This section of the module walks through **nine key decisions** to make when you create an EC2 instance by using the AWS Management Console **Launch Instance Wizard**.

➤ Along the way, essential Amazon EC2 concepts will be explored.

The screenshot shows the AWS EC2 Management Console dashboard. On the left, there's a sidebar with links like EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES (with sub-links for Instances, Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations), IMAGES (AMIs, Bundle Tasks), and ELASTIC BLOCK STORE (Volumes, Snapshots). The main content area has a heading 'Resources' with a message about using the US East (N. Virginia) region. It lists 0 Running Instances, 0 Dedicated Hosts, 0 Volumes, 1 Key Pairs, and 0 Placement Groups. Below this is a 'Create Instance' section with a 'Launch Instance' button, and a 'Migrate a Machine' section with a 'Get started with CloudEndure Migration' link. At the bottom, there are 'Service Health' and 'Scheduled Events' sections, along with links for Feedback, English (US), and other AWS services.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

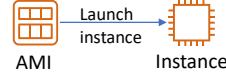
331

# 1. Select an AMI



**Choices made using the Launch Instance Wizard:**

1. **AMI**
2. **Instance Type**
3. **Network settings**
4. **IAM role**
5. **User data**
6. **Storage options**
7. **Tags**
8. **Security group**
9. **Key pair**



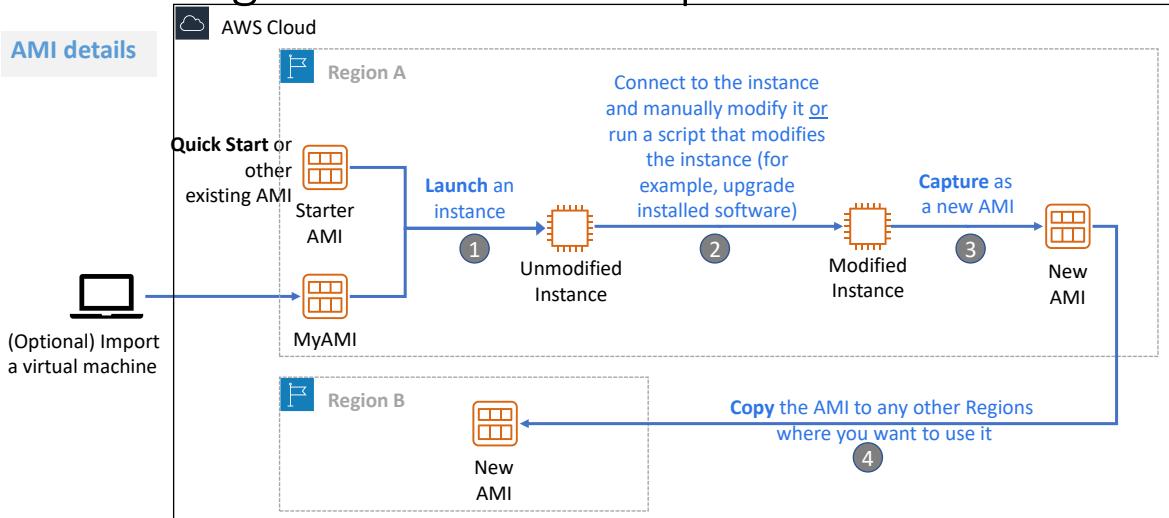
- **Amazon Machine Image (AMI)**
  - Is a template that is used to create an EC2 instance (which is a **virtual machine, or VM**, that runs in the AWS Cloud)
  - Contains a **Windows** or **Linux** operating system
  - Often also has some **software** pre-installed
- **AMI choices:**
  - Quick Start – *Linux and Windows AMIs that are provided by AWS*
  - My AMIs – *Any AMIs that you created*
  - AWS Marketplace – *Pre-configured templates from third parties*
  - Community AMIs – *AMIs shared by others; use at your own risk*



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

332

## Creating a new AMI: Example



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

333

## 2. Select an instance type



### Choices made using the Launch Instance Wizard:

1. AMI
2. Instance Type
3. Network settings
4. IAM role
5. User data
6. Storage options
7. Tags
8. Security group
9. Key pair

- Consider your use case
  - How will the EC2 instance you create be used?
- The **instance type** that you choose determines –
  - Memory (RAM)
  - Processing power (CPU)
  - Disk space and disk type (Storage)
  - Network performance
- Instance type categories –
  - General purpose
  - Compute optimized
  - Memory optimized
  - Storage optimized
  - Accelerated computing
- Instance types offer *family, generation, and size*



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

334

## EC2 instance type naming and sizes

### Instance type details

#### Instance type naming

- Example: **t3.large**
  - T is the family name
  - 3 is the generation number
  - Large is the size

### Example instance sizes

Instance Name	vCPU	Memory (GB)	Storage
t3.nano	2	0.5	EBS-Only
t3.micro	2	1	EBS-Only
t3.small	2	2	EBS-Only
t3.medium	2	4	EBS-Only
t3.large	2	8	EBS-Only
t3.xlarge	4	16	EBS-Only
t3.2xlarge	8	32	EBS-Only

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

335

## Select instance type: Based on use case

Instance type details		General Purpose	Compute Optimized	Memory Optimized	Accelerated Computing	Storage Optimized
Instance Types	a1, m4, m5, t2, t3	c4, c5	r4, r5, x1, z1	f1, g3, g4, p2, p3	d2, h1, i3	
Use Case	Broad	High performance	In-memory databases	Machine learning	Distributed file systems	

## Instance types: Networking features

- The network bandwidth (Gbps) varies by instance type.
  - See [Amazon EC2 Instance Types](#) to compare.
- To maximize networking and bandwidth performance of your instance type:
  - If you have interdependent instances, launch them into a [cluster placement group](#).
  - Enable enhanced networking.
- Enhanced networking types are supported on most instance types.
  - See the [Networking and Storage Features](#) documentation for details.
- Enhanced networking types –
  - Elastic Network Adapter (ENA):** Supports network speeds of up to 100 Gbps.
  - Intel 82599 Virtual Function interface:** Supports network speeds of up to 10 Gbps.

### 3. Specify network settings

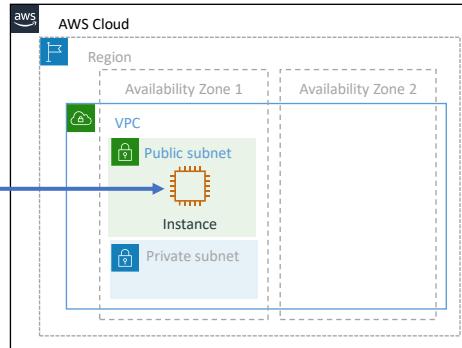


#### Choices made by using the Launch Instance Wizard:

1. AMI
2. Instance Type
3. Network settings
4. IAM role
5. User data
6. Storage options
7. Tags
8. Security group
9. Key pair

- Where should the instance be deployed?
  - Identify the **VPC** and optionally the **subnet**
- Should a **public IP address** be automatically assigned?
  - To make it internet-accessible

*Example: specify to deploy the instance here*



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

338

### 4. Attach IAM role (optional)

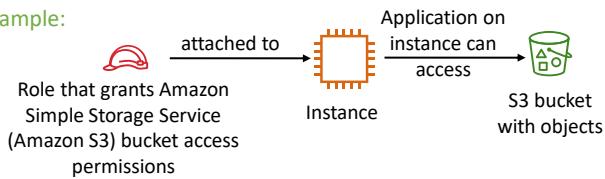


#### Choices made by using the Launch Instance Wizard:

1. AMI
2. Instance Type
3. Network settings
4. IAM role
5. User data
6. Storage options
7. Tags
8. Security group
9. Key pair

- Will software on the EC2 instance need to interact with other AWS services?
  - If yes, attach an appropriate **IAM Role**.
- An AWS Identity and Access Management (IAM) role that is attached to an EC2 instance is kept in an **instance profile**.
- You are *not* restricted to attaching a role only at instance launch.
  - You can also attach a role to an instance that already exists.

*Example:*



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

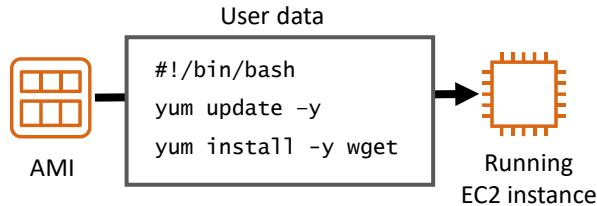
339

## 5. User data script (optional)



### Choices made by using the Launch Instance Wizard:

1. AMI
2. Instance Type
3. Network settings
4. IAM role
5. User data
6. Storage options
7. Tags
8. Security group
9. Key pair



- Optionally specify a user data script at instance launch
- Use **user data** scripts to customize the runtime environment of your instance
  - Script runs the first time the instance starts
- Can be used strategically
  - For example, reduce the number of custom AMIs that you build and maintain

## 6. Specify storage



### Choices made by using the Launch Instance Wizard:

1. AMI
2. Instance Type
3. Network settings
4. IAM role
5. User data
6. Storage options
7. Tags
8. Security group
9. Key pair

- Configure the **root volume**
  - Where the guest operating system is installed
- Attach **additional storage volumes** (optional)
  - AMI might already include more than one volume
- For each volume, specify:
  - The **size** of the disk (in GB)
  - The **volume type**
    - Different types of solid state drives (SSDs) and hard disk drives (HDDs) are available
  - If the volume will be deleted when the instance is terminated
  - If **encryption** should be used



# Amazon EC2 storage options

- **Amazon Elastic Block Store (Amazon EBS) –**
  - Durable, block-level storage volumes.
  - You can stop the instance and start it again, and the data will still be there.
- **Amazon EC2 Instance Store –**
  - Ephemeral storage is provided on disks that are attached to the host computer where the EC2 instance is running.
  - If the instance stops, data stored here is deleted.
- Other options for storage (not for the root volume) –
  - Mount an [Amazon Elastic File System \(Amazon EFS\)](#) file system.
  - Connect to [Amazon Simple Storage Service \(Amazon S3\)](#).

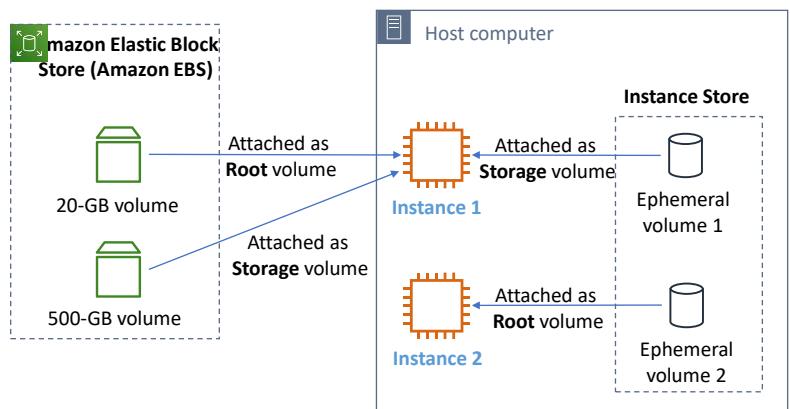
© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

342

## Example storage options



- **Instance 1 characteristics –**
  - It has an **Amazon EBS root volume** type for the operating system.
  - What will happen if the instance is stopped and then started again?
- **Instance 2 characteristics –**
  - It has an **Instance Store root volume** type for the operating system.
  - What will happen if the instance stops (because of user error or a system malfunction)?



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

343

## 7. Add tags



### Choices made by using the Launch Instance Wizard:

1. AMI
2. Instance Type
3. Network settings
4. IAM role
5. User data
6. Storage options
7. Tags
8. Security group
9. Key pair

- A **tag** is a label that you can assign to an AWS resource.
  - Consists of a *key* and an optional *value*.
- Tagging is how you can attach **metadata** to an EC2 instance.
- Potential benefits of tagging—Filtering, automation, cost allocation, and access control.

### Example:

Key	(128 characters maximum)	Value	(256 characters maximum)
Name	WebServer1		
<b>Add another tag</b>		(Up to 50 tags maximum)	

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

344

## 8. Security group settings



### Choices made by using the Launch Instance Wizard:

1. AMI
2. Instance Type
3. Network settings
4. IAM role
5. User data
6. Storage options
7. Tags
8. Security group
9. Key pair

- A **security group** is a **set of firewall rules** that control traffic to the instance.
  - It exists *outside* of the instance's guest OS.
- Create **rules** that specify the **source** and which **ports** that network communications can use.
  - Specify the **port** number and the **protocol**, such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP).
  - Specify the **source** (for example, an IP address or another security group) that is allowed to use the rule.

Type	Protocol	Port Range	Source
SSH	TCP	22	My IP 72.21.198.67/32

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

345

## 9. Identify or create the key pair



### Choices made by using the Launch Instance Wizard:

1. AMI
2. Instance Type
3. Network settings
4. IAM role
5. User data
6. Storage options
7. Tags
8. Security group
9. Key pair

- At instance launch, you specify an existing key pair *or* create a new key pair.
- A **key pair** consists of –
  - A **public key** that AWS stores.
  - A **private key** file that you store.
- It enables secure connections to the instance.
- **For Windows AMIs –**
  - Use the private key to obtain the administrator password that you need to log in to your instance.
- **For Linux AMIs –**
  - Use the private key to use SSH to securely connect to your instance.



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

346

## Amazon EC2 console view of a running EC2 instance



The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with navigation links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, AMIs, and Bundle Tasks. The main content area has tabs for Launch Instance, Connect, and Actions. Below that is a search bar and a table with one row. The table columns include Name, Instance ID, Instance Type, Instance State, Status Checks, Public DNS (IPv4), and IPv4 Public IP. The instance listed is i-092b6f3efba959a53, which is running. Below the table, there's a detailed view for the same instance, showing fields like Description, Status Checks, Monitoring, and Tags. The instance details include its ID, state, type, availability zone, security groups, and network interfaces.

Name	Instance ID	Instance Type	Instance State	Status Checks	Public DNS (IPv4)	IPv4 Public IP
	i-092b6f3efba959a53	t2.micro	running	Initializing	ec2-54-159-171-63.compute-1.amazonaws.com	54.159.171.63

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

347

## Another option: Launch an EC2 instance with the AWS Command Line Interface



- EC2 instances can also be created programmatically.
- This example shows how simple the command can be.
  - This command assumes that the key pair and security group already exist.
  - More options could be specified. See the [AWS CLI Command Reference](#) for details.

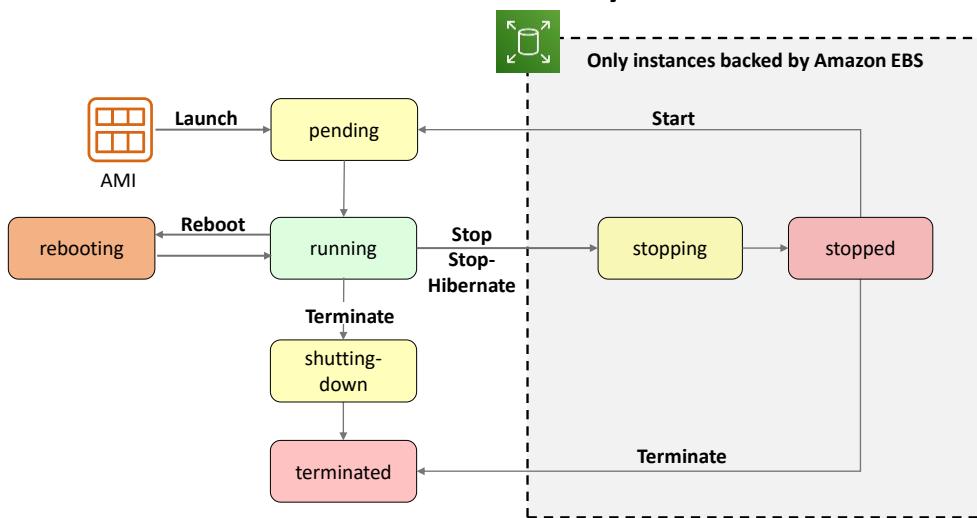


AWS Command Line Interface (AWS CLI)

### Example command:

```
aws ec2 run-instances \
--image-id ami-1a2b3c4d \
--count 1 \
--instance-type c3.large \
--key-name MyKeyPair \
--security-groups MySecurityGroup \
--region us-east-1
```

## Amazon EC2 instance lifecycle



# Consider using an Elastic IP address



- **Rebooting** an instance will *not* change any IP addresses or DNS hostnames.
- When an instance is **stopped** and then **started** again –
  - The *public IPv4* address and *external DNS hostname* will change.
  - The *private IPv4* address and *internal DNS hostname* do *not* change.
- If you require a persistent public IP address –
  - Associate an **Elastic IP address** with the instance.
- Elastic IP address characteristics –
  - Can be associated with instances in the Region as needed.
  - Remains allocated to your account until you choose to release it.



Elastic IP  
Address

## EC2 instance metadata

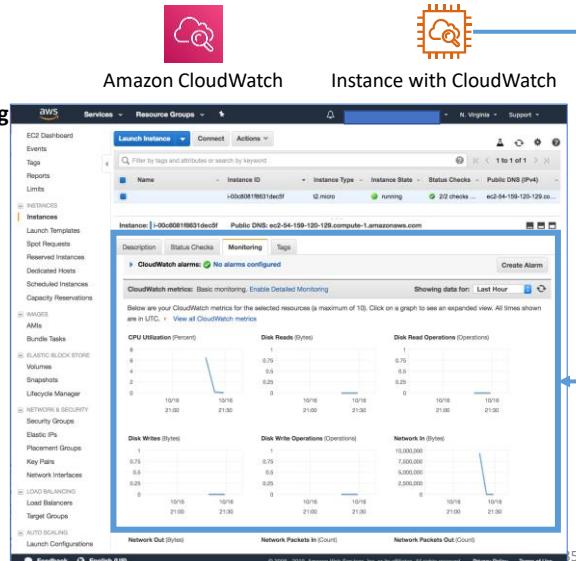
- **Instance metadata** is data about your instance.
- While you are connected to the instance, you can view it –
  - In a browser: `http://169.254.169.254/latest/meta-data/`
  - In a terminal window: `curl http://169.254.169.254/latest/meta-data/`
- Example retrievable values –
  - Public IP address, private IP address, public hostname, instance ID, security groups, Region, Availability Zone.
  - Any user data specified at instance launch can also be accessed at: `http://169.254.169.254/latest/user-data/`
- It can be used to configure or manage a running instance.
  - For example, author a configuration script that reads the metadata and uses it to configure applications or OS settings.

# Amazon CloudWatch for monitoring



- Use **Amazon CloudWatch** to monitor EC2 instances
  - Provides near-real-time metrics
  - Provides charts in the Amazon EC2 console **Monitoring** tab that you can view
  - Maintains 15 months of historical data
- **Basic monitoring**
  - Default, no additional cost
  - Metric data sent to CloudWatch every 5 minutes

- **Detailed monitoring**
  - Fixed monthly rate for seven pre-selected metrics
  - Metric data delivered every 1 minute



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

53

## Section 2 key takeaways



- **Amazon EC2** enables you to run Windows and Linux **virtual machines** in the cloud.
- You launch **EC2 instances** from an **AMI** template into a VPC in your account.
- You can choose from many **instance types**. Each instance type offers different combinations of CPU, RAM, storage, and networking capabilities.
- You can configure **security groups** to control access to instances (specify allowed ports and source).
- **User data** enables you to specify a script to run the first time that an instance launches.
- Only **instances that are backed by Amazon EBS** can be stopped.
- You can use **Amazon CloudWatch** to capture and review metrics on EC2 instances.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

354

# Recorded Amazon EC2 demonstration

355



aws academy

## Set up demo

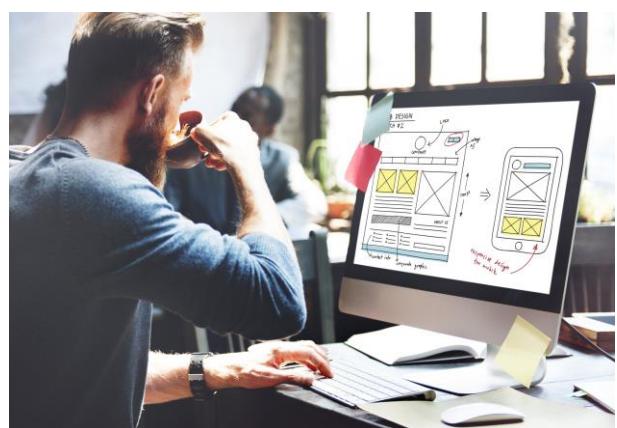
Amazon Elastic Compute Cloud  
(Amazon EC2)



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

# Lab 3: Introduction to Amazon EC2

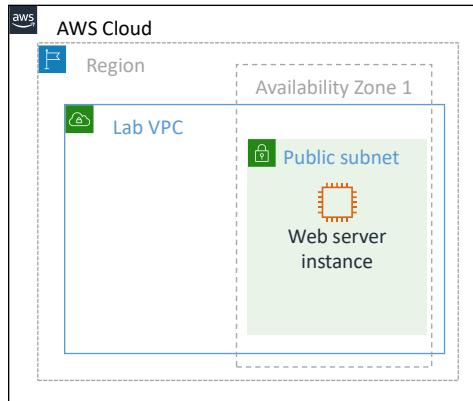
356



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Lab 3 scenario

In this lab, you will launch and configure your first virtual machine that runs on Amazon EC2.



