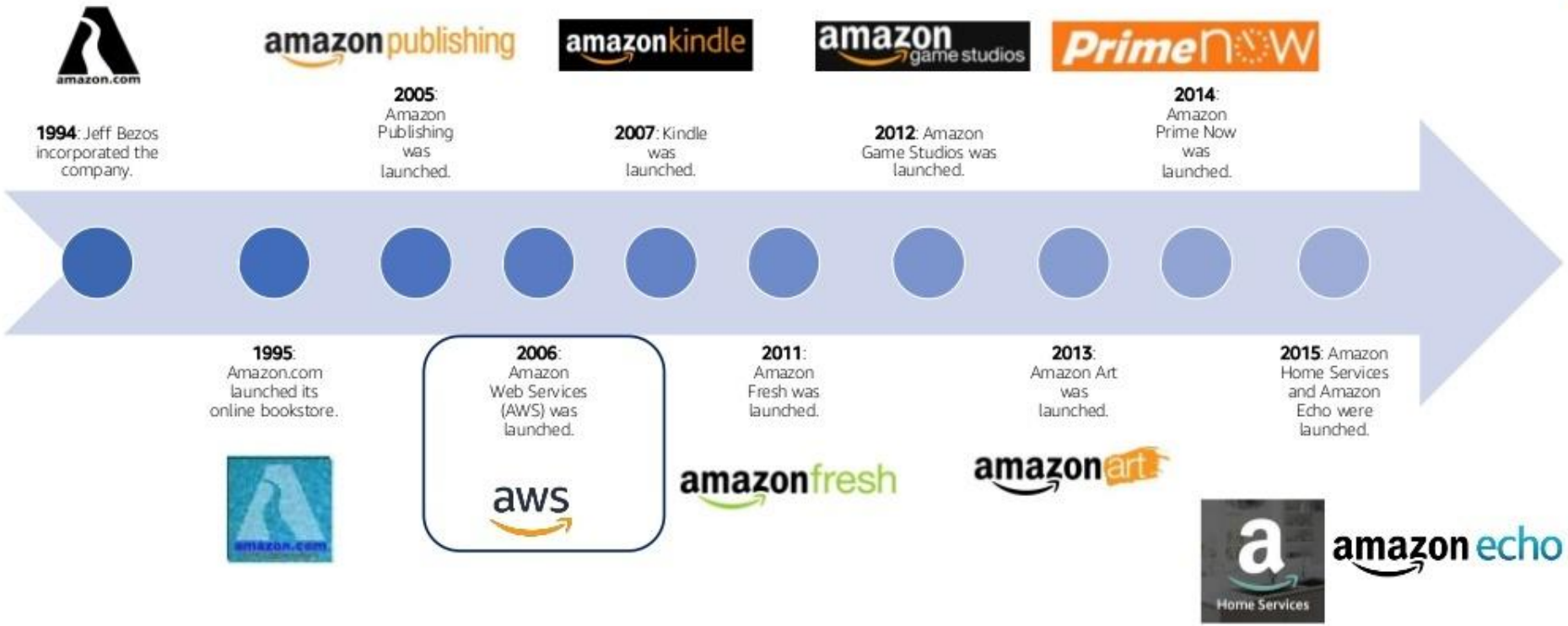
Module 1
Introduction to AWS

Amazon Web Services (AWS)

Enable businesses and developers to use web services to build scalable, sophisticated applications.

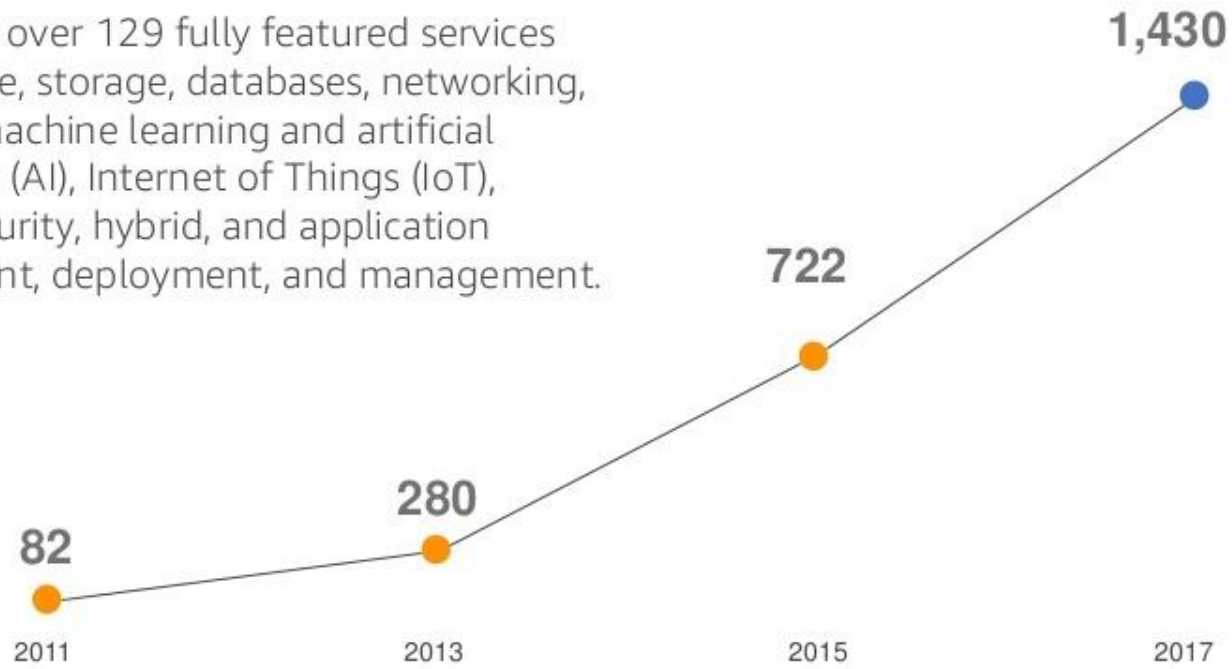
Amazon History



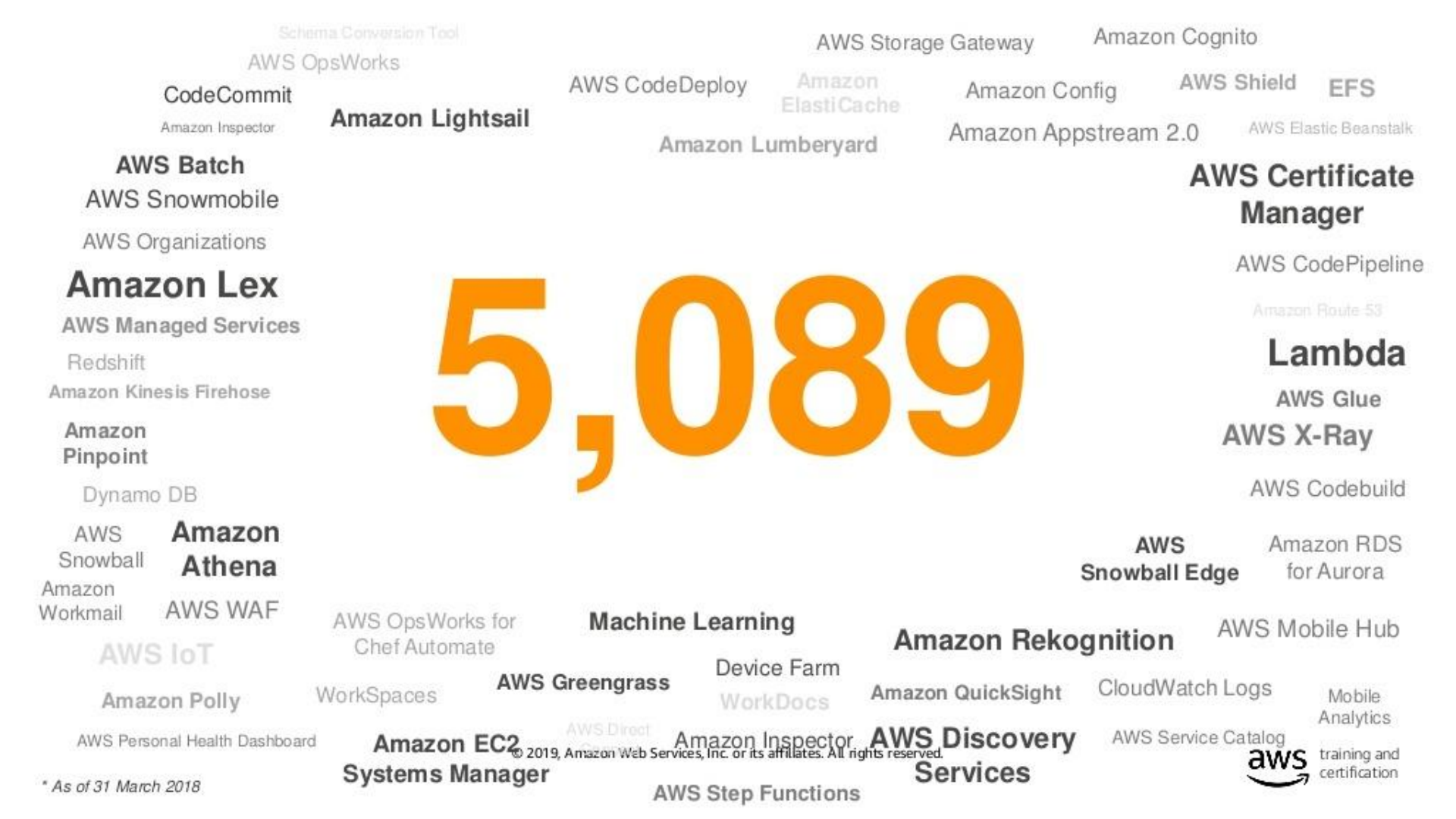
aws training and certification

AWS Pace of Innovation

AWS offers over 129 fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, and application development, deployment, and management.



** As of 31 March 2018*


Schema Conversion Tool
AWS OpsWorks
CodeCommit
Amazon Inspector
Amazon Lightsail
AWS Storage Gateway
Amazon Cognito
AWS CodeDeploy
Amazon ElastiCache
Amazon Config
AWS Shield
EFS
Amazon Appstream 2.0
AWS Elastic Beanstalk
Amazon Lumberyard
AWS Batch
AWS Snowmobile
AWS Certificate Manager
AWS Organizations
Amazon Lex
AWS CodePipeline
AWS Managed Services
Amazon Route 53
5,089
Redshift
Lambda
Amazon Kinesis Firehose
AWS Glue
Amazon Pinpoint
AWS X-Ray
Dynamo DB
AWS Codebuild
AWS Snowball
Amazon Athena
AWS Snowball Edge
Amazon RDS for Aurora
Amazon Workmail
AWS WAF
AWS OpsWorks for Chef Automate
Machine Learning
AWS Mobile Hub
Amazon Rekognition
AWS IoT
Device Farm
AWS Greengrass
Amazon QuickSight
CloudWatch Logs
Amazon Polly
WorkSpaces
WorkDocs
Mobile Analytics
AWS Direct
AWS Personal Health Dashboard
Amazon EC2
Amazon Inspector
AWS Discovery Services
AWS Service Catalog
Systems Manager
AWS Step Functions
training and certification
* As of 31 March 2018
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Cloud Computing

Applications


Virtual Desktops


Collaboration and Sharing

Platform Services

Databases	Analytics	App Services	Deployment and Management	Mobile Services
Relational	Cluster Computing	Queuing	Containers	Identity
NoSQL	Real-time	Orchestration	Dev/ops Tools	Sync
Caching	Data Warehouse	App Streaming	Resource Templates	Mobile Analytics
	Data Workflows	Transcoding	Usage Tracking	Notifications
		Email	Monitoring and Logs	
		Search		

Foundation Services


Compute
(Virtual, Auto-scaling and Load Balancing)


Networking


Storage
(Object, Block and Archive)

Infrastructure

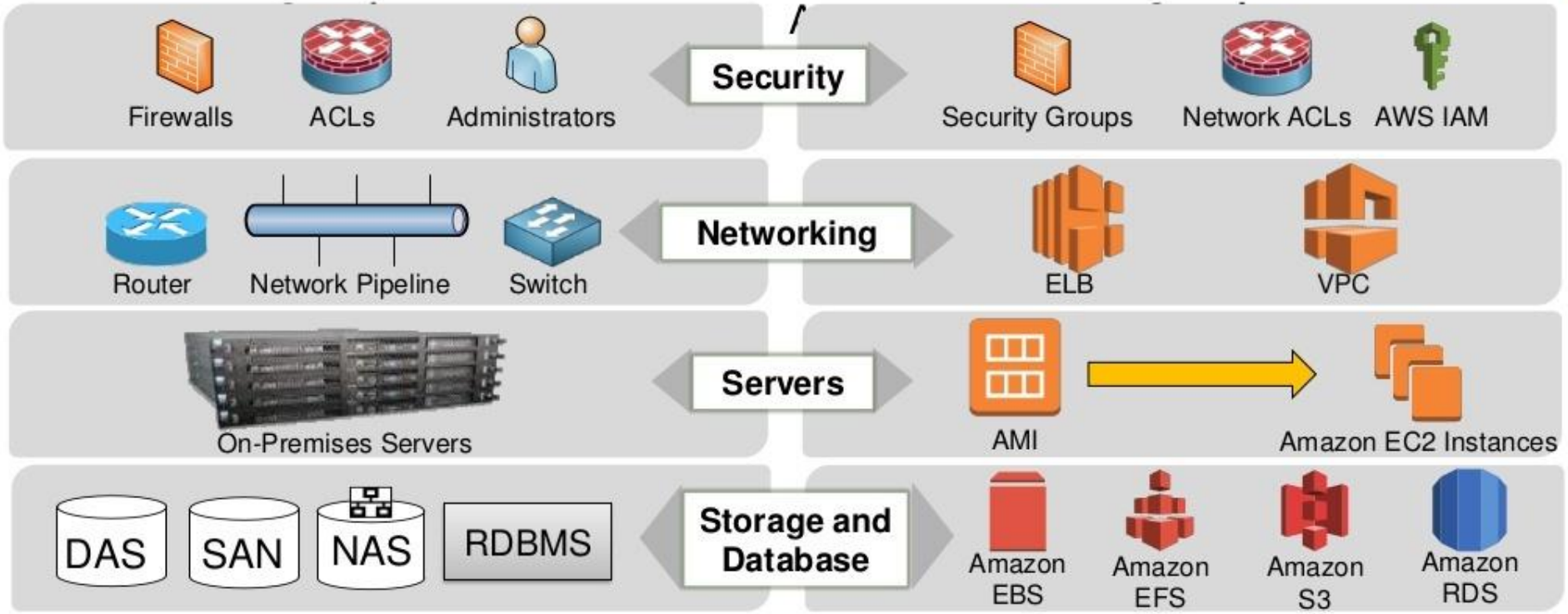
Regions

Availability Zones


Edge Locations

aws training and certification

AWS Core Infrastructure and Services



aws training and certification

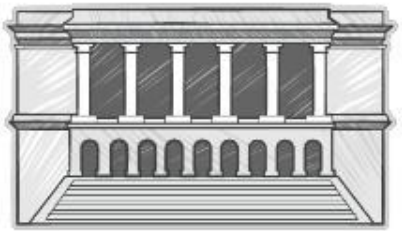
AWS Customers

Enterprise Customers

Amazon Web Services delivers a mature set of services specifically designed for the unique security, compliance, privacy, and governance requirements of large organizations.

Public Sector

Paving the way for innovation and supporting world-changing projects in government, education and nonprofit organizations.



Startups

From the spark of an idea, to your first customer, to IPO and beyond, let Amazon Web Services help you build and grow your startup.

Advantages and Benefits of AWS Cloud Computing

Trade **capital expense** for **flexible expense**.

Increase **speed** and **agility**.

Benefit from **massive economies of scale**.

Stop spending money on running and maintaining data centers.

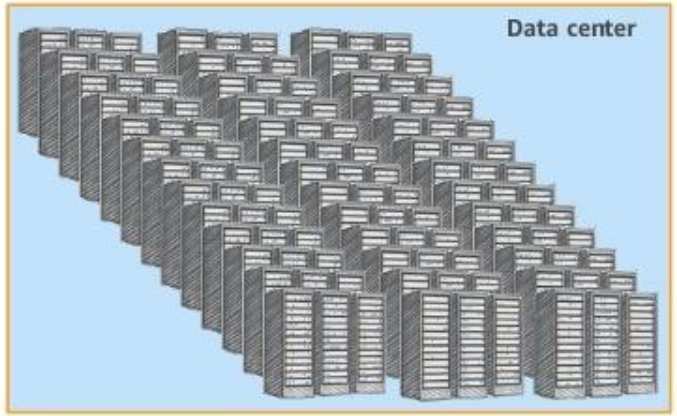
Eliminate guessing on your capacity needs.

Go global in minutes.

AWS Global Infrastructure

AWS Data Centers

- A single data center typically houses several thousands of servers.



- All data centers are online.
  - No data center is "cold".

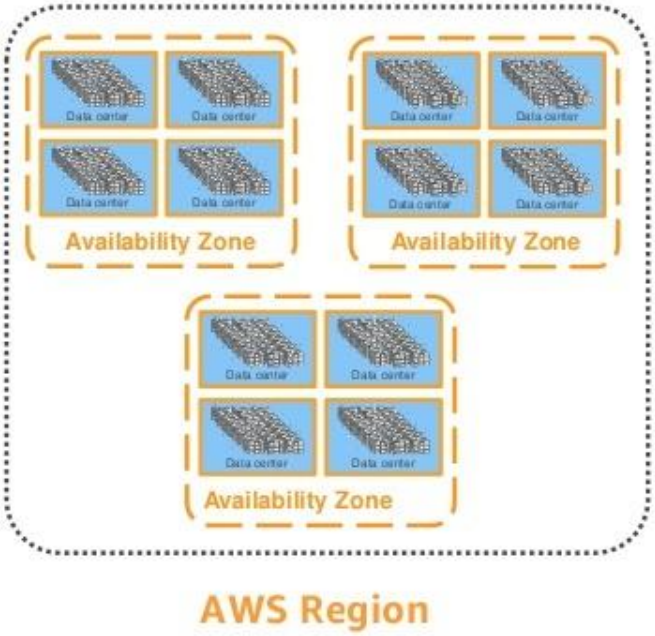
- AWS custom network equipment:
  - Multi-ODM sourced.
  - Amazon custom network protocol stack.

AWS Availability Zones (AZ)

- Each Availability Zone is:
  - Made up of **one or more** data centers.
  - Designed for **fault isolation**.
  - Interconnected with other Availability Zones using high-speed **private** links.
- You choose your Availability Zones.
- AWS recommends replicating across AZs for resiliency.

AWS Regions

- Each region is made up of **two or more Availability Zones**.
- AWS has **20 regions** worldwide.
- You enable and control **data replication** across regions.
- Communication between regions uses **AWS backbone network** connections infrastructure.



AWS Global Infrastructure Map

aws training and certification

AWS Global Infrastructure – Edge Locations

- 149* Edge Locations in 65 cities
- Local points of presence that support AWS services like:


Amazon Route 53


Amazon CloudFront

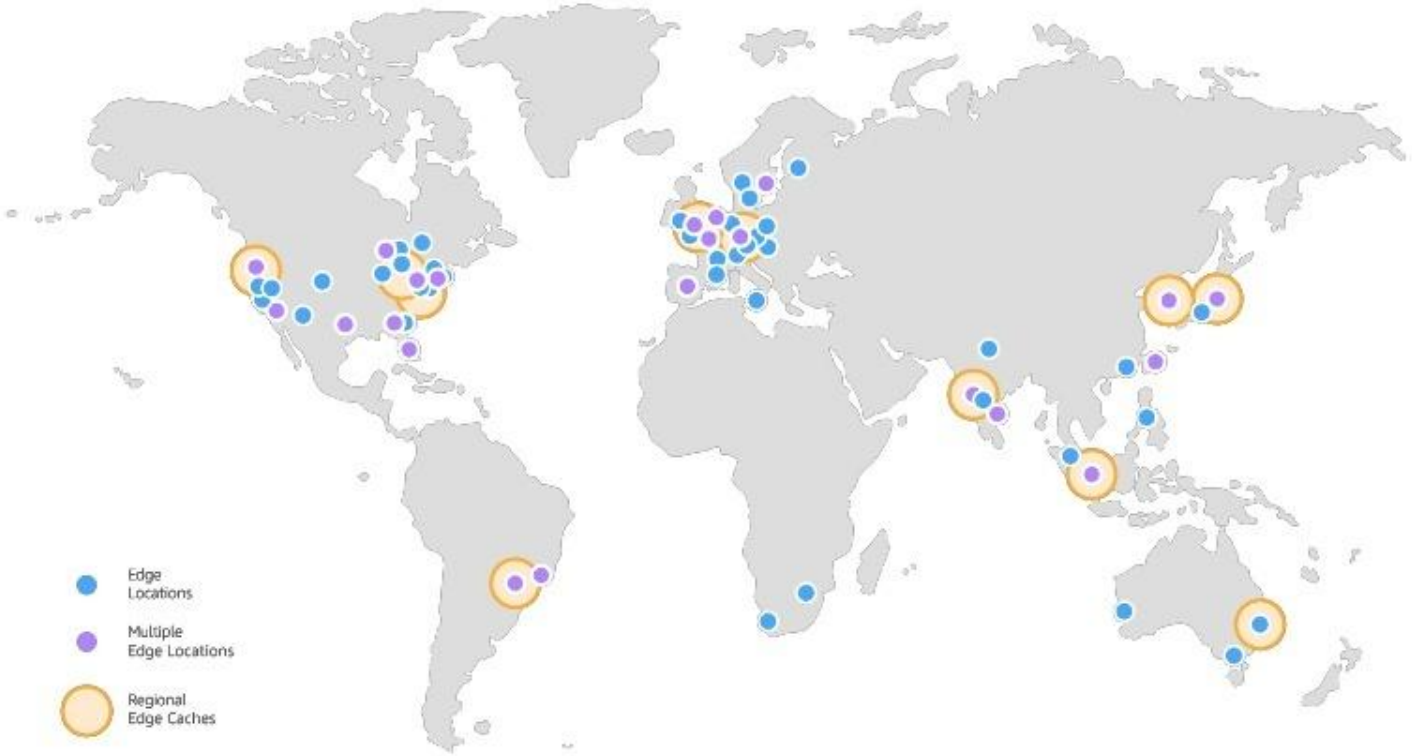

AWS WAF


AWS Shield


Lambda@Edge

*as of January 2019

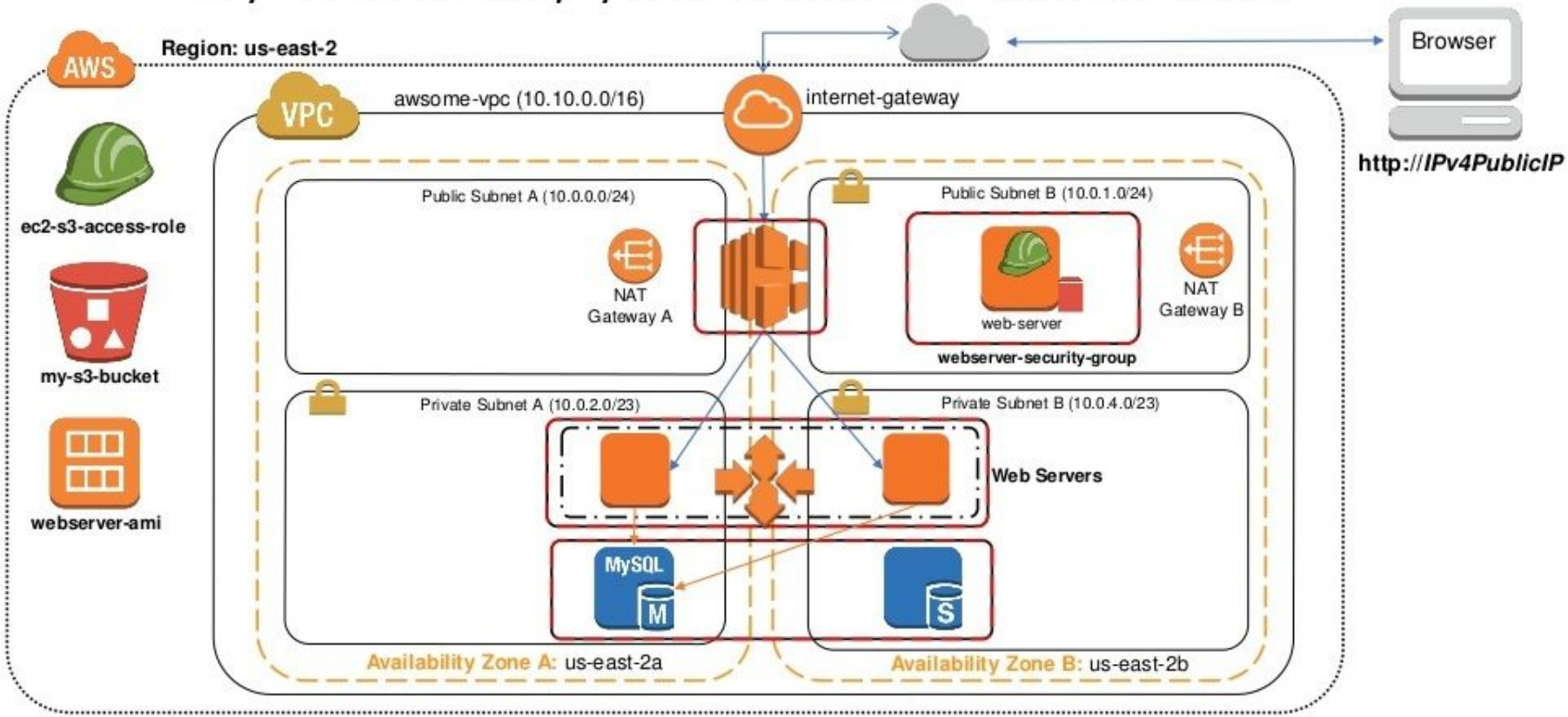
AWS Global Infrastructure:
Edge Locations and Regional Edge Caches



aws training and certification

Instructor Demo
AWS Management Console

By the end, you'll understand this



aws training and certification

Module 2
AWS Foundational Services

Module 2 Layout

- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Block Store (EBS)
- Amazon Virtual Private Cloud (VPC)
- Demo: Launching a Web Server
- Amazon Simple Storage Service (S3)
- Demo: Amazon S3

Amazon Elastic Compute Cloud (EC2)

Amazon Elastic Compute Cloud (EC2)

Amazon EC2

- **Resizable** compute capacity
- Complete control of your computing resources
- **Reduced time required** to obtain and boot new server instances

Amazon EC2 Facts

- Scale capacity as your computing requirements change
- Pay only for capacity that you actually use
- Choose Linux or Windows
- Deploy across AWS Regions and Availability Zones for reliability
- Use tags to help manage your Amazon EC2 resources

Launching an Amazon EC2 Instance

1. **Determine the AWS Region** in which you want to launch the Amazon EC2 instance.
2. **Launch** an Amazon EC2 instance from a pre-configured Amazon Machine Image (AMI).
3. **Choose an instance type** based on CPU, memory, storage, and network requirements.
4. **Configure** network, IP address, security groups, storage volume, tags, and key pair.

1. Determine the AWS Region

AWS Global Infrastructure Map

aws training and certification

2. Launch from an AMI

Amazon Machine Image (AMI) Details

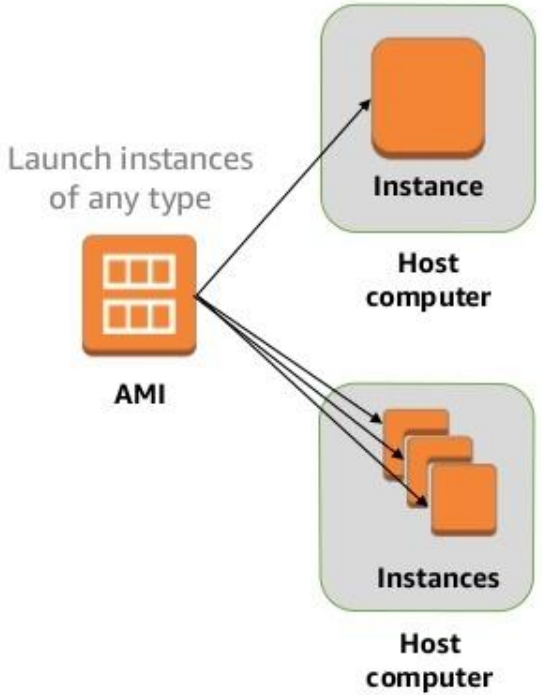
An AMI includes the following:

- A template for the root volume for the instance (for example, an operating system, an application server, and applications).
- Launch permissions that control which AWS accounts can use the AMI to launch instances.
- A block device mapping that specifies the volumes to attach to the instance when it is launched.

Instances and AMIs

Select an AMI based on:

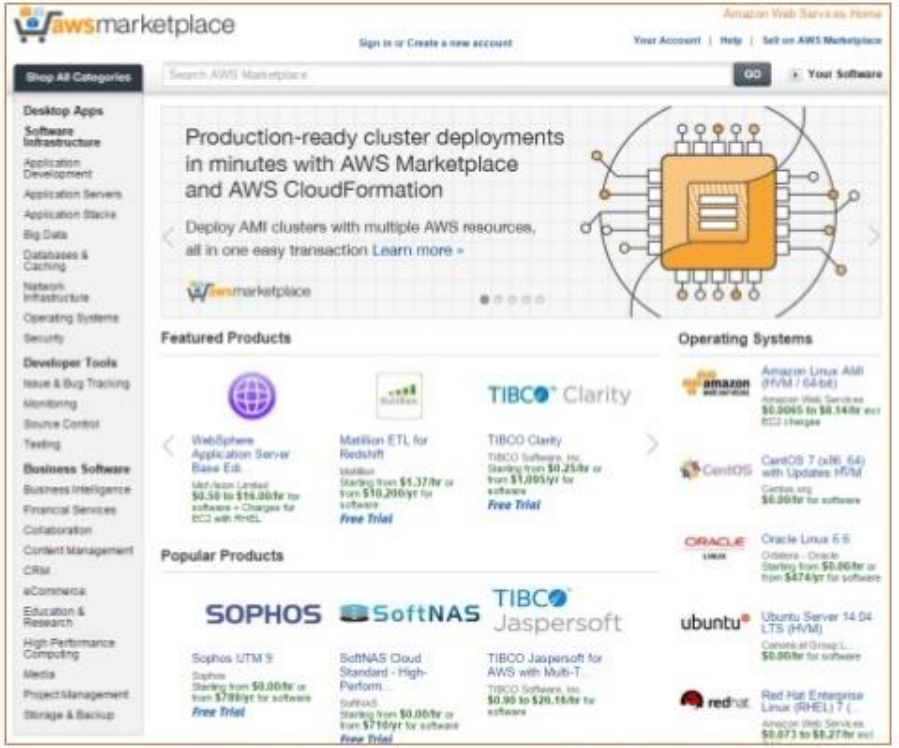
- Region
- Operating system
- Architecture (32/64bit x86 or 64-bit ARM)
- Launch permissions
- Storage for the root device



AWS Marketplace – IT Software Optimized for the Cloud

- Online store to discover, purchase, and deploy IT software on top of the AWS infrastructure.
- Catalog of **4,500+ IT software** solutions including Paid, BYOL, Open Source, SaaS, and free-to-try options.
- **Pre-configured** to operate on AWS.
- Software checked by AWS for security and operability.
- Deploys to AWS environment in minutes.
- Flexible, usage-based billing models.
- Software charges **billed to AWS account**.