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

357

## Lab 3: Tasks

- Task 1 – Launch Your Amazon EC2 Instance
- Task 2 – Monitor Your Instance
- Task 3 – Update Your Security Group and Access the Web Server
- Task 4 – Resize Your Instance: Instance Type and EBS Volume
- Task 5 – Explore EC2 Limits
- Task 6 – Test Termination Protection

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

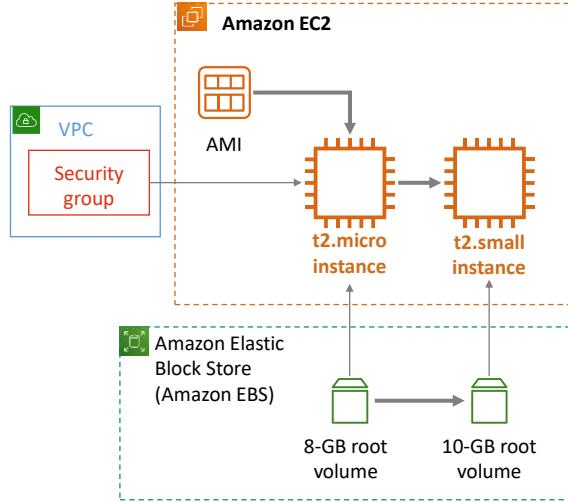
358

# Lab 3: Final product



By the end of the lab, you will have:

1. Launched an instance that is configured as a web server
2. Viewed the instance system log
3. Reconfigured a security group
4. Modified the instance type and root volume size



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

359

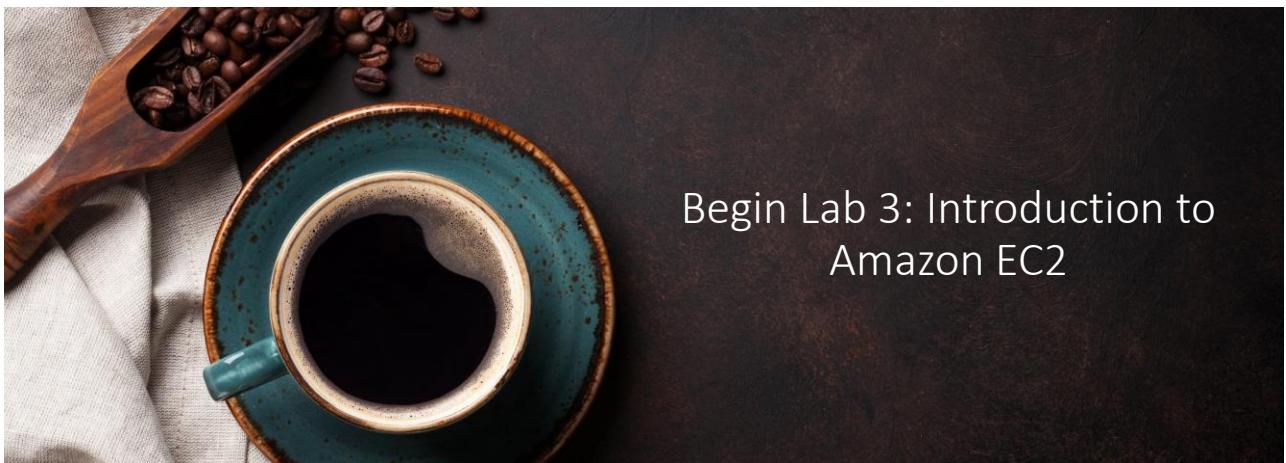


~ 35 minutes



[Begin Lab 3: Introduction to AWS IAM](#)

Begin Lab 3: Introduction to Amazon EC2



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

360



## Lab debrief: Key takeaways



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

361

## Activity: Amazon EC2

362



Photo by Pixabay from Pexels.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Activity: Gather information

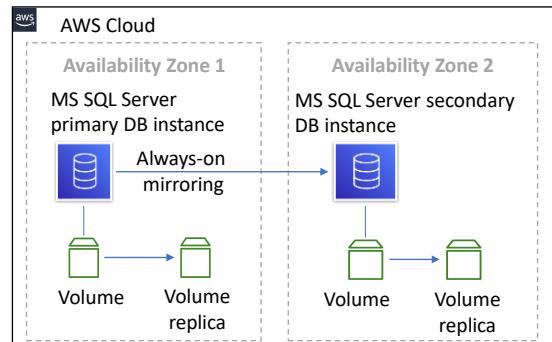
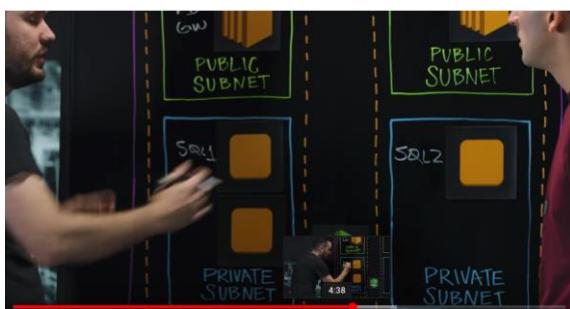


Amazon EC2



Amazon RDS

**AWS Quick Starts**  
Automated, gold-standard deployments in the AWS Cloud



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

363

## Activity: Check your understanding

- Between Amazon EC2 or Amazon RDS, which provides a managed service? What does *managed service* mean?
  - ANSWER:** Amazon RDS provides a managed service. Amazon RDS handles provisioning, installation and patching, automated backups, restoring snapshots from points in time, high availability, and monitoring.
- Name at least one advantage of deploying Microsoft SQL Server on Amazon EC2 instead of Amazon RDS.
  - ANSWER:** Amazon EC2 offers complete control over every configuration, the OS, and the software stack.
- What advantage does the Quick Start provide over a manual installation on Amazon EC2?
  - ANSWER:** The Quick Start is a reference architecture with proven best practices built into the design.
- Which deployment option offers the best approach for all use cases?
  - ANSWER:** Neither. The correct deployment option depends on your specific needs.
- Which approach costs more: using Amazon EC2 or using Amazon RDS?
  - ANSWER:** It depends. Managing the database deployment on Amazon EC2 requires more customer oversight and time. If time is your priority, then Amazon RDS might be less expensive. If you have in-house expertise, Amazon EC2 might be more cost-effective.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

364

## Module 6: Compute

# Section 3: Amazon EC2 cost optimization

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



# Amazon EC2 pricing models



## On-Demand Instances

- Pay by the hour
- No long-term commitments.
- Eligible for the [AWS Free Tier](#).

## Dedicated Hosts

- A physical server with EC2 instance capacity fully dedicated to your use.

## Dedicated Instances

- Instances that run in a VPC on hardware that is dedicated to a single customer.

## Reserved Instances

- Full, partial, or no upfront payment for instance you reserve.
- Discount on hourly charge for that instance.
- 1-year or 3-year term.

## Scheduled Reserved Instances

- Purchase a capacity reservation that is always available on a recurring schedule you specify.
- 1-year term.

## Spot Instances

- Instances run as long as they are available and your bid is above the Spot Instance price.
- They can be interrupted by AWS with a 2-minute notification.
- Interruption options include terminated, stopped or hibernated.
- Prices can be significantly less expensive compared to On-Demand Instances
- Good choice when you have flexibility in when your applications can run.

*Per second billing* available for On-Demand Instances, Reserved Instances, and Spot Instances that run Amazon Linux or Ubuntu.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

366

## Amazon EC2 pricing models: Benefits



On-Demand Instances	Spot Instances	Reserved Instances	Dedicated Hosts
<ul style="list-style-type: none"> <li>Low cost and flexibility</li> </ul>	<ul style="list-style-type: none"> <li>Large scale, dynamic workload</li> </ul>	<ul style="list-style-type: none"> <li>Predictability ensures compute capacity is available when needed</li> </ul>	<ul style="list-style-type: none"> <li>Save money on licensing costs</li> <li>Help meet compliance and regulatory requirements</li> </ul>

## Amazon EC2 pricing models: Use cases



Spiky Workloads



Time-Insensitive Workloads



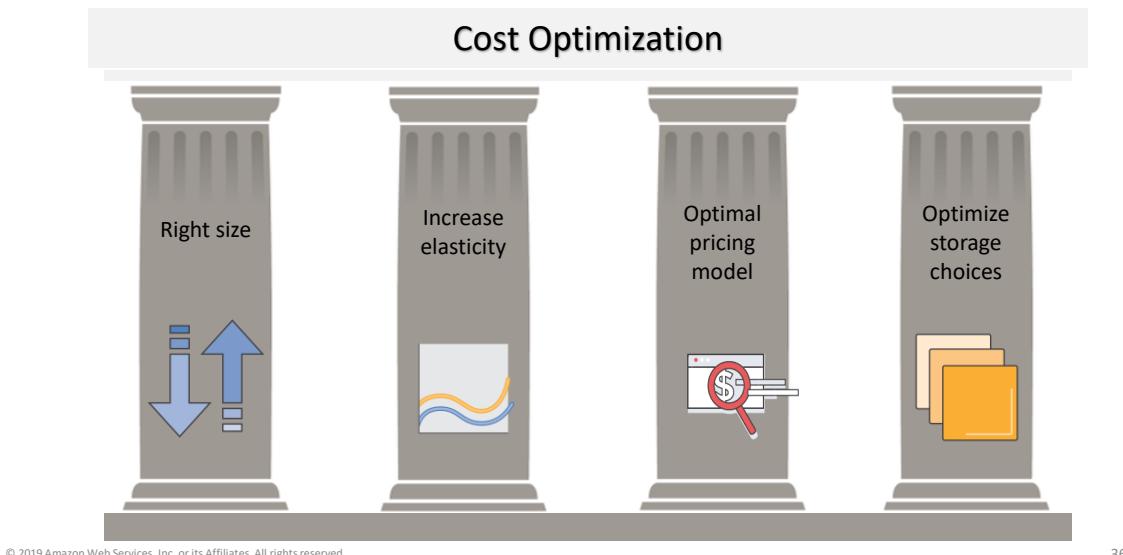
Steady-State Workloads



Highly Sensitive Workloads

On-Demand Instances	Spot Instances	Reserved Instances	Dedicated Hosts
<ul style="list-style-type: none"> <li>Short-term, spiky, or unpredictable workloads</li> <li>Application development or testing</li> </ul>	<ul style="list-style-type: none"> <li>Applications with flexible start and end times</li> <li>Applications only feasible at very low compute prices</li> <li>Users with urgent computing needs for large amounts of additional capacity</li> </ul>	<ul style="list-style-type: none"> <li>Steady state or predictable usage workloads</li> <li>Applications that require reserved capacity, including disaster recovery</li> <li>Users able to make upfront payments to reduce total computing costs even further</li> </ul>	<ul style="list-style-type: none"> <li>Bring your own license (BYOL)</li> <li>Compliance and regulatory restrictions</li> <li>Usage and licensing tracking</li> <li>Control instance placement</li> </ul>

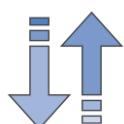
# The four pillars of cost optimization



## Pillar 1: Right size

### Pillars:

1. Right size
2. Increase elasticity
3. Optimal pricing model
4. Optimize storage choices



### ✓ Provision instances to match the need

- CPU, memory, storage, and network throughput
- Select appropriate [instance types](#) for your use

### ✓ Use Amazon CloudWatch metrics

- How idle are instances? When?
- Downsize instances

### ✓ Best practice: Right size, then reserve

## Pillar 2: Increase elasticity

### Pillars:

1. Right-Size
- 2. Increase Elasticity**
3. Optimal pricing model
4. Optimize storage choices



✓ **Stop or hibernate** Amazon EBS-backed instances that are not actively in use

- Example: non-production development or test instances

✓ Use **automatic scaling** to match needs based on usage

- Automated and time-based elasticity

## Pillar 3: Optimal pricing model

### Pillars:

1. Right-Size
2. Increase Elasticity
- 3. Optimal pricing model**
4. Optimize storage choices



✓ Leverage the right pricing model for your use case

- Consider your usage patterns

✓ Optimize and *combine* purchase types

✓ Examples:

- Use **On-Demand Instances** and **Spot Instances** for variable workloads
- Use **Reserved Instances** for predictable workloads

✓ Consider serverless solutions (AWS Lambda)

## Pillar 4: Optimize storage choices

### Pillars:

1. Right-Size
2. Increase Elasticity
3. Optimal pricing model
- 4. Optimize storage choices**



- ✓ Reduce costs while maintaining storage performance and availability
- ✓ Resize EBS volumes
- ✓ Change EBS volume types
  - ✓ Can you meet performance requirements with less expensive storage?
  - ✓ Example: [Amazon EBS Throughput Optimized HDD \(st1\)](#) storage typically costs half as much as the default [General Purpose SSD \(gp2\)](#) storage option.
- ✓ Delete EBS snapshots that are no longer needed
- ✓ Identify the most appropriate destination for specific types of data
  - ✓ Does the application need the instance to reside on Amazon EBS?
  - ✓ Amazon S3 storage options with lifecycle policies can reduce costs

## Measure, monitor, and improve

- Cost optimization is an ongoing process.
- Recommendations –
  - Define and enforce [cost allocation tagging](#).
  - Define metrics, set targets, and review regularly.
  - Encourage teams to [architect for cost](#).
  - Assign the responsibility of optimization to an individual or to a team.



## Section 3 key takeaways



375



- **Amazon EC2 pricing models** include On-Demand Instances, Reserved Instances, Spot Instances, Dedicated Instances, and Dedicated Hosts.
- **Spot Instances** can be interrupted with a 2-minute notification. However, they can offer significant cost savings over On-Demand Instances.
- The **four pillars of cost optimization** are:
  - Right size
  - Increase elasticity
  - Optimal pricing model
  - Optimize storage choices

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Module 6: Compute

## Section 4: Container services

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



# Container basics

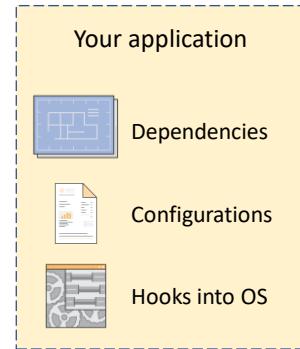


- **Containers** are a method of operating system virtualization.

- Benefits –

- Repeatable.
- Self-contained environments.
- Software runs the same in different environments.
  - Developer's laptop, test, production.
- Faster to launch and stop or terminate than virtual machines

Your Container



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

377

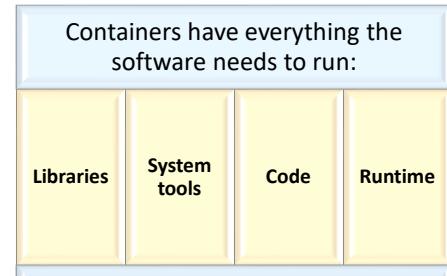
# What is Docker?



- **Docker** is a software platform that enables you to build, test, and deploy applications quickly.
- You run containers on Docker.
  - Containers are created from a template called an *image*.
- A **container** has everything a software application needs to run.



Container

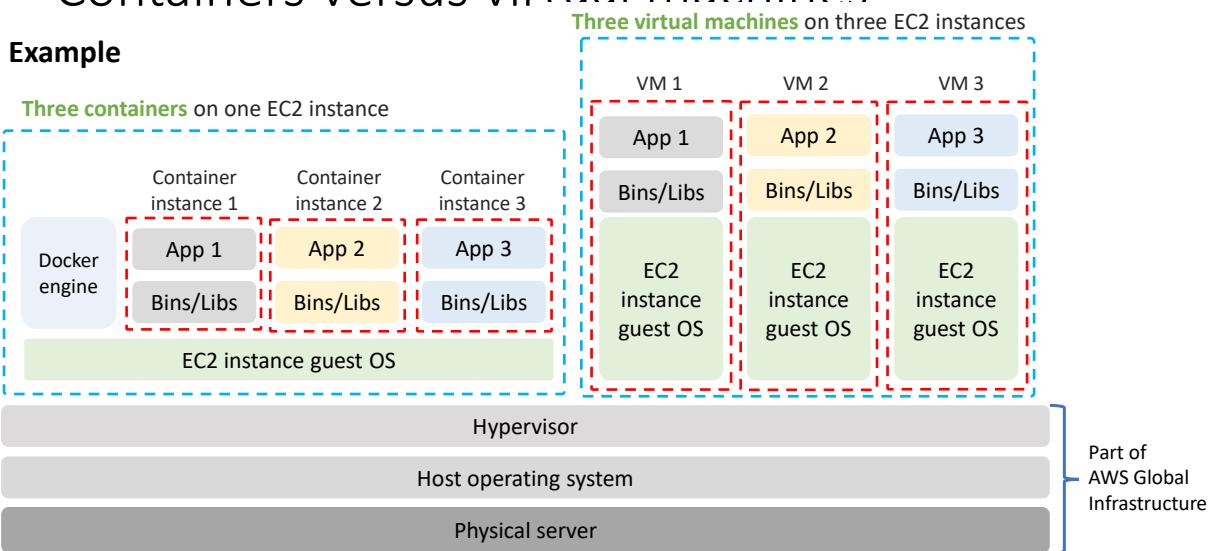


© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

378

# Containers versus virtual machines

## Example



© 2019 Amazon Web Services, Inc. or Its Affiliates. All rights reserved.

379

## Amazon Elastic Container Service (Amazon ECS)

- **Amazon Elastic Container Service (Amazon ECS)** –
  - A highly scalable, fast, **container management service**
- **Key benefits** –
  - Orchestrates the running of Docker containers
  - Maintains and scales the fleet of nodes that run your containers
  - Removes the complexity of standing up the infrastructure
- **Integrated with features that are familiar to Amazon EC2 service users** –
  - Elastic Load Balancing
  - Amazon EC2 security groups
  - Amazon EBS volumes
  - IAM roles

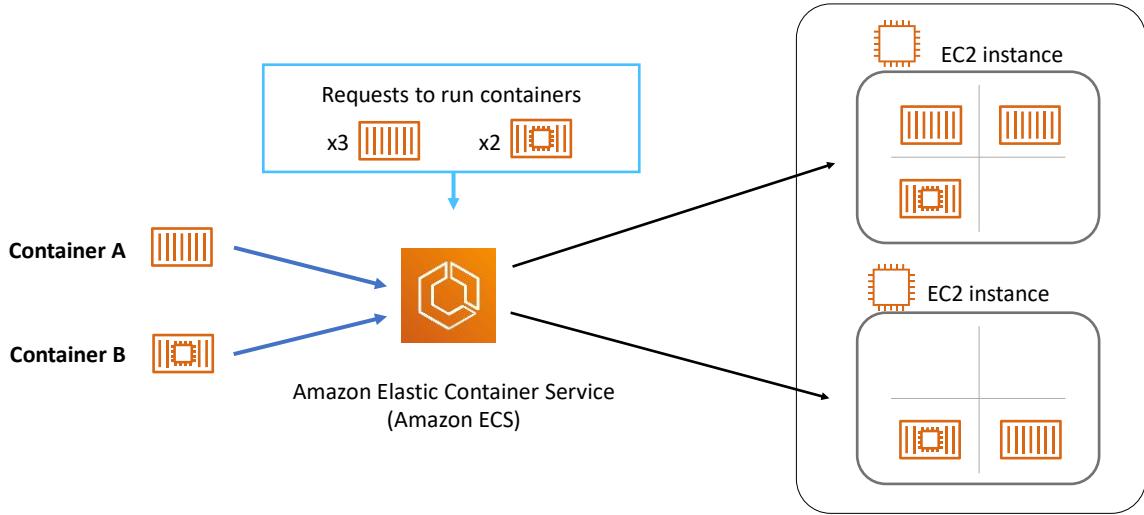


Amazon Elastic  
Container Service

© 2019 Amazon Web Services, Inc. or Its Affiliates. All rights reserved.