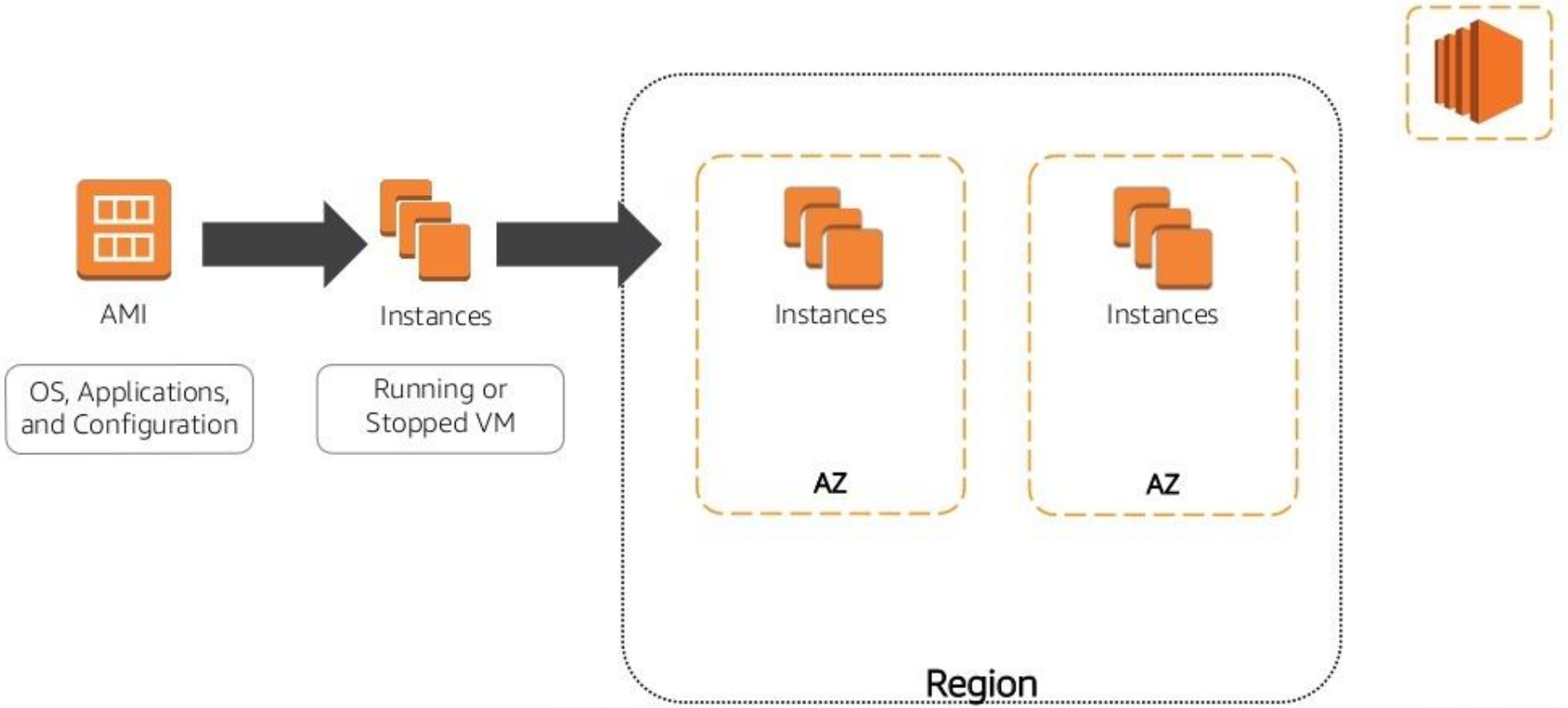
Includes AWS Test Drive.



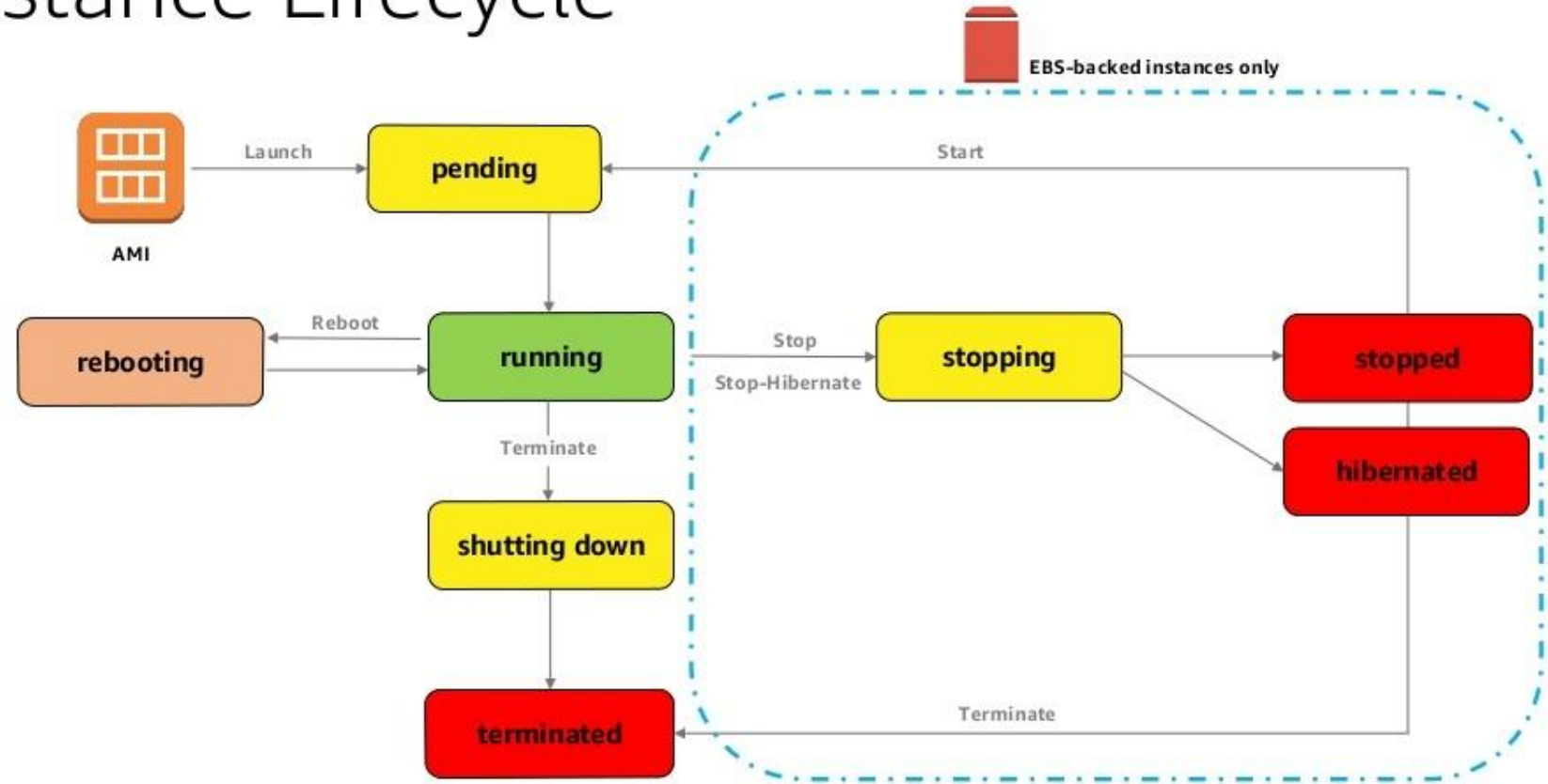
https://aws.amazon.com/marketplace

aws training and certification

Amazon EC2 Instances



Instance Lifecycle



3. Choose an Instance Type

Choosing the Right Amazon EC2 Instance

EC2 instance types are optimized for different use cases and workload requirements and come in multiple sizes.

Consider the following when choosing your instances:

- Core count
- Memory size
- Storage size and type
- Network performance
- CPU technologies

Intel Processor Technologies

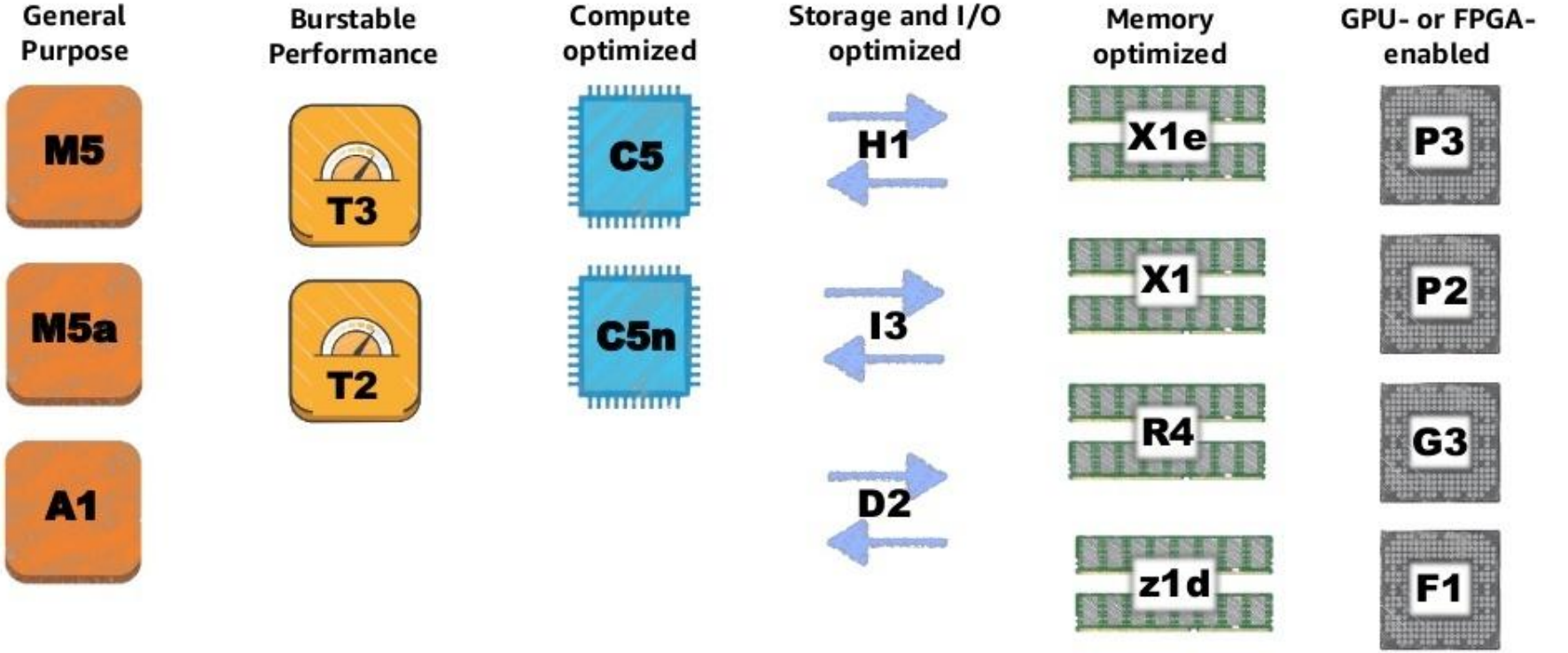
AWS customers can choose EC2 instances with **Intel® Xeon® processors** for high performance.

- **Intel AVX (AVX, AVX2 and AVX-512)** – Highly parallel HPC workloads.
- **Intel AES-NI** – Accelerates encryption/decryption of data.
- **Intel Turbo Boost Technology** – More computing power when you need it with performance that adapts to spikes in your workload.
- **Intel Transactional Synchronization (TSX) Extensions** – Enable execution of transactions that are independent to accelerate throughput.
- **P state & C state control** – Ability to individually tune each cores performance & sleep states to improve application performance.

C5n Instance Example

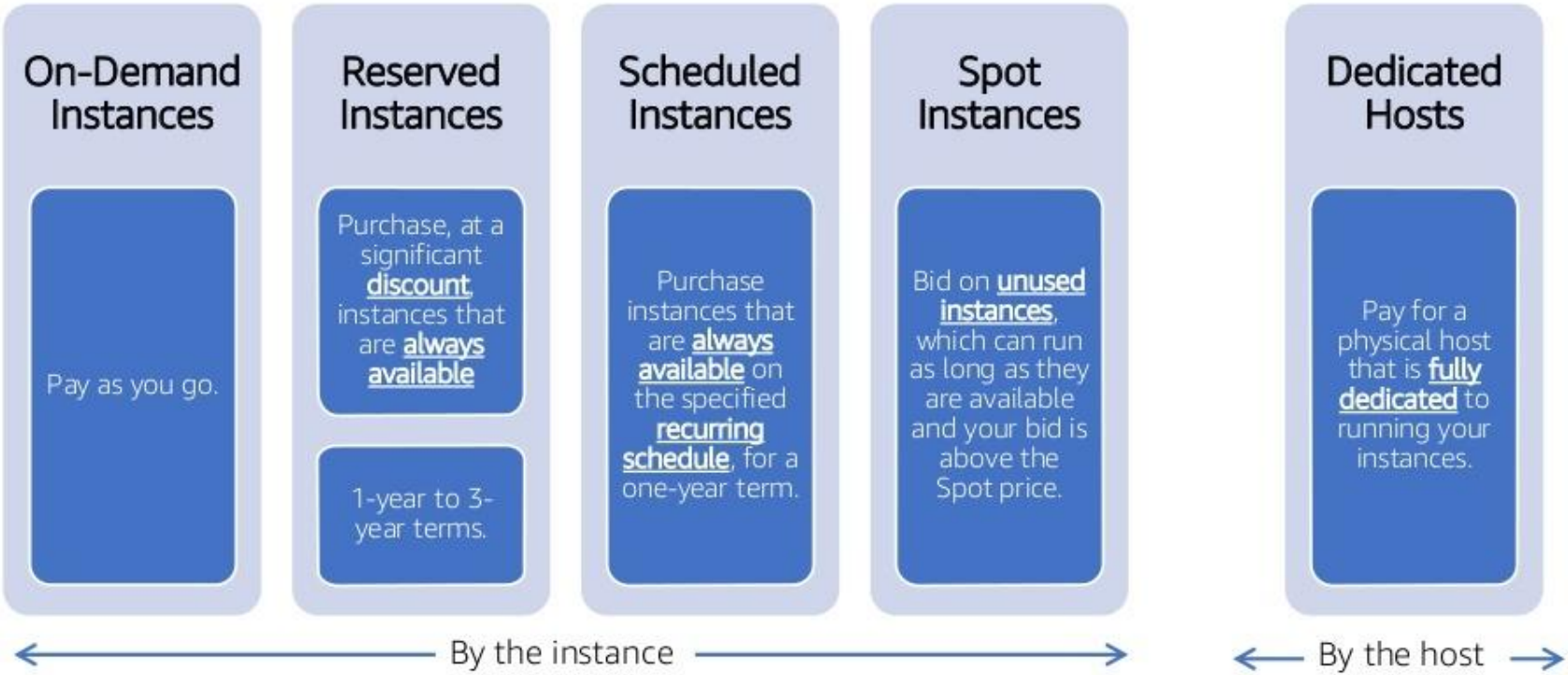
- c5n.18xlarge offers 72 vCPUs and 192 GiB of memory
- Up to 100 Gbps of network bandwidth
- 3.0 GHz Intel Xeon Platinum processors with Intel Advanced Vector Extension 512 (AVX-512) instruction set
- Run each core at up to 3.5 GHz using Intel Turbo Boost Technology
- Based on the next generation AWS Nitro System

Broad Set of Compute Instance Types



aws training and certification

Amazon EC2 Purchasing Models



4. Configure your instance

Instance User Data

- Can be passed to the instance at launch.
- Can be used to perform common automated configuration tasks.
- Runs scripts after the instance starts.

Adding User Data

- You can specify user data when launching an instance.
- User data can be:
  - Linux script – executed by **cloud-init**
  - Windows batch or PowerShell scripts – executed by **EC2Launch** or **EC2Config** service
- User data scripts run once per instance ID by default.

User Data Example Linux

```
#!/bin/sh
yum -y install httpd
chkconfig httpd on
/etc/init.d/httpd start
```

User data shell scripts must start with the #! characters and the path to the interpreter you want to read the script.

Install Apache web server
Enable the web server
Start the web server

User Data Example Windows

```
<powershell>
Import-Module ServerManager
```

Import the Server Manager module for Windows PowerShell.

```
Install-WindowsFeature web-server, web-webserver
Install-WindowsFeature web-mgmt-tools
</powershell>
```

Install IIS
Install Web Management Tools

Instance Metadata

- Is data about your instance.
- Can be used to configure or manage a running instance.
- To get the instance metadata from within a running instance, use the following URI:

```
http://169.254.169.254/latest/meta-data/
```

Metadata:
Availability Zone:
us-east-1a
Instance type:
i3.2xlarge
Public IP:
52.7.197.98

Metadata:
Availability Zone:
us-east-1d
Instance type:
c5.18xlarge
Public IP:
34.234.30.48

Other compute services

Amazon Elastic Container Service
Run and Manage Docker Containers

Amazon Elastic Container Service for Kubernetes
Run Managed Kubernetes on AWS

AWS Fargate
Run Containers without Managing Servers or Clusters

AWS Lambda
Run your Code in Response to Events

VMware Cloud on AWS
Build a Hybrid Cloud without Custom Hardware

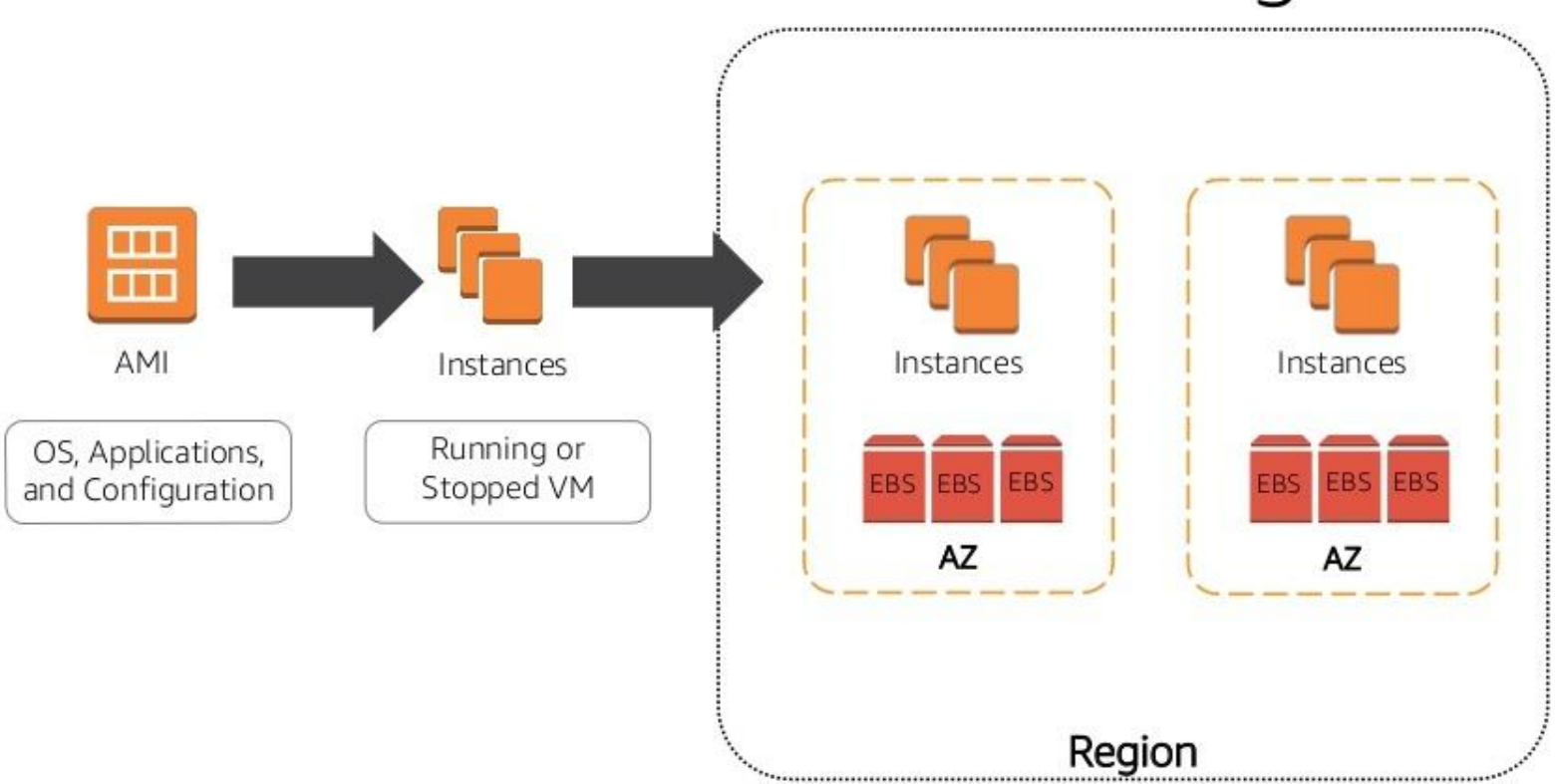
Block Storage Service
Amazon Elastic Block Store (EBS)

Amazon Elastic Block Store (EBS)

Amazon EBS

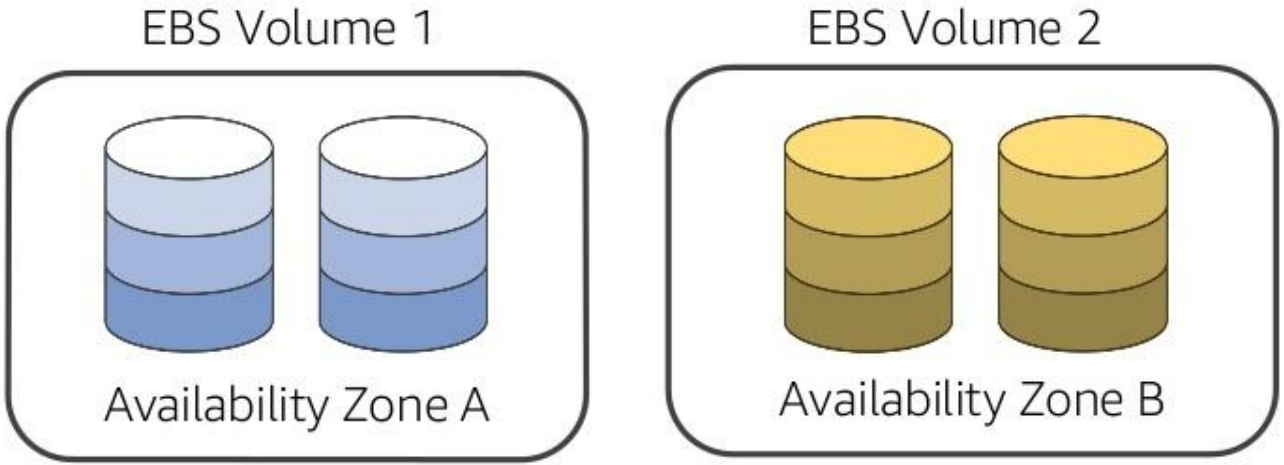
- **Persistent block level storage** volumes offer consistent and low-latency performance.
- Stored data is automatically replicated within its Availability Zone.
- Snapshots are stored durably in Amazon S3.

Persistent EC2 Instance storage



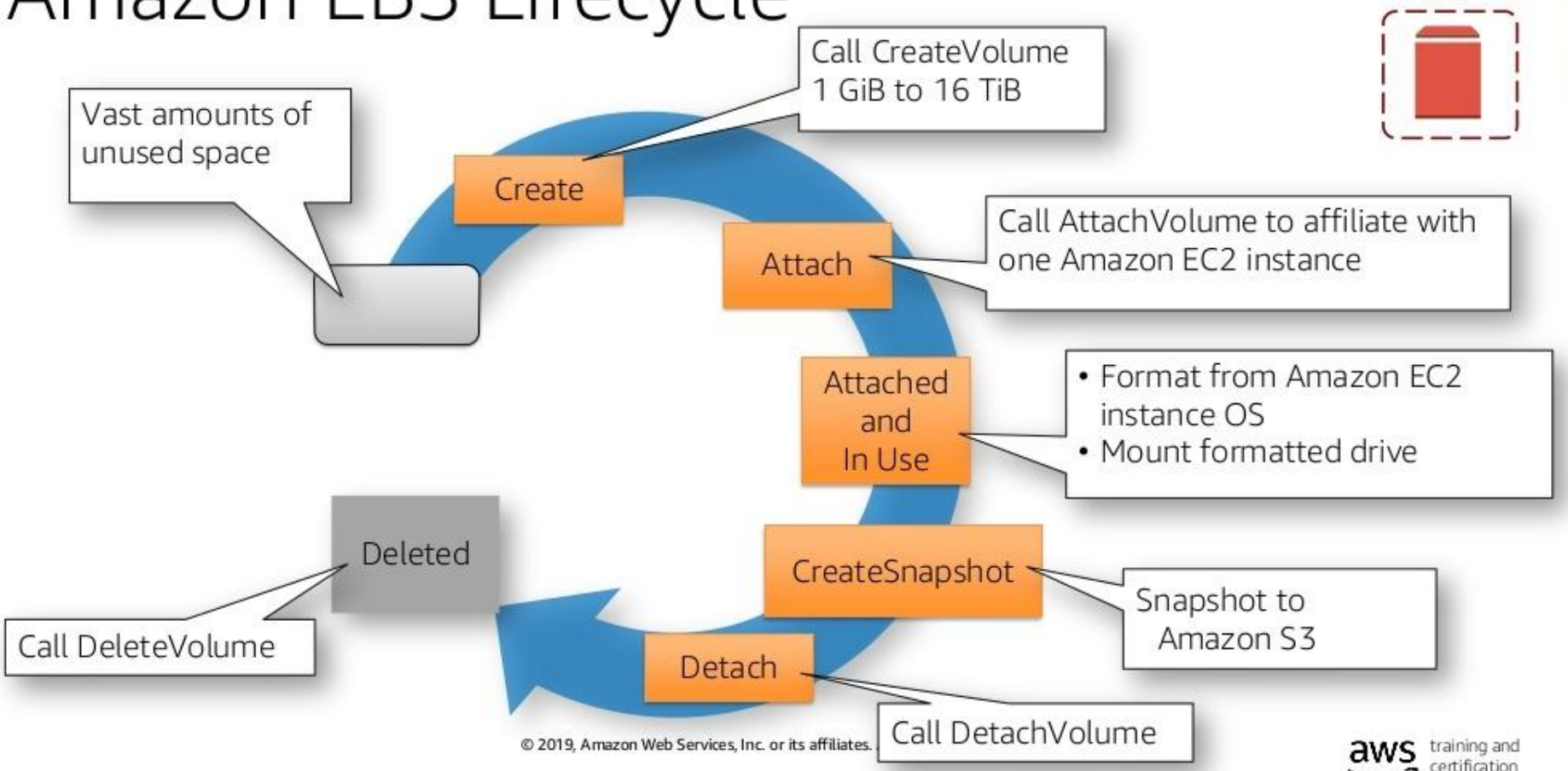
Amazon EBS Scope

Amazon EBS volumes are in a single Availability Zone



Volume data is replicated across multiple servers in an Availability Zone.

Amazon EBS Lifecycle



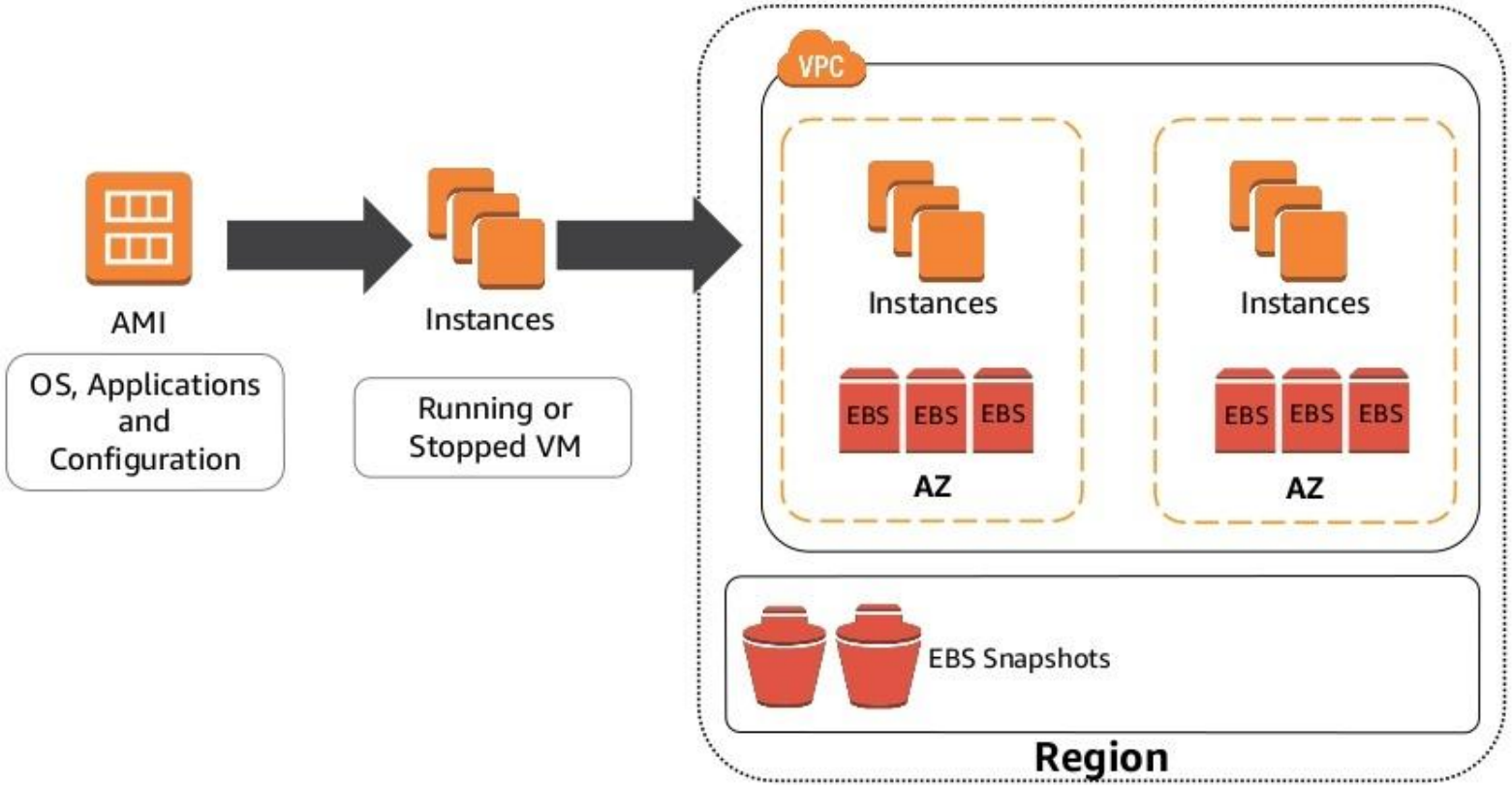
Amazon EBS Volume Types

- SSD-backed volumes are
  - Optimized for **transactional** workloads that involve **frequent read/write** operations with **small I/O** size.
  - Dominant in **IOPS** performance.
- HDD-backed volumes are
  - Optimized for **large streaming** workloads.
  - Dominant in **throughput** (measured in MiB/s).

Amazon EBS Facts

- EBS is recommended when data must be quickly accessible and requires long-term persistence.
- You can launch your EBS volumes as encrypted volumes – data stored at rest on the volume, disk I/O, and snapshots created from the volume are all encrypted.
- You can create point-in-time snapshots of EBS volumes, which are persisted to Amazon S3.

Amazon EC2 Instances



Amazon EC2 Instance Store

- Is local, complimentary direct attached block storage.
- Includes availability, number of disks, and size based on EC2 instance type.
- Is optimized for up to 3.3 million random Read IOPS and 1.4 million Write IOPS. (i3.16xlarge)
- Is SSD or HDD.
- Has no persistence.
- Automatically deletes data when an EC2 instance stops, fails or is terminated.

Amazon EBS vs. Amazon EC2 Instance Store

- Amazon EBS
  - Data stored on an Amazon EBS volume can persist independently of the life of the instance.
  - Storage is **persistent**.
- Amazon EC2 Instance Store
  - Data stored on a local instance store persists only as long as the instance is running or rebooting.
  - Storage is **ephemeral**.

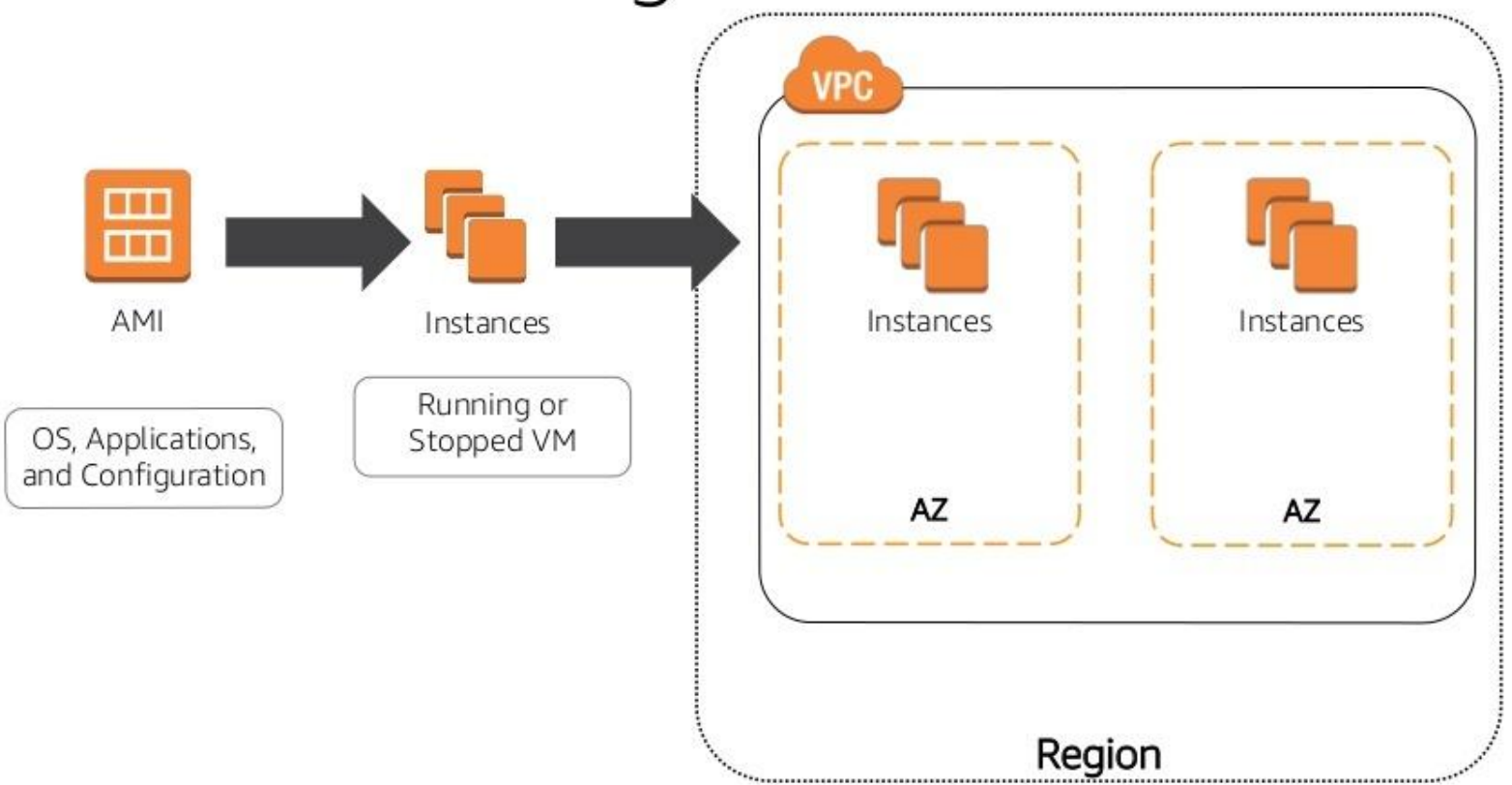
Networking
Amazon VPC

Amazon Virtual Private Cloud (VPC)

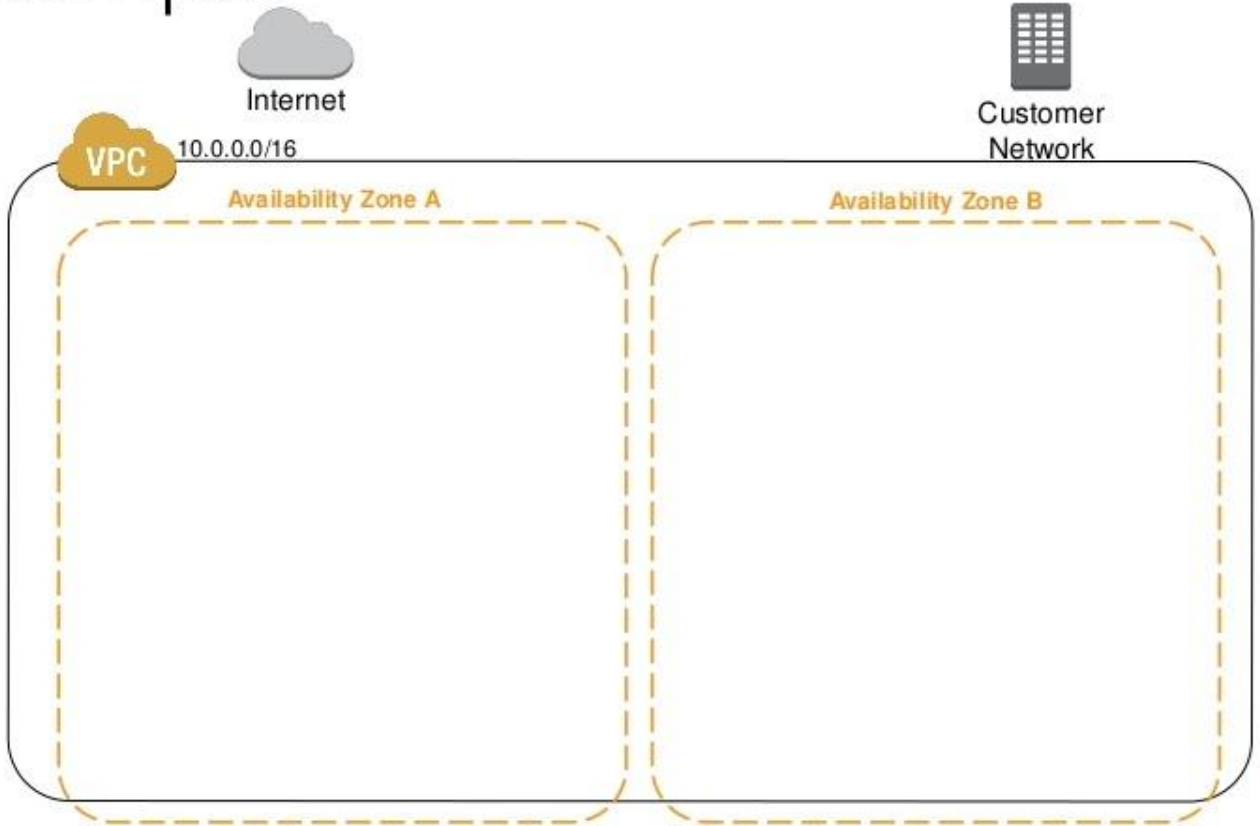
Amazon
VPC

- Provision a **private, isolated virtual network** on the AWS cloud.
- Have complete control over your virtual networking environment.

EC2 networking with VPC



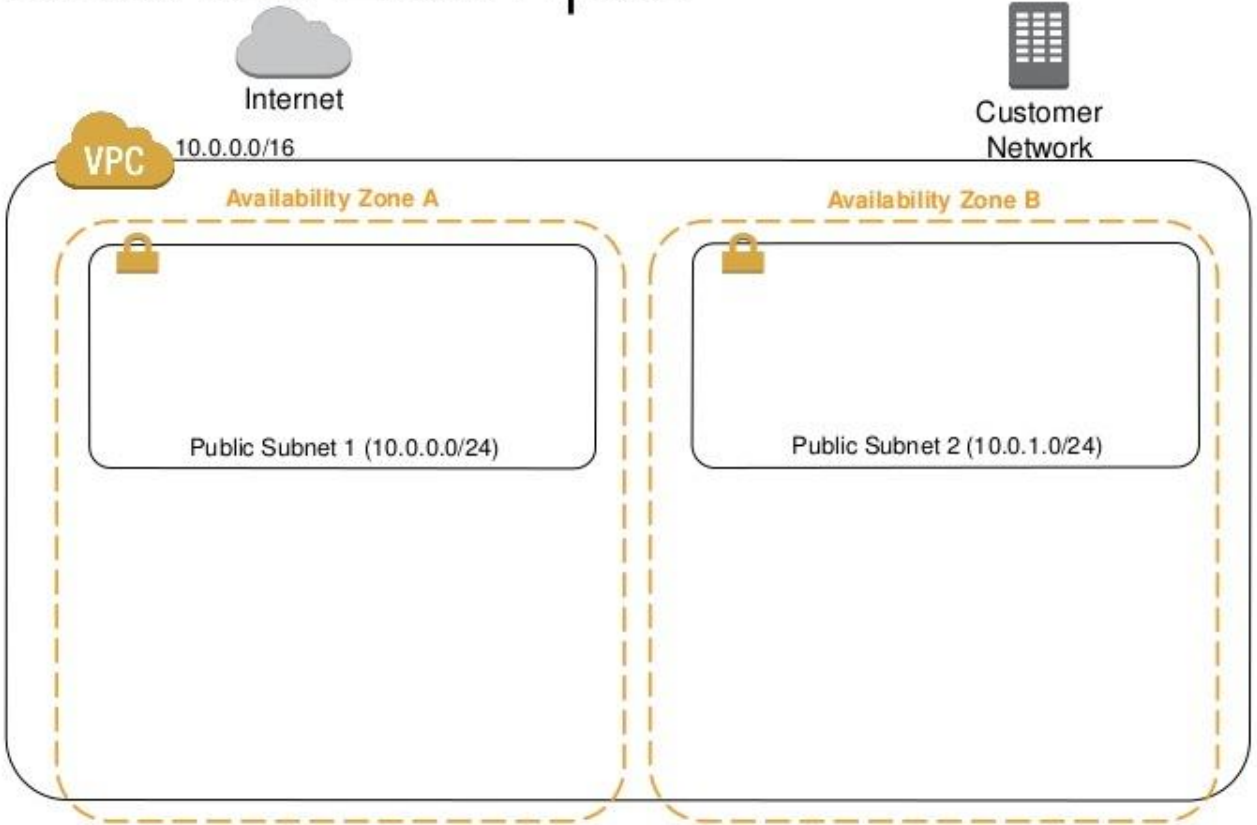
VPC Example



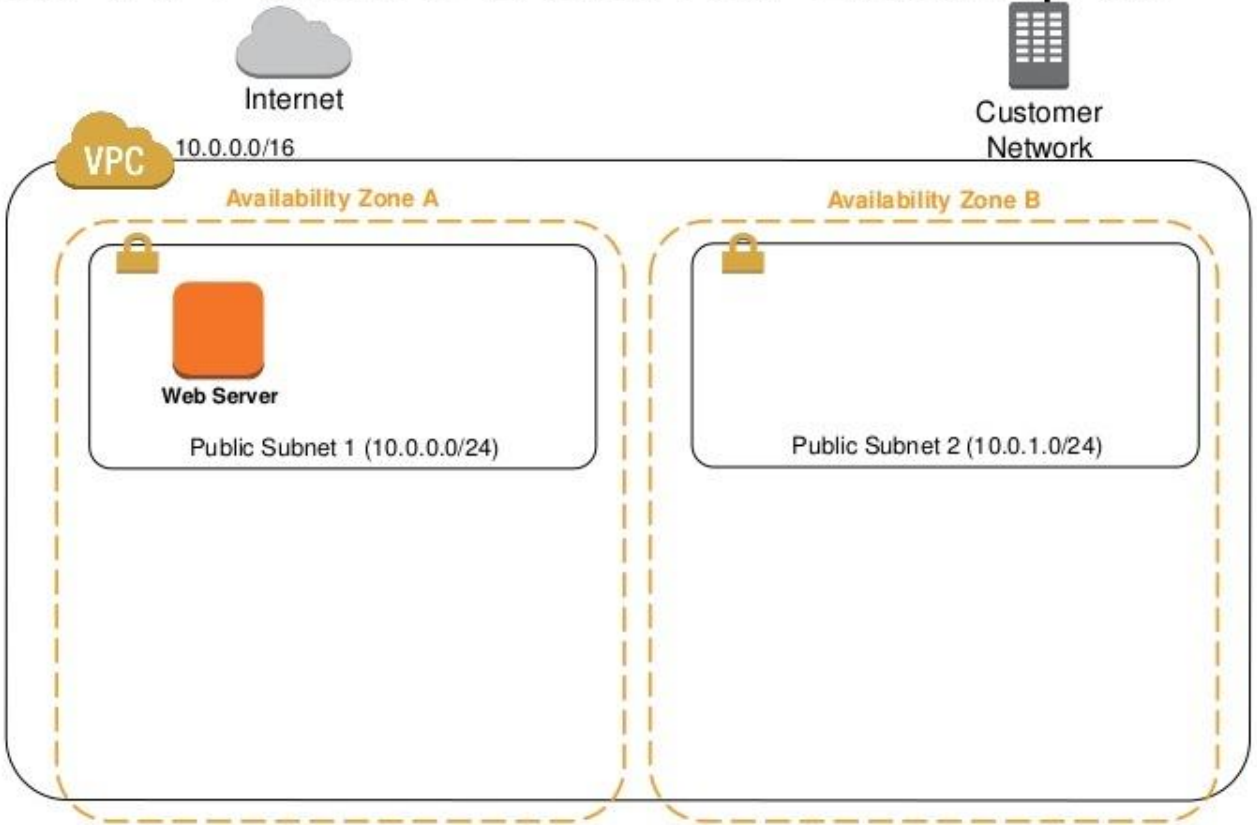
VPC and Subnets

- A VPC resides within a single Region
- A subnet defines a range of IP addresses within your VPC.
- Each subnet must reside entirely within one Availability Zone and cannot span zones.
- You can launch AWS resources into a subnet that you select.
- A public subnet (DMZ) should be used for resources that will be accessed directly over the Internet.

Public Subnet Example



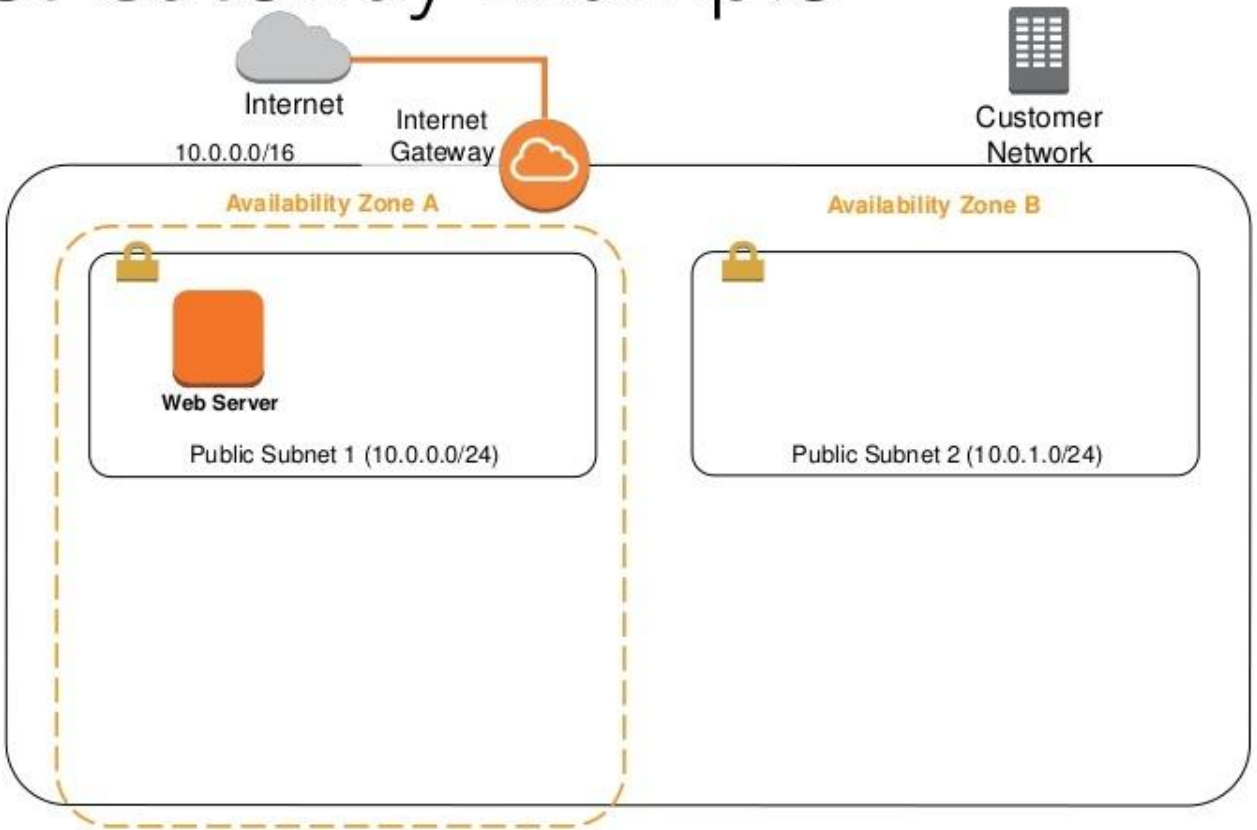
Instance in Public Subnet Example



VPC and Gateways

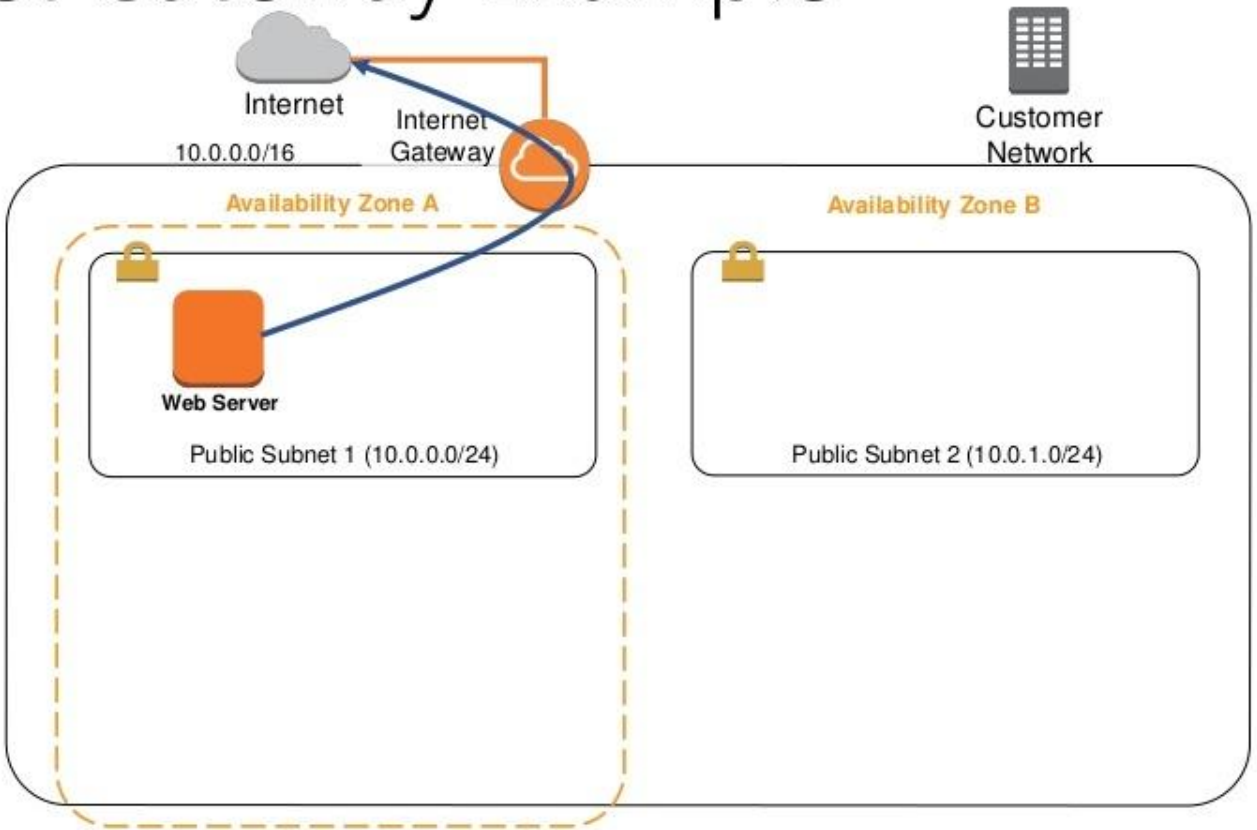
- An Internet Gateway allows communication to and from the Internet

Internet Gateway Example



Region – US East (Ohio)

Internet Gateway Example

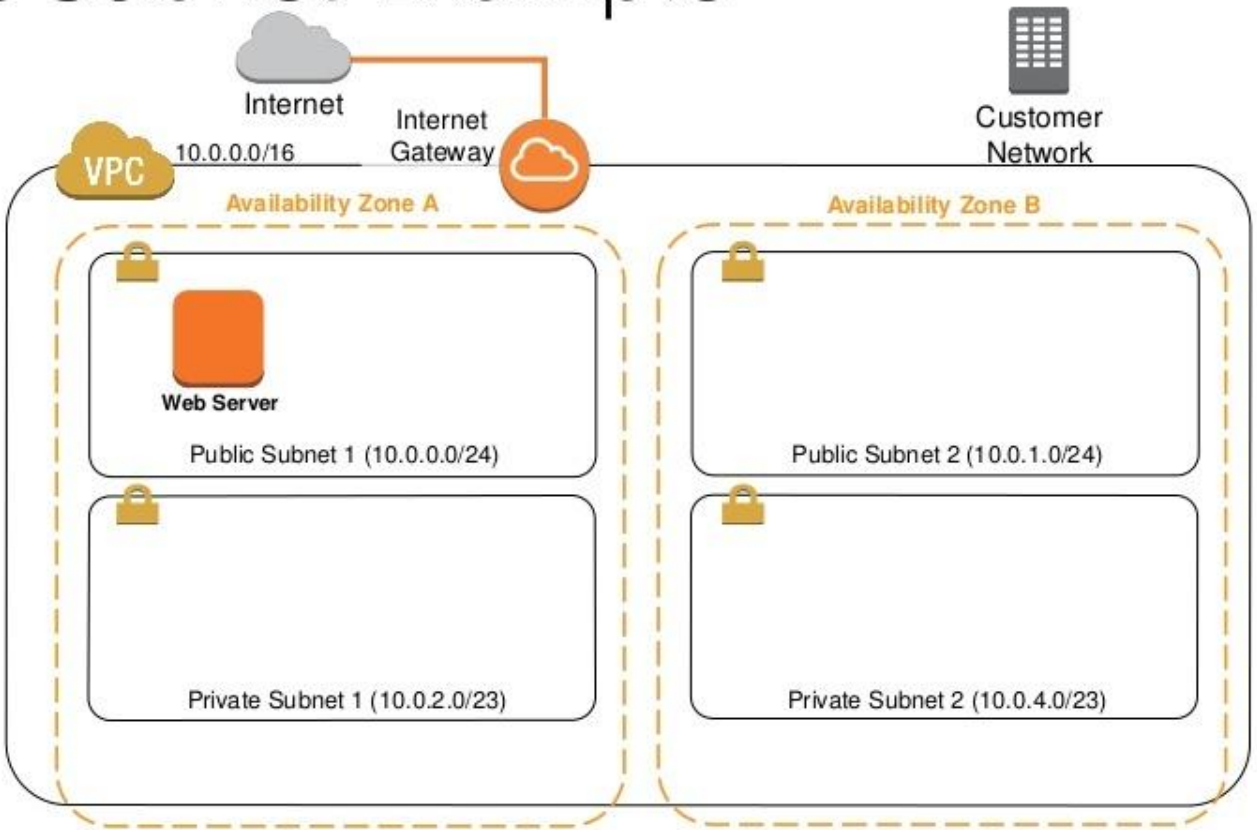


Region – US East (Ohio)

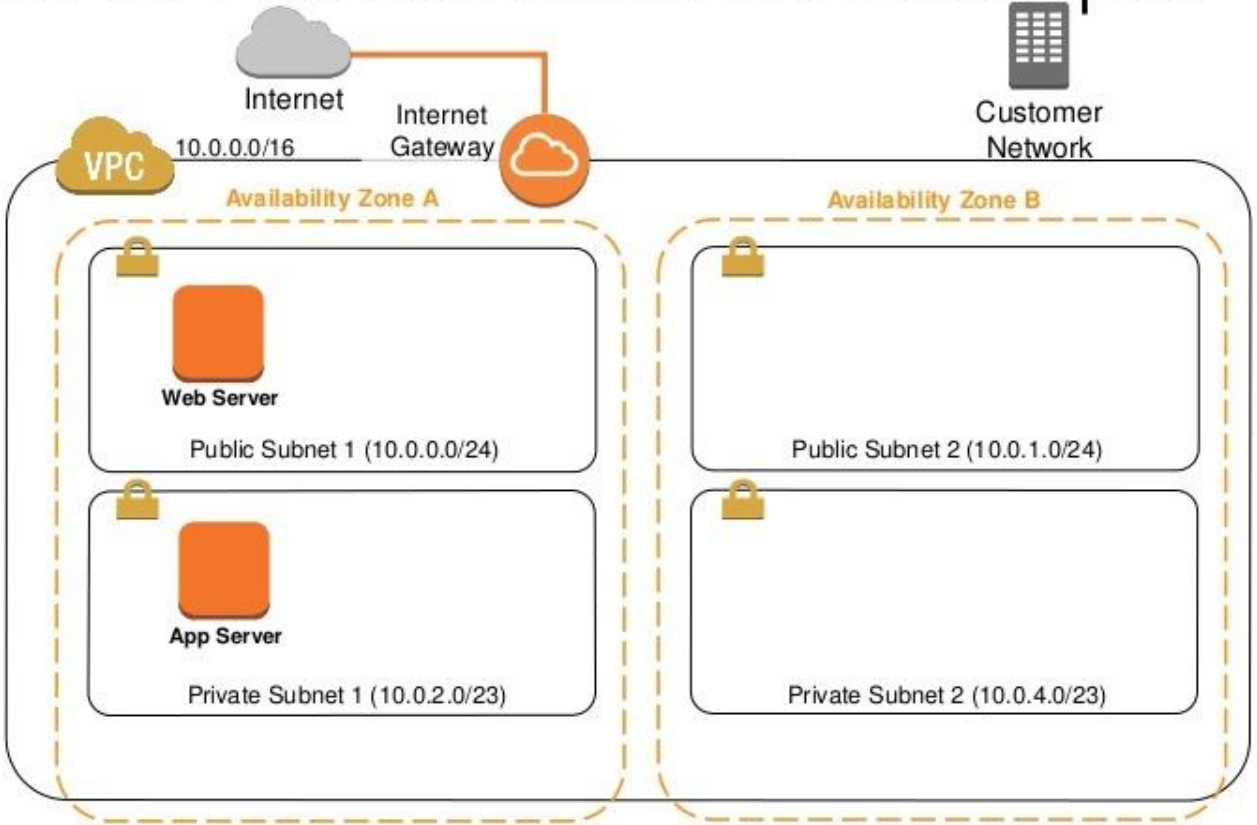
VPC and Subnets

- A VPC resides within a single Region
- A subnet defines a range of IP addresses within your VPC.
- Each subnet must reside entirely within one Availability Zone and cannot span zones.
- You can launch AWS resources into a subnet that you select.
- A public subnet (DMZ) should be used for resources that will be accessed over the Internet.
- A private subnet should be used for resources that won't be accessible over the Internet.