380

# Amazon ECS orchestrates containers



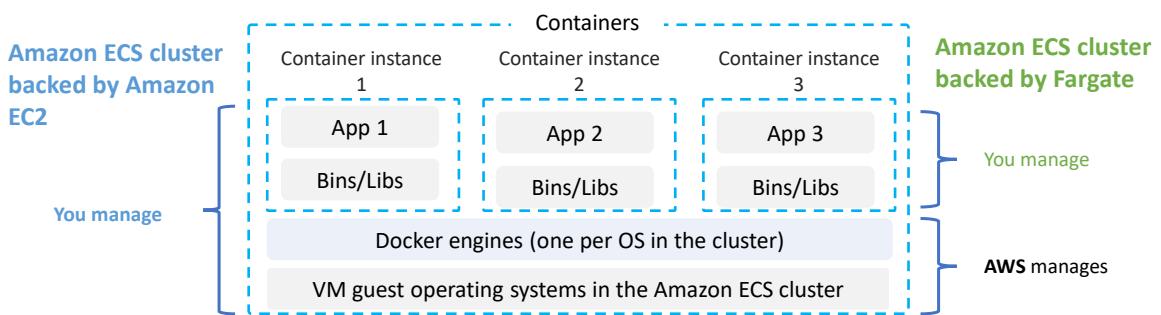
© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

ECS cluster

381

## Amazon ECS cluster options

- **Key question:** Do *you* want to manage the Amazon ECS cluster that runs the containers?
  - If **yes**, create an **Amazon ECS cluster backed by Amazon EC2** (provides more granular control over infrastructure)
  - If **no**, create an **Amazon ECS cluster backed by AWS Fargate** (easier to maintain, focus on your applications)



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

382

# What is Kubernetes?

- Kubernetes is open source software for container orchestration.
  - Deploy and **manage containerized applications at scale.**
  - The same toolset can be used on premises and in the cloud.
- Complements Docker.
  - Docker enables you to run multiple containers on a single OS host.
  - Kubernetes **orchestrates** multiple Docker hosts (nodes).
- Automates –
  - Container provisioning.
  - Networking.
  - Load distribution.
  - Scaling.

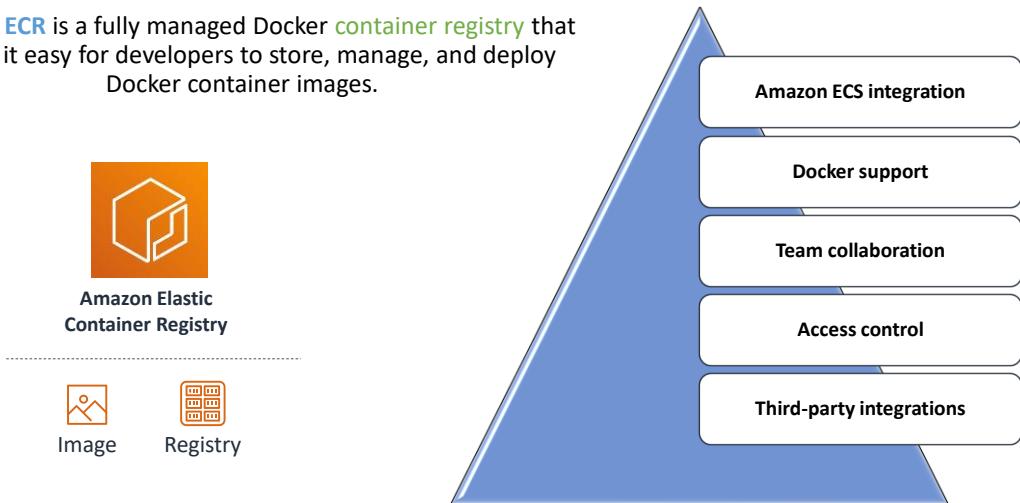
## Amazon Elastic Kubernetes Service (Amazon EKS)

- Amazon Elastic Kubernetes Service (**Amazon EKS**)
  - Enables you to run Kubernetes on AWS
  - Certified Kubernetes conformant (supports easy migration)
  - Supports Linux and Windows containers
  - Compatible with Kubernetes community tools and supports popular Kubernetes add-ons
- Use Amazon EKS to –
  - Manage clusters of Amazon EC2 compute instances
  - Run containers that are orchestrated by Kubernetes on those instances



## Amazon Elastic Container Registry (Amazon ECR)

**Amazon ECR** is a fully managed Docker **container registry** that makes it easy for developers to store, manage, and deploy Docker container images.



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.  
© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

385

## Section 4 key takeaways

386



- **Containers** can hold everything that an application needs to run.
- **Docker** is a software platform that packages software into containers.
  - A single application can span multiple containers.
- Amazon Elastic Container Service (**Amazon ECS**) orchestrates the running of Docker containers.
- **Kubernetes** is open source software for container orchestration.
- Amazon Elastic Kubernetes Service (**Amazon EKS**) enables you to run Kubernetes on AWS
- Amazon Elastic Container Registry (**Amazon ECR**) enables you to store, manage, and deploy your Docker containers.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

**Module 6: Compute**

## Section 5: Introduction to AWS Lambda

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

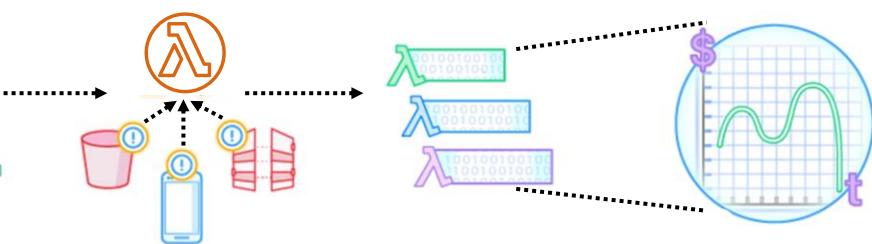


387

## AWS Lambda: Run code without servers

AWS Lambda is a **serverless** compute service.

### Upload your code



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

388

# Benefits of Lambda



AWS  
Lambda



It supports multiple programming languages



Completely automated administration



Built-in fault tolerance



It supports the orchestration of multiple functions



Pay-per-use pricing

# AWS Lambda event sources

## Event sources



Configure other AWS services as **event sources** to invoke your function as shown here.

Alternatively, invoke a Lambda function from the Lambda console, AWS SDK, or AWS CLI.



Lambda  
function



AWS Lambda

Running of your code  
(only when triggered)

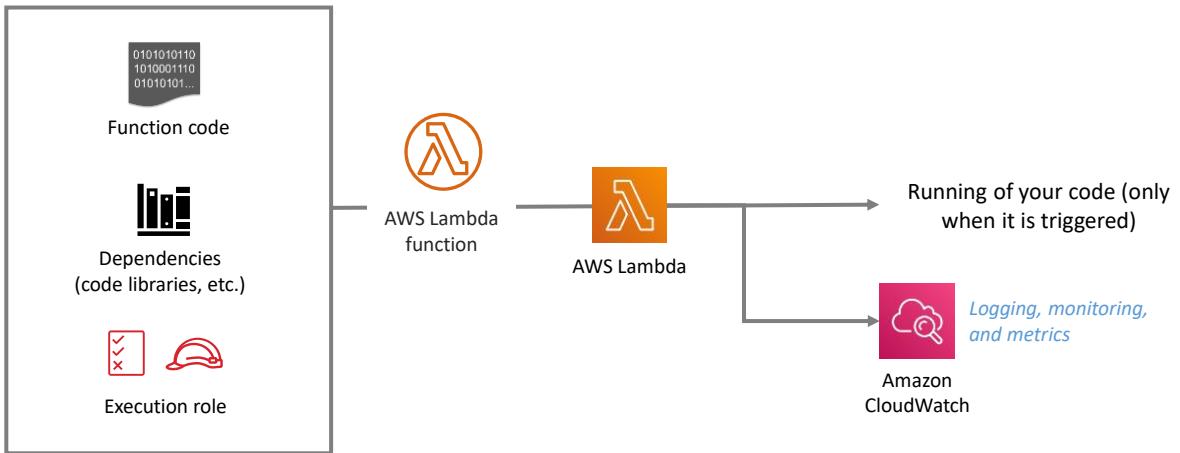


Amazon  
CloudWatch

*Logging, monitoring,  
and metrics*

# AWS Lambda function configuration

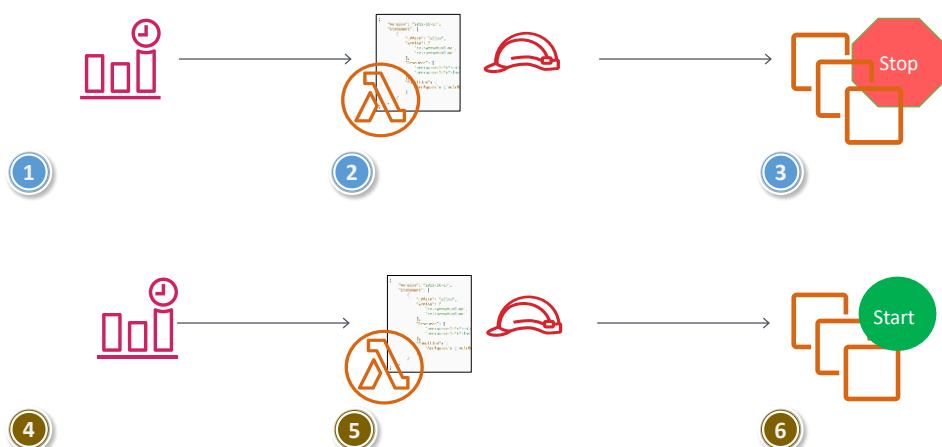
## Lambda function configuration



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

391

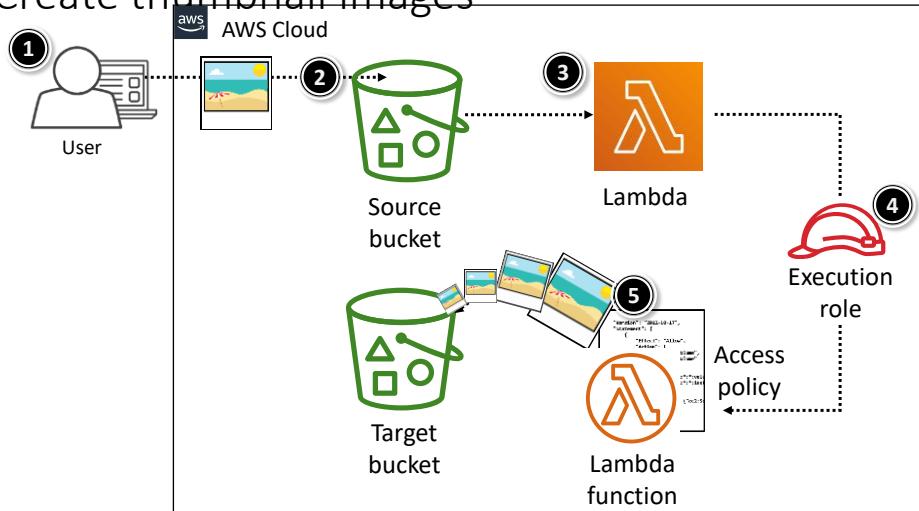
## Schedule-based Lambda function example: Start and stop EC2 instances



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.  
© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

392

## Event-based Lambda function example: Create thumbnail images



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

393

## AWS Lambda quotas

### Soft limits per Region:

- Concurrent executions = 1,000
- Function and layer storage = 75 GB

### Hard limits for individual functions:

- Maximum function memory allocation = 3,008 MB
- Function timeout = 15 minutes
- Deployment package size = 250 MB unzipped, including layers

Additional limits also exist. Details are in the [AWS Lambda quotas](#) documentation.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.  
© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

394

## Section 5 key takeaways



395



- **Serverless computing** enables you to build and run applications and services without provisioning or managing servers.
- **AWS Lambda** is a serverless compute service that provides built-in fault tolerance and automatic scaling.
- An **event source** is an AWS service or developer-created application that triggers a Lambda function to run.
- The maximum memory allocation for a single Lambda function is 3,008 MB.
- The maximum run time for a Lambda function is 15 minutes.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Activity: Create an AWS Lambda Stopinator Function

396



### To complete this activity:

- Go to the hands-on lab environment and launch the AWS Lambda activity.
- Follow the instructions that are provided in the hands-on lab environment.

Photo by Pixabay from Pexels.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Activity debrief: key takeaways



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

397

### Module 6: Compute

## Section 6: Introduction to AWS Elastic Beanstalk

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

# AWS Elastic Beanstalk

- An easy way to get **web applications** up and running
- A **managed service** that automatically handles –
  - Infrastructure provisioning and configuration
  - Deployment
  - Load balancing
  - Automatic scaling
  - Health monitoring
  - Analysis and debugging
  - Logging
- No additional charge for Elastic Beanstalk
  - Pay only for the underlying resources that are used



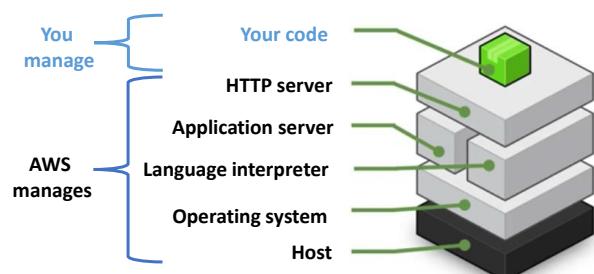
**AWS Elastic Beanstalk**

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

399

## AWS Elastic Beanstalk deployments

- It supports web applications written for common platforms
  - Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker
- You upload your code
  - Elastic Beanstalk automatically handles the deployment
  - Deploys on servers such as Apache, NGINX, Passenger, Puma, and Microsoft Internet Information Services (IIS)



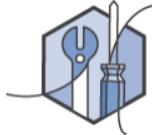
© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

400

# Benefits of Elastic Beanstalk



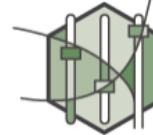
Fast and simple to start using



Developer productivity



Difficult to outgrow



Complete resource control



## Activity: AWS Elastic Beanstalk

### To complete this activity:

- Go to the hands-on lab environment and launch the AWS Elastic Beanstalk activity.
- Follow the instructions that are provided in the hands-on lab environment.



## Activity debrief: Key takeaways



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

403

## Section 6 key takeaways



404

- **AWS Elastic Beanstalk** enhances developer productivity.
  - Simplifies the process of deploying your application.
  - Reduces management complexity.
- Elastic Beanstalk supports **Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker**
- There is no charge for Elastic Beanstalk. Pay only for the AWS resources that you use.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Module 6: Compute

## Module wrap-up

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Module summary

In summary, in this module, you learned how to:

- Provide an overview of different AWS compute services in the cloud
- Demonstrate why to use Amazon Elastic Compute Cloud (Amazon EC2)
- Identify the functionality in the Amazon EC2 console
- Perform basic functions in Amazon EC2 to build a virtual computing environment
- Identify Amazon EC2 cost optimization elements
- Demonstrate when to use AWS Elastic Beanstalk
- Demonstrate when to use AWS Lambda
- Identify how to run containerized applications in a cluster of managed servers

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

406

## Complete the knowledge check



## Sample exam question

Which AWS service helps developers quickly deploy resources which can make use of different programming languages, such as .NET and Java?

- A. AWS CloudFormation
- B. AWS SQS
- C. AWS Elastic Beanstalk
- D. Amazon Elastic Compute Cloud (Amazon EC2)

# Additional resources

- [Amazon EC2 Documentation](#)
- [Amazon EC2 Pricing](#)
- [Amazon ECS Workshop](#)
- [Running Containers on AWS](#)
- [Amazon EKS Workshop](#)
- [AWS Lambda Documentation](#)
- [AWS Elastic Beanstalk Documentation](#)
- [Cost Optimization Playbook](#)

Thank you

AWS Academy Cloud Foundations

# Module 7: Storage

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Module overview



### Topics

- Amazon Elastic Block Store (Amazon EBS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Elastic File System (Amazon EFS)
- Amazon Simple Storage Service Glacier

### Demos

- Amazon EBS console
- Amazon S3 console
- Amazon EFS console
- Amazon S3 Glacier console

### Lab

- Working with Amazon EBS

### Activities

- Storage solution case study



### Knowledge check

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

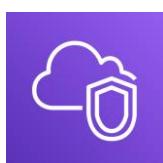
412

# Module objectives

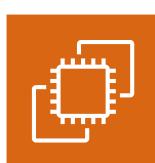
After completing this module, you should be able to:

- Identify the different types of storage
- Explain Amazon S3
- Identify the functionality in Amazon S3
- Explain Amazon EBS
- Identify the functionality in Amazon EBS
- Perform functions in Amazon EBS to build an Amazon EC2 storage solution
- Explain Amazon EFS
- Identify the functionality in Amazon EFS
- Explain Amazon S3 Glacier
- Identify the functionality in Amazon S3 Glacier
- Differentiate between Amazon EBS, Amazon S3, Amazon EFS, and Amazon S3 Glacier

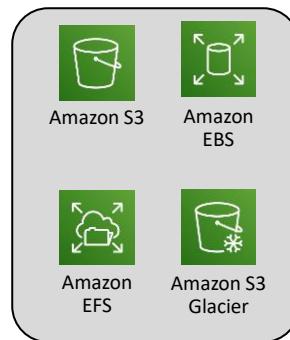
# Core AWS services



**Amazon Virtual Private Cloud (Amazon VPC)**



**Amazon Elastic Compute Cloud (Amazon EC2)**



**Storage**



**AWS Identity and Access Management (IAM)**



**Database**

## Module 7: Storage

# Section 1: Amazon Elastic Block Store (Amazon EBS)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



# Storage



## Amazon Elastic Block Store (Amazon EBS)

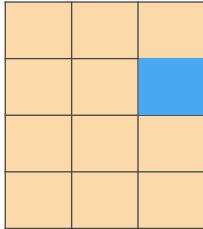
© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

416

## AWS storage options: Block storage versus object storage

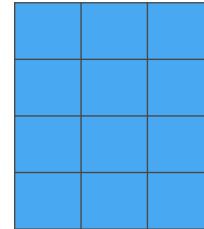


What if you want to change one character in a 1-GB file?