Private Subnet Example



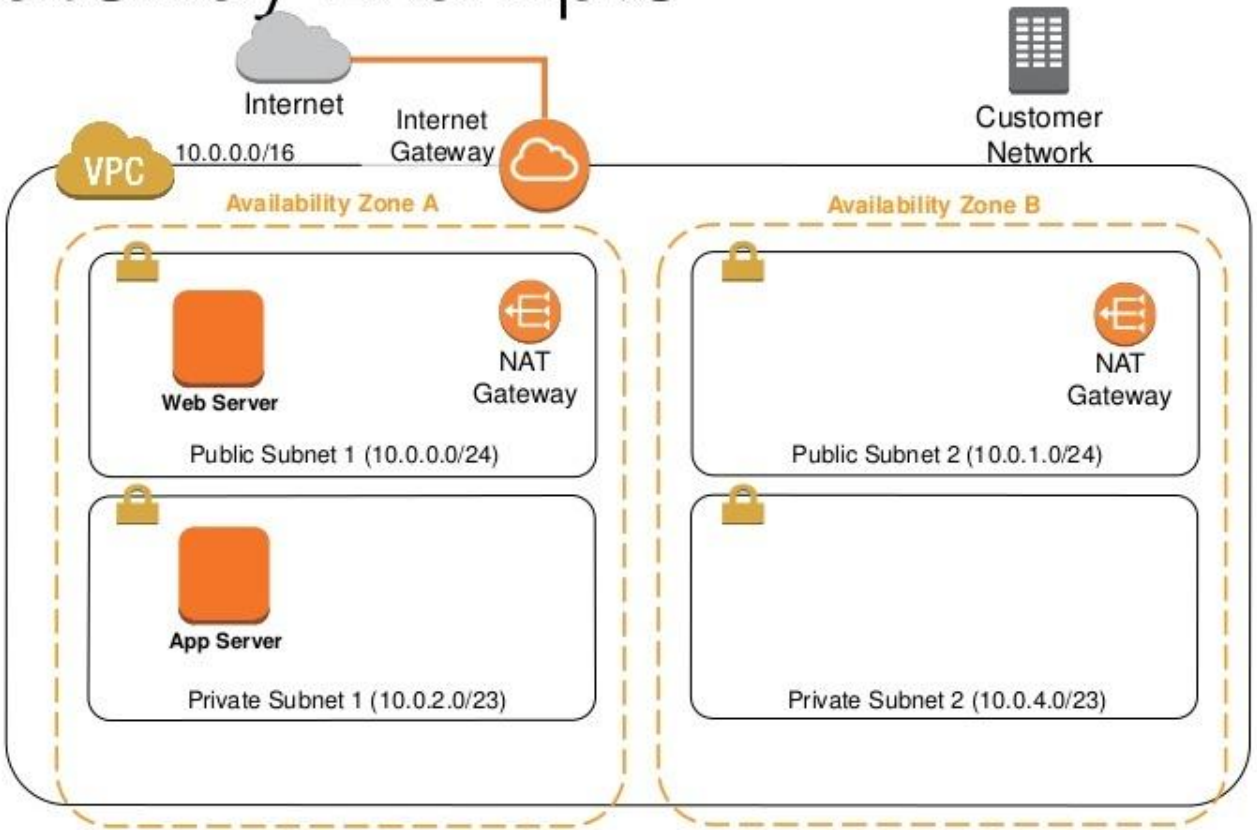
Instance in Private Subnet Example



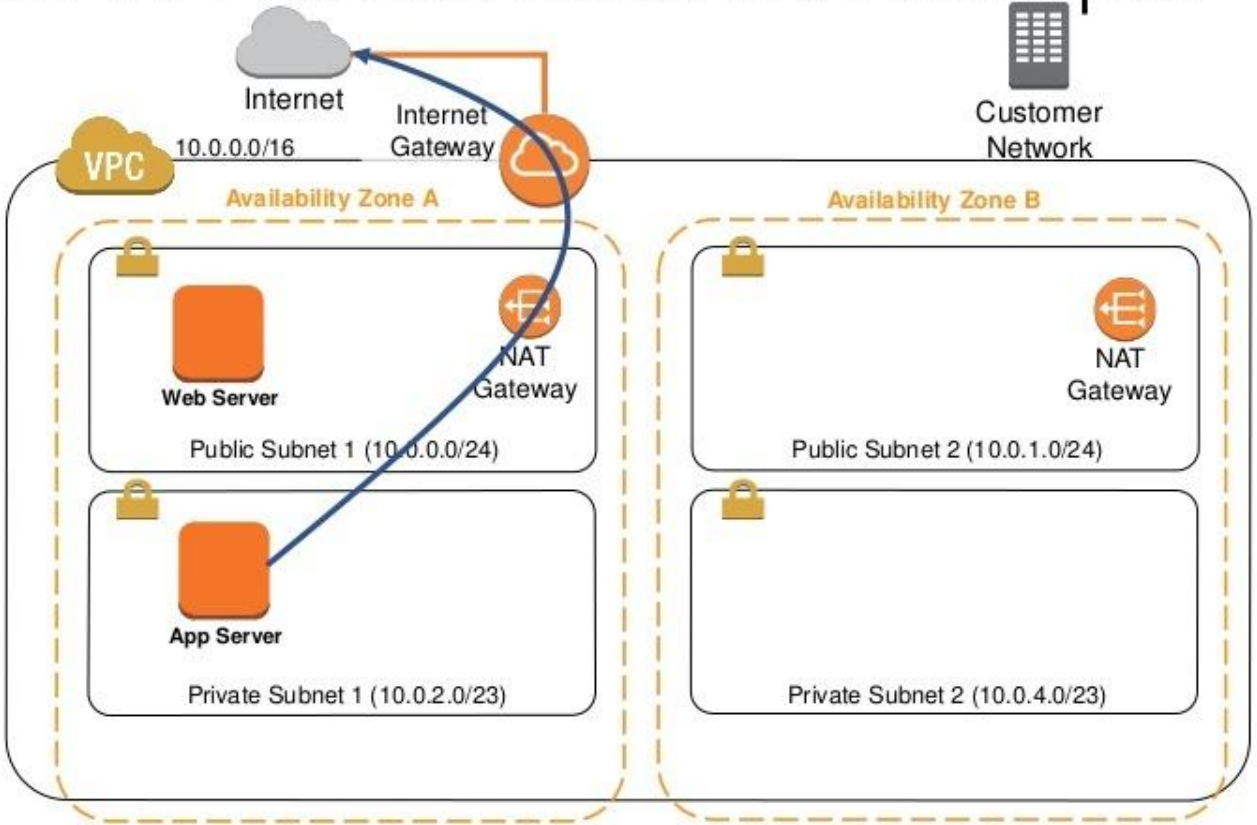
VPC and Gateways

- An Internet Gateway allows communication to and from the Internet
- A NAT Gateway enables instances in the private subnets to initiate outbound traffic to the Internet

NAT Gateway Example



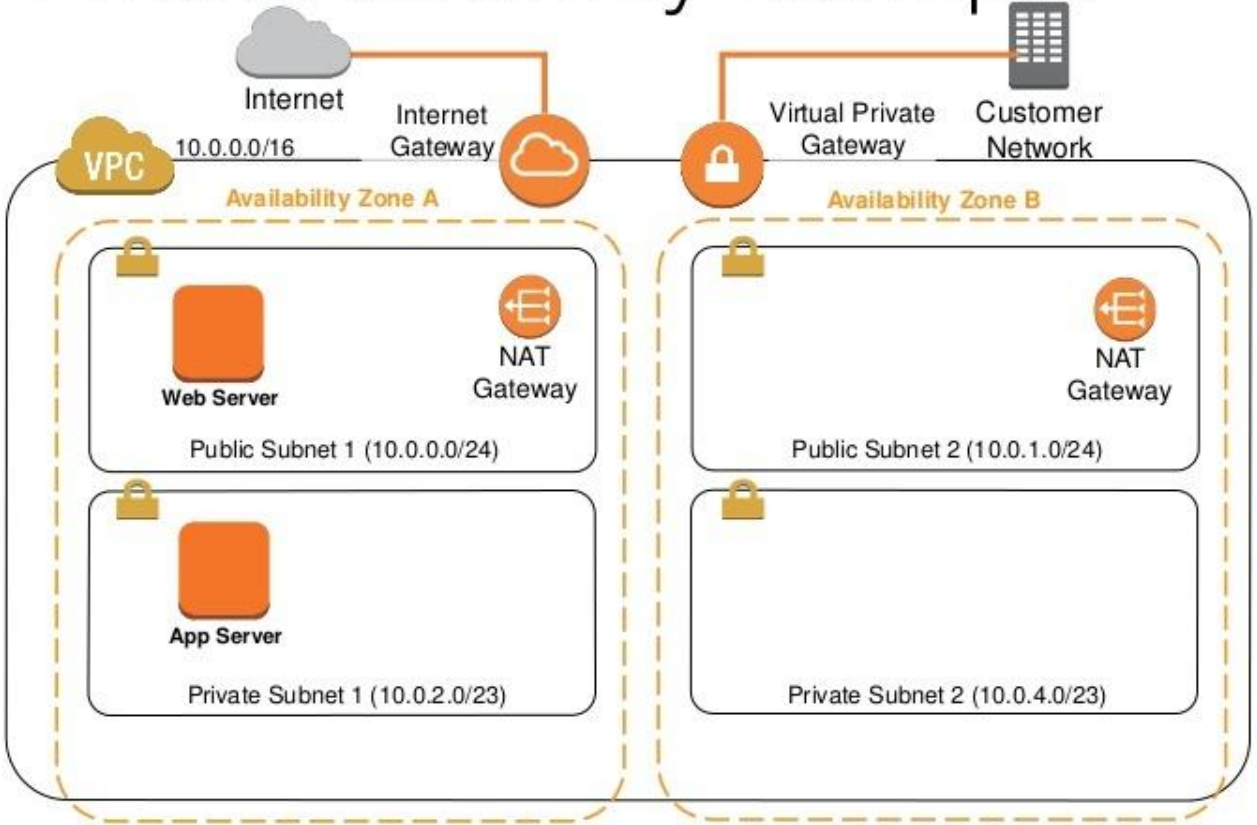
Instance in Private Subnet Example



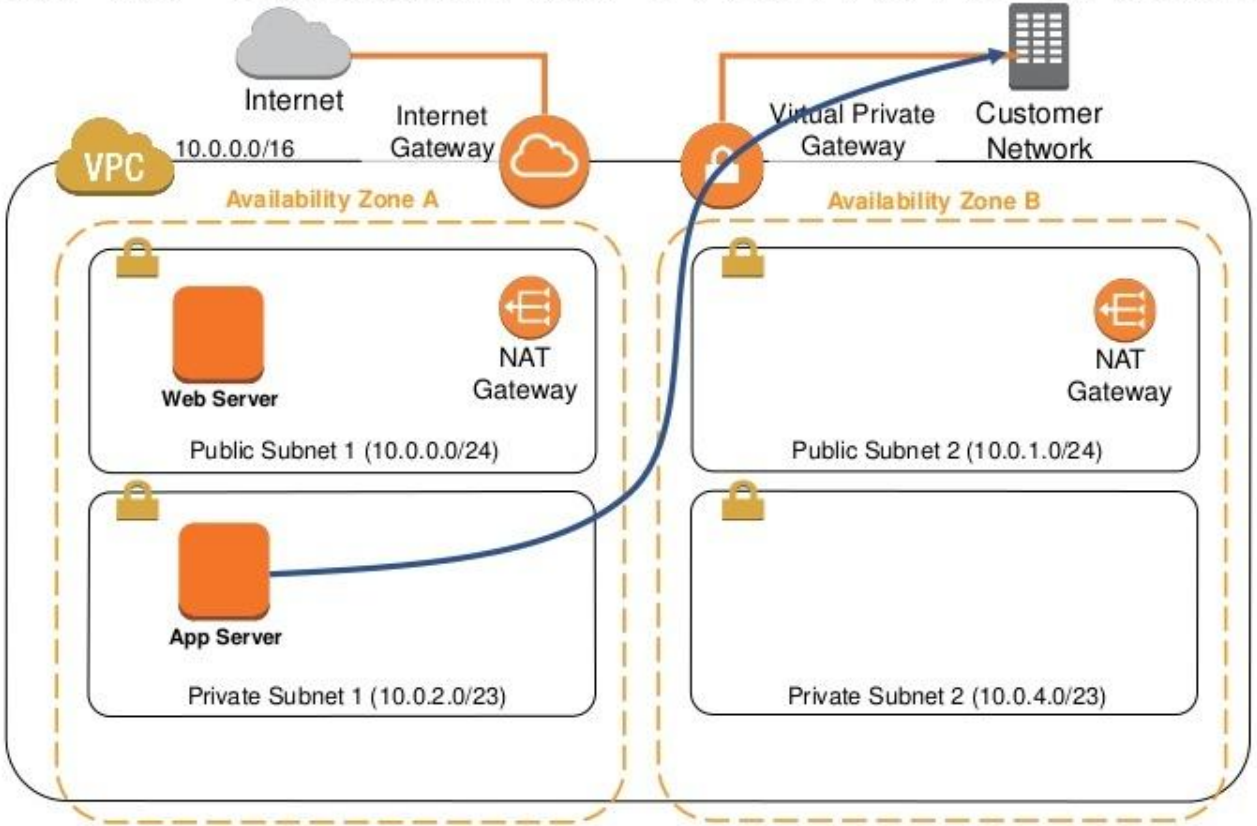
VPC and Gateways

- An Internet Gateway allows communication to and from the Internet
- A NAT Gateway enables instances in the private subnets to initiate outbound traffic to the Internet
- A Virtual Private Gateway enables access to and from your remote network
  - Hardware VPN
  - Direct Connect

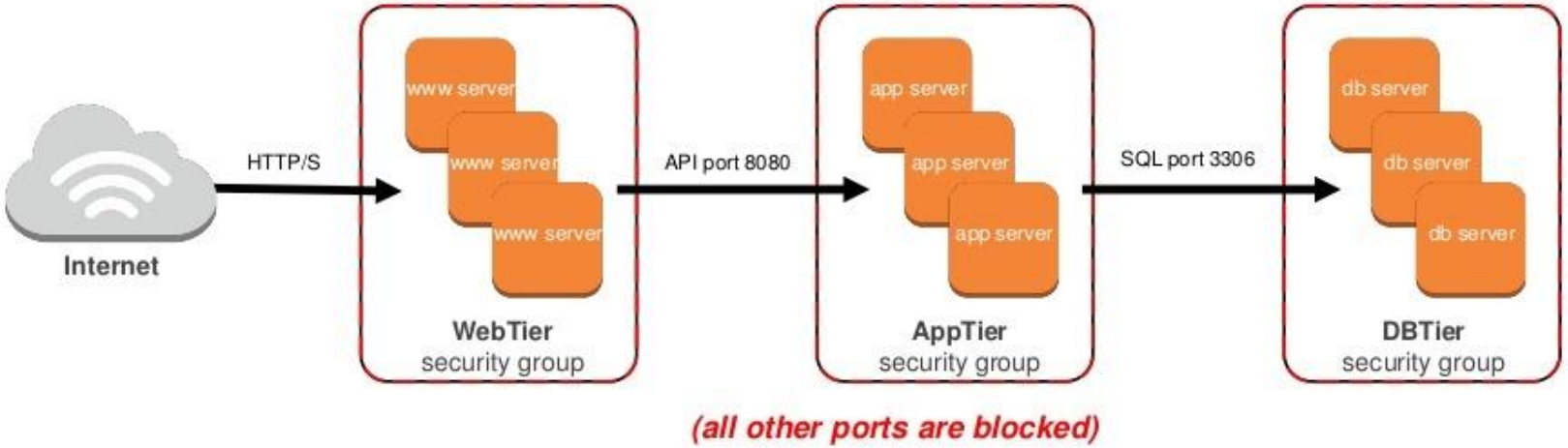
Virtual Private Gateway Example



Instance to Customer Network Example

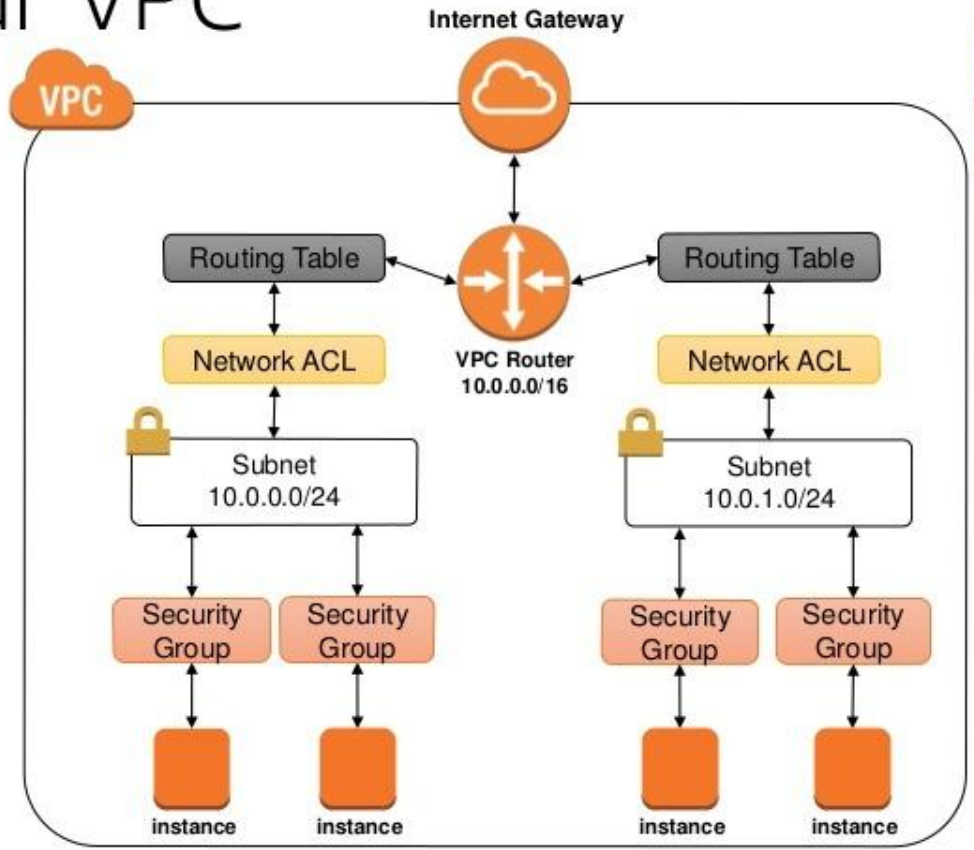


AWS Multi-Tier Security Groups



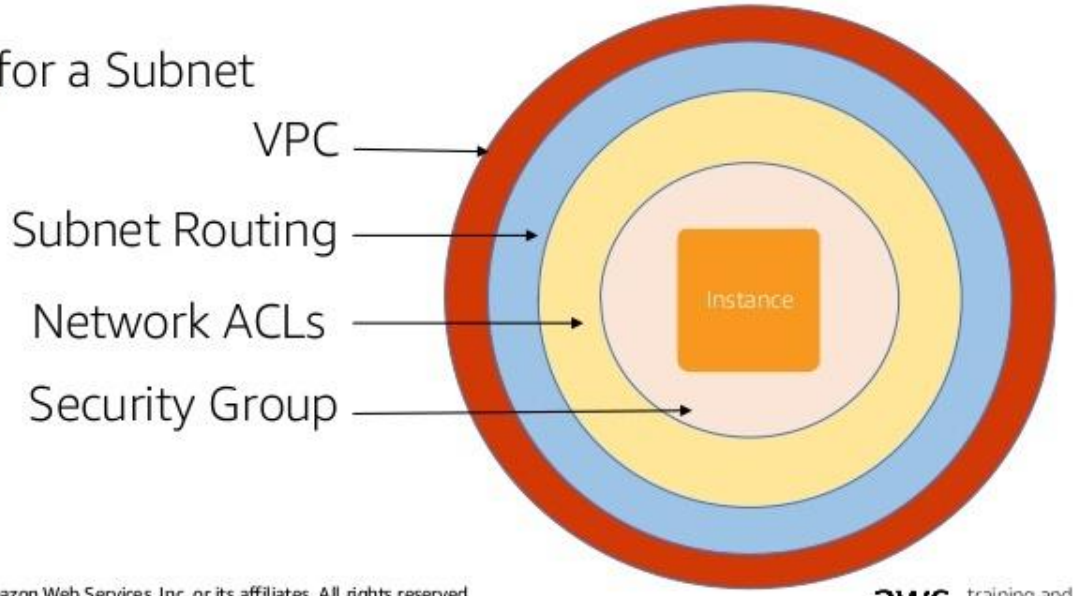
Security in Your VPC

- Internet Gateway
- Route Table
- Network access control lists (ACLs)
- Security groups
- EC2 Key Pairs



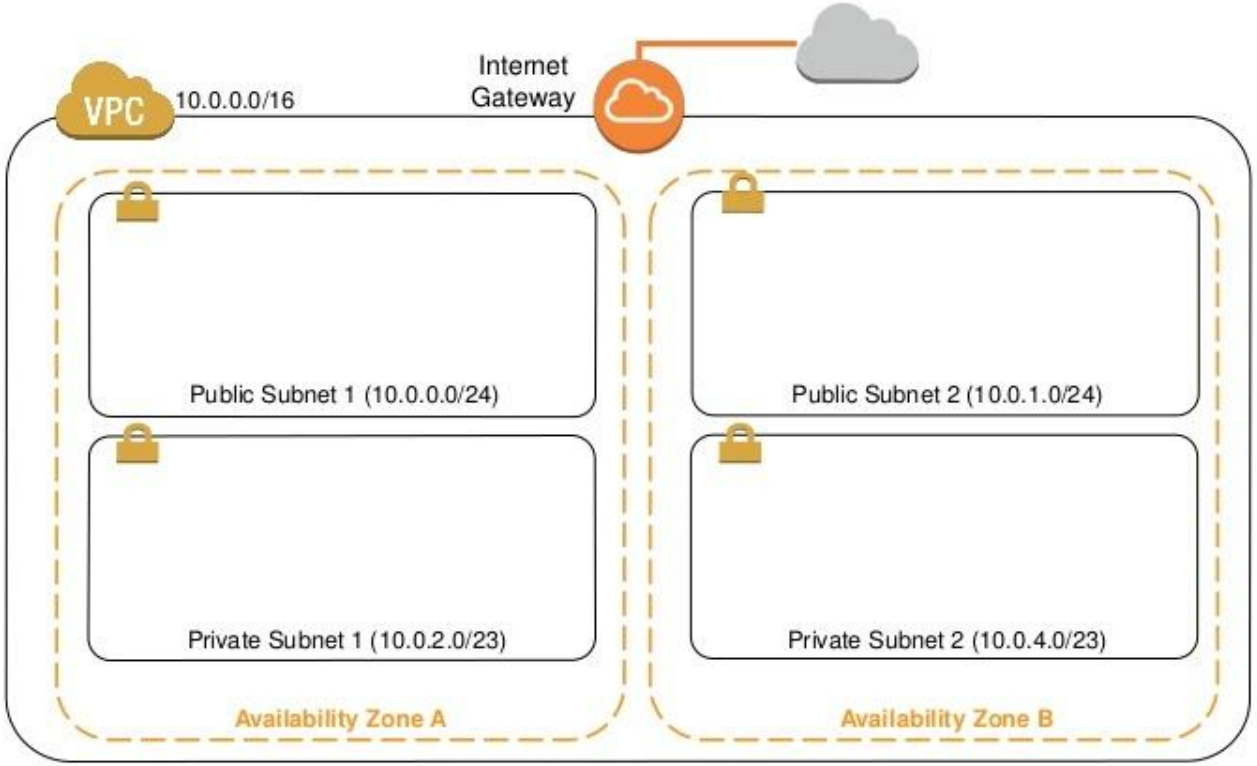
Layered Security

- Security Groups
  - Stateful Firewall for an EC2 Instance
- Network ACLs:
  - Optional Stateless Firewall for a Subnet

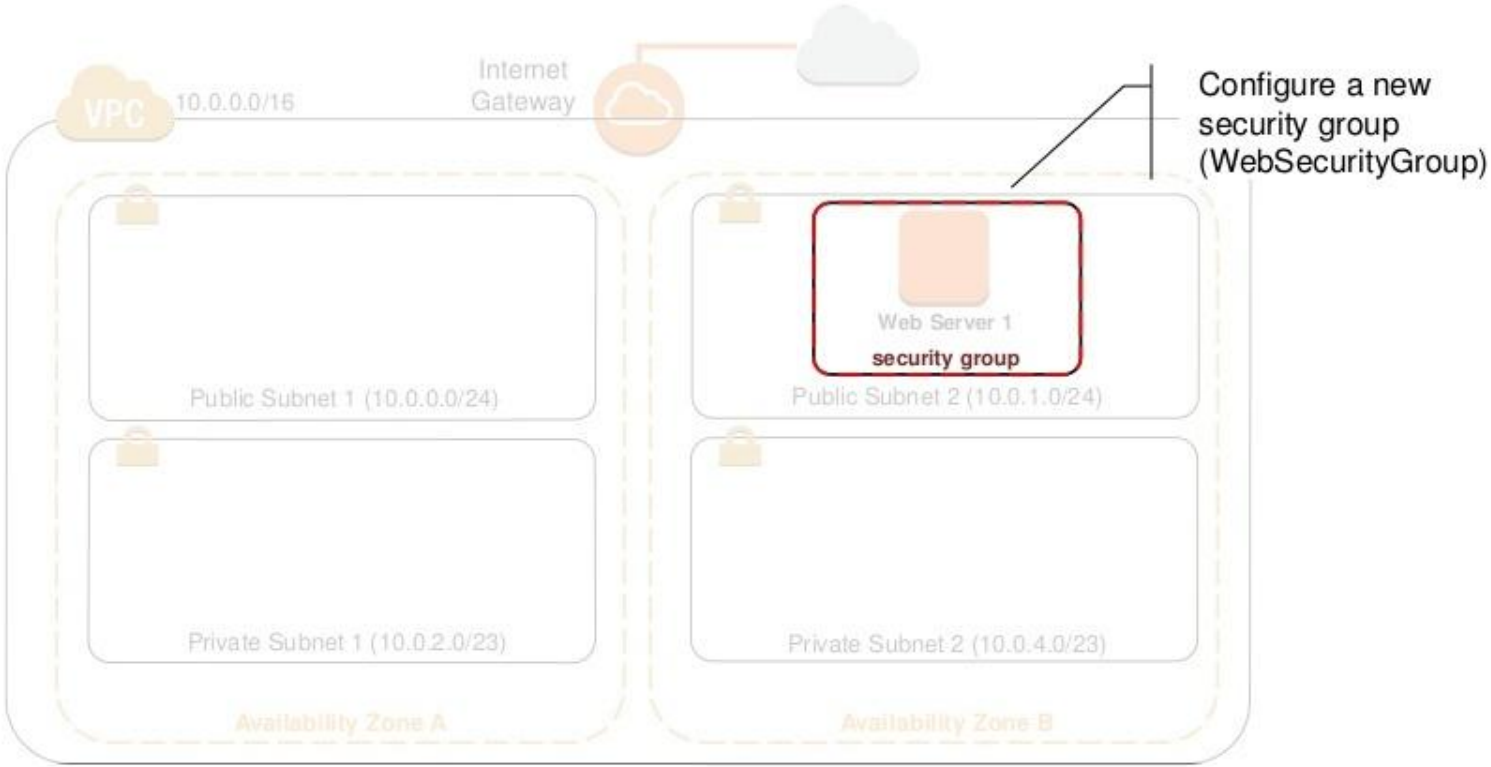


Instructor Demo
Launch a Web Server

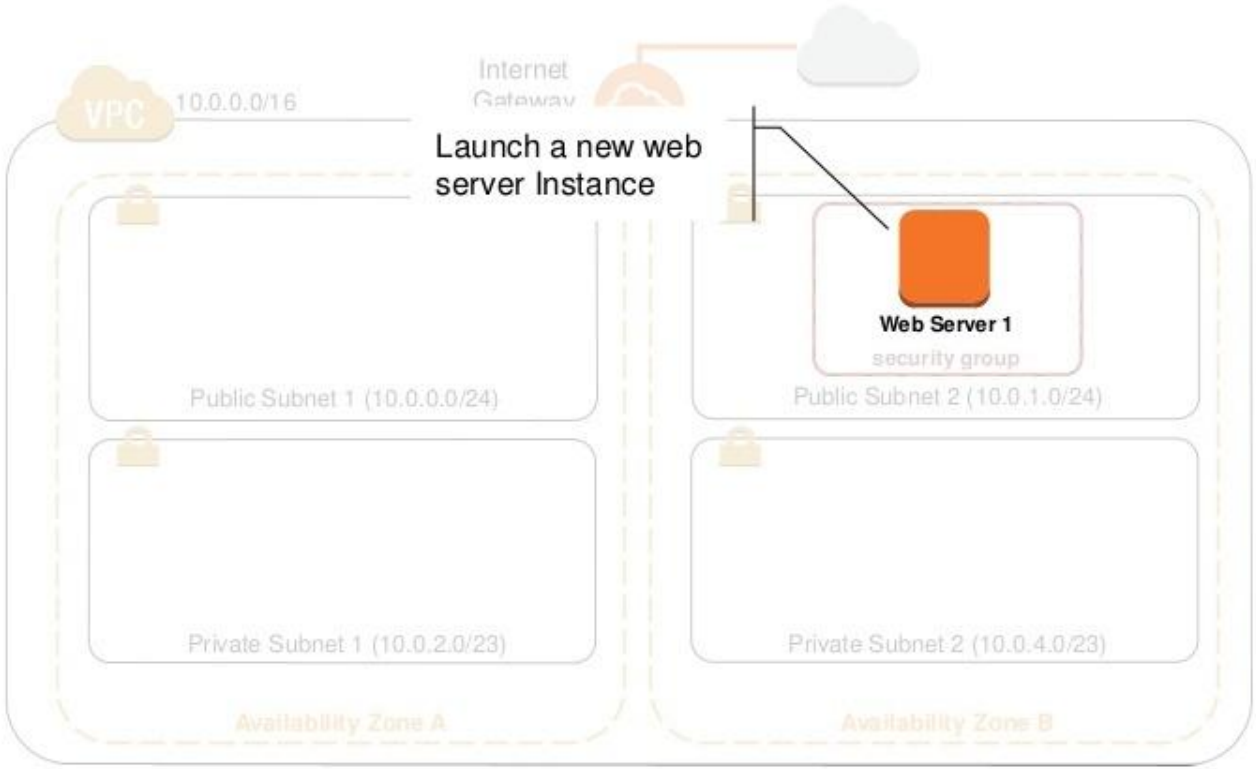
What We're Starting With



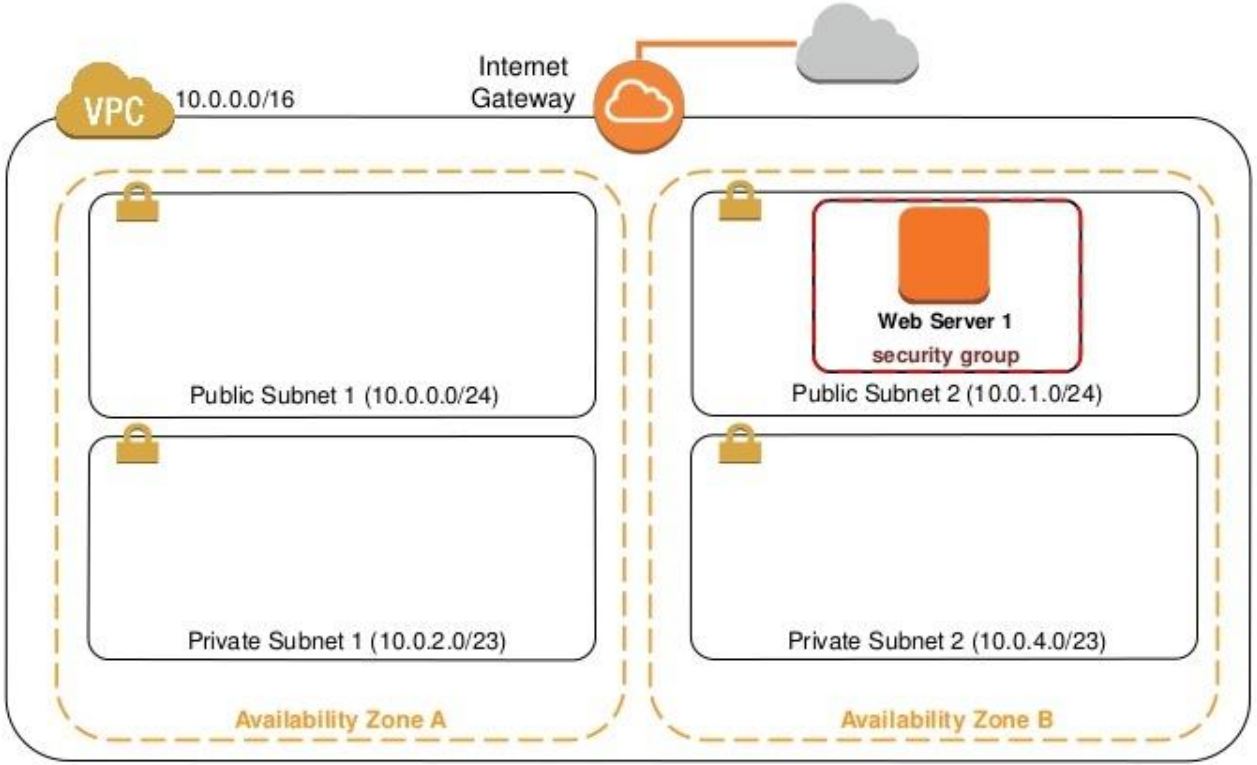
Launch a Web Server



Launch a Web Server



Launch a Web Server



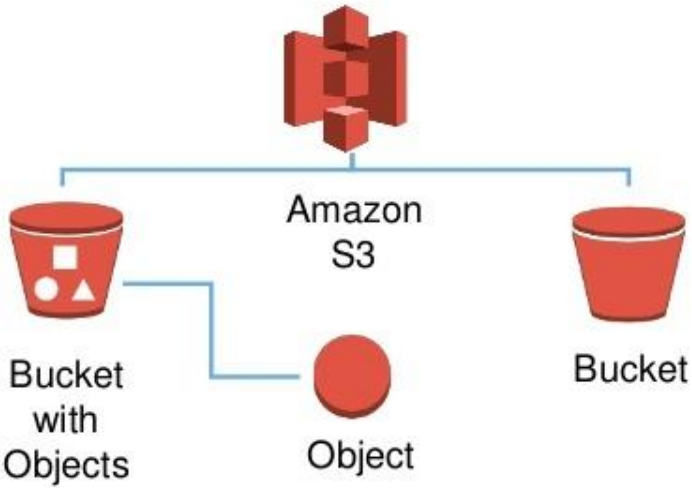
Object Storage Service
Amazon S3

Amazon Simple Storage Service (S3)

Amazon S3

- Storage for the Internet
- Natively online, HTTP/S access
- Storage that allows you to store and retrieve **any amount of data**, any time, from anywhere on the web
- **Highly scalable**, reliable, fast and durable