**Block storage**

Change one block (piece of the file) that contains the character



**Object storage**

Entire file must be updated

## Amazon EBS

Amazon EBS enables you to **create individual storage volumes** and **attach them** to an Amazon EC2 instance:

- Amazon EBS offers block-level storage.
- Volumes are automatically replicated within its Availability Zone.
- It can be backed up automatically to Amazon S3 through snapshots.
- Uses include –
  - Boot volumes and storage for Amazon Elastic Compute Cloud (Amazon EC2) instances
  - Data storage with a file system
  - Database hosts
  - Enterprise applications

# Amazon EBS volume types

	Solid State Drives (SSD)		Hard Disk Drives (HDD)	
	General Purpose	Provisioned IOPS	Throughput-Optimized	Cold
Maximum Volume Size	16 TiB	16 TiB	16 TiB	16 TiB
Maximum IOPS/Volume	16,000	64,000	500	250
Maximum Throughput/Volume	250 MiB/s	1,000 MiB/s	500 MiB/s	250 MiB/s

# Amazon EBS volume type use cases

Solid State Drives (SSD)		Hard Disk Drives (HDD)	
General Purpose	Provisioned IOPS	Throughput-Optimized	Cold
<ul style="list-style-type: none"> <li>This type is recommended for most workloads</li> <li>System boot volumes</li> <li>Virtual desktops</li> <li>Low-latency interactive applications</li> <li>Development and test environments</li> </ul>	<ul style="list-style-type: none"> <li>Critical business applications that require sustained IOPS performance, or more than 16,000 IOPS or 250 MiB/second of throughput per volume</li> <li>Large database workloads</li> </ul>	<ul style="list-style-type: none"> <li>Streaming workloads that require consistent, fast throughput at a low price</li> <li>Big data</li> <li>Data warehouses</li> <li>Log processing</li> <li>It cannot be a boot volume</li> </ul>	<ul style="list-style-type: none"> <li>Throughput-oriented storage for large volumes of data that is infrequently accessed</li> <li>Scenarios where the lowest storage cost is important</li> <li>It cannot be a boot volume</li> </ul>

# Amazon EBS features

- **Snapshots –**
  - Point-in-time snapshots
  - Recreate a new volume at any time
- **Encryption –**
  - Encrypted Amazon EBS volumes
  - No additional cost
- **Elasticity –**
  - Increase capacity
  - Change to different types



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Amazon EBS: Volumes, IOPS, and pricing

### 1. Volumes –

- Amazon EBS volumes persist independently from the instance.
- All volume types are charged by the amount that is provisioned per month.

### 2. IOPS –

- General Purpose SSD:
  - Charged by the amount that you provision in GB per month until storage is released.
- Magnetic:
  - Charged by the number of requests to the volume.
- Provisioned IOPS SSD:
  - Charged by the amount that you provision in IOPS (multiplied by the percentage of days that you provision for the month).

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

422

# Amazon EBS: Snapshots and data transfer

### 3. Snapshots –

- Added cost of Amazon EBS snapshots to Amazon S3 is per GB-month of data stored.

### 4. Data transfer –

- Inbound data transfer is free.
- Outbound data transfer across Regions incurs charges.



## Section 1 key takeaways



### Amazon EBS features:

- Persistent and customizable block storage for Amazon EC2
- HDD and SSD types
- Replicated in the same Availability Zone
- Easy and transparent encryption
- Elastic volumes
- Back up by using snapshots

## Recorded demo: Amazon Elastic Block Store

425



aws academy

### Set up demo

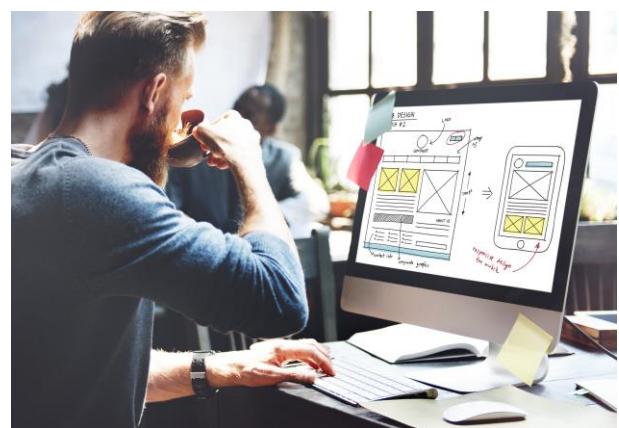
Amazon Elastic Block Store (EBS)



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Lab 4: Working with Amazon EBS

426



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Lab 4: Scenario

This lab is designed to show you how to create an Amazon EBS volume. After you create the volume, you will attach the volume to an Amazon EC2 instance, configure the instance to use a virtual disk, create a snapshot and then restore from the snapshot.



## Lab 4: Final product





## Lab debrief: Key takeaways



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

429

### Module 7: Storage

## Section 2: Amazon Simple Storage Service (Amazon S3)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

# Storage



## Amazon Simple Storage Service (Amazon S3)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

431

## Amazon S3 overview

- Data is stored as objects in buckets
- Virtually unlimited storage
  - Single object is limited to 5 TB
- Designed for 11 9s of durability
- Granular access to bucket and objects

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

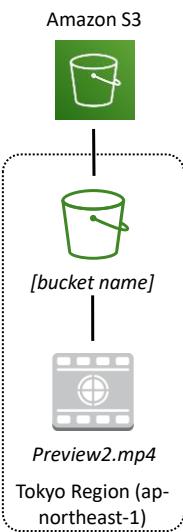
432

# Amazon S3 storage classes

Amazon S3 offers a range of object-level storage classes that are designed for different use cases:

- Amazon S3 Standard
- Amazon S3 Intelligent-Tiering
- Amazon S3 Standard-Infrequent Access (Amazon S3 Standard-IA)
- Amazon S3 One Zone-Infrequent Access (Amazon S3 One Zone-IA)
- Amazon S3 Glacier
- Amazon S3 Glacier Deep Archive

# Amazon S3 bucket URLs (two styles)



To upload your data:

1. Create a **bucket** in an AWS Region.
2. Upload almost any number of **objects** to the bucket.

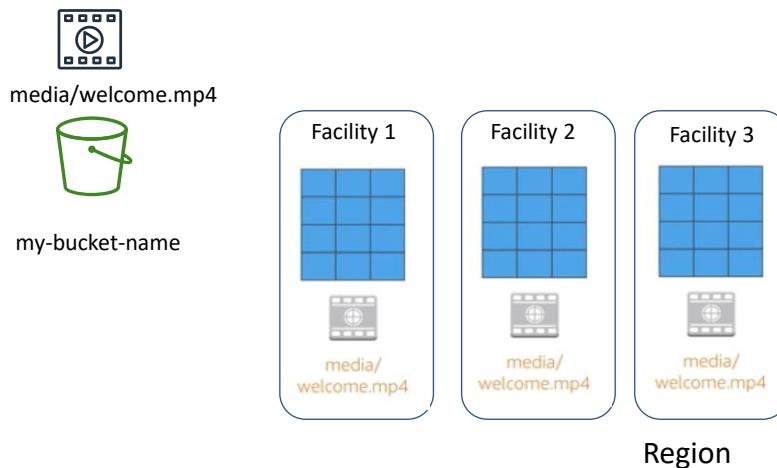
Bucket path-style URL endpoint:

`https://s3.ap-northeast-1.amazonaws.com/bucket-name`

Bucket virtual hosted-style URL endpoint:

`https://bucket-name.s3-ap-northeast-1.amazonaws.com`

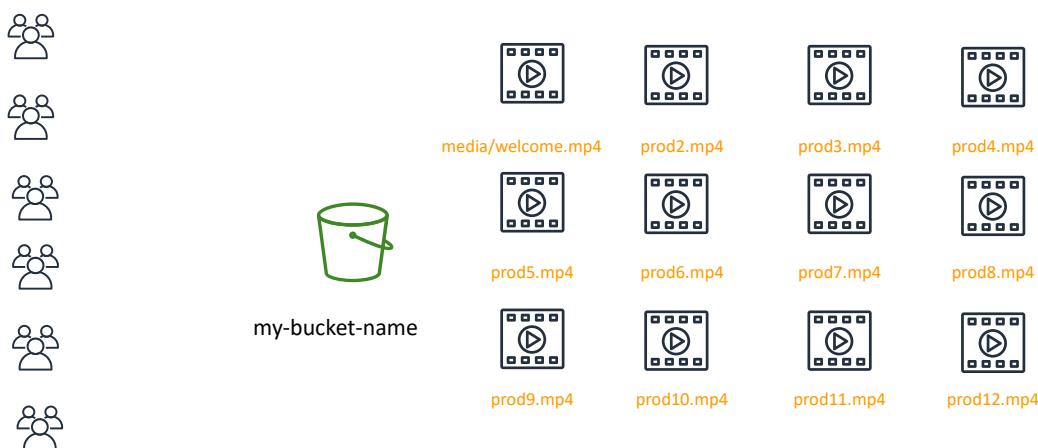
Data is redundantly stored in the Region



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

435

Designed for seamless scaling



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

436

## Access the data anywhere



AWS Management  
Console



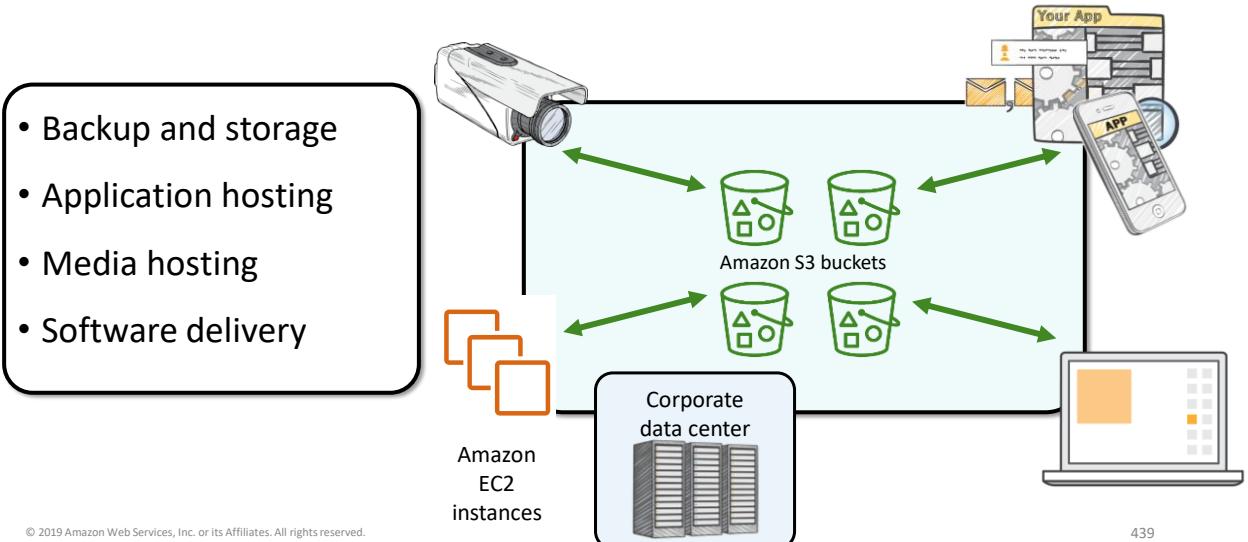
SDK

## Common use cases

- Storing application assets
- Static web hosting
- Backup and disaster recovery (DR)
- Staging area for big data
- *Many more....*



## Amazon S3 common scenarios



## Amazon S3 pricing

- Pay only for what you use, including –
  - GBs per month
  - Transfer OUT to other Regions
  - PUT, COPY, POST, LIST, and GET requests
- You do not pay for –
  - Transfers IN to Amazon S3
  - Transfers OUT from Amazon S3 to Amazon CloudFront or Amazon EC2 in the same Region

# Amazon S3: Storage pricing

To estimate Amazon S3 costs, consider the following:

## 1. Storage class type –

- Standard storage is designed for:
  - 11 9s of durability
  - Four 9s of availability
- S3 Standard-Infrequent Access (S-IA) is designed for:
  - 11 9s of durability
  - Three 9s of availability

## 2. Amount of storage –

- The number and size of objects

# Amazon S3: Storage pricing

## 3. Requests –

- The number and type of requests (**GET, PUT, COPY**)
- Type of requests:
  - Different rates for GET requests than other requests.

## 4. Data transfer –

- Pricing is based on the amount of data that is transferred out of the Amazon S3 Region
  - Data transfer in is free, but you incur charges for data that is transferred out.

## Section 2 key takeaways



443



- Amazon S3 is a fully managed cloud storage service.
- You can store a virtually unlimited number of objects.
- You pay for only what you use.
- You can access Amazon S3 at any time from anywhere through a URL.
- Amazon S3 offers rich security controls.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Recorded demo: Amazon Simple Storage System

444



### Set up demo

Amazon S3



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

**Module 7: Storage**

## Section 3: Amazon Elastic File System (Amazon EFS)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



# Storage



## Amazon Elastic File System (Amazon EFS)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

446

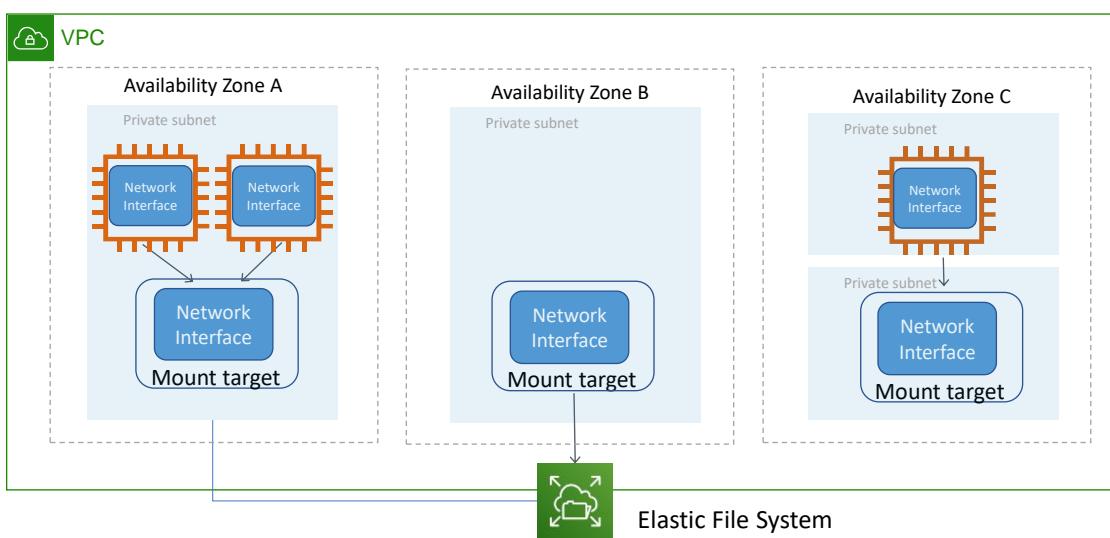
# Amazon EFS features

- File storage in the AWS Cloud
- Works well for big data and analytics, media processing workflows, content management, web serving, and home directories
- Petabyte-scale, low-latency file system
- Shared storage
- Elastic capacity
- Supports Network File System (NFS) versions 4.0 and 4.1 (NFSv4)
- Compatible with all Linux-based AMIs for Amazon EC2

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

447

# Amazon EFS architecture



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

448

# Amazon EFS implementation

- ① Create your Amazon EC2 resources and launch your Amazon EC2 instance.
- ② Create your Amazon EFS file system.
- ③ Create your mount targets in the appropriate subnets.
- ④ Connect your Amazon EC2 instances to the mount targets.
- ⑤ Verify the resources and protection of your AWS account.

# Amazon EFS resources

## File system

- Mount target
  - Subnet ID
  - Security groups
  - One or more per file system
  - Create in a VPC subnet
  - One per Availability Zone
  - Must be in the same VPC
- Tags
  - Key-value pairs



## Section 3 key takeaways



451

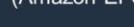
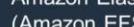


- Amazon EFS provides file storage over a network.
- Perfect for big data and analytics, media processing workflows, content management, web serving, and home directories.
- Fully managed service that eliminates storage administration tasks.
- Accessible from the console, an API, or the CLI.
- Scales up or down as files are added or removed and you pay for what you use.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Recorded demo: Amazon Elastic File System

452



Module 7: Storage

## Section 4: Amazon S3 Glacier

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



# Storage



## Amazon S3 Glacier

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

454

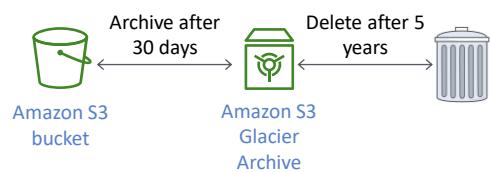
# Amazon S3 Glacier review

Amazon S3 Glacier is a data archiving service that is designed for [security](#), [durability](#), and an [extremely low cost](#).

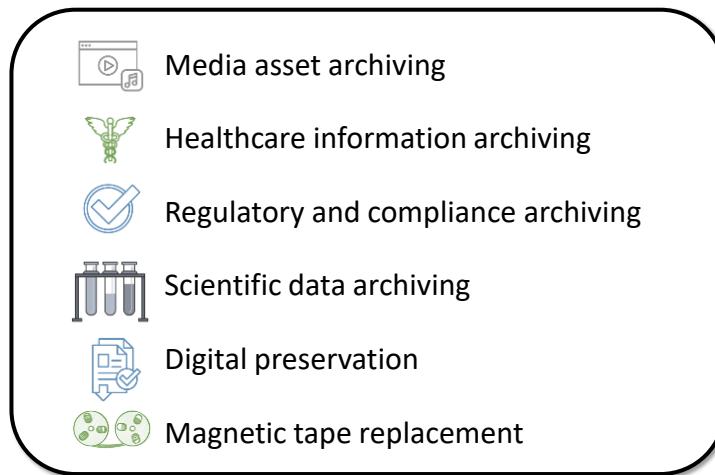
- Amazon S3 Glacier is designed to provide 11 9s of durability for objects.
- It supports the encryption of data in transit and at rest through Secure Sockets Layer (SSL) or Transport Layer Security (TLS).
- The Vault Lock feature enforces compliance through a policy.
- Extremely low-cost design works well for long-term archiving.
  - Provides three options for access to archives—expedited, standard, and bulk—retrieval times range from a few minutes to several hours.

# Amazon S3 Glacier

- Storage service for low-cost data archiving and long-term backup
- You can configure lifecycle archiving of Amazon S3 content to Amazon S3 Glacier
- Retrieval options –
  - Standard: 3–5 hours
  - Bulk: 5–12 hours
  - Expedited: 1–5 minutes



## Amazon S3 Glacier use cases



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

457

## Using Amazon S3 Glacier

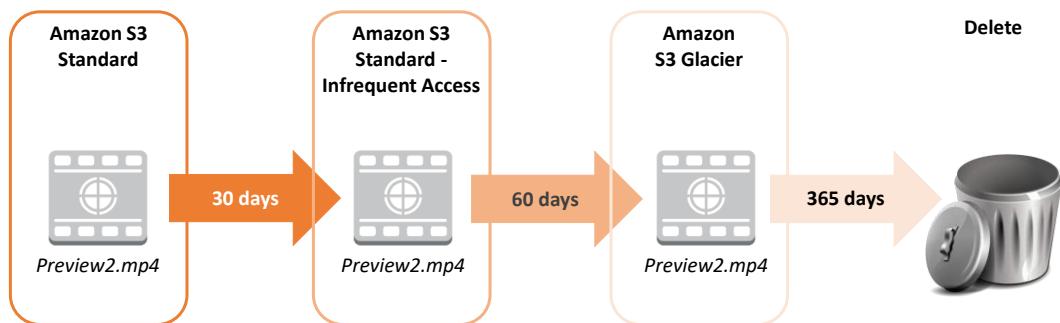


© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

458

# Lifecycle policies

[Amazon S3 lifecycle policies](#) enable you to delete or move objects based on age.



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

459

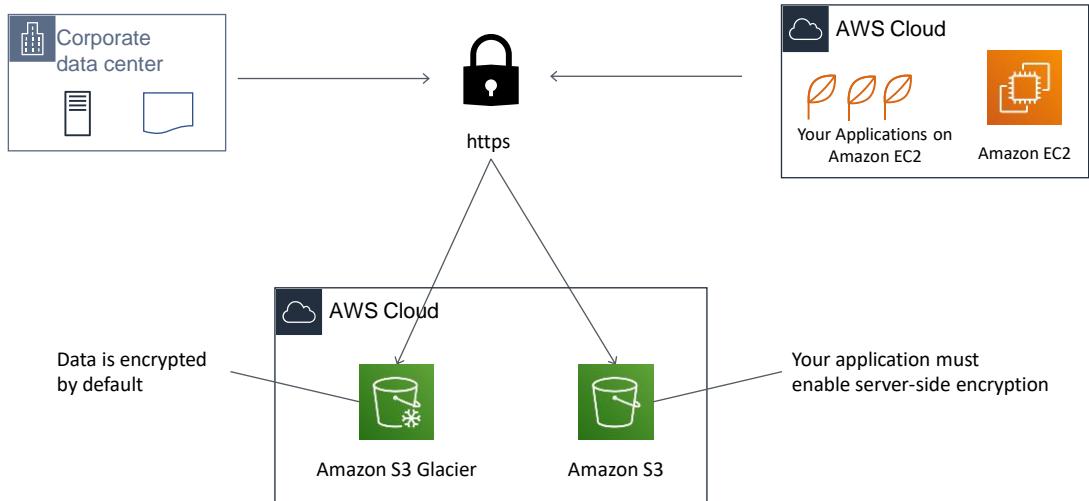
# Storage comparison

	Amazon S3	Amazon S3 Glacier
Data Volume	No limit	No limit
Average Latency	ms	minutes/hours
Item Size	5 TB maximum	40 TB maximum
Cost/GB per Month	Higher cost	Lower cost
Billed Requests	PUT, COPY, POST, LIST, and GET	UPLOAD and retrieval
Retrieval Pricing	¢ Per request	¢¢ Per request and per GB

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

460

# Server-side encryption



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

461

# Security with Amazon S3 Glacier



**Amazon S3  
Glacier**



**Control access with  
IAM**



**Amazon S3 Glacier encrypts  
your data with AES-256**



**Amazon S3 Glacier manages  
your keys for you**

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

462

## Section 4 key takeaways



463



- Amazon S3 Glacier is a data archiving service that is designed for security, durability, and an extremely low cost.
- Amazon S3 Glacier pricing is based on Region.
- Its extremely low-cost design works well for long-term archiving.
- The service is designed to provide 11 9s of durability for objects.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Recorded demo:  
Amazon S3 Glacier

464



## Set up demo

Amazon Glacier

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Activity: Storage Case Studies

465

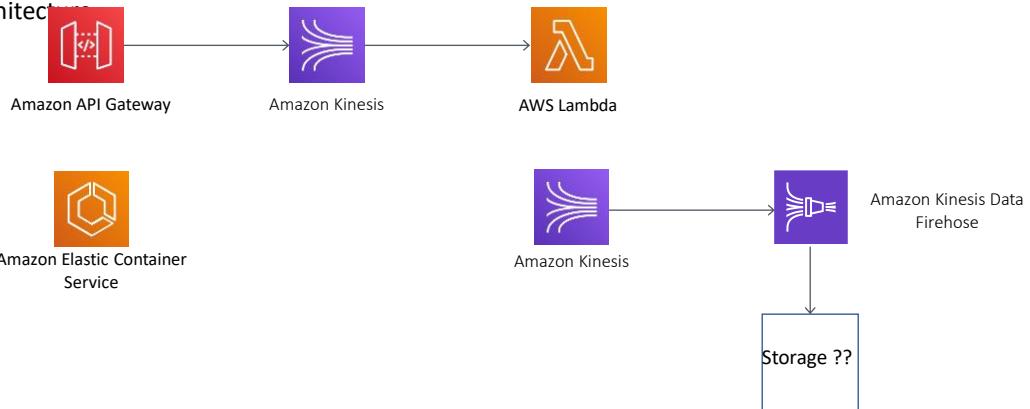


Photo by panumas nikhomkhai from Pexels.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Storage case study activity

**Case 1:** A data analytics company for travel sites must store billions of customer events per day. They use the data analytics services that are in the diagram. The following diagram illustrates their architecture.

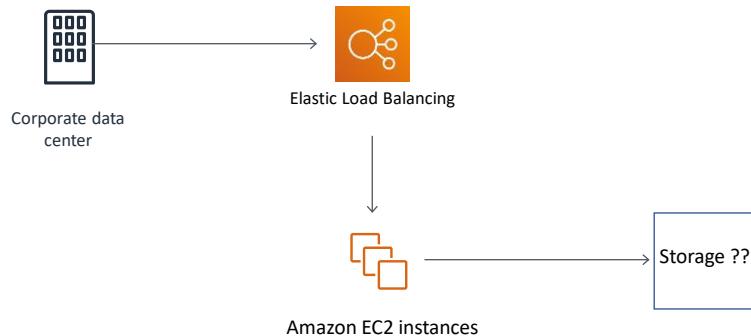


© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

466

# Storage case study activity

**Case 2:** A collaboration software company processes email for enterprise customers. They have more than 250 enterprise customers and more than half a million users. They must store petabytes of data for their customers. The following diagram illustrates their architecture.

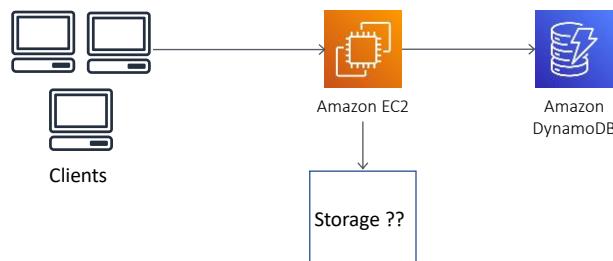


© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

467

# Storage case study activity

**Case 3:** A data protection company must be able to ingest and store large amounts of customer data and help their customers meet compliance requirements. They use Amazon EC2 for scalable compute and Amazon DynamoDB for duplicate data and metadata lookups. The following diagram illustrates their architecture.



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

468

## Module 7: Storage

# Module wrap-up

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



# Module summary

In summary, in this module, you learned how to:

- Identify the different types of storage
- Explain Amazon S3
- Identify the functionality in Amazon S3
- Explain Amazon EBS
- Identify the functionality in Amazon EBS
- Perform functions in Amazon EBS to build an Amazon EC2 storage solution
- Explain Amazon EFS
- Identify the functionality in Amazon EFS
- Explain Amazon S3 Glacier
- Identify the functionality in Amazon S3 Glacier
- Differentiate between Amazon EBS, Amazon S3, Amazon EFS, and Amazon S3 Glacier

## Complete the knowledge check



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

471

## Sample exam question

A company wants to store data that is not frequently accessed. What is the best and cost-effective solution that should be considered?

- A. AWS Storage Gateway
- B. Amazon Simple Storage Service Glacier
- C. Amazon Elastic Block Store (Amazon EBS)
- D. Amazon Simple Storage Service (Amazon S3)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

472

# Additional resources

- [AWS Storage page](#)
- [Storage Overview](#)
- [Recovering files from an Amazon EBS volume backup](#)
- [Confused by AWS Storage Options? S3, EFS, EBS Explained](#)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

473

Thank you

© 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. Corrections or feedback on the course, please email us at: [aws-course-feedback@amazon.com](mailto:aws-course-feedback@amazon.com). For all other questions, contact us at: <https://aws.amazon.com/contact-us/aws-training/>. All trademarks are the property of their owners.



AWS Academy Cloud Foundations

# Module 8: Databases

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Module overview



### Topics

- Amazon Relational Database Service (Amazon RDS)
- Amazon DynamoDB
- Amazon Redshift
- Amazon Aurora

### Demos

- Amazon RDS console
- Amazon DynamoDB console

### Lab

- Lab 5: Build Your DB Server and Interact with Your DB Using an App

### Activity

- Database case studies



### Knowledge check

# Module objectives

After completing this module, you should be able to:

- Explain Amazon Relational Database Service (Amazon RDS)
- Identify the functionality in Amazon RDS
- Explain Amazon DynamoDB
- Identify the functionality in Amazon DynamoDB
- Explain Amazon Redshift
- Explain Amazon Aurora
- Perform tasks in an RDS database, such as launching, configuring, and interacting

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

477

Module 8: Databases

## Section 1: Amazon Relational Database Service

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



# Amazon Relational Database Service



Amazon Relational Database  
Service (Amazon RDS)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

479

## Unmanaged versus managed services

### Unmanaged:

*Scaling, fault tolerance, and availability are managed by you.*



### Managed:

*Scaling, fault tolerance, and availability are typically built in to the service.*



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

480

# Challenges of relational databases

- Server maintenance and energy footprint
- Software installation and patches
- Database backups and high availability
- Limits on scalability
- Data security
- Operating system (OS) installation and patches

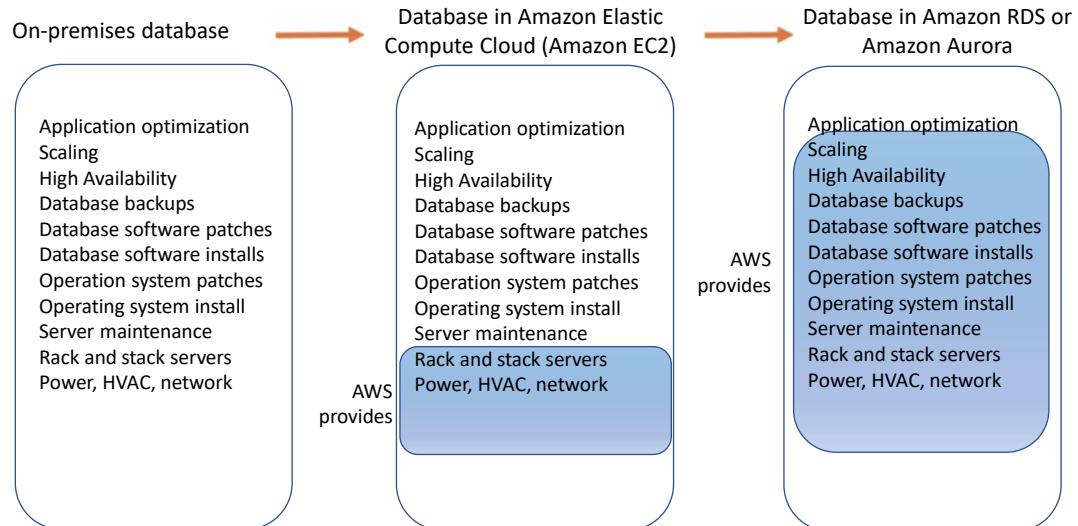


# Amazon RDS

Managed service that sets up and operates a relational database in the cloud.



## From on-premises databases to Amazon RDS



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

483

## Managed services responsibilities

### You manage:

- Application optimization



### AWS manages:

- OS installation and patches
- Database software installation and patches
- Database backups
- High availability
- Scaling
- Power and racking and stacking servers
- Server maintenance

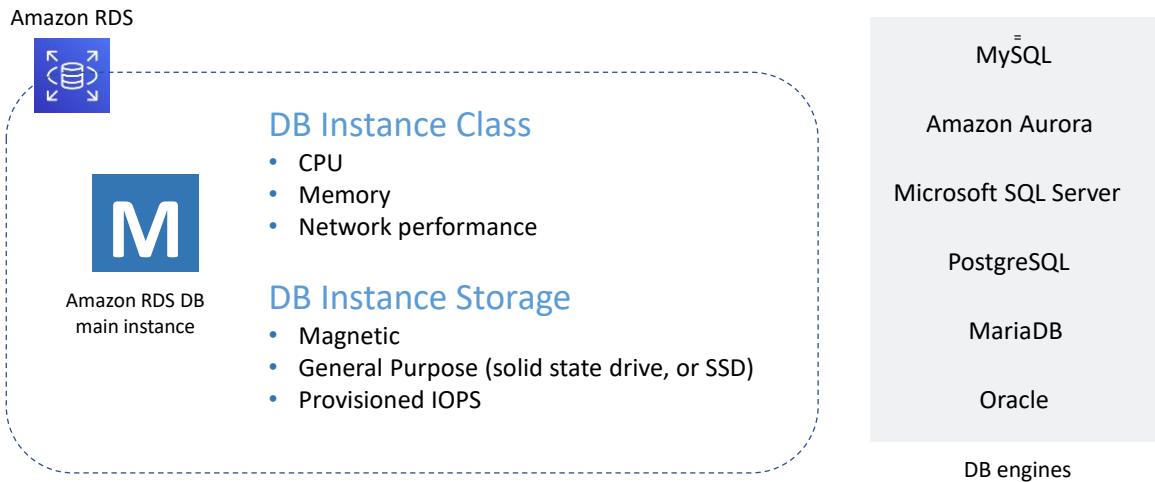


Amazon RDS

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

484

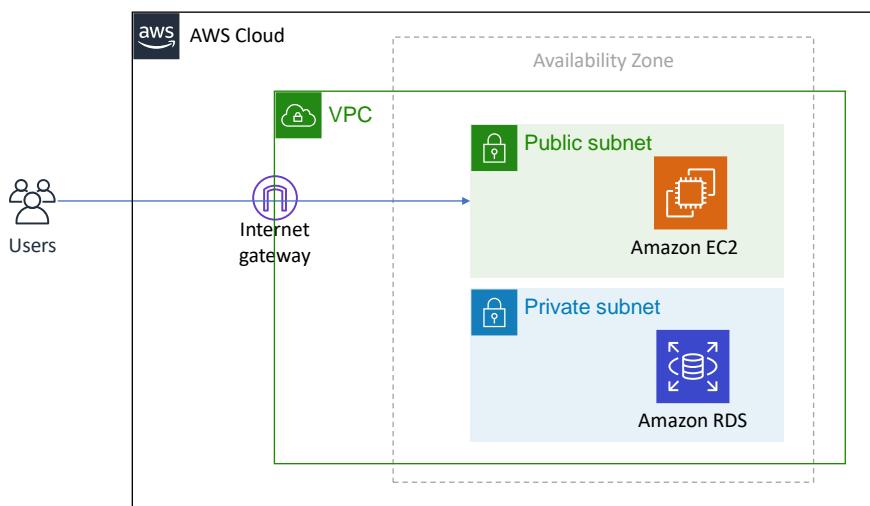
# Amazon RDS DB instances



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

485

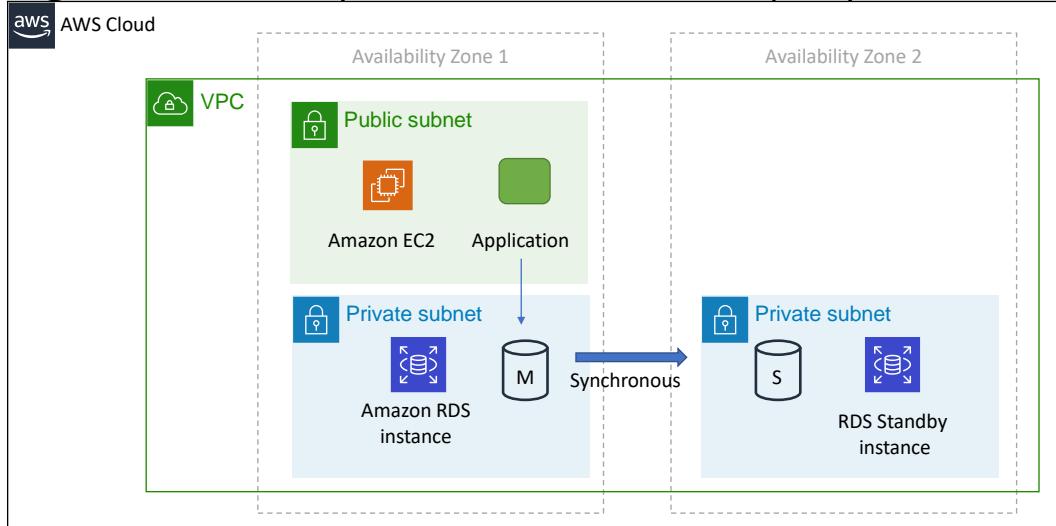
## Amazon RDS in a virtual private cloud (VPC)



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

486

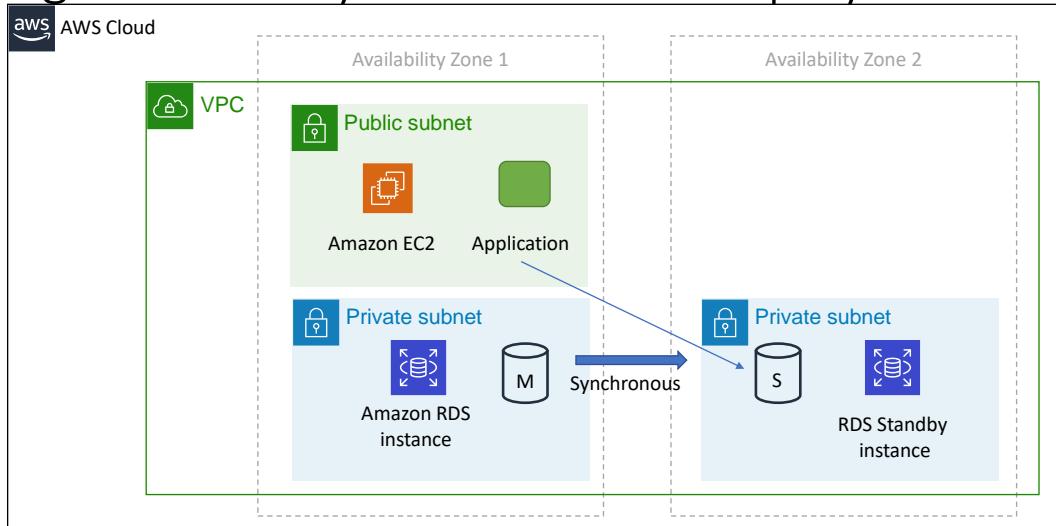
## High availability with Multi-AZ deployment



© 2019 Amazon Web Services, Inc. or Its Affiliates. All rights reserved.

487

## High availability with Multi-AZ deployment 2



© 2019 Amazon Web Services, Inc. or Its Affiliates. All rights reserved.