Amazon S3 Concepts



- Amazon S3 stores data as objects within **buckets**
- An object is composed of a file and optionally any **metadata** that describes that file
- You **control access** to the bucket and its objects

Object Keys

An **object key** is the unique identifier for an **object** in a **bucket**.

http://doc.s3.amazonaws.com/2018-06-07/photo.gif

Bucket

Object Key

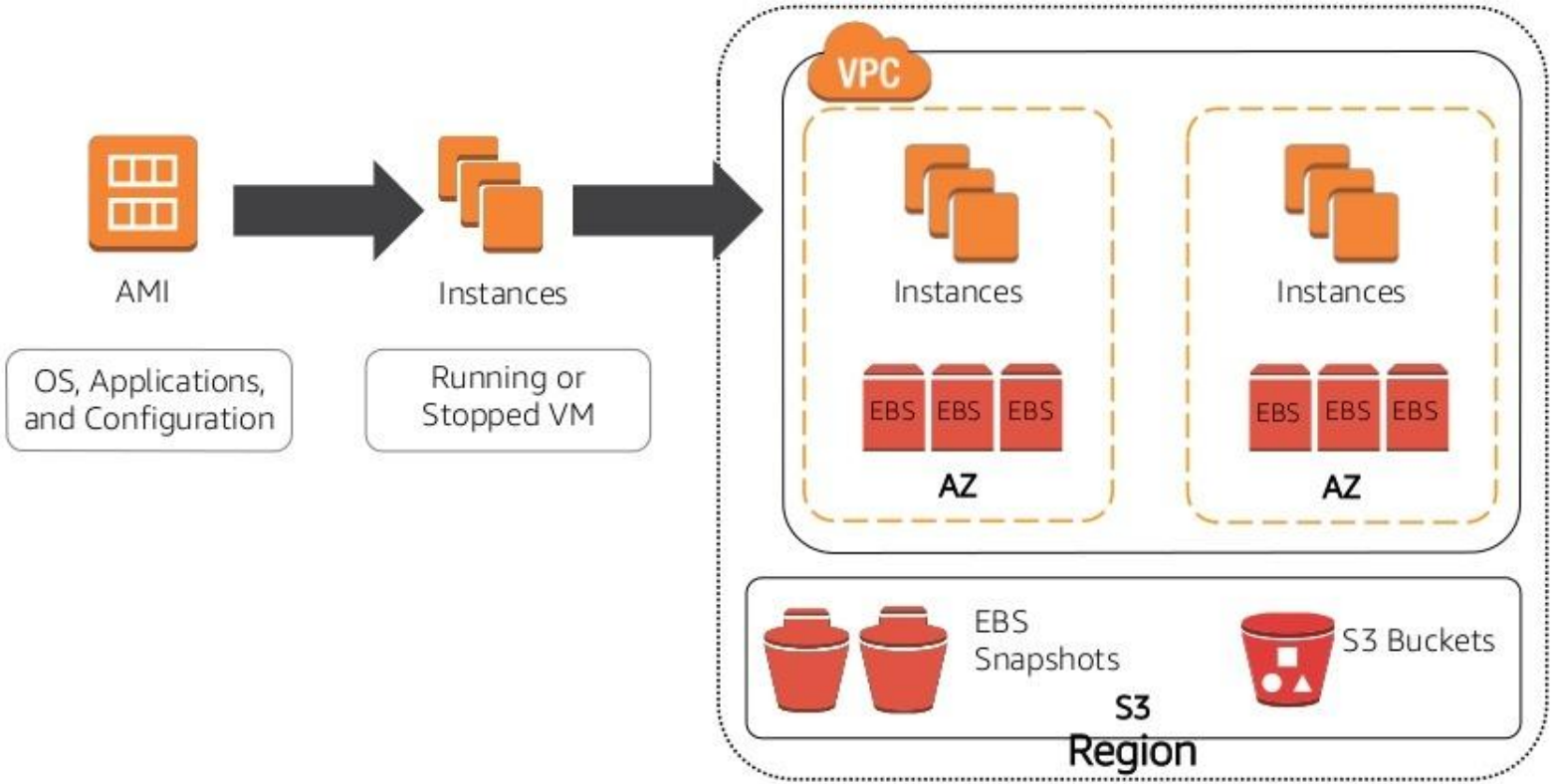
Common Use Scenarios

- Storage and backup
- Application file hosting
- Media hosting
- Software delivery
- Store AMIs and snapshots

Amazon S3 Facts

- Can store an unlimited number of objects in a bucket
- Objects can be up to 5 TB; no bucket size limit
- Designed for 99.999999999% durability and 99.99% availability of objects over a given year for S3 Standard
- Can use HTTP/S endpoints to store and retrieve any amount of data, at any time, from anywhere on the web
- Can use optional server-side encryption using AWS or customer-managed provided client-side encryption
- Auditing is provided by access logs

S3 Data is stored within the AWS Region



Amazon S3 Region Considerations

- Amazon S3 creates a bucket in the region you select.
- You can choose a region to:
  - Optimize **latency**
  - Minimize **costs**
- Address **regulatory requirements**
- Objects stored in a region **never leave the region** unless you explicitly transfer them to another region.

Amazon S3 Security

- You can control access to buckets and objects with:
  - Access Control Lists (ACLs)
  - Bucket policies
  - Identity and Access Management (IAM) policies
- You can upload or download data to Amazon S3 via SSL/TLS encrypted endpoints.
- You can encrypt data Client-Side and/or Server-Side.

Amazon S3 Versioning

- Protects from accidental overwrites and deletes with no performance penalty.
- Generates a new version with every upload.
- Allows easily retrieval of deleted objects or roll back to previous versions.
- Two states of an Amazon S3 bucket
  - Versioning-suspended
  - Versioning-enabled

Versioning Enabled

Amazon S3 Pricing

- Pay only for what you use
- No minimum fee
- Estimate monthly bill using the AWS Simple Monthly Calculator (https://calculator.s3.amazonaws.com/index.html)
- Pricing is available as:
  - Storage Pricing
  - Request Pricing
  - Data Transfer Pricing: data transferred out of Amazon S3

Amazon S3 Object Lifecycle

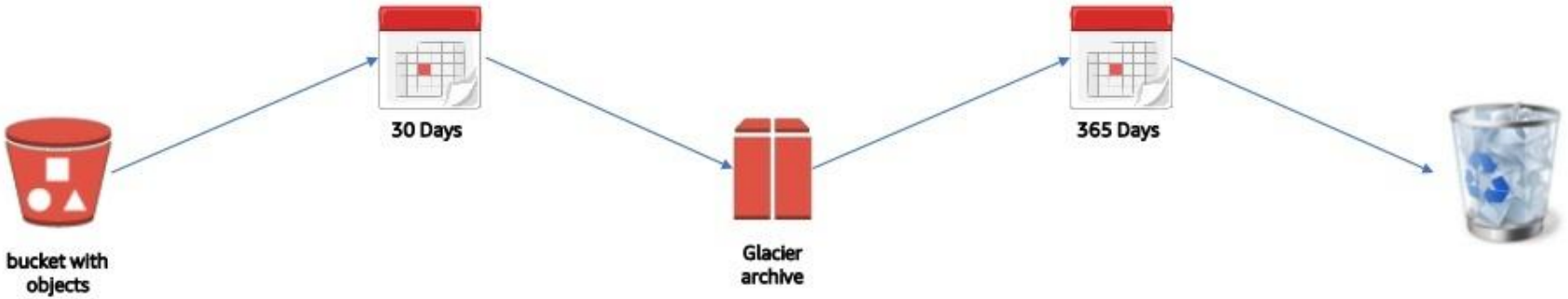
Lifecycle management defines how Amazon S3 manages objects during their lifetime.

Some objects might have a well-defined lifecycle:

- Log files
- Archive documents & digital media
- Financial and healthcare records
- Raw genomics sequence data
- Long-term database backups
- Data that must be retained for regulatory compliance

Amazon S3 + Amazon Glacier

S3 Lifecycle policies allow you to delete or move objects based on age and set rules per S3 bucket.



Amazon S3 Storage Classes

Storage Class	Durability	Availability	Other Considerations
Amazon S3 Standard	99.999999999%	99.99%	• For frequently accessed data
Amazon S3 Standard - Infrequent Access (IA)	99.999999999%	99.9%	• For infrequently accessed data • Retrieval fee associated with objects
Intelligent Tiering	99.999999999%	99.9%	• Data with changing or unknown access patterns • Monitoring and automation fees per object apply. No retrieval fees.
One Zone-IA	99.999999999%	99.5%	• Infrequently accessed data • Retrieval fee associated with objects • No physical AZ lost resiliency

Amazon Glacier

- Long term low-cost archiving service
- Optimal for infrequently accessed data
- Designed for 99.999999999% durability
- Retrieval time:
  - Expedited: 1 – 5 minutes
  - Standard: 3 – 5 hours
  - Bulk: 5 – 12 hours

Amazon S3 + Glacier

Storage Class	Durability	Availability	Other Considerations
Amazon S3 Standard	99.999999999%	99.99%	• For frequently accessed data
Amazon S3 Standard - Infrequent Access (IA)	99.999999999%	99.9%	• For infrequently accessed data • Retrieval fee associated with objects
Intelligent Tiering	99.999999999%	99.9%	• Data with changing or unknown access patterns • Monitoring and automation fees per object apply. No retrieval fees.
One Zone-IA	99.999999999%	99.5%	• Infrequently accessed data • Retrieval fee associated with objects • No physical AZ lost resiliency
Glacier	99.999999999%	N/A	• Long term data archiving • Per GB retrieval fees apply. • 99.99% availability **once restored**

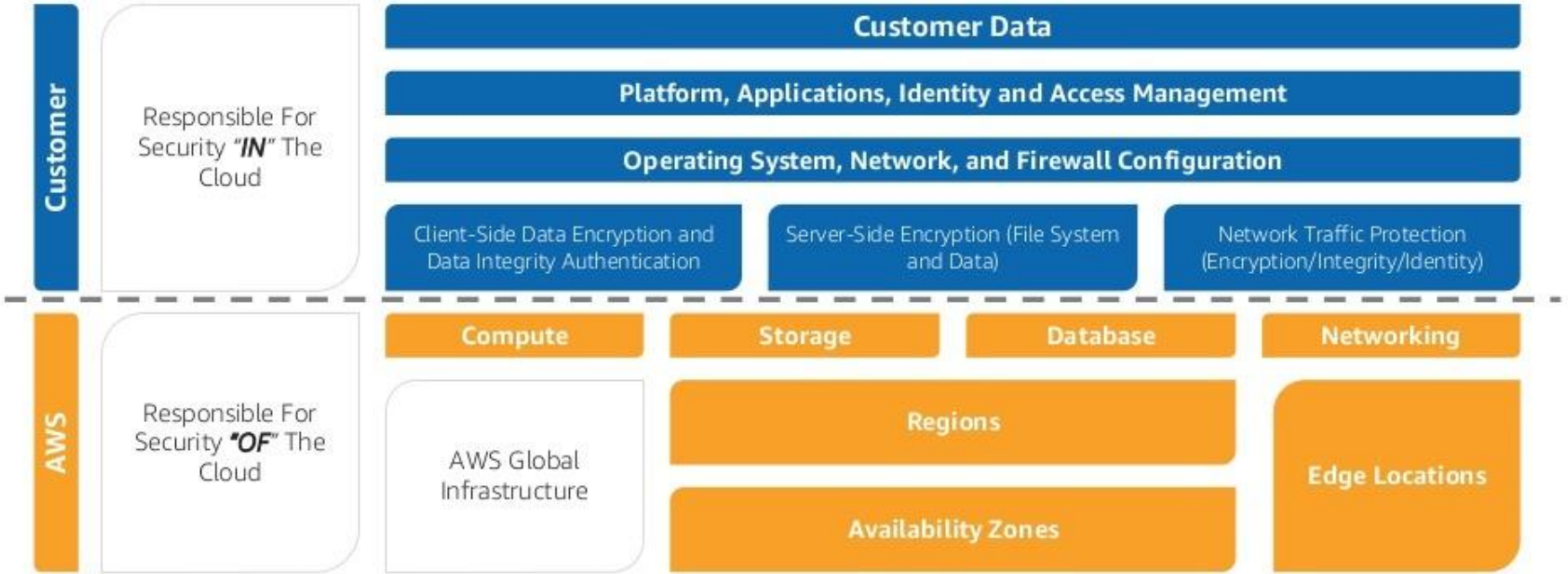
Amazon EBS and Amazon S3

	Amazon EBS	Amazon S3
Paradigm	Block storage with file system	Object store
Performance	Very fast	Fast
Redundancy	Across multiple servers in an Availability Zone	Across multiple facilities in a Region
Security	EBS Encryption – Data volumes and Snapshots	Encryption
Direct Access from the Internet?	No	Yes (with proper credentials or ACL)
Typical use case	It is a disk drive	Online storage

Instructor Demo
Amazon S3

Module 3
Security, Identity, and Access Management

Shared Responsibility Model



Physical Security

- 24/7 trained security staff
- AWS data centers in nondescript and undisclosed facilities
- Two-factor authentication for authorized staff
- Authorization for data center access

Hardware, Software, and Network

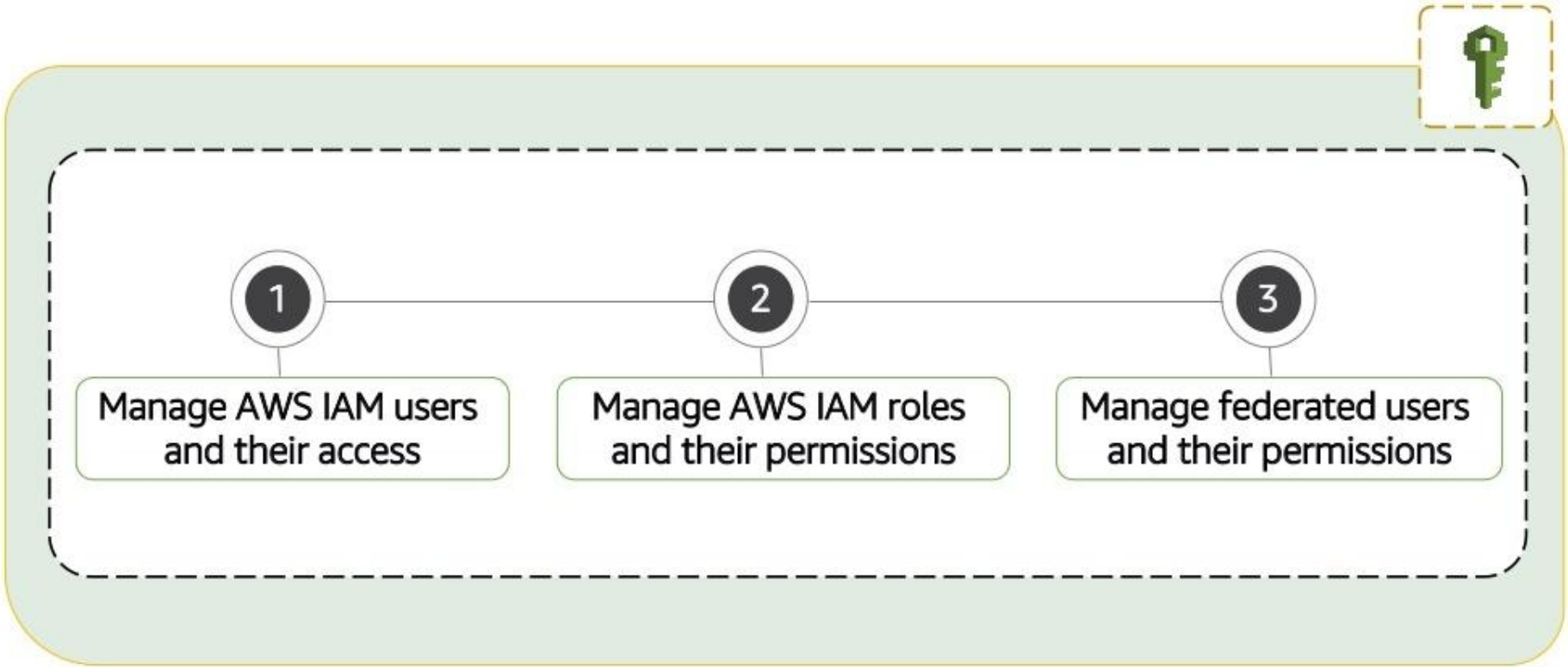
- Automated change-control process
- Bastion servers that record all access attempts
- Firewall and other boundary devices
- AWS monitoring tools

Assurance Programs

Network Security

SSL Endpoints	Security Groups	VPC
Secure Transmission	**Instance Firewalls**	**Network Control**
Use secure endpoints to establish secure communication sessions (HTTPS).	Use security groups to configure firewall rules for instances.	Use public and private subnets, NAT, and VPN support in your virtual private cloud to create low-level networking constraints for resource access.

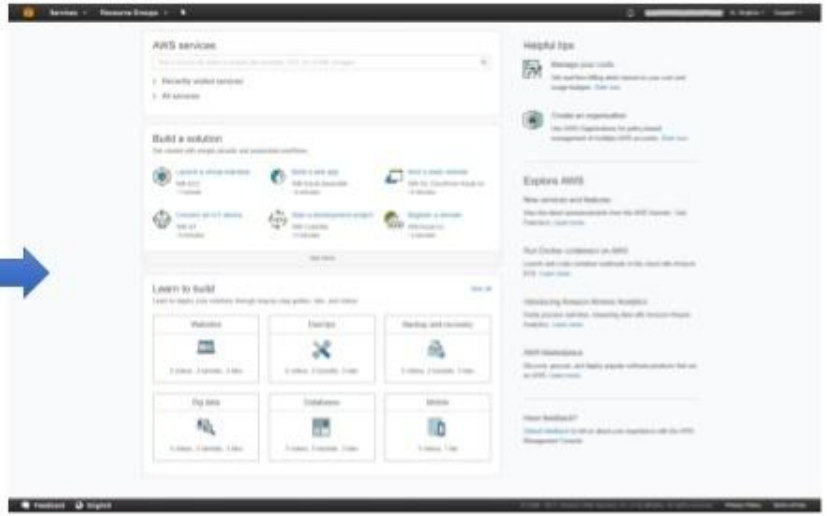
AWS Identity and Access Management (IAM)



AWS IAM Authentication

- AWS Management Console:
  - User Name and Password

IAM User



AWS IAM Authentication

- AWS CLI or SDK API:
  - Access Key and Secret Key

IAM User

```
Access Key ID: AKIAIOSFODNN7EXAMPLE
Secret Access Key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

AWS CLI

```
[redacted]:~ [redacted]$ aws configure
AWS Access Key ID [**********O22A]:
AWS Secret Access Key [**********4m8i]:
Default region name [ap-southeast-1]:
Default output format [json]:
```

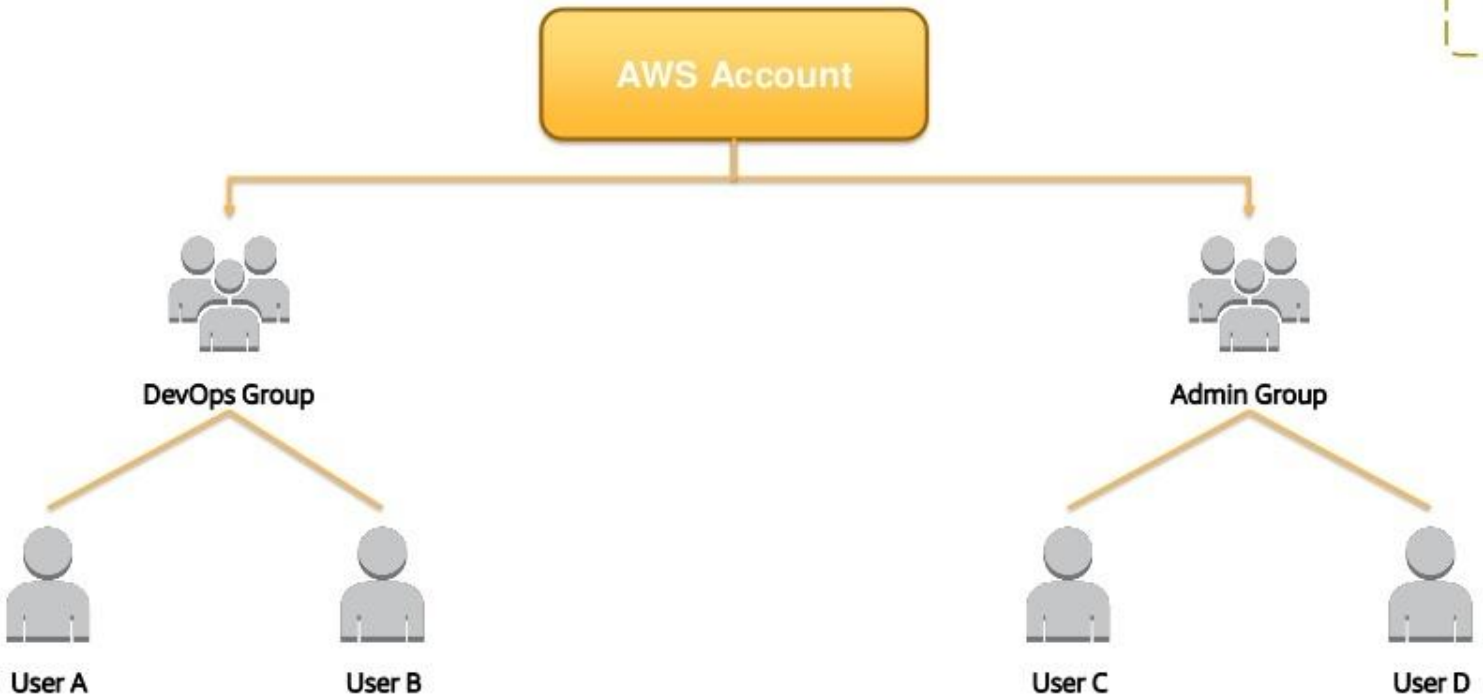
AWS SDK & API

Java

Python

.NET

AWS IAM User Management - Groups



AWS IAM Authorization

Authorization

- Policies:
  - Are JSON documents to describe permissions.
  - Are assigned to users or groups.

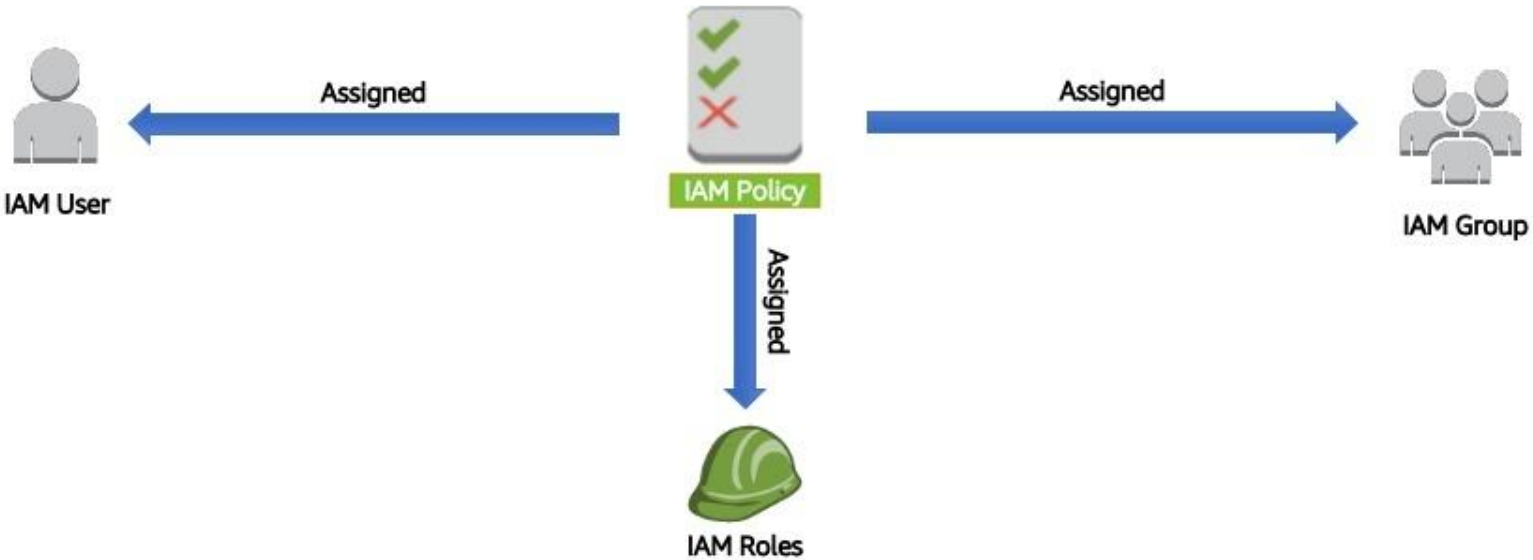
IAM User

IAM Group

AWS IAM Policy Elements

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
         "Sid": "Stmt1453690971587",
            "Action": [
              "ec2:Describe*",
              "ec2:StartInstances",
              "ec2:StopInstances"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
              "IpAddress": {
                    "aws:SourceIp": "54.64.34.65/32"
              }
            }
     },
     {
            "Sid": "Stmt1453690998327",
            "Action": [
              "s3:GetObject*"
            ],
          "Effect": "Allow",
          "Resource": "arn:aws:s3:::example_bucket/*"
          }
   ]
}
```

AWS IAM Policy Assignment

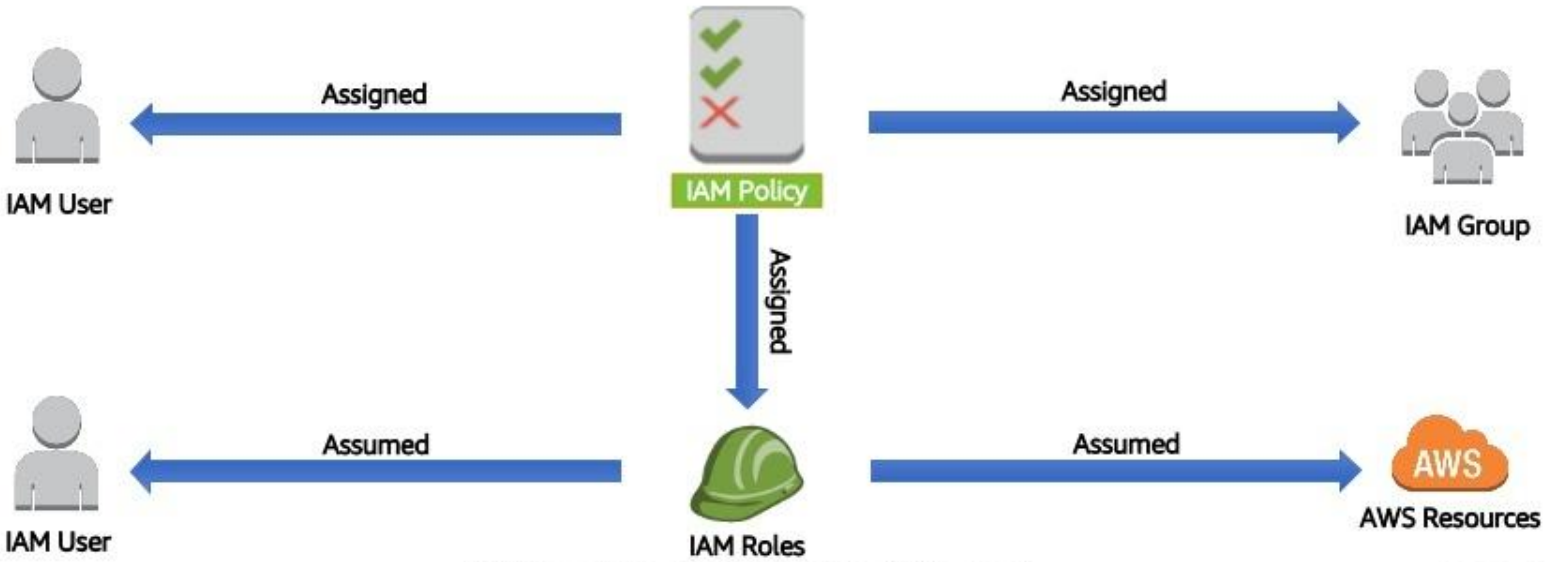


AWS IAM Roles

- An IAM role uses a policy.
- An IAM role has no associated credentials.
- IAM users, applications, and services may assume IAM roles.

IAM Roles

AWS IAM Policy Assignment



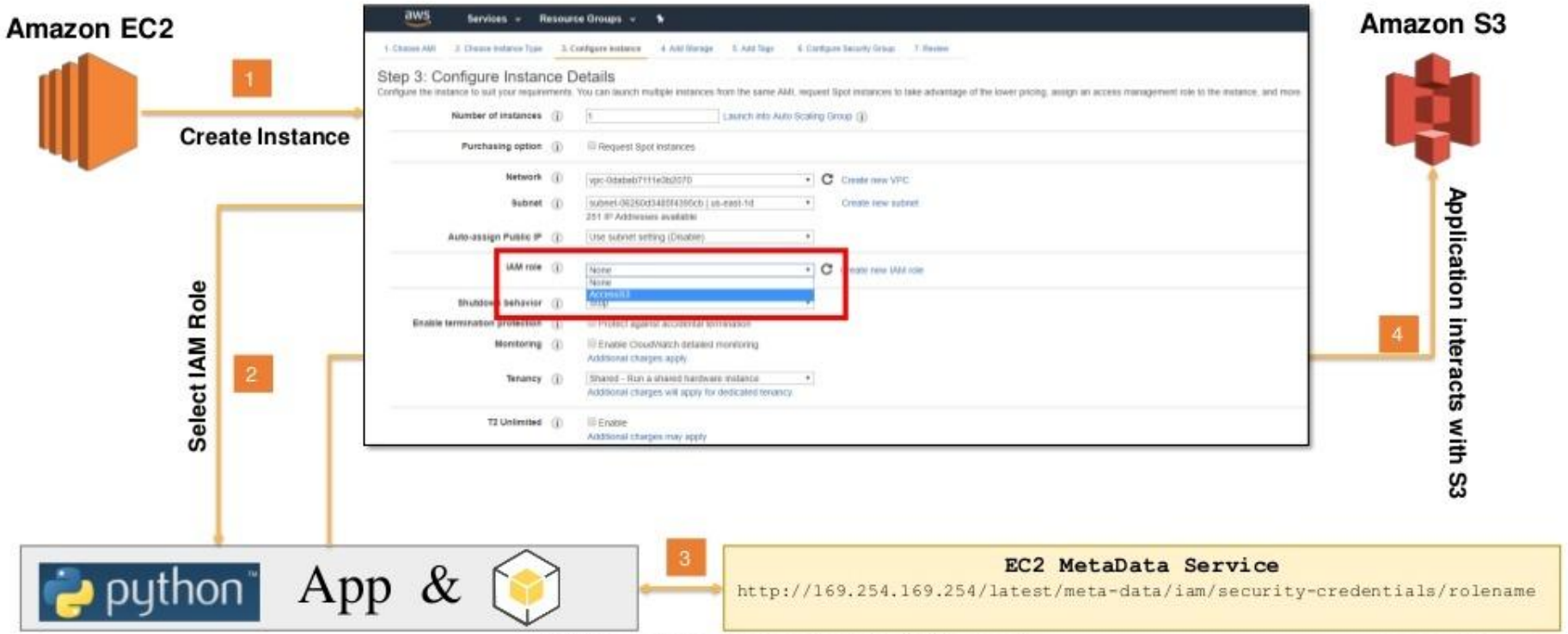
aws training and certification

Example: Application Access to AWS Resources

- Python application hosted on an Amazon EC2 Instance needs to interact with Amazon S3.
- AWS credentials are required:
  - ~~Option 1: Store AWS Credentials on the Amazon EC2 instance.~~
  - Option 2: Securely distribute AWS credentials to AWS Services and Applications.

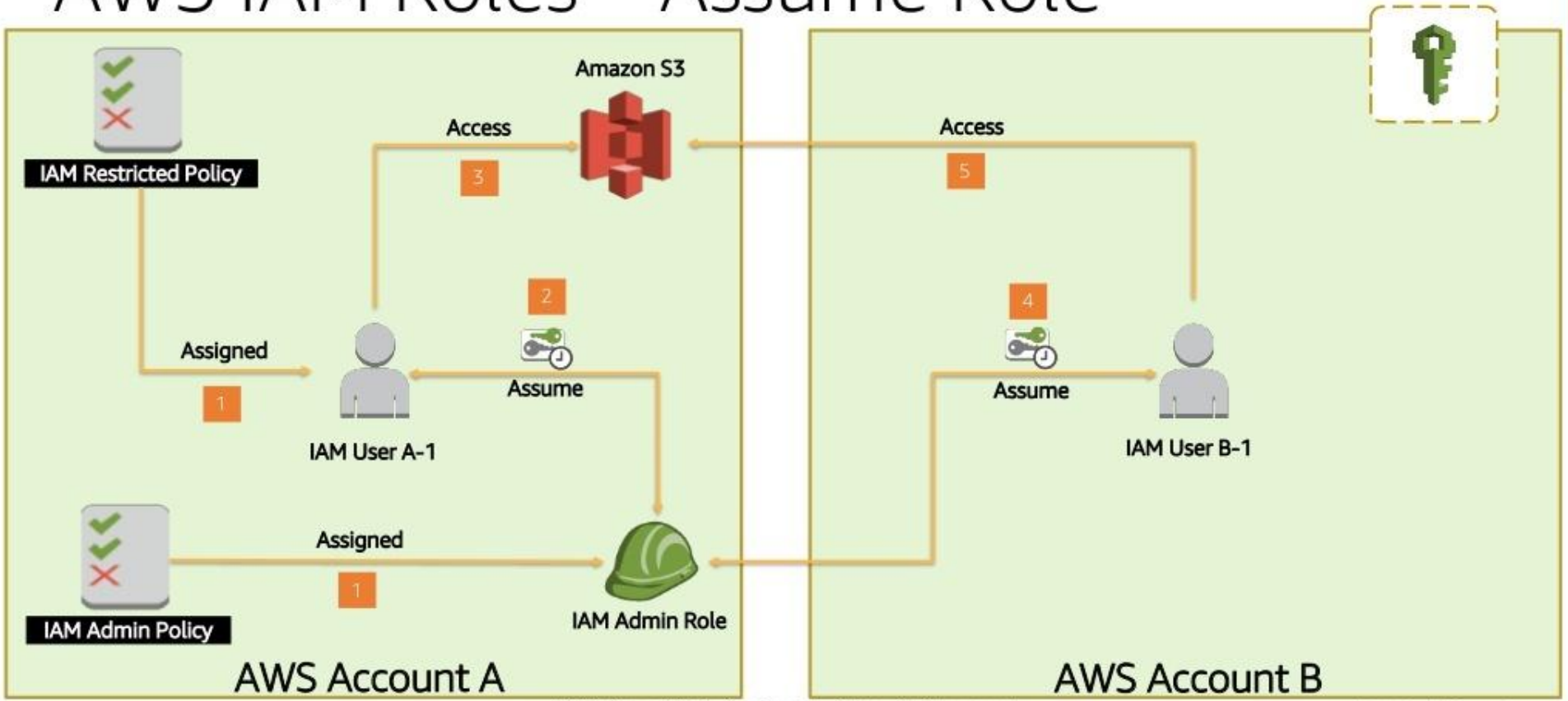
IAM Roles

AWS IAM Roles - Instance Profiles



aws training and certification

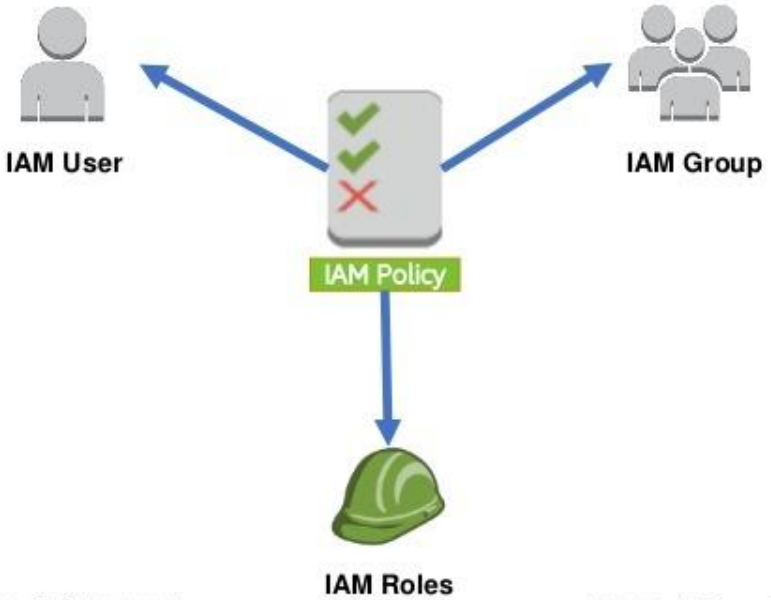
AWS IAM Roles – Assume Role



Application Authentication

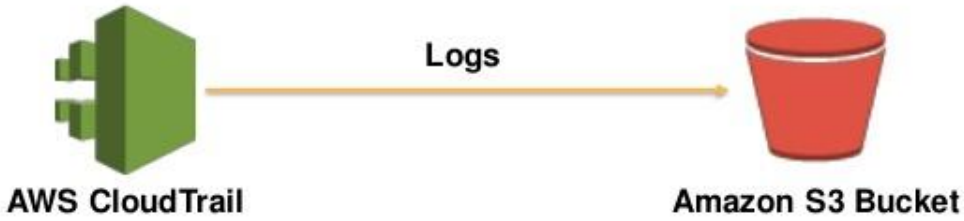
AWS IAM Authentication and Authorization

- Authentication
  - AWS Management Console
    - User Name and Password
  - AWS CLI or SDK API
    - Access Key and Secret Key
- Authorization
  - Policies



AWS CloudTrail

- Records AWS API calls for accounts.
- Delivers log files with information to an Amazon S3 bucket.
- Logs calls made using the AWS Management Console, AWS SDKs, AWS CLI and higher-level AWS services.



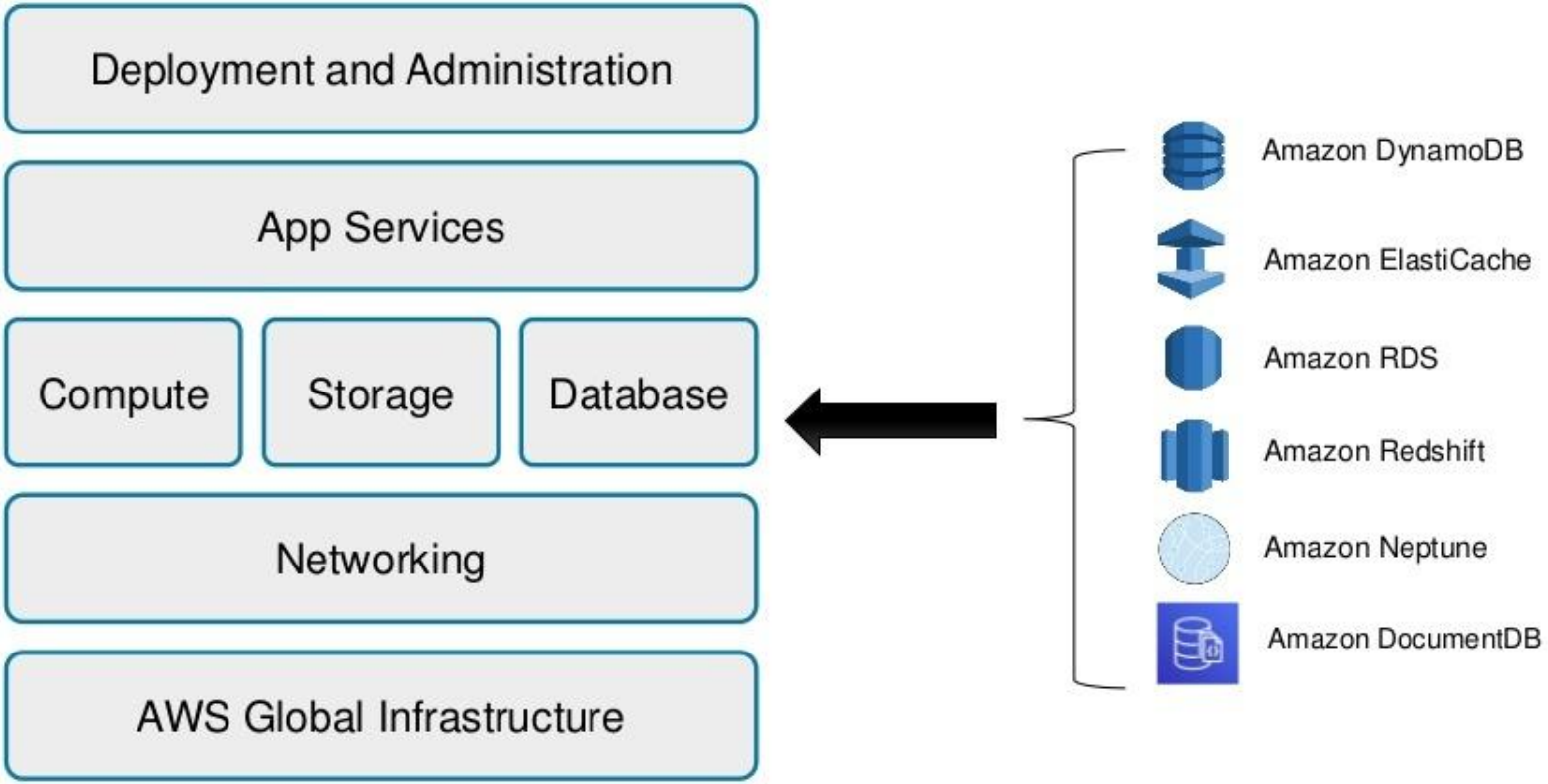
Instructor Demo
IAM

AWS IAM Best Practices

- **Delete** AWS account (root) access keys.
- Create **individual** IAM users.
- **Use groups** to assign permissions to IAM users.
- Grant **least privilege**.
- Configure a **strong password policy**.
- Enable **MFA** for privileged users.
- Use **roles for applications** that run on Amazon EC2 instances.
- Delegate by **using roles** instead of by sharing credentials.

Module 4
Databases

AWS Managed Database Services



Data Storage Considerations

- No one size fits all.
- Analyze your data requirements by considering:
  - Data formats
  - Data size
  - Query frequency
  - Data access speed
  - Data retention period

Amazon Relational Database Service (RDS)

Amazon RDS

- Cost-efficient and **resizable capacity**
- Manages time-consuming **database administration** tasks
- Access to the full capabilities of **Amazon Aurora**, **MySQL**, **MariaDB**, **Microsoft SQL Server**, **Oracle**, and **PostgreSQL** databases
- Deployable **on-premises** on Vmware (in preview)

Amazon RDS

- Simple and fast to deploy
- Manages common database administrative tasks
- Compatible with your applications
- Fast, predictable performance
- Simple and fast to scale
- Secure
- Cost-effective

MySQL
PostgreSQL
Microsoft SQL Server
MariaDB
Amazon Aurora
ORACLE

DB Instances

- DB Instances are the basic building blocks of Amazon RDS.
- They are an isolated database environment in the cloud.
- They can contain multiple user-created databases.

How Amazon RDS Backups Work

- **Automatic Backups**:
  - Restore your database to a point in time.
  - Are enabled by default.
  - Let you choose a retention period up to 35 days.
- **Manual Snapshots**:
  - Let you build a new database instance from a snapshot.
  - Are initiated by the user.
  - Persist until the user deletes them.
  - Are stored in Amazon S3.

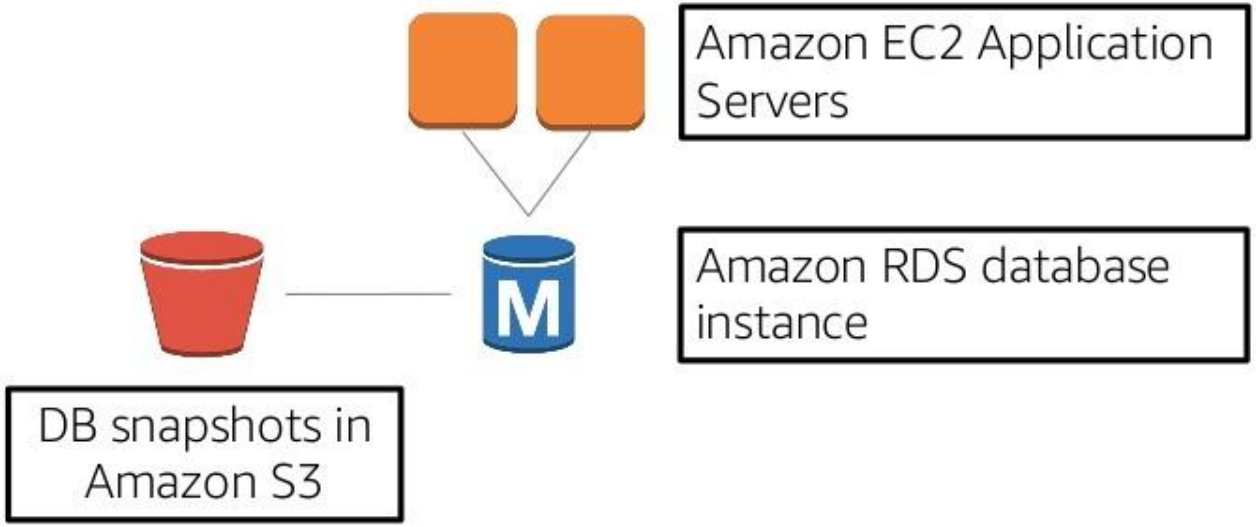
Cross-Region Snapshots

- Are a copy of a database snapshot stored in a different AWS Region.
- Provide a backup for disaster recovery.
- Can be used as a base for migration to a different region.

Amazon RDS Security

- Use IAM policies to grant access to RDS resources.
- Use Security Groups.
- Use Secure Socket Layer (SSL) connections with DB instances (Amazon Aurora, Oracle, MySQL, MariaDB, PostgreSQL, Microsoft SQL Server).
- Use RDS encryption to secure instances and snapshots at rest.
- Use network encryption and transparent data encryption (TDE) with Oracle DB and Microsoft SQL Server instances.
- Use security features of your DB engine to control access to DB instance.

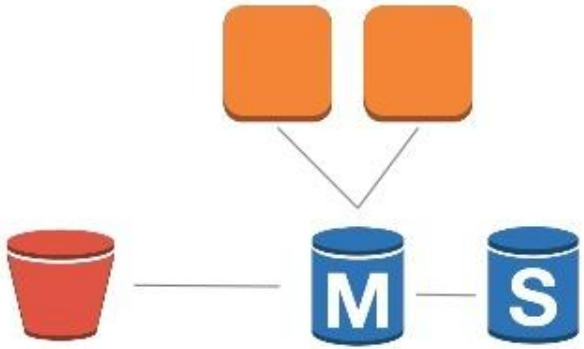
A Simple Application Architecture



Multi-AZ RDS Deployment

- With Multi-AZ operation, your database is synchronously replicated to another Availability Zone in the same AWS Region.
- Failover to the standby automatically occurs in case of master database failure.
- Planned maintenance is applied first to standby databases.

A Resilient, Durable Application Architecture



Application, in Amazon EC2 instances

Amazon RDS database instances: Master and Multi-AZ standby

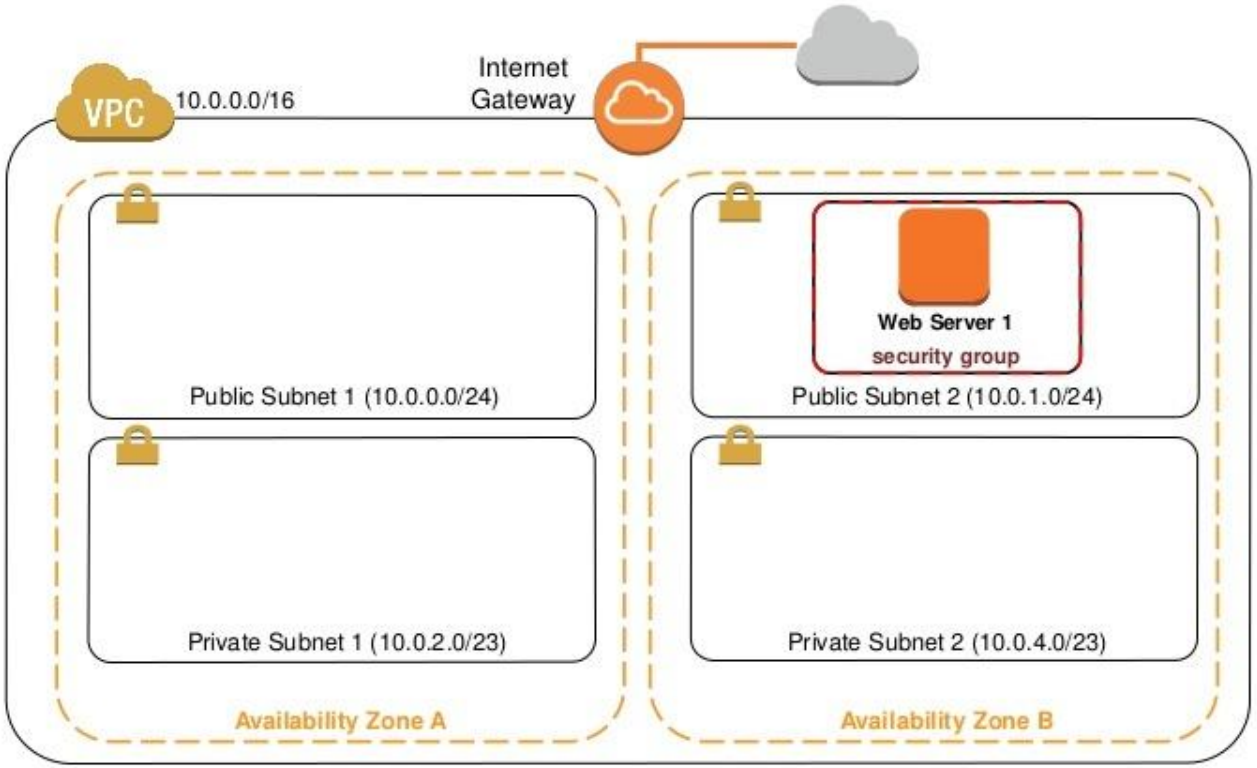
DB snapshots in Amazon S3

Amazon RDS Best Practices

- Monitor your memory, CPU, and storage usage.
- Use Multi-AZ deployments.
- Enable automatic backups.
- Set the backup window to occur during the daily low in WriteIOPS.
- To increase the I/O capacity of a DB instance:
  - Migrate to a DB instance class with high I/O capacity.
  - Convert from standard storage to provisioned IOPS storage and use a DB instance class optimized for provisioned IOPS.
  - Provision additional throughput capacity (if using provisioned IOPS storage).
- Test failover for your DB instance.

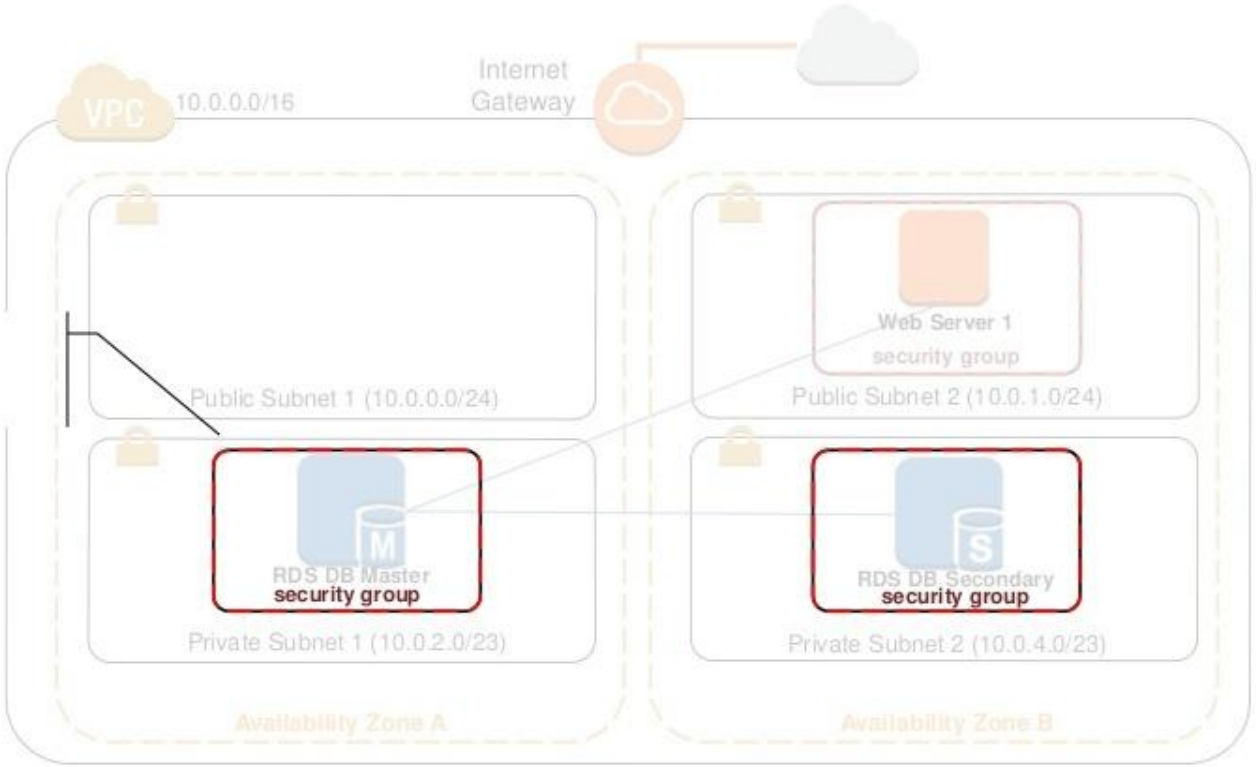
Instructor Demo (Part 1)
Build a database cluster

What We're Starting With



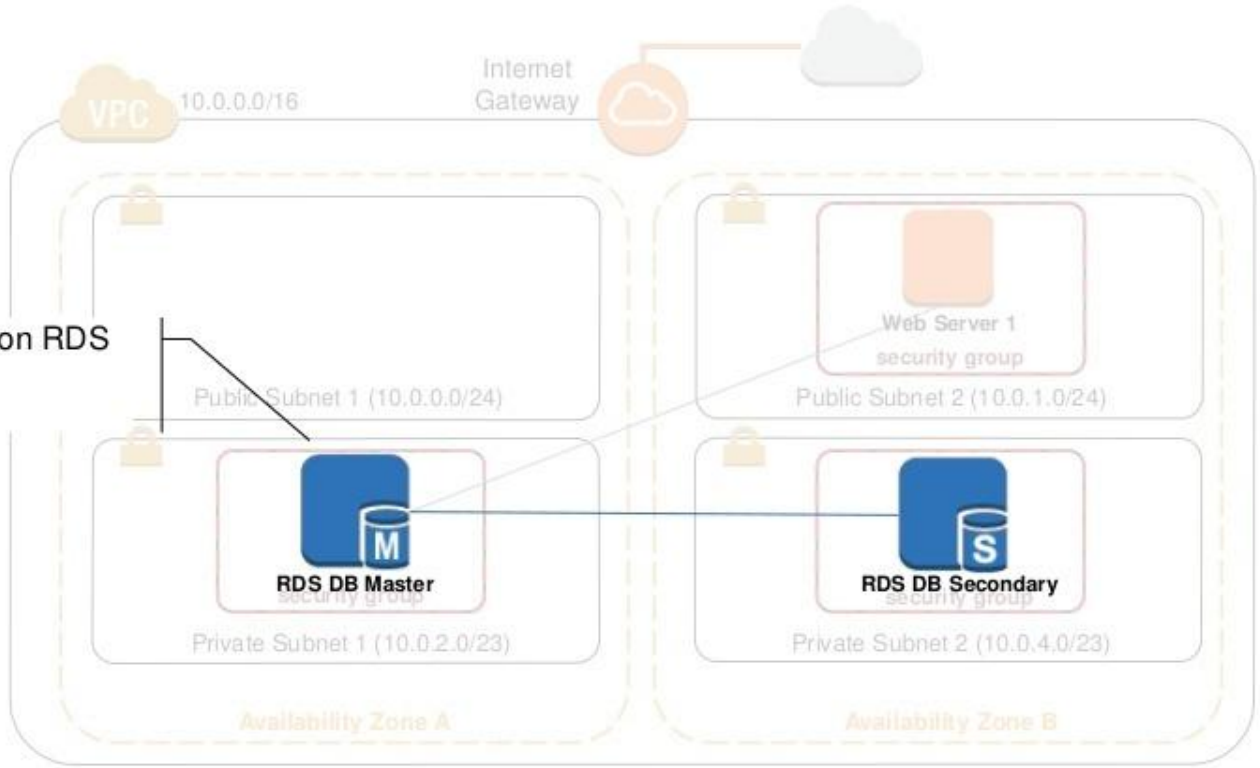
Build a Database Cluster

Create a security group for the RDS instances



Build a Database Cluster

Deploy Amazon RDS in a multi-AZ configuration

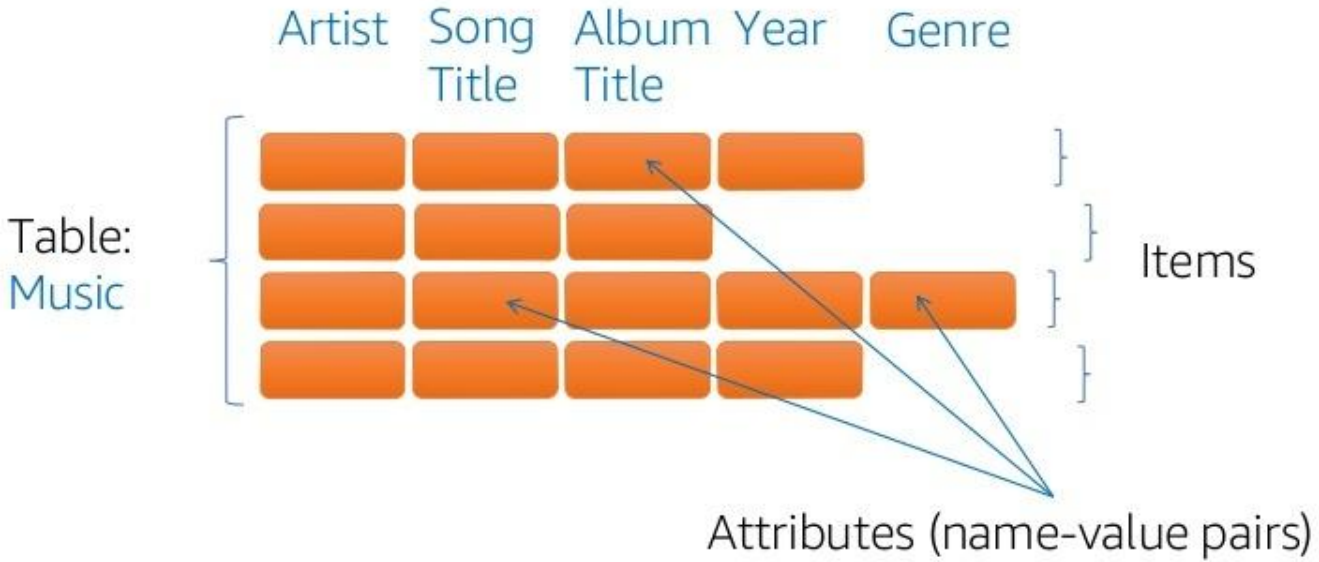


Amazon DynamoDB

Amazon DynamoDB

- Allows you to store any amount of data with no **limits**.
- Provides fast, predictable performance using **SSDs**.
- Allows you to easily provision and change the **request capacity** needed for each table.
- Is a **fully managed, NoSQL** database service.

DynamoDB Data Model



Primary Keys

Table: Music
Partition Key: Artist
Sort Key: Song Title

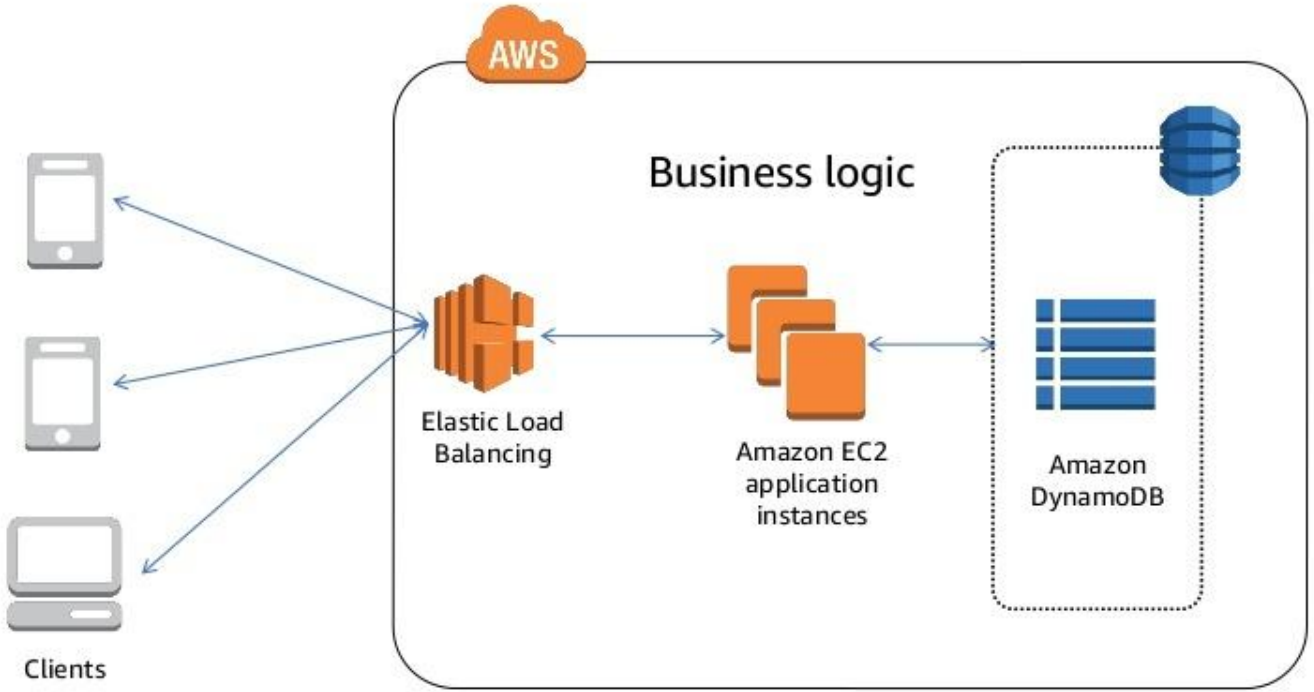
Supported Operations

- **Query**:
  - Query a table using the partition key and an optional sort key filter.
  - If the table has a secondary index, query using its key.
  - It is the **most efficient way to retrieve items** from a table or secondary index.
- **Scan**:
  - You can scan a table or secondary index.
  - Scan reads every item – **slower than querying**.

Provisioned Throughput

- You specify how much provisioned throughput capacity you need for reads and writes with optional auto-scaling.
- Alternatively, use on-demand capacity mode
- Amazon DynamoDB allocates the necessary machine resources to meet your needs.