488

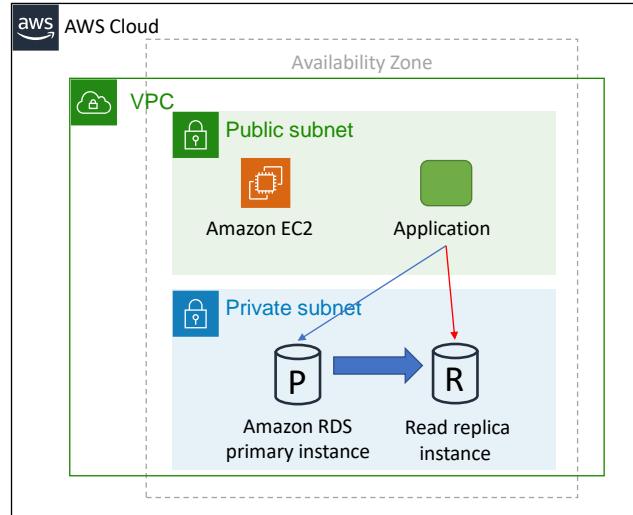
# Amazon RDS read replicas

## Features

- Offers asynchronous replication
- Can be promoted to primary if needed

## Functionality

- Use for read-heavy database workloads
- Offload read queries



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

489

## Use cases

<b>Web and mobile applications</b>	<ul style="list-style-type: none"> <li>✓ High throughput</li> <li>✓ Massive storage scalability</li> <li>✓ High availability</li> </ul>
<b>Ecommerce applications</b>	<ul style="list-style-type: none"> <li>✓ Low-cost database</li> <li>✓ Data security</li> <li>✓ Fully managed solution</li> </ul>
<b>Mobile and online games</b>	<ul style="list-style-type: none"> <li>✓ Rapidly grow capacity</li> <li>✓ Automatic scaling</li> <li>✓ Database monitoring</li> </ul>

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

490

# When to Use Amazon RDS



## Use Amazon RDS when your application requires:

- Complex transactions or complex queries
- A medium to high query or write rate – Up to 30,000 IOPS (15,000 reads + 15,000 writes)
- No more than a single worker node or shard
- High durability

## Do not use Amazon RDS when your application requires:

- Massive read/write rates (for example, 150,000 write/second)
- Sharding due to high data size or throughput demands
- Simple GET or PUT requests and queries that a NoSQL database can handle
- Relational database management system (RDBMS) customization

## Amazon RDS: Clock-hour billing and database characteristics

### Clock-hour billing –

- Resources incur charges when running

### Database characteristics –

- Physical capacity of database:
  - Engine
  - Size
  - Memory class

Amazon RDS: DB purchase type and multiple DB instances

### **DB purchase type –**

- On-Demand Instances
  - Compute capacity by the hour
- Reserved Instances
  - Low, one-time, upfront payment for database instances that are reserved with a 1-year or 3-year term

### **Number of DB instances –**

- Provision multiple DB instances to handle peak loads

# Amazon RDS: Storage

### **Provisioned storage –**

- No charge
  - Backup storage of up to 100 percent of database storage for an active database
- Charge (*GB/month*)
  - Backup storage for terminated DB instances

### **Additional storage –**

- Charge (*GB/month*)
  - Backup storage in addition to provisioned storage

# Amazon RDS: Deployment type and data transfer

## Requests –

- The number of input and output requests that are made to the database

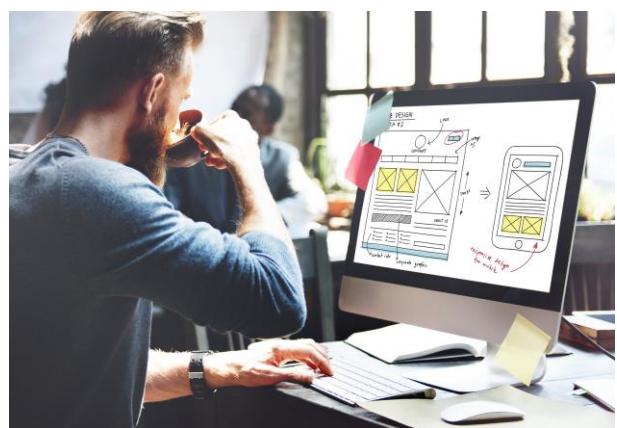
## Deployment type—Storage and I/O charges vary, depending on whether you deploy to –

- Single Availability Zone
- Multiple Availability Zones

## Data transfer –

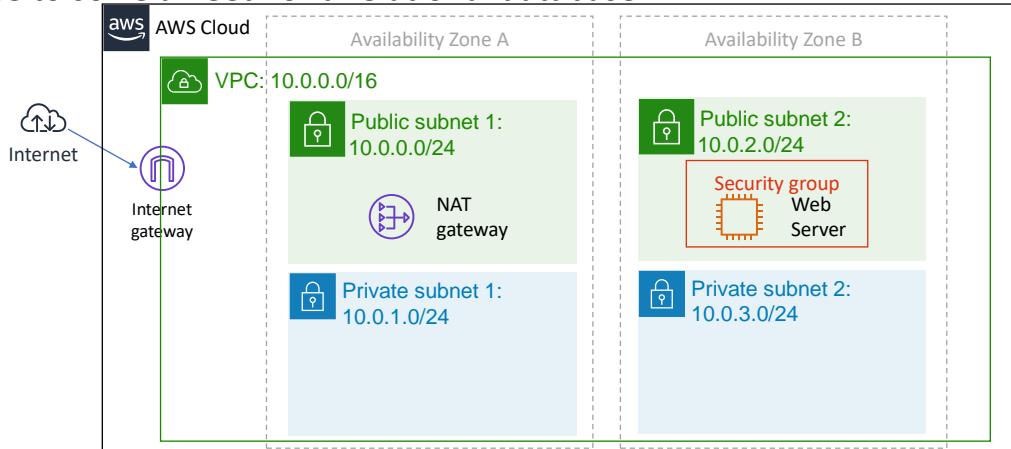
- No charge for inbound data transfer
- Tiered charges for outbound data transfer

Build Your DB  
Server and  
Interact with Your  
DB Using an App



## Lab 5: Scenario

This lab is designed to show you how to use an AWS managed database instance to solve a need for a relational database.



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

497

## Lab 5: Tasks

**Security group**

Create a **VPC security group**.

**Private subnet**

Create a **DB subnet group**.



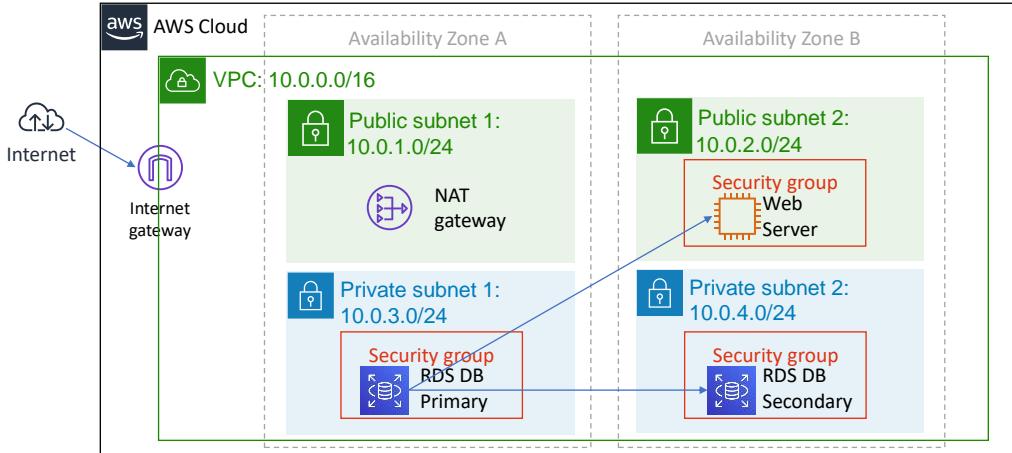
Amazon RDS

Create an **Amazon RDS DB instance** and interact with your database.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

498

# Lab 5: Final product



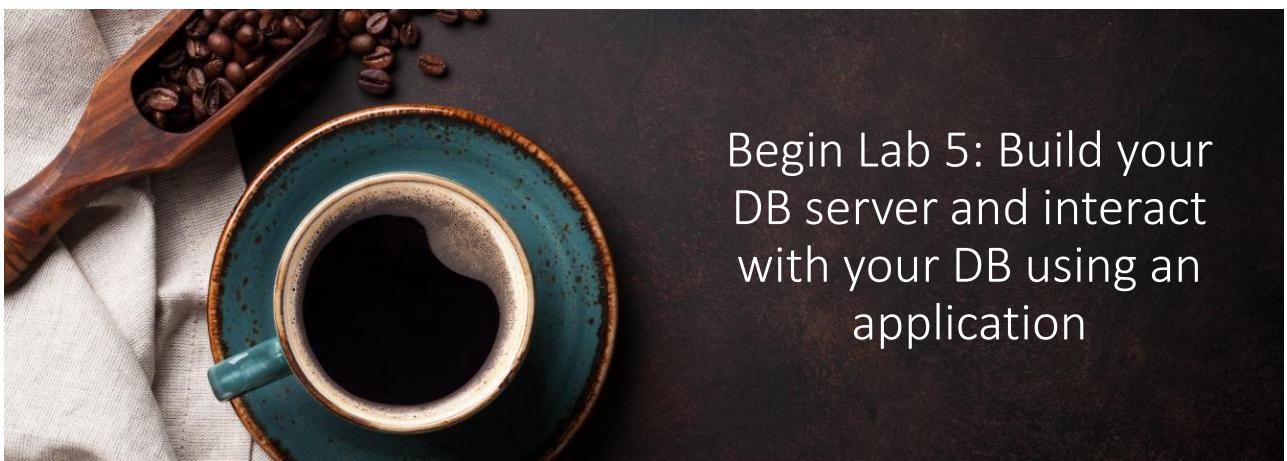
© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

499



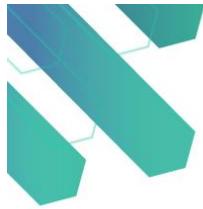
**aws** academy

Begin Lab 5: Build your DB server and interact with your DB using an application



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

500



## Lab debrief: key takeaways



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

501

## Recorded demo: Amazon RDS

502



### Set up demo

Amazon Relational Database Service (RDS)

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Section 1 key takeaways



503



- With Amazon RDS, you can set up, operate, and scale relational databases in the cloud.

- Features –**

- Managed service
- Accessible via the console, AWS Command Line Interface (AWS CLI), or application programming interface (API) calls
- Scalable (compute and storage)
- Automated redundancy and backup are available
- Supported database engines:
  - Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle, Microsoft SQL Server

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Module 8: Databases

## Section 2: Amazon DynamoDB

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Relational versus non-relational databases

	Relational (SQL)	Non-Relational												
Data Storage	Rows and columns	Key-value, document, graph												
Schemas	Fixed	Dynamic												
Querying	Uses SQL	Focuses on collection of documents												
Scalability	Vertical	Horizontal												
Example	<table border="1"> <thead> <tr> <th>ISBN</th> <th>Title</th> <th>Author</th> <th>Format</th> </tr> </thead> <tbody> <tr> <td>3111111223439</td> <td>Withering Depths</td> <td>Jackson, Mateo</td> <td>Paperback</td> </tr> <tr> <td>312222223439</td> <td>Wily Willy</td> <td>Wang, Xiulan</td> <td>Ebook</td> </tr> </tbody> </table>	ISBN	Title	Author	Format	3111111223439	Withering Depths	Jackson, Mateo	Paperback	312222223439	Wily Willy	Wang, Xiulan	Ebook	{         ISBN: 3111111223439,         Title: "Withering Depths",         Author: "Jackson, Mateo",         Format: "Paperback"       }
ISBN	Title	Author	Format											
3111111223439	Withering Depths	Jackson, Mateo	Paperback											
312222223439	Wily Willy	Wang, Xiulan	Ebook											

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

505

## What is Amazon DynamoDB?

Fast and flexible NoSQL database service for any scale



**Amazon DynamoDB**

- NoSQL database tables
- Virtually unlimited storage
- Items can have differing attributes
- Low-latency queries
- Scalable read/write throughput

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

506

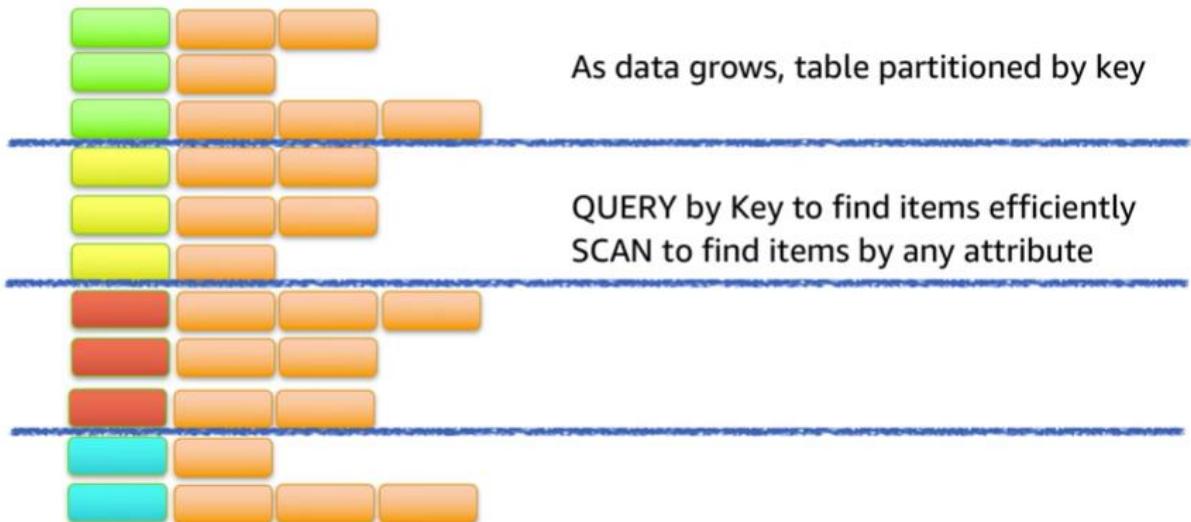
## Amazon DynamoDB core components

- Tables, items, and attributes are the core DynamoDB components
  - DynamoDB supports two different kinds of primary keys: Partition key and partition and sort key

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

507

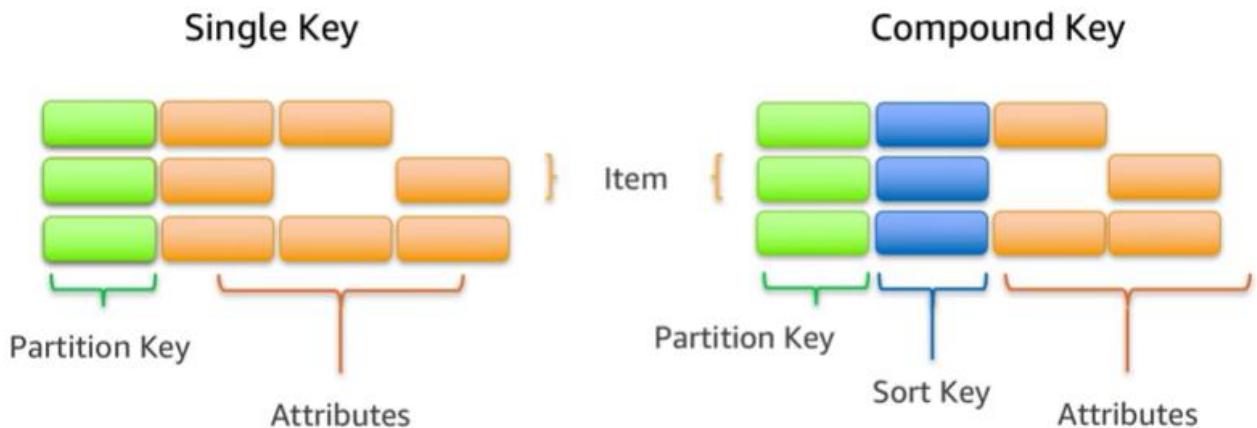
## Partitioning



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

508

Items in a table must have a key



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

509

## Section 2 key takeaways



510

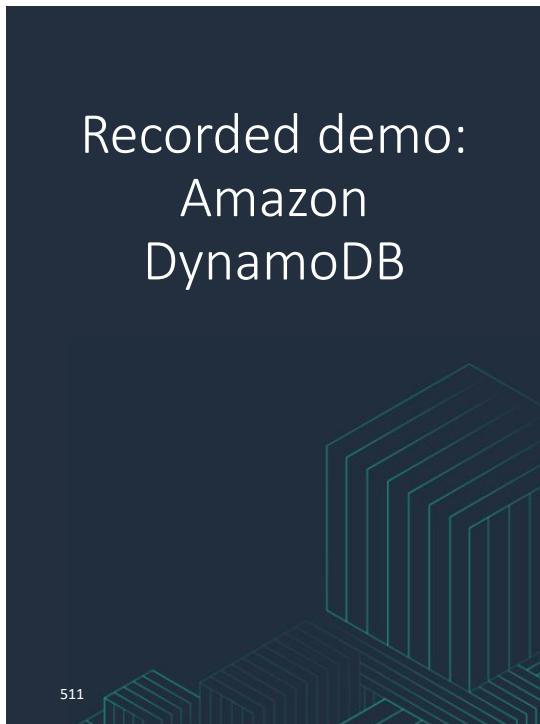


### Amazon DynamoDB:

- Runs exclusively on SSDs.
- Supports document and key-value store models.
- Replicates your tables automatically across your choice of AWS Regions.
- Works well for mobile, web, gaming, adtech, and Internet of Things (IoT) applications.
- Is accessible via the console, the AWS CLI, and API calls.
- Provides consistent, single-digit millisecond latency at any scale.
- Has no limits on table size or throughput.

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Recorded demo:  
Amazon  
DynamoDB



**aws academy**

**Set up demo**  
Amazon DynamoDB



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Amazon DynamoDB demonstration



### Amazon DynamoDB

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. Its flexible data model and reliable performance make it a great fit for mobile, web, gaming, ad-tech, IoT, and many other applications.

[Create table](#)

[Getting started guide](#)



Create tables



Add and query items



Monitor and manage tables

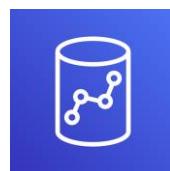
Module 8: Databases

## Section 3: Amazon Redshift

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.



# Amazon Redshift

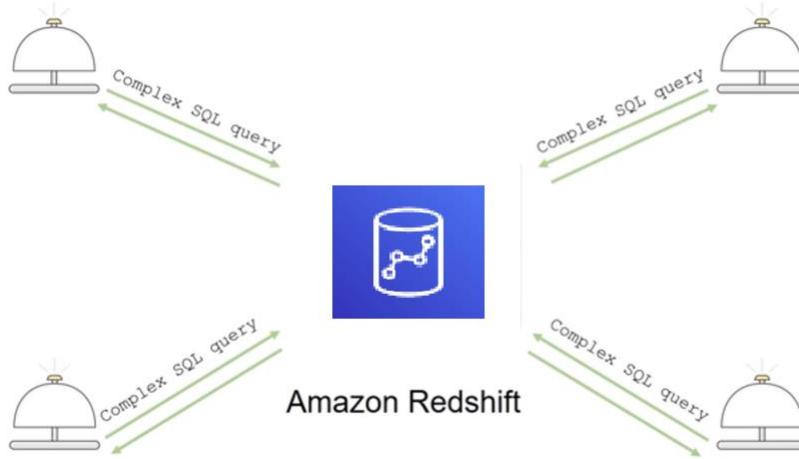


Amazon Redshift

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

514

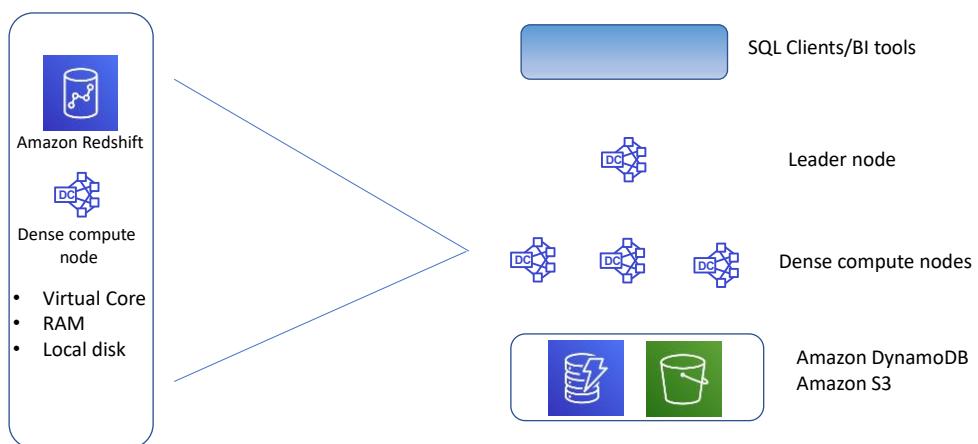
# Introduction to Amazon Redshift



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

515

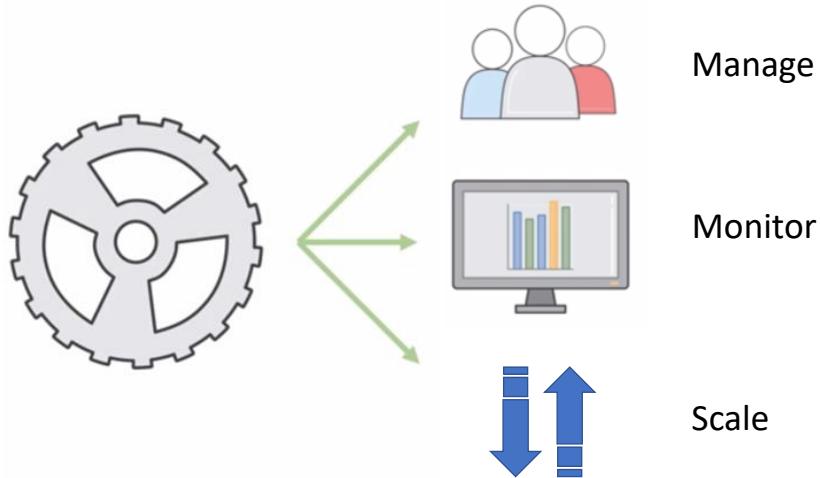
# Parallel processing architecture



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

516

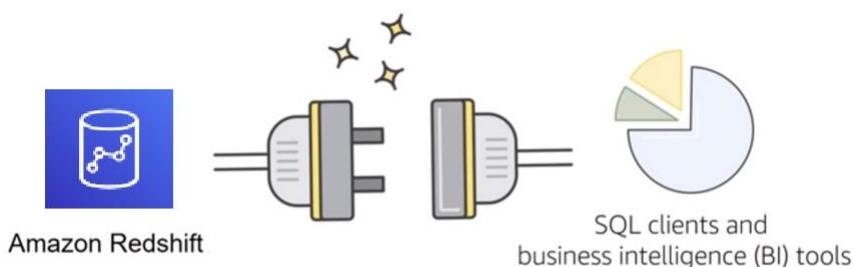
## Automation and scaling



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

517

## Compatibility

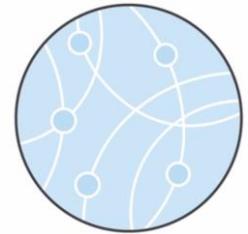


© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

518

## Amazon Redshift use cases

- Enterprise data warehouse (EDW)
  - Migrate at a pace that customers are comfortable with
  - Experiment without large upfront cost or commitment
  - Respond faster to business needs
- Big data
  - Low price point for small customers
  - Managed service for ease of deployment and maintenance
  - Focus more on data and less on database management



## Amazon Redshift use cases 2

- Software as a service (SaaS)
  - Scale the data warehouse capacity as demand grows
  - Add analytic functionality to applications
  - Reduce hardware and software costs





## Section 3 key takeaways



521

### Amazon Redshift features:

- Fast, fully managed data warehouse service
- Easily scale with no downtime
- Columnar storage and parallel processing architectures
- Automatically and continuously monitors cluster
- Encryption is built in

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Module 8: Databases

## Section 4: Amazon Aurora



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

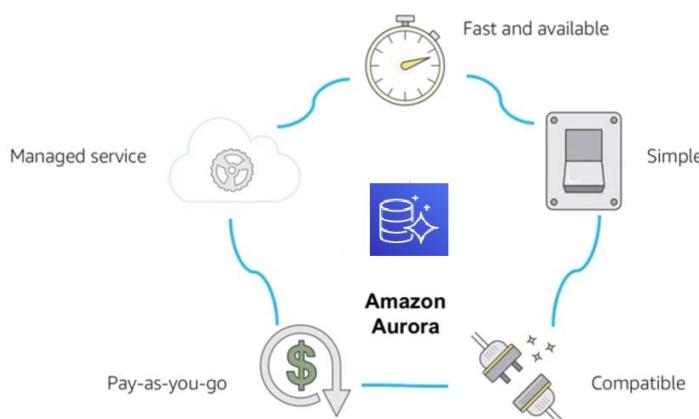
# Amazon Aurora



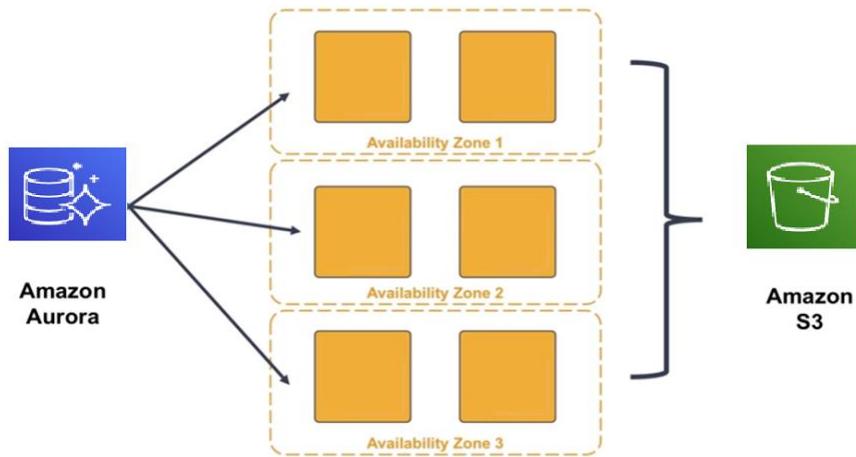
Amazon Aurora

- Enterprise-class relational database
- Compatible with MySQL or PostgreSQL
- Automate time-consuming tasks (such as provisioning, patching, backup, recovery, failure detection, and repair).

## Amazon Aurora service benefits



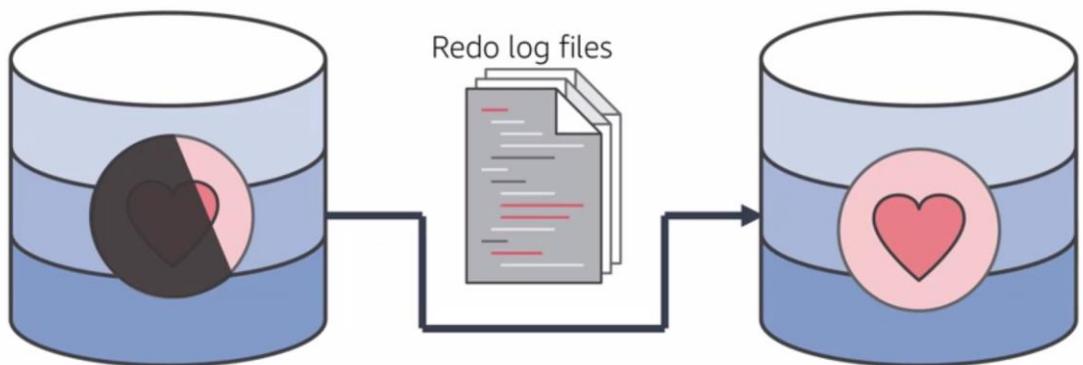
## High availability



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

525

## Resilient design



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

526



## Section 4 key takeaways



527

### Amazon Aurora features:

- High performance and scalability
- High availability and durability
- Multiple levels of security
- Compatible with MySQL and PostgreSQL
- Fully managed

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

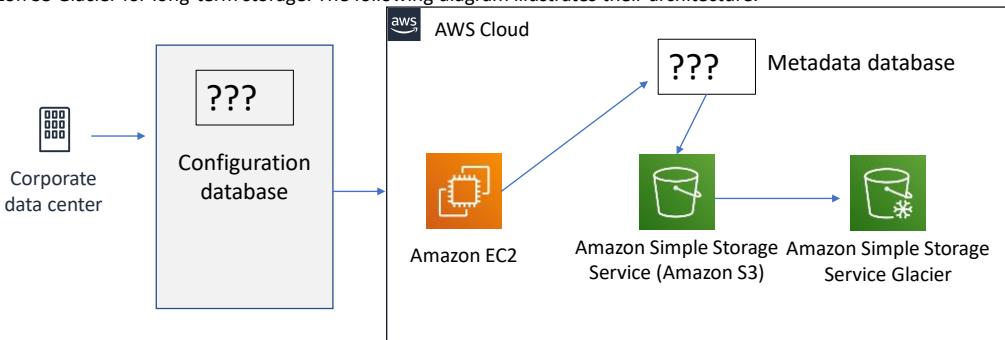
## The right tool for the right job

### What are my requirements?

Enterprise-class relational database	Amazon RDS
Fast and flexible NoSQL database service for any scale	Amazon DynamoDB
Operating system access or application features that are not supported by AWS database services	Databases on Amazon EC2
Specific case-driven requirements (machine learning, data warehouse, graphs)	AWS purpose-built database services

# Database case study activity 1

Case 1: A data protection and management company that provides services to enterprises. They must provide database services for over 55 petabytes of data. They have two types of data that require a database solution. First, they need a relational database store for configuration data. Second, they need a store for unstructured metadata to support a de-duplication service. After the data is de-duplicated, it is stored in Amazon S3 for quick retrieval, and eventually moved to Amazon S3 Glacier for long-term storage. The following diagram illustrates their architecture.

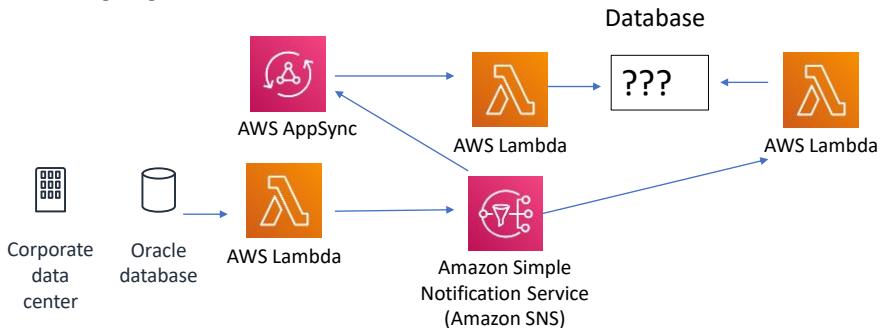


© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

529

# Database case study activity 2

Case 2: A commercial shipping company that uses an on-premises legacy data management system. They must migrate to a serverless ecosystem while they continue to use their existing database system, which is based on Oracle. They are also in the process of decomposing their highly structured relational data into semistructured data. The following diagram illustrates their architecture.

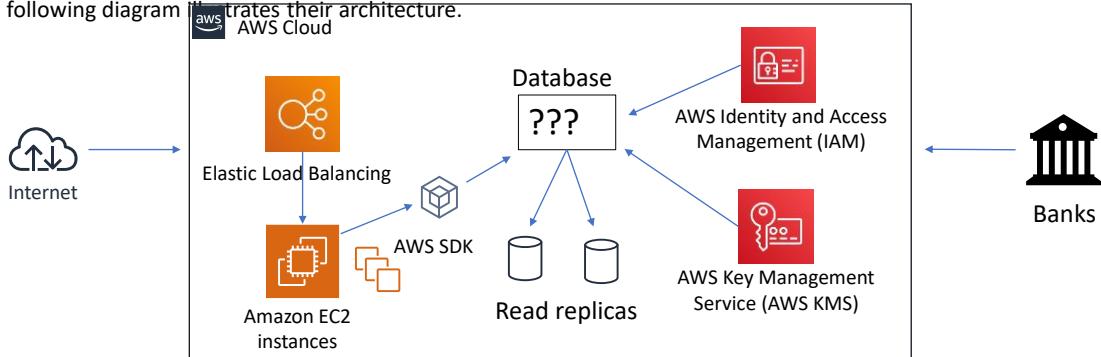


© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

530

# Database case study activity 3

Case 3: An online payment processing company that processes over 1 million transactions per day. They must provide services to ecommerce customers who offer flash sales (sales that offer greatly reduced prices for a limited time), where demand can increase by 30 times in a short time period. They use IAM and AWS KMS to authenticate transactions with financial institutions. They need high throughput for these peak loads. The following diagram illustrates their architecture.



© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

531

Module 8: Databases

Module wrap-up

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

# Module summary

In summary, in this module, you learned how to:

- Explain Amazon Relational Database Service (Amazon RDS)
- Identify the functionality in Amazon RDS
- Explain Amazon DynamoDB
- Identify the functionality in Amazon DynamoDB
- Explain Amazon Redshift
- Explain Amazon Aurora
- Perform tasks in an RDS database, such as launching, configuring, and interacting

## Complete the knowledge check



## Sample exam question

Which of the following is a fully-managed NoSQL database service?

- A. Amazon Relational Database Service (Amazon RDS)
- B. Amazon DynamoDB
- C. Amazon Aurora
- D. Amazon Redshift

## Additional resources

- [AWS Database page](#)
- [Amazon RDS page](#)
- [Overview of Amazon database services](#)
- [Getting started with AWS databases](#)

# Thank you

© 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. Corrections or feedback on the course, please email us at: [aws-course-feedback@amazon.com](mailto:aws-course-feedback@amazon.com). For all other questions, contact us at: <https://aws.amazon.com/contact-us/aws-training/>. All trademarks are the property of their owners.



AWS Academy Cloud Foundations

## Module 10: Automatic Scaling and Monitoring



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

# Module overview



## Topics

- Elastic Load Balancing
- Amazon CloudWatch
- Amazon EC2 Auto Scaling

## Activities

- Elastic Load Balancing activity
- Amazon CloudWatch activity

## Lab

- Scale and Load Balance Your Architecture



## Knowledge check

# Module objectives

After completing this module, you should be able to:

- Indicate how to distribute traffic across Amazon Elastic Compute Cloud (Amazon EC2) instances by using Elastic Load Balancing
- Identify how Amazon CloudWatch enables you to monitor AWS resources and applications in real time
- Explain how Amazon EC2 Auto Scaling launches and releases servers in response to workload changes
- Perform scaling and load balancing tasks to improve an architecture

**Module 10: Automatic Scaling and Monitoring**

## Section 1: Elastic Load Balancing

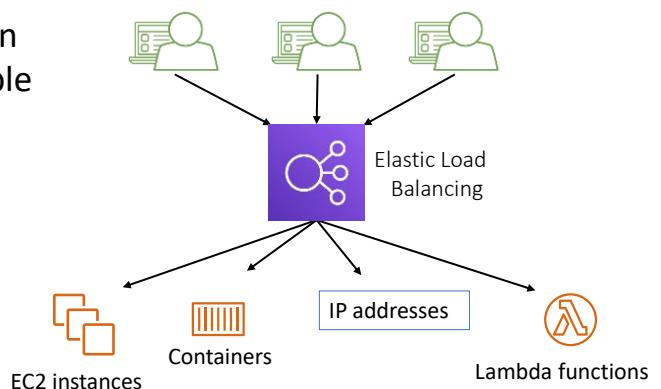
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## Elastic Load Balancing



- Distributes incoming application or network traffic across multiple targets in a single Availability Zone or across multiple Availability Zones.
- Scales your load balancer as traffic to your application changes over time.



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

542

# Types of load balancers

Application Load Balancer	Network Load Balancer	Classic Load Balancer (Previous Generation)
<ul style="list-style-type: none"> <li>Load balancing of HTTP and HTTPS traffic</li> <li>Routes traffic to targets based on content of request</li> <li>Provides advanced request routing targeted at the delivery of modern application architectures, including microservices and containers</li> <li>Operates at the application layer (OSI model layer 7)</li> </ul>	<ul style="list-style-type: none"> <li>Load balancing of TCP, UDP, and TLS traffic where extreme performance is required</li> <li>Routes traffic to targets based on IP protocol data</li> <li>Can handle millions of requests per second while maintaining ultra-low latencies</li> <li>Is optimized to handle sudden and volatile traffic patterns</li> <li>Operates at the transport layer (OSI model layer 4)</li> </ul>	<ul style="list-style-type: none"> <li>Load balancing of HTTP, HTTPS, TCP, and SSL traffic</li> <li>Load balancing across multiple EC2 instances</li> <li>Operates at both the application and transport layers.</li> </ul>

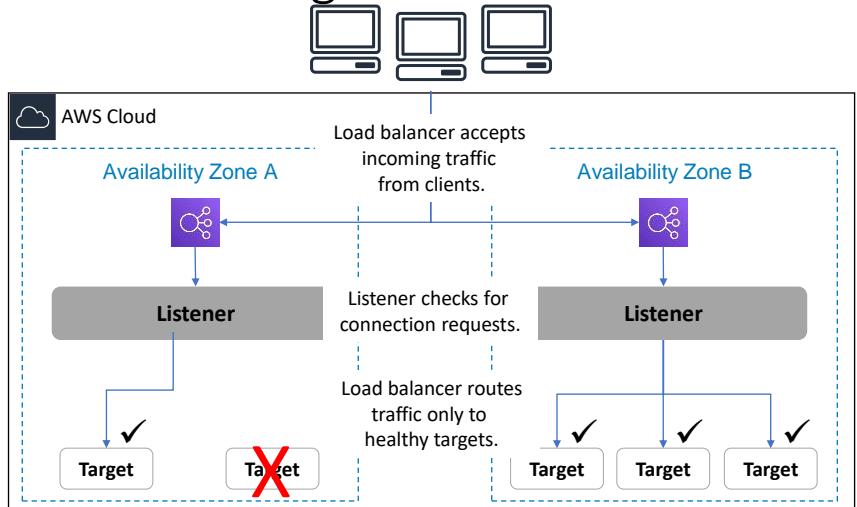
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

543

## How Elastic Load Balancing works

- With Application Load Balancers and Network Load Balancers, you **register targets in target groups**, and route traffic to the target groups.
- With Classic Load Balancers, you **register instances with the load balancer**.

Load balancer performs health checks to monitor health of registered targets.



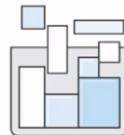
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

544

# Elastic Load Balancing use cases



Highly available and fault-tolerant applications



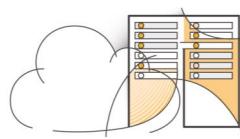
Containerized applications



Elasticity and scalability



Virtual private cloud (VPC)



Hybrid environments

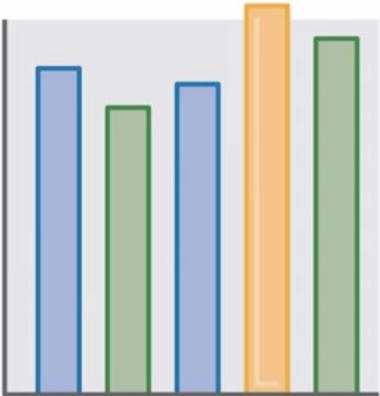


Invoke Lambda functions over HTTPS

## Activity: Elastic Load Balancing

You must support traffic to a containerized application.	Application Load Balancer
You have extremely spiky and unpredictable TCP traffic.	Network Load Balancer
You need simple load balancing with multiple protocols.	Classic Load Balancer
You need to support a static or Elastic IP address, or an IP target outside a VPC.	Network Load Balancer
You need a load balancer that can handle millions of requests per second while maintaining low latencies.	Network Load Balancer
You must support HTTPS requests.	Application Load Balancer

# Load balancer monitoring



- **Amazon CloudWatch metrics** – Used to verify that the system is performing as expected and creates an alarm to initiate an action if a metric goes outside an acceptable range.
- **Access logs** – Capture detailed information about requests sent to your load balancer.
- **AWS CloudTrail logs** – Capture the who, what, when, and where of API interactions in AWS services.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

547

## Section 1 key takeaways



548



- Elastic Load Balancing distributes incoming application or network traffic across multiple targets in one or more Availability Zones.
- Elastic Load Balancing supports three types of load balancers:
  - Application Load Balancer
  - Network Load Balancer
  - Classic Load Balancer
- ELB offers instance health checks, security, and monitoring.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

**Module 10: Automatic Scaling and Monitoring**

## Section 2: Amazon CloudWatch

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

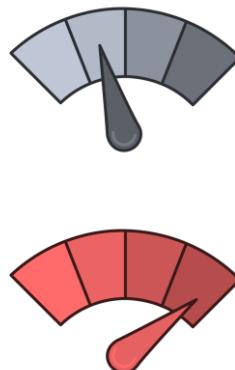
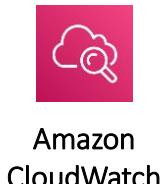


## Monitoring AWS resources

To use AWS efficiently, you need insight into your AWS resources:

- How do you know when you should **launch more Amazon EC2 instances?**
- Is your **application's performance or availability** being affected by a lack of sufficient capacity?
- How much of your infrastructure is actually **being used?**

# Amazon CloudWatch



- Monitors –
  - AWS resources
  - Applications that run on AWS
- Collects and tracks –
  - Standard metrics
  - Custom metrics
- Alarms –
  - Send notifications to an Amazon SNS topic
  - Perform Amazon EC2 Auto Scaling or Amazon EC2 actions
- Events –
  - Define rules to match changes in AWS environment and route these events to one or more target functions or streams for processing

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

551

## CloudWatch alarms



- Create alarms based on –
  - Static threshold
  - Anomaly detection
  - Metric math expression
- Specify –
  - Namespace
  - Metric
  - Statistic
  - Period
  - Conditions
  - Additional configuration
  - Actions

**Statistic**

 x

**Period**

 ▼

**Conditions**

**Threshold type**

**Static**  
Use a value as a threshold

**Anomaly detection**  
Use a band as a threshold

Whenever CPUUtilization is...  
Define the alarm condition

**Greater**  
> threshold

**Greater/Equal**  
>= threshold

**Lower/Equal**  
<= threshold

**Lower**  
< threshold

than...  
Define the threshold value

 ▼

Must be a number

▶ Additional configuration

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

552

## Activity: Amazon CloudWatch



Amazon EC2

If average CPU utilization is > 60% for 5 minutes...

Correct!



Amazon RDS

If the number of simultaneous connections is > 10 for 1 minute...

Correct!



Amazon S3

If the maximum bucket size in bytes is around 3 for 1 day...