Architecture



Amazon RDS and Amazon DynamoDB

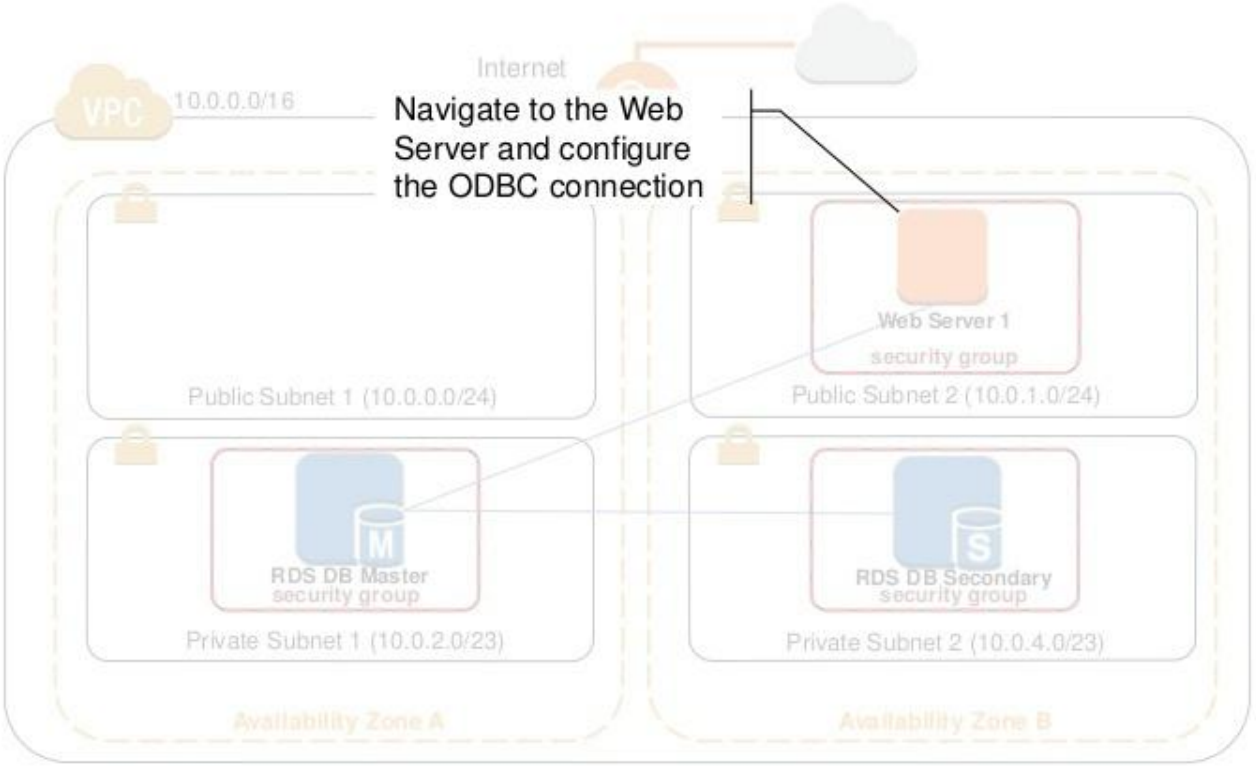
Factors	Relational (Amazon RDS)	NoSQL (Amazon DynamoDB)
Application Type	Existing database apps Business process–centric apps	New web-scale applications Large number of small writes and reads
Application Characteristics	**Relational** data models, transactions **Complex** queries, joins, and updates	Simple data models, transactions Range queries, simple updates
Scaling	Application or **DBA–architected** (clustering, partitions, sharding)	**Seamless, on-demand scaling** based on application requirements
QoS	Performance–depends on data model, indexing, query, and storage optimization Reliability and availability Durability	Performance–**Automatically optimized** by the system Reliability and availability Durability

Database Considerations

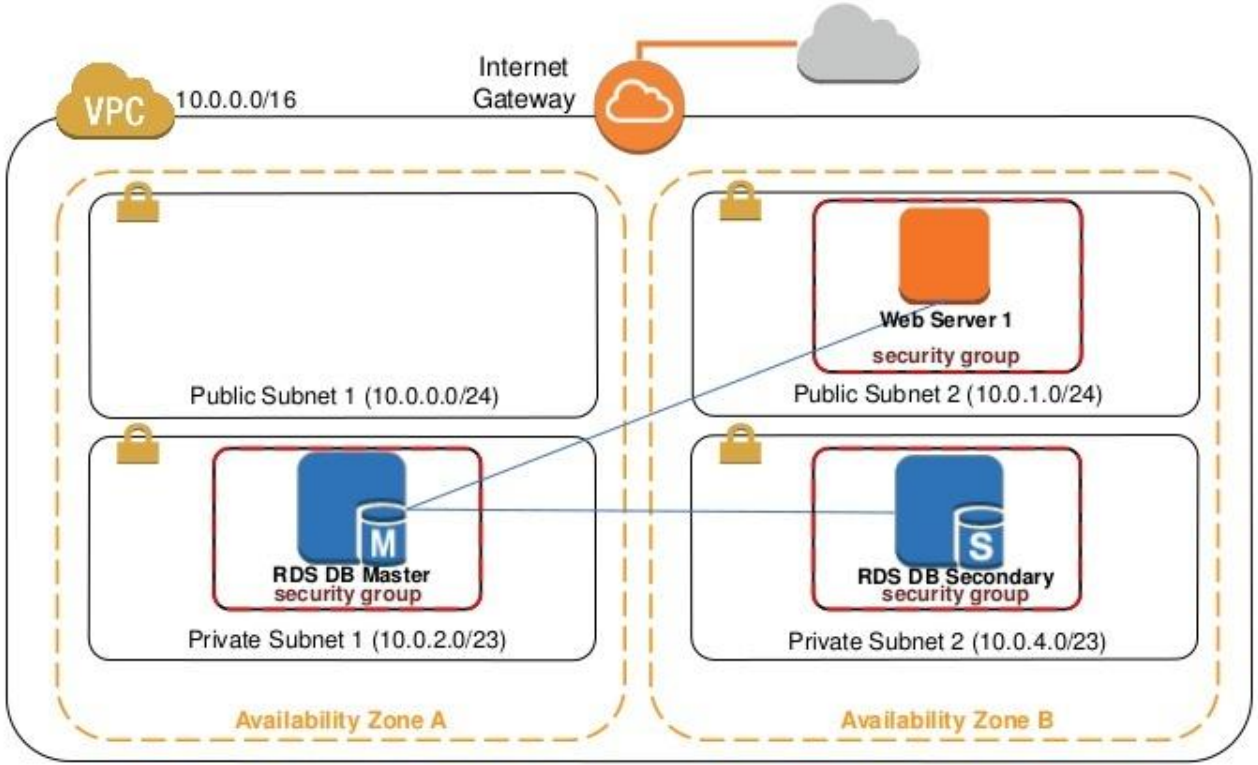
If You Need	Consider Using
A relational database service with minimal administration	**Amazon RDS** - Choice of Amazon Aurora, MySQL, MariaDB, Microsoft SQL Server, Oracle, or PostgreSQL database engines - Scale compute and storage - Multi-AZ availability 
A fast, highly scalable NoSQL database service	**Amazon DynamoDB** - Extremely fast performance - Seamless scalability and reliability - Low cost 
A database you can manage on your own	Your choice of **AMIs** on Amazon EC2 and EBS that provide scaling for compute and storage, complete control over instances, and more. 

Instructor Demo (Part 2)
Interact with the database using an application

Build a Database Cluster and Connect to It

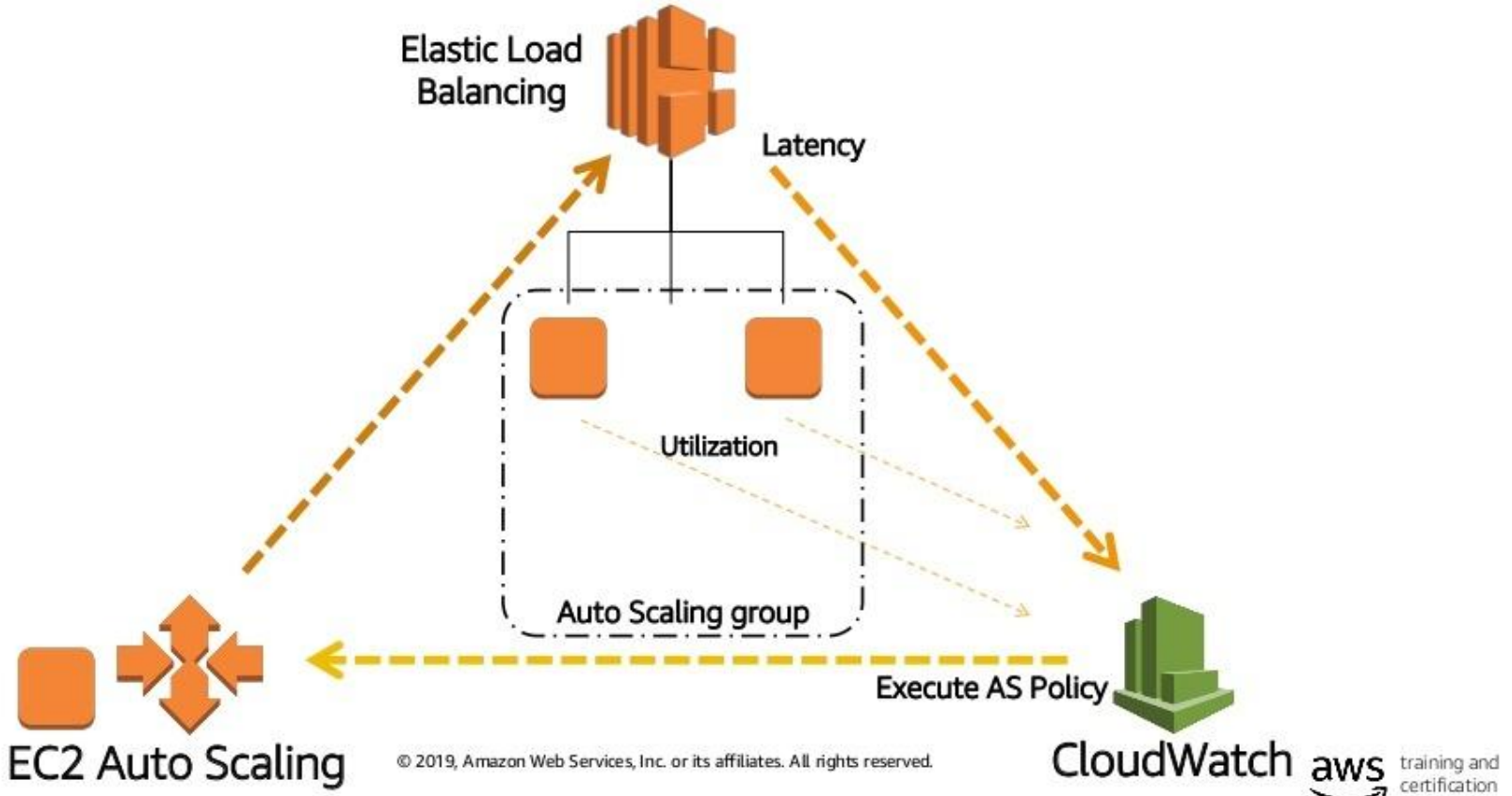


Build a Database Cluster and Connect to It



Module 5
AWS Elasticity and Management Tools

Trio of Services



aws training and certification

Elastic Load Balancing

Elastic Load Balancing

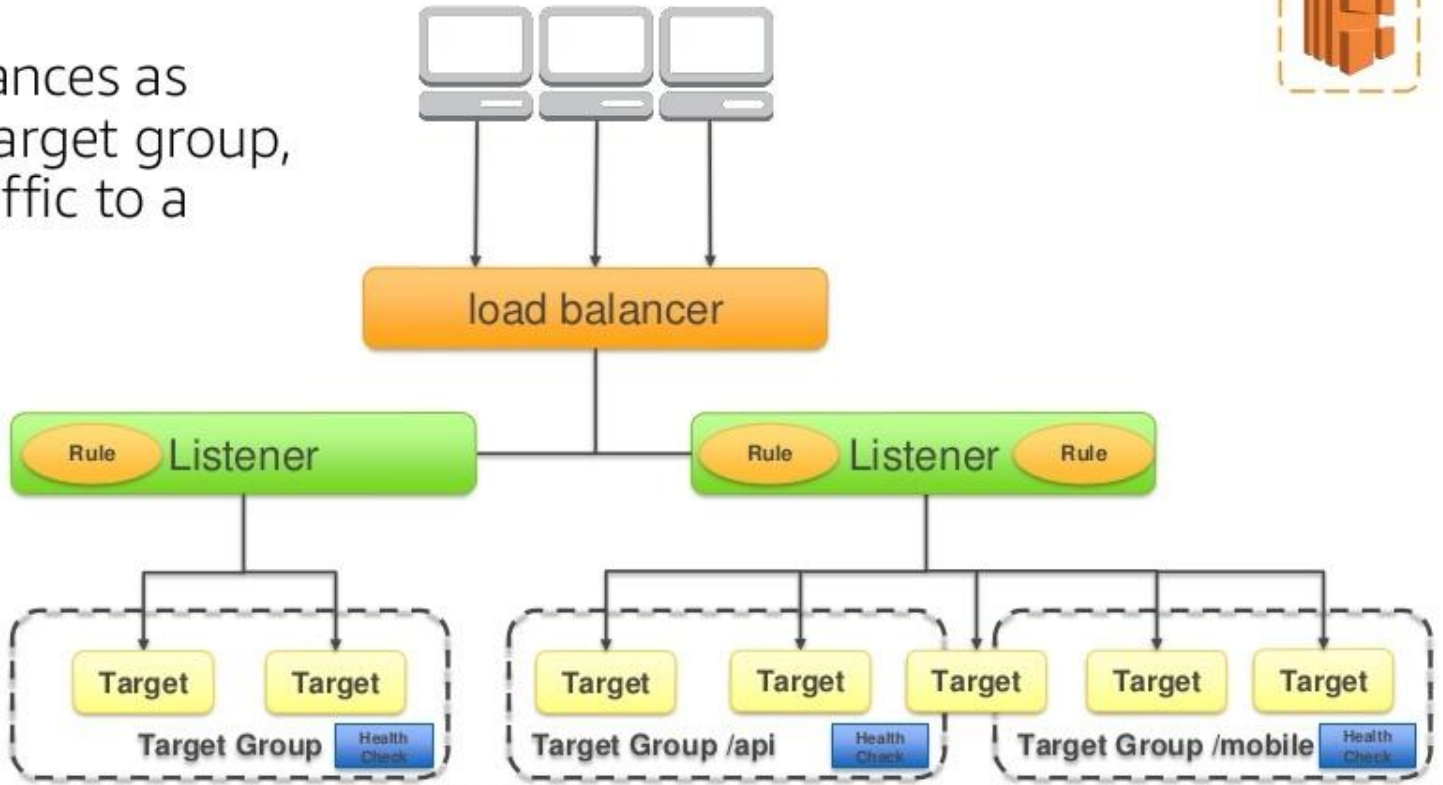
- **Distributes** traffic across multiple EC2 instances, in multiple Availability Zones
- Supports **health checks** to detect unhealthy Amazon EC2 instances
- Supports the **routing and load balancing** of HTTP, HTTPS, SSL, and TCP traffic to Amazon EC2 instances

Elastic Load Balancing types

Application Load Balancer (ALB)	Network Load Balancer (NLB)	Classic Load Balancer (CLB)
		PREVIOUS GENERATION for HTTP, HTTPS, and TCP
• Flexible application management • Advanced load balancing of HTTP and HTTPS traffic • Operates at the request level (layer 7)	• Extreme performance and static IP for your application • Load balancing of TCP traffic • Operates at the connection level (Layer 4)	• Existing application that was built within the EC2-Classic network • Operates at both the request level and connection level

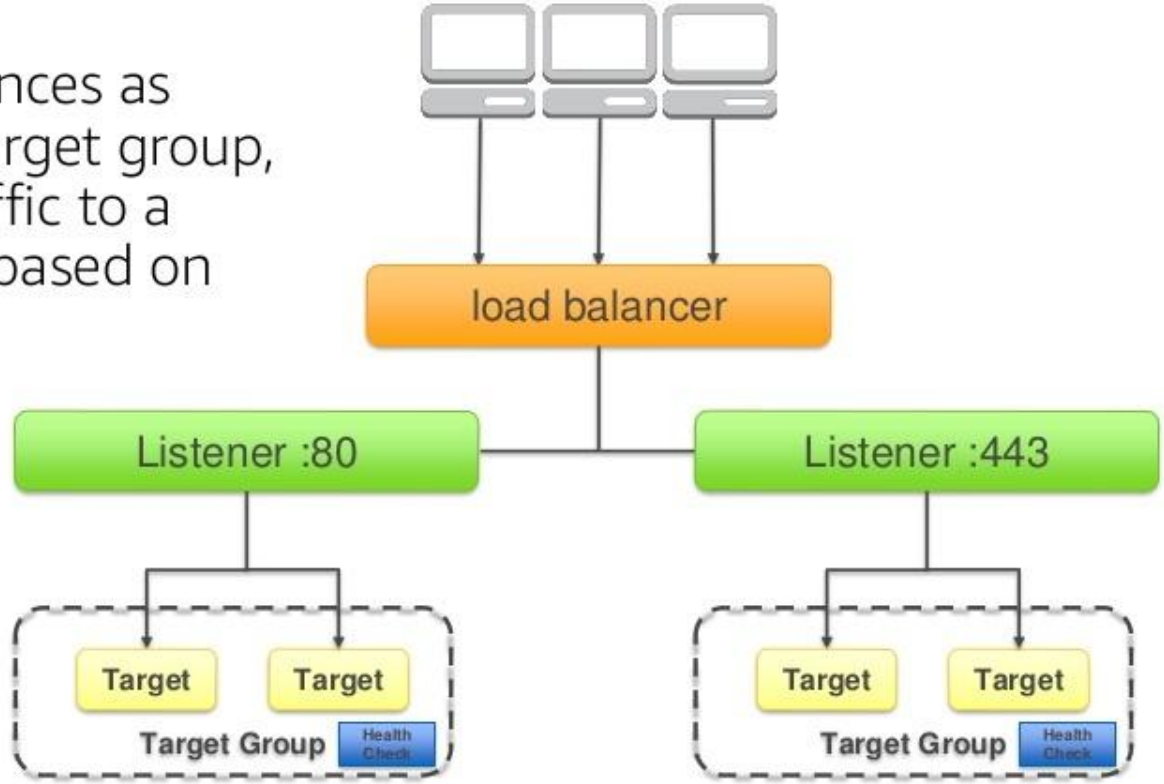
Application Load Balancer

Register instances as targets in a target group, and route traffic to a target group.



Network Load Balancer

Register instances as targets in a target group, and route traffic to a target group based on port.



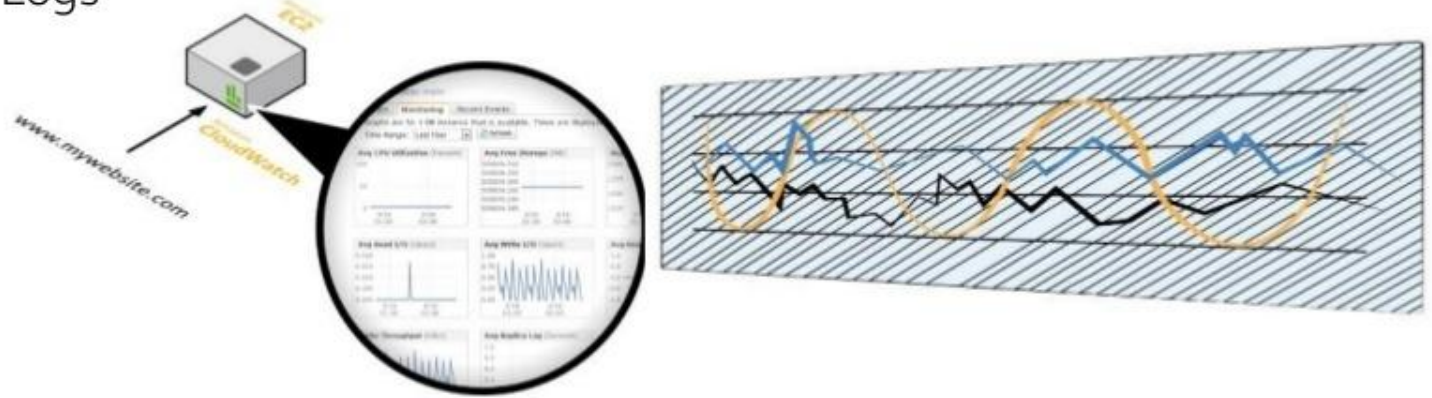
Amazon CloudWatch

Amazon CloudWatch

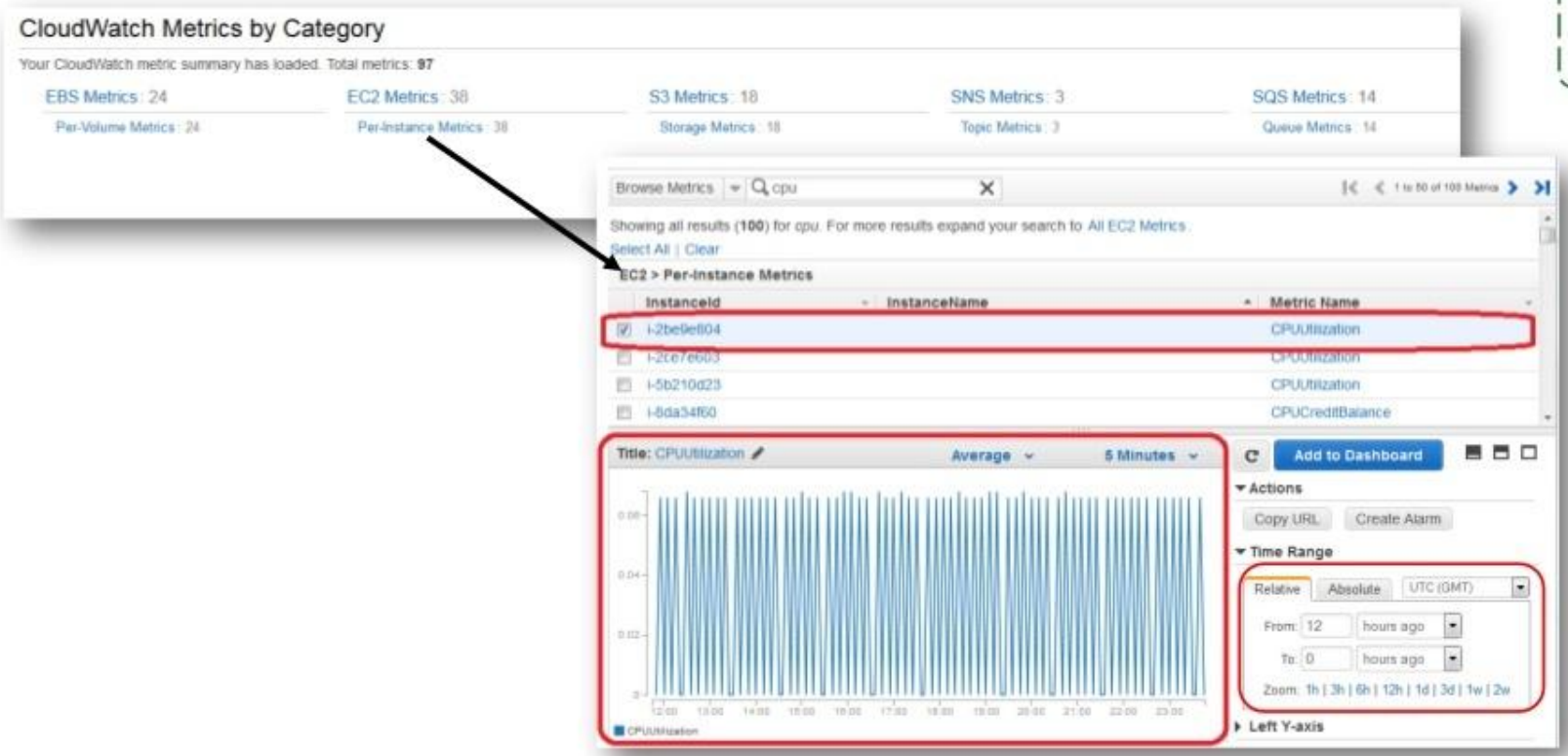
- A **monitoring service** for AWS cloud resources and the applications you run on AWS
- **Visibility into** resource utilization, operational performance, and overall demand patterns
- **Custom application-specific** metrics of your own
- **Accessible** via AWS Management Console, APIs, SDK, or CLI

Amazon CloudWatch Facts

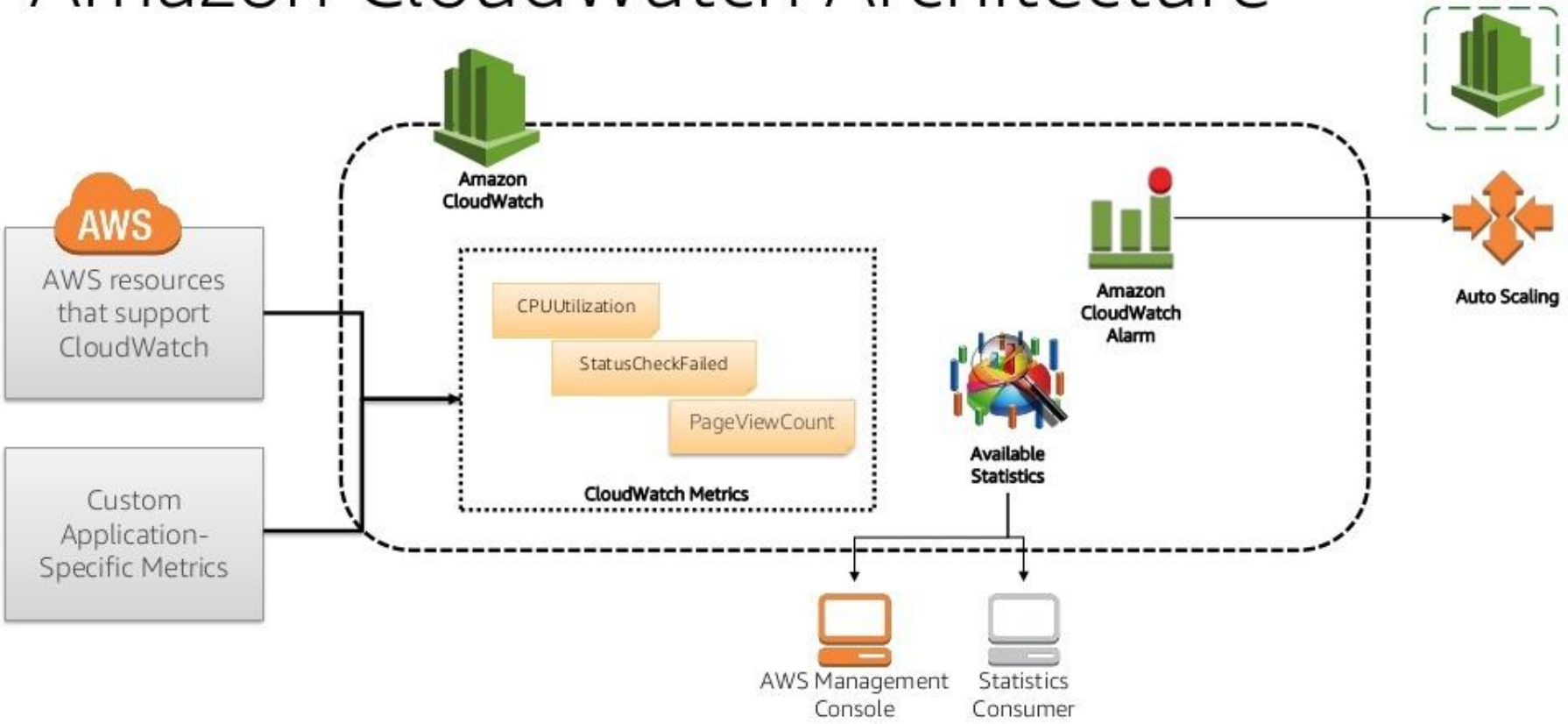
- Collects metrics from other AWS resources
  - View graphics and statistics
- Set and Trigger Alarms
- Collect Logs



CloudWatch Metrics Examples



Amazon CloudWatch Architecture



EC2 Auto Scaling

Auto Scaling

- Scale your Amazon EC2 capacity automatically
- Well-suited for applications that experience variability in usage
- Available at no additional charge

EC2 Auto Scaling Benefits

Better Fault Tolerance

Better Availability

Better Cost Management

EC2 Auto Scaling Components

Launch Configuration

Auto Scaling Group

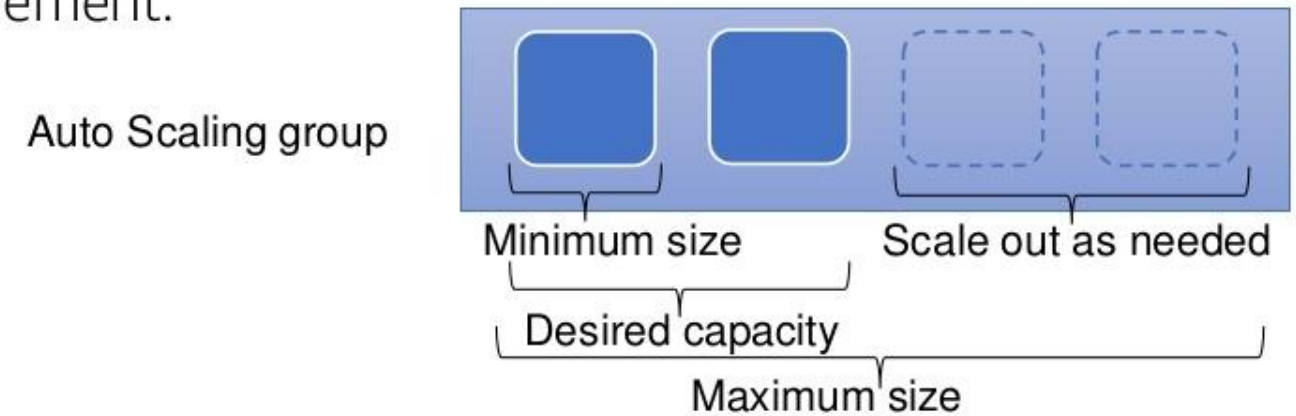
Scaling Plan

EC2 Auto Scaling Launch Configurations

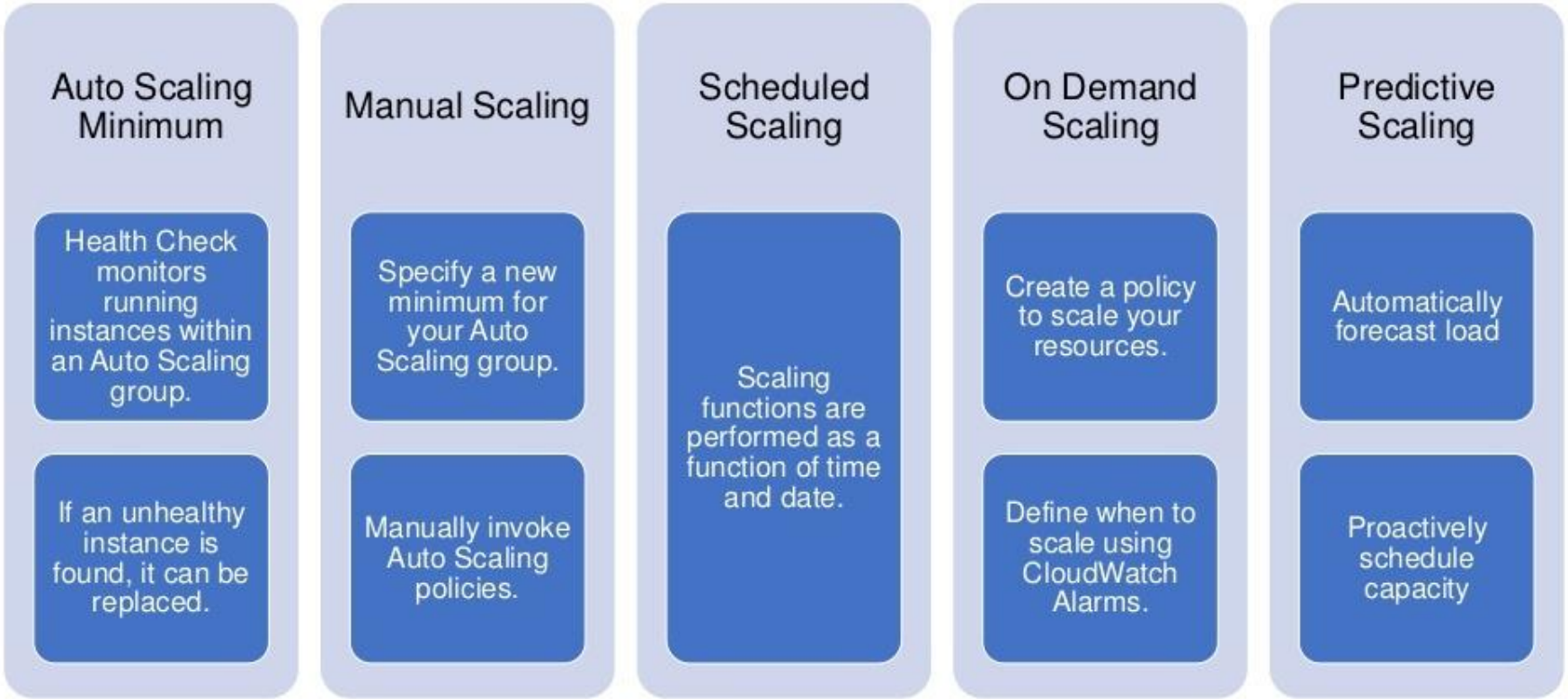
- A launch configuration is a **template** that an Auto Scaling group uses to launch EC2 instances.
- When you create a launch configuration, you can specify:
  - AMI ID
  - Instance type
  - User data
  - Block device mapping
  - Security groups
  - Key pair