Incorrect. *Around* is not a threshold option. You must specify a threshold of >, >=, <=, or <.



Elastic Load Balancing

If the number of healthy hosts is < 5 for 10 minutes...

Correct!



Amazon Elastic Block Store

If the volume of read operations is > 1,000 for 10 seconds...

Incorrect. You must specify a statistic (for example, *average volume*).

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

553

## Section 2 key takeaways



554



- Amazon CloudWatch helps you monitor your AWS resources—and the applications that you run on AWS—in real time.
- CloudWatch enables you to –
  - Collect and track standard and custom metrics.
  - Set alarms to automatically send notifications to SNS topics, or perform Amazon EC2 Auto Scaling or Amazon EC2 actions.
  - Define rules that match changes in your AWS environment and route these events to targets for processing.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

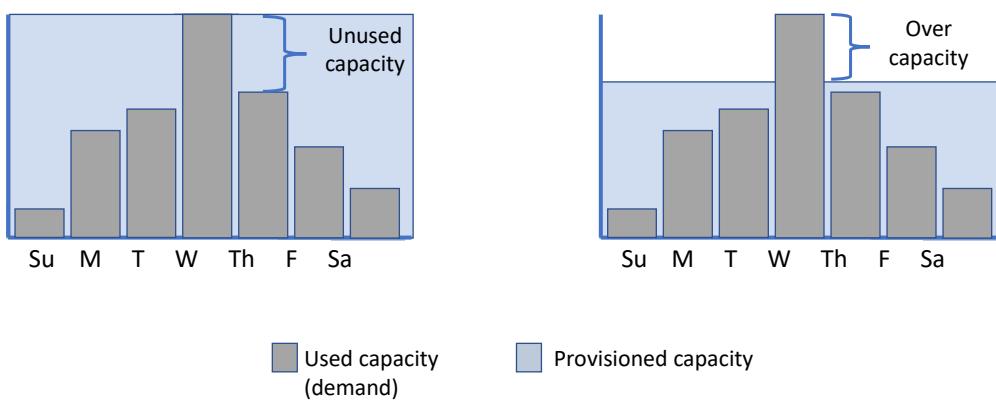
**Module 10: Automatic Scaling and Monitoring**

## Section 3: Amazon EC2 Auto Scaling

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



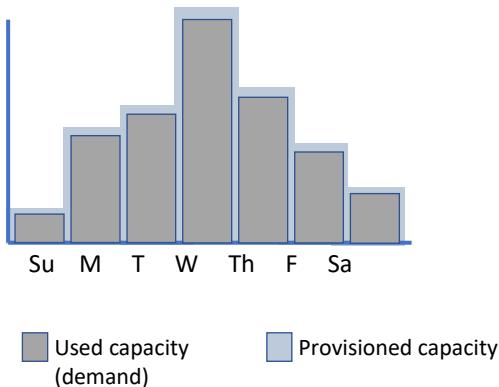
### Why is scaling important?



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

556

# Amazon EC2 Auto Scaling



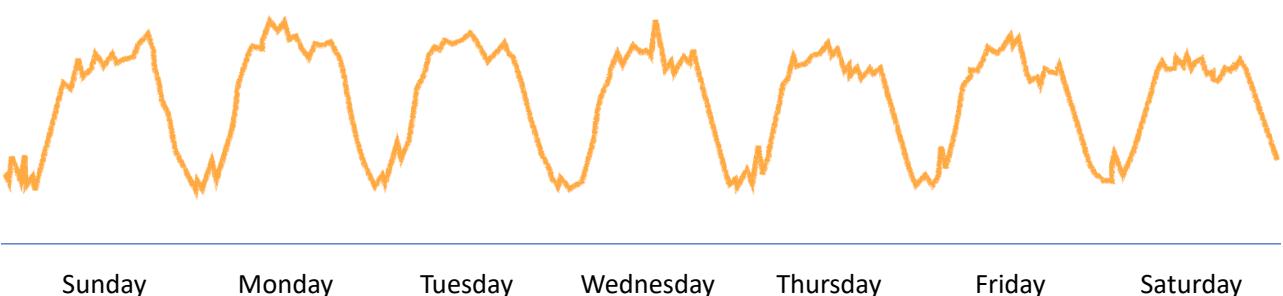
- Helps you maintain application availability
- Enables you to automatically add or remove EC2 instances according to conditions that you define
- Detects impaired EC2 instances and unhealthy applications, and replaces the instances without your intervention
- Provides several scaling options – Manual, scheduled, dynamic or on-demand, and predictive

© 2019 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

557

## Typical weekly traffic at Amazon.com

Provisioned capacity



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

558

## November traffic to Amazon.com

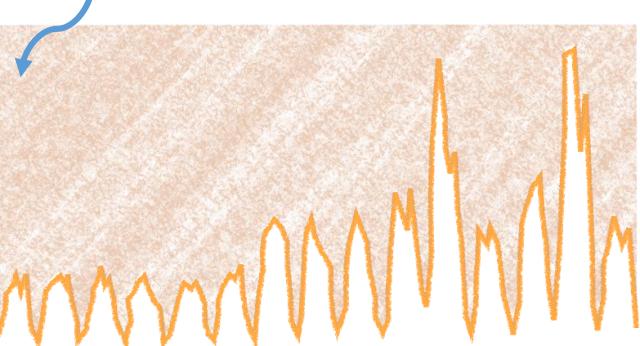
Provisioned capacity

**76 percent**

The challenge is to efficiently guess the unknown quantity of how much compute capacity you need.

**24 percent**

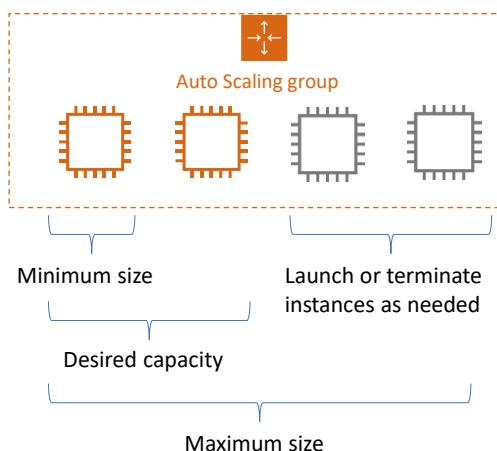
November



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

559

## Auto Scaling groups

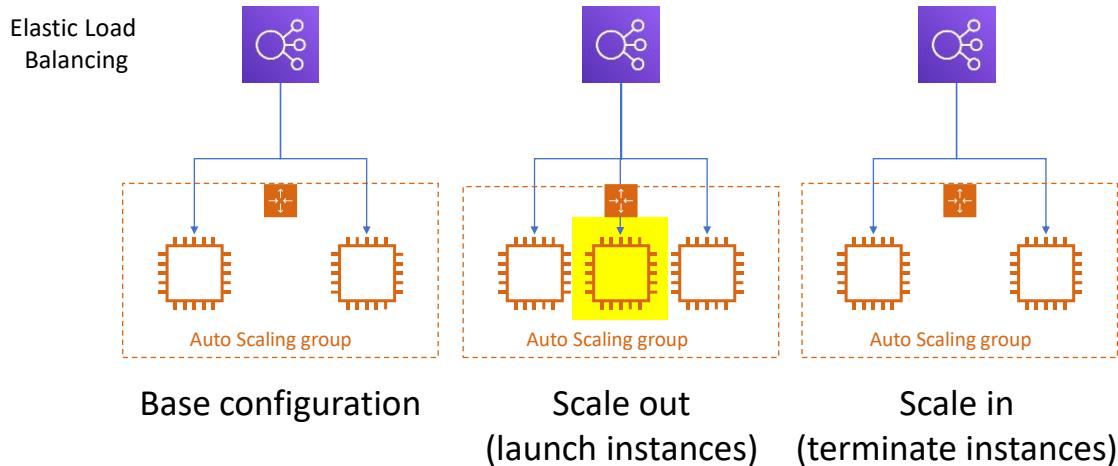


An **Auto Scaling group** is a collection of EC2 instances that are treated as a logical grouping for the purposes of automatic scaling and management.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

560

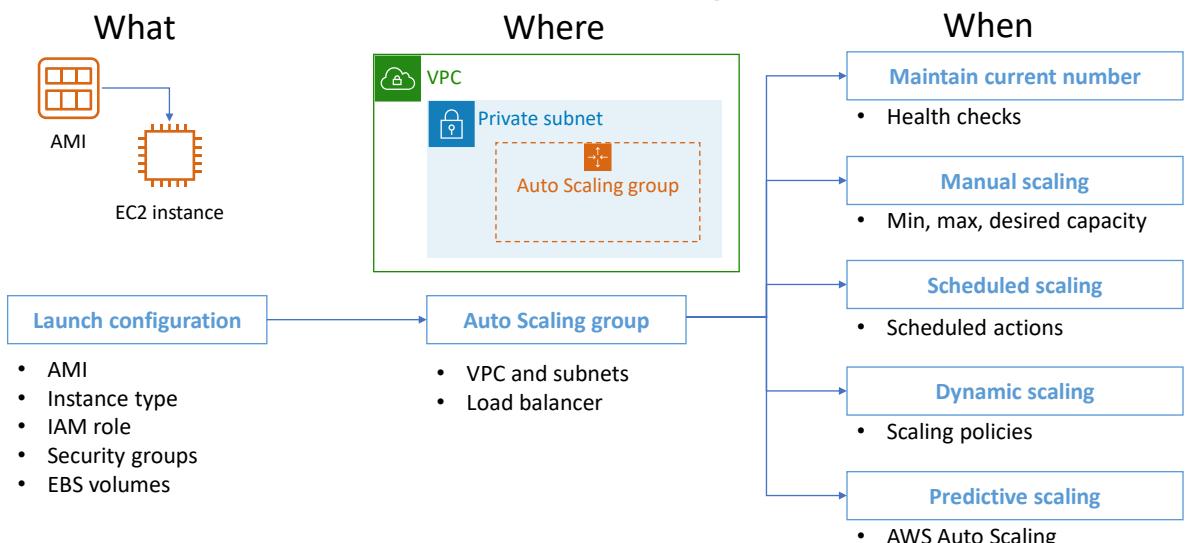
# Scaling out versus scaling in



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

561

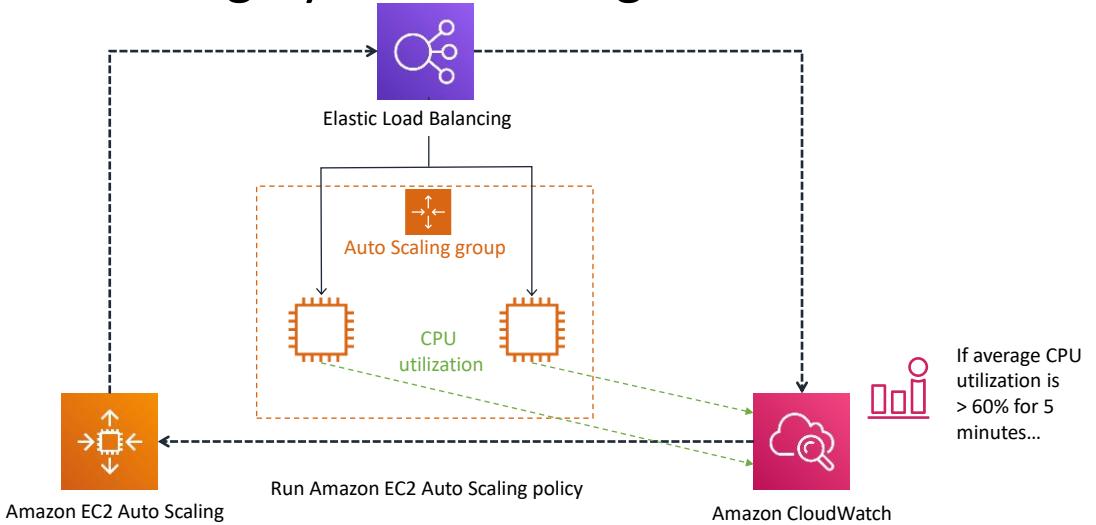
## How Amazon EC2 Auto Scaling works



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

562

# Implementing dynamic scaling



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

563

## AWS Auto Scaling



### AWS Auto Scaling

- Monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost
- Provides a simple, powerful user interface that enables you to build scaling plans for resources, including –
  - Amazon EC2 instances and Spot Fleets
  - Amazon Elastic Container Service (Amazon ECS) Tasks
  - Amazon DynamoDB tables and indexes
  - Amazon Aurora Replicas

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

564

## Section 3 key takeaways



565

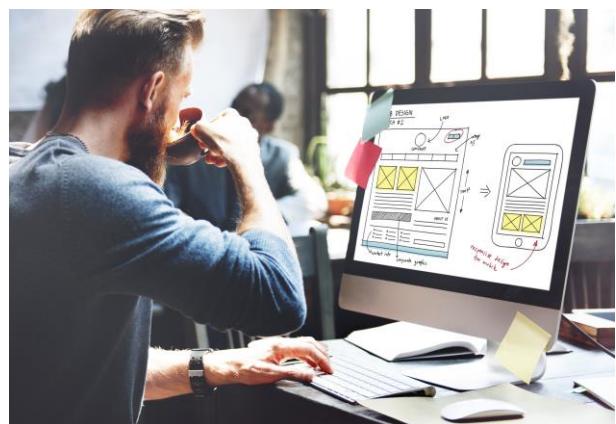


- Scaling enables you to respond quickly to changes in resource needs.
- Amazon EC2 Auto Scaling maintains application availability by automatically adding or removing EC2 instances.
- An Auto Scaling group is a collection of EC2 instances.
- A launch configuration is an instance configuration template.
- Dynamic scaling uses Amazon EC2 Auto Scaling, CloudWatch, and Elastic Load Balancing.
- AWS Auto Scaling is a separate service from Amazon EC2 Auto Scaling.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

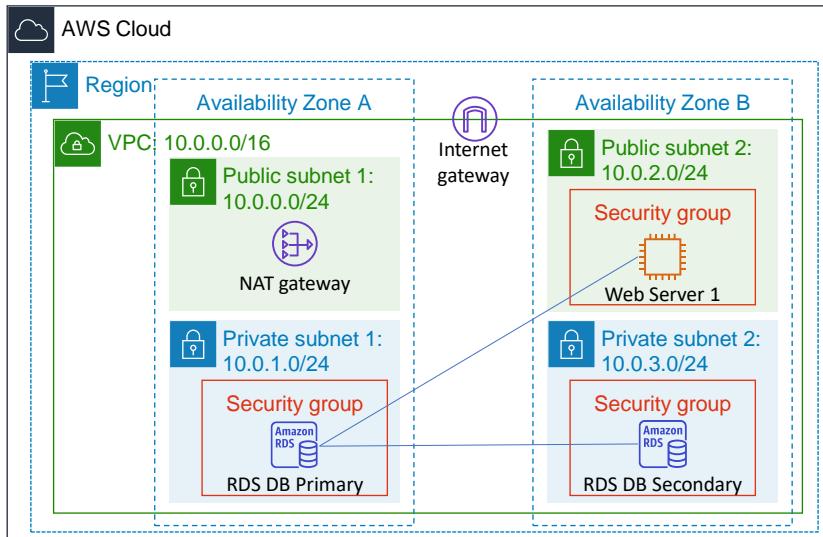
## Lab 6: Scale and Load Balance Your Architecture

566



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## Lab 6: Scenario



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

567

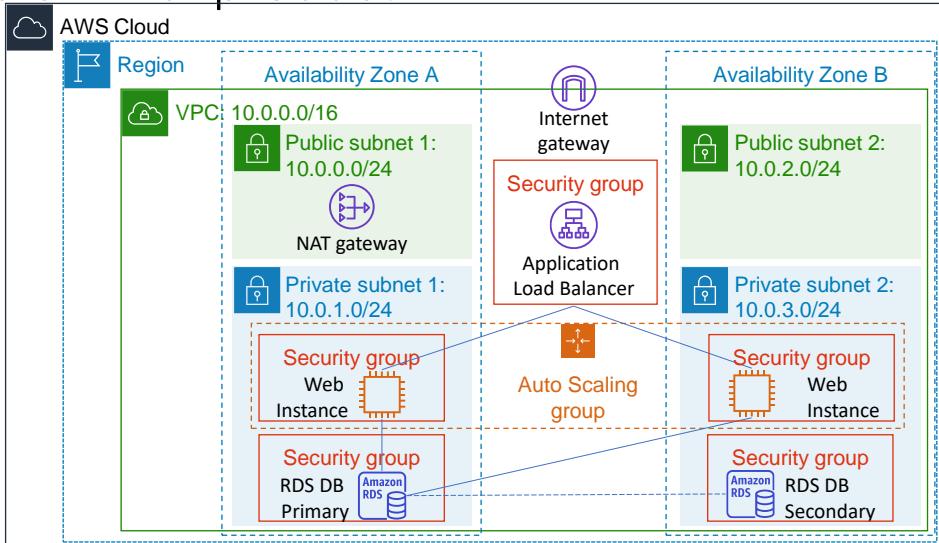
## Lab 6: Tasks

- Create an Amazon Machine Image (AMI) from a running instance.
- Create an Application Load Balancer.
- Create a launch configuration and an Auto Scaling group.
- Automatically scale new instances within a private subnet.
- Create Amazon CloudWatch alarms and monitor performance of your infrastructure.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

568

# Lab 6: Final product



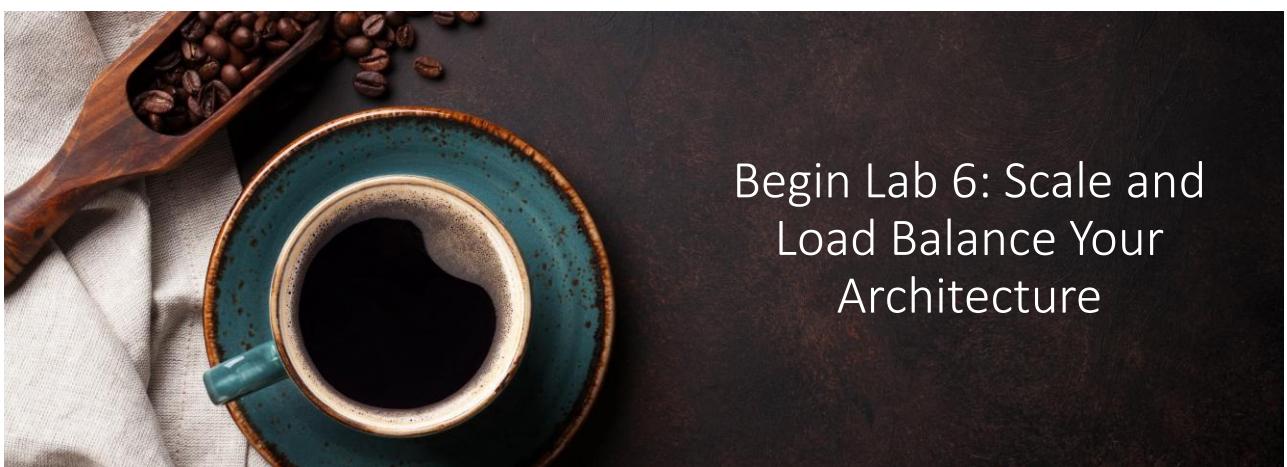
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

569



**aws** academy

Begin Lab 6: Scale and  
Load Balance Your  
Architecture



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

570



## Lab debrief: Key takeaways



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

571

### Module 10: Automatic Scaling and Monitoring

## Module wrap-up

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

# Module summary

In summary, in this module you learned how to:

- Indicate how to distribute traffic across Amazon Elastic Compute Cloud (Amazon EC2) instances using Elastic Load Balancing.
- Identify how Amazon CloudWatch enables you to monitor AWS resources and applications in real time.
- Explain how Amazon EC2 Auto Scaling launches and releases servers in response to workload changes.
- Perform scaling and load balancing tasks to improve an architecture.

## Complete the knowledge check



## Sample exam question

Which service would you use to send alerts based on Amazon CloudWatch alarms?

- A. Amazon Simple Notification Service
- B. AWS CloudTrail
- C. AWS Trusted Advisor
- D. Amazon Route 53

Thank you