EC2 Auto Scaling Groups

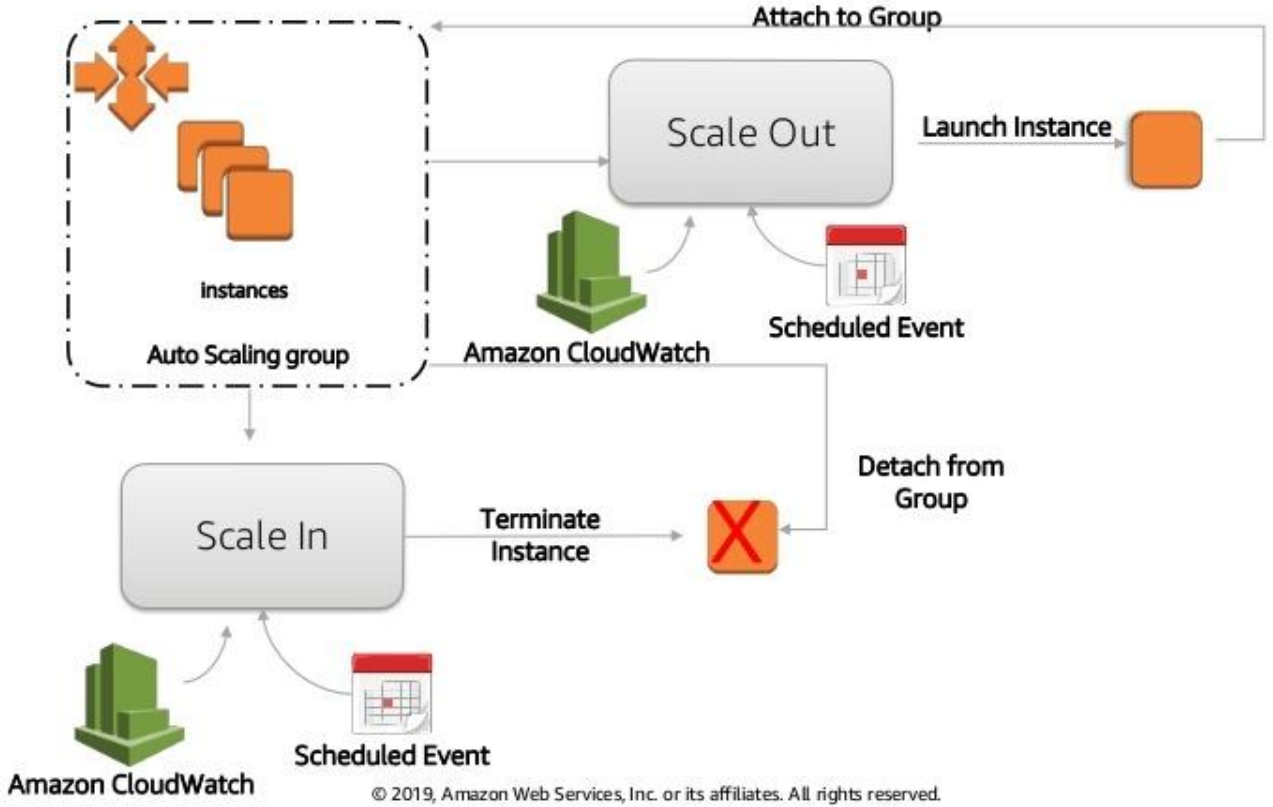
- Contain a collection of EC2 instances that share similar characteristics.
- Instances in an Auto Scaling group are treated as a logical grouping for the purpose of instance scaling and management.



EC2 Auto Scaling



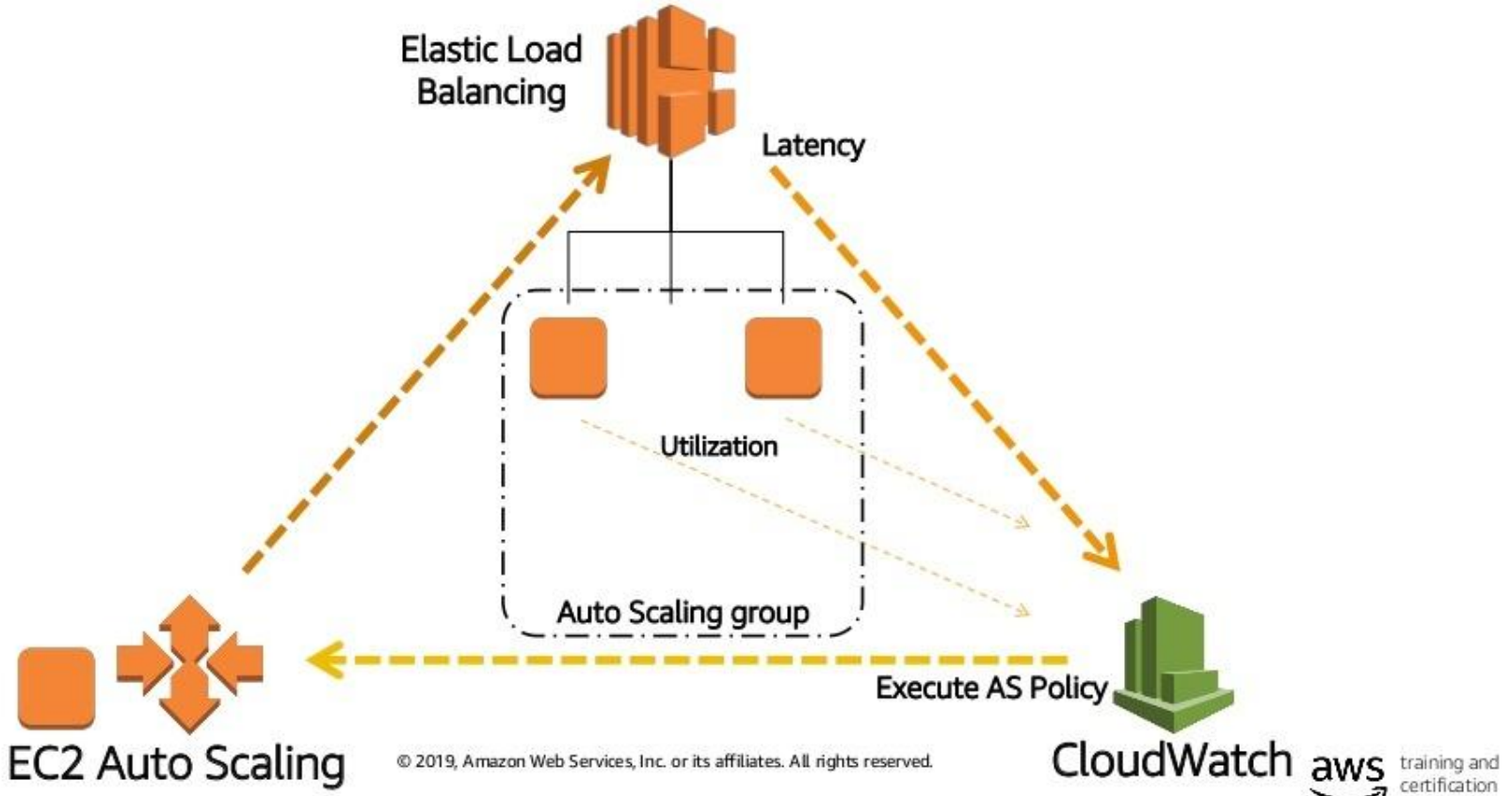
EC2 Auto Scaling Basic Lifecycle



AWS Auto Scaling

- Monitors your applications and adjusts capacity
- Build scaling plans for resources including:
  - Amazon EC2 instances and Spot Fleets
  - Amazon ECS tasks
  - Amazon DynamoDB tables and indexes
  - Amazon Aurora Replicas
- Amazon EC2 Auto Scaling is part of AWS Auto Scaling

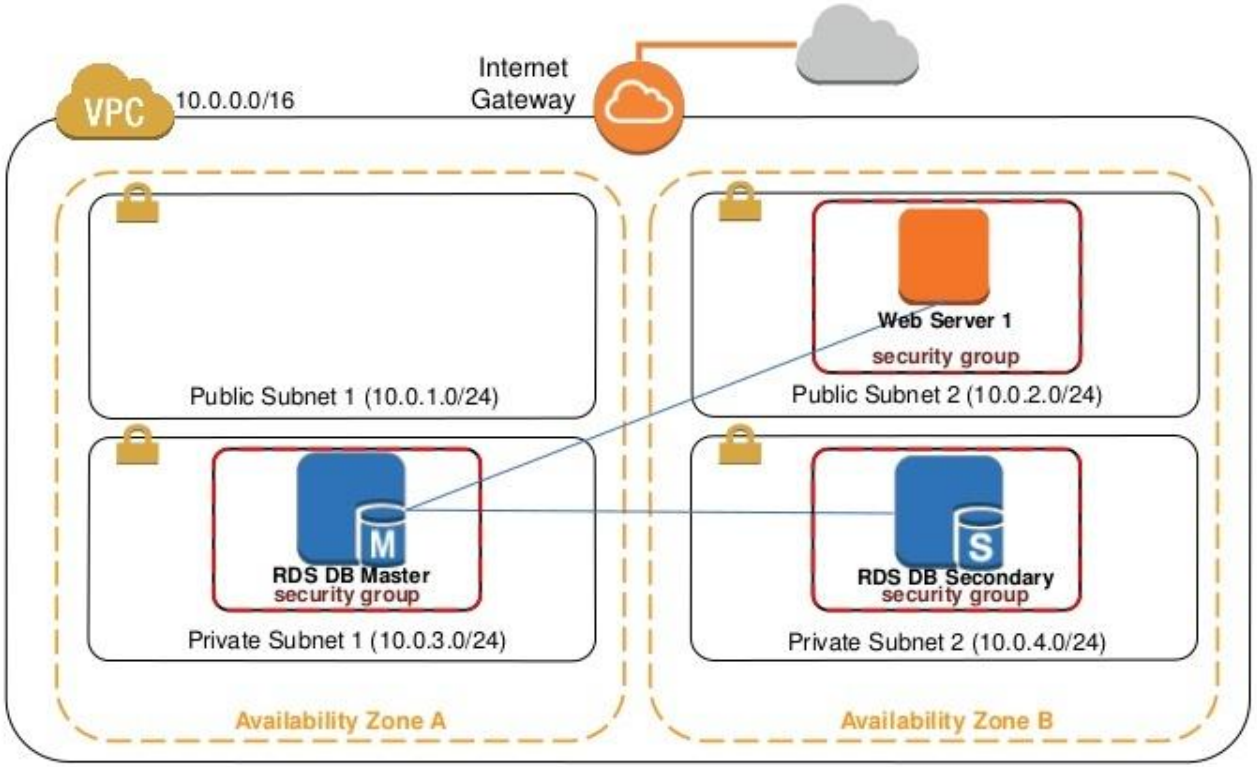
Trio of Services



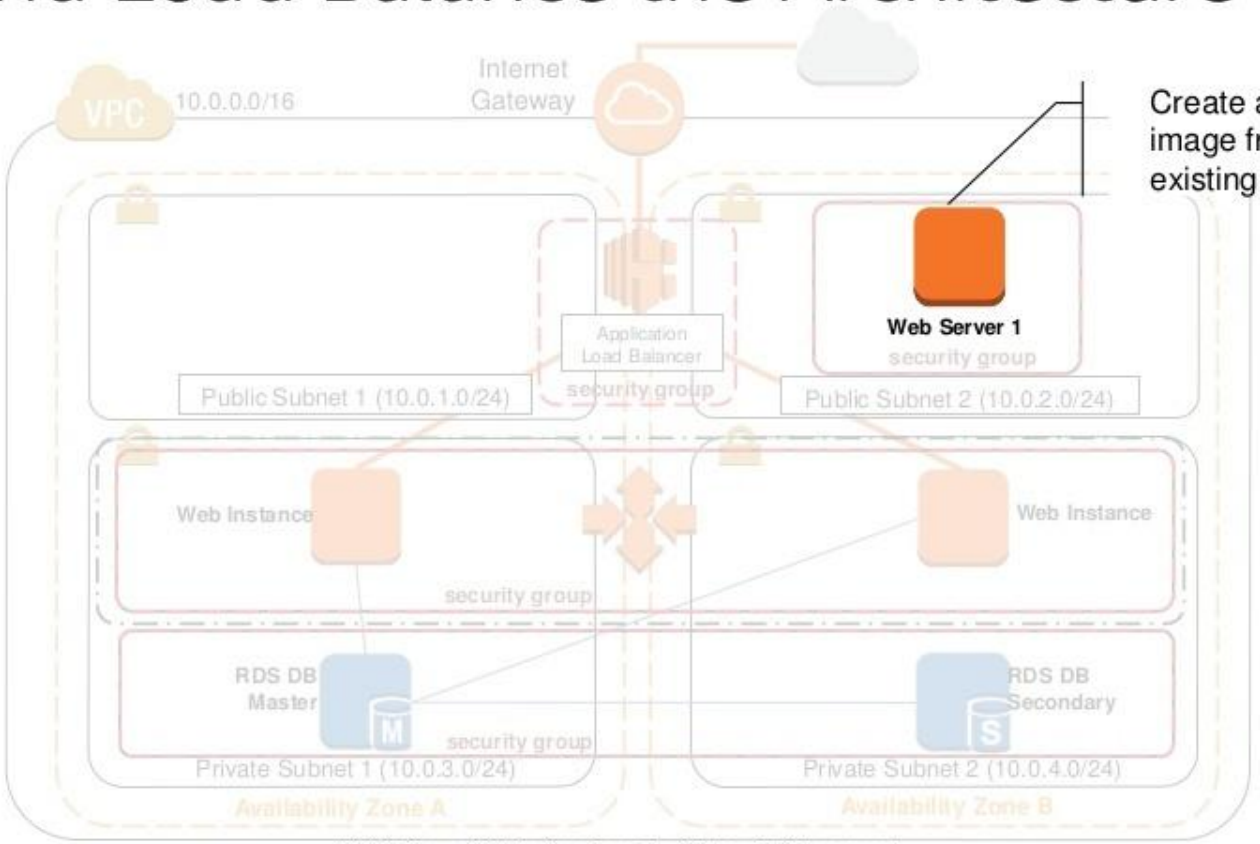
aws training and certification

Instructor Demo
Scale and Load Balance the Architecture

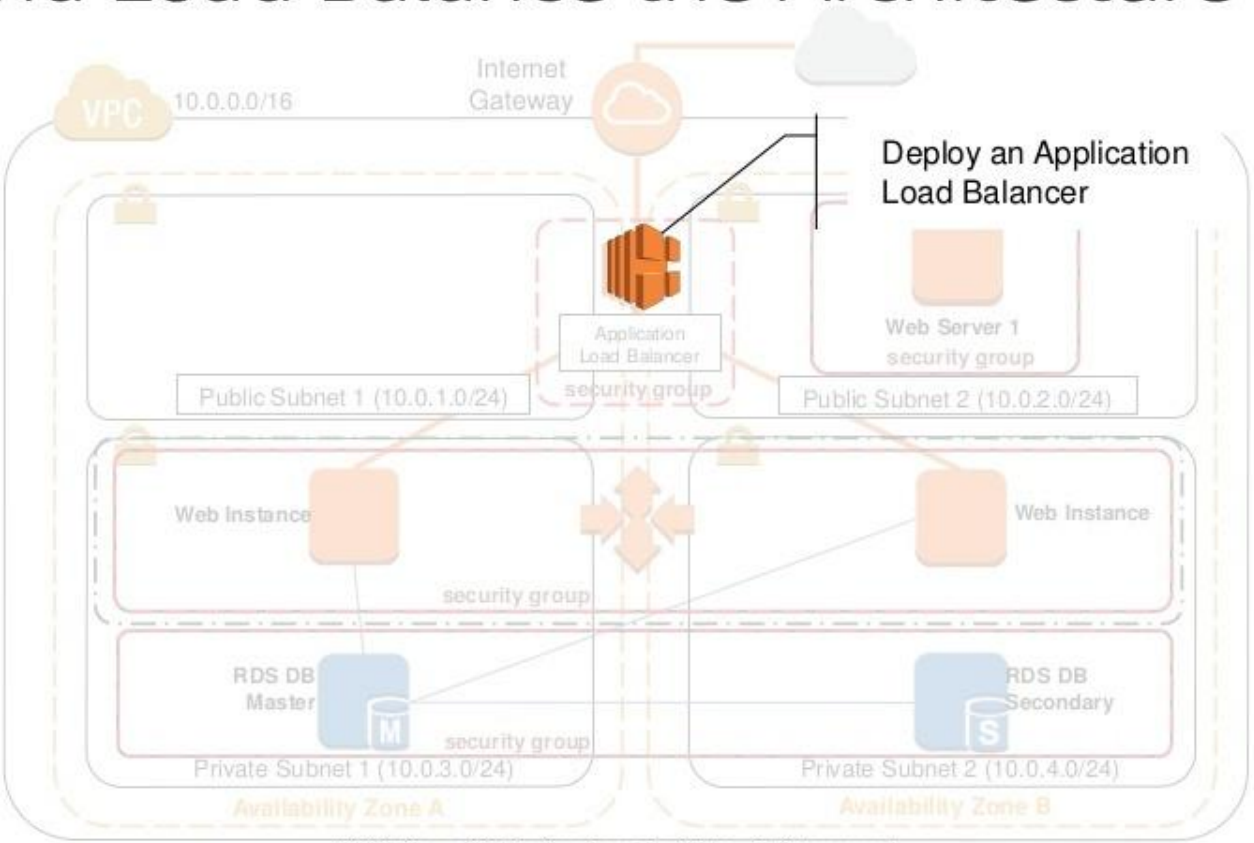
What We're Starting With



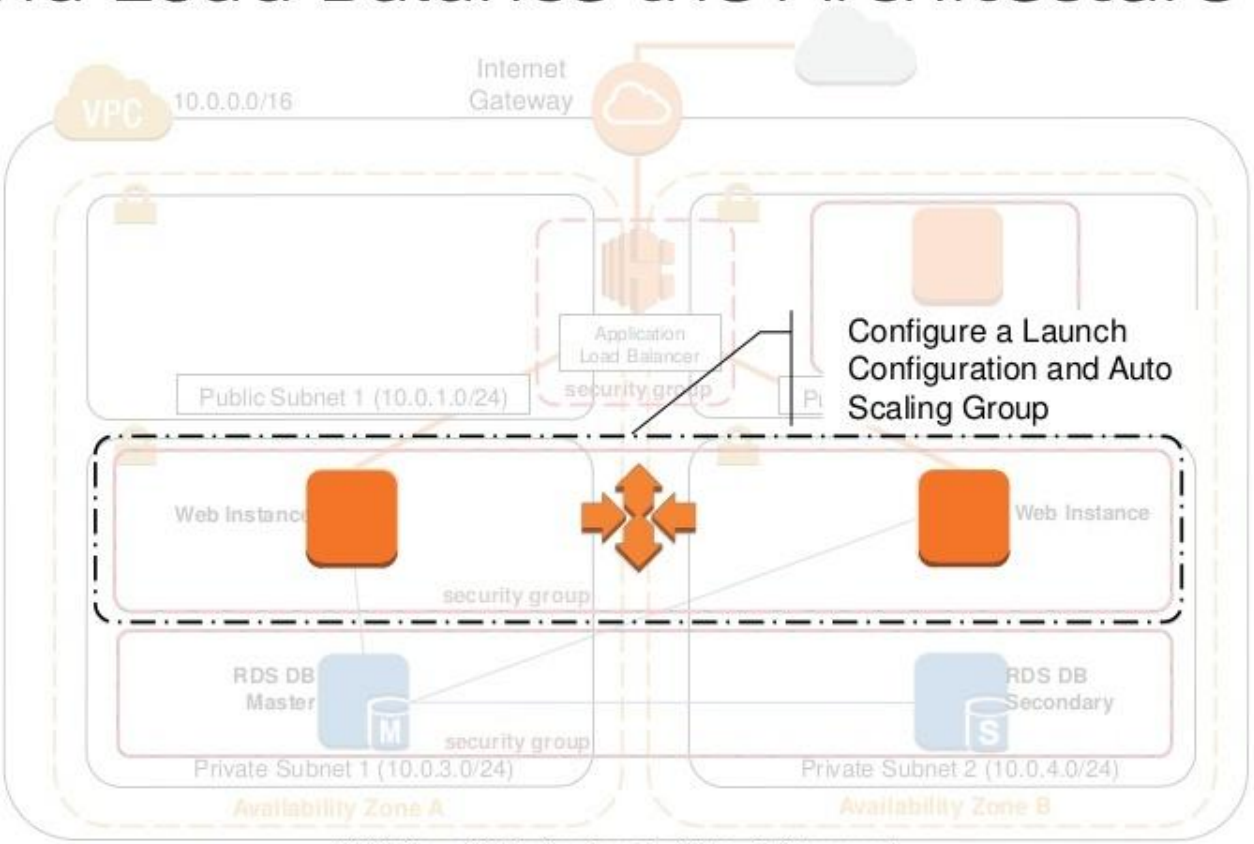
Scale and Load Balance the Architecture



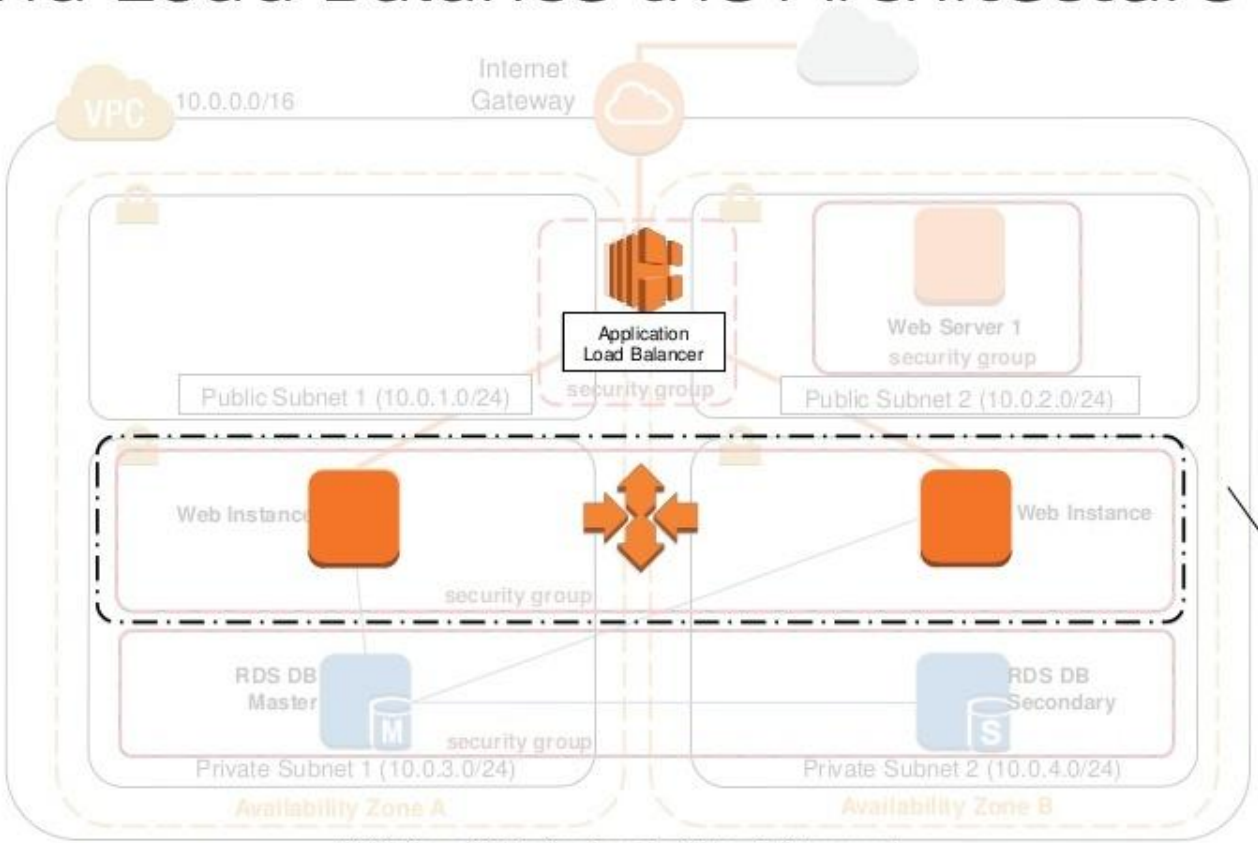
Scale and Load Balance the Architecture



Scale and Load Balance the Architecture

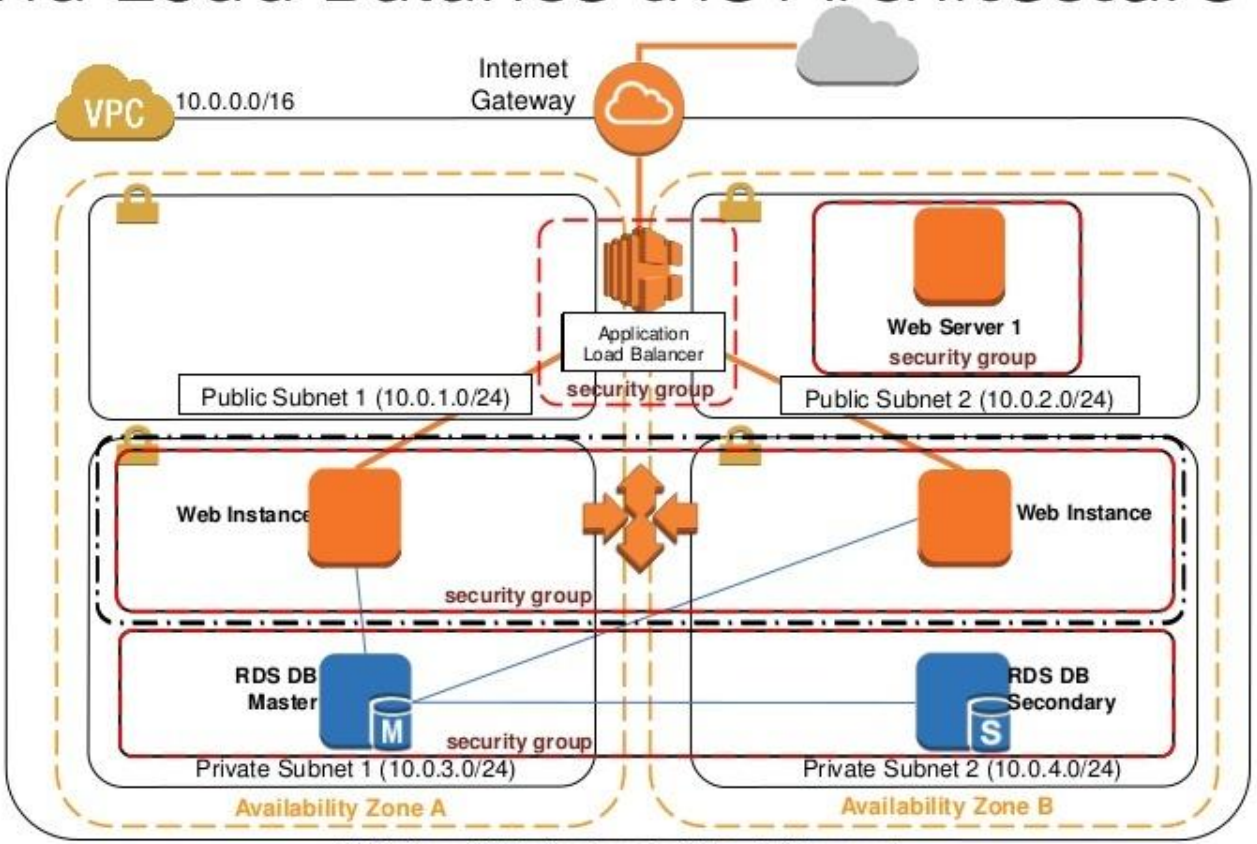


Scale and Load Balance the Architecture



Test and monitor your Auto Scaling Group

Scale and Load Balance the Architecture



AWS Trusted Advisor

AWS Trusted Advisor

- **Best practice** and recommendation engine.
- Provides AWS customers with performance and security recommendations in four categories:
  - **Cost optimization**
  - **Security**
  - **Fault tolerance**
  - **Performance improvement.**

AWS Trusted Advisor?

A service providing guidance to help you reduce cost, increase performance, and improve security

aws training and certification

Trusted Advisor: Core vs. Full

Core Checks and Recommendations (included)

- Seven core checks around security and performance
- Service Limits

Full Trusted Advisor Benefits (With Business or Enterprise support)

- Full set of checks
- Notifications
- Programmatic Access via API

Cost Optimization

- Amazon EC2 Reserved Instance Optimization
- Low-utilization Amazon EC2 Instances
- Idle load balancers
- Underutilized Amazon EBS volumes
- Amazon RDS idle DB instances
- Amazon EC2 Reserved Instance Lease Expiration

aws training and certification

Security

- Security groups – Unrestricted Access
- AWS IAM use
- Amazon S3 bucket permissions
- MFA on Root Account
- AWS IAM password policy
- Amazon RDS security group access risk

Fault Tolerance

- Amazon EBS Snapshots
- Load balancer optimization
- Auto Scaling Group Resources
- Amazon RDS Multi-AZ
- Amazon RDS Backups
- ELB connection draining

aws training and certification

Performance Improvement

- High-utilization Amazon EC2 instances
- Service limits
- Large number of rules in EC2 security group
- Overutilized Amazon EBS Magnetic volumes
- Amazon EC2 to EBS throughput optimization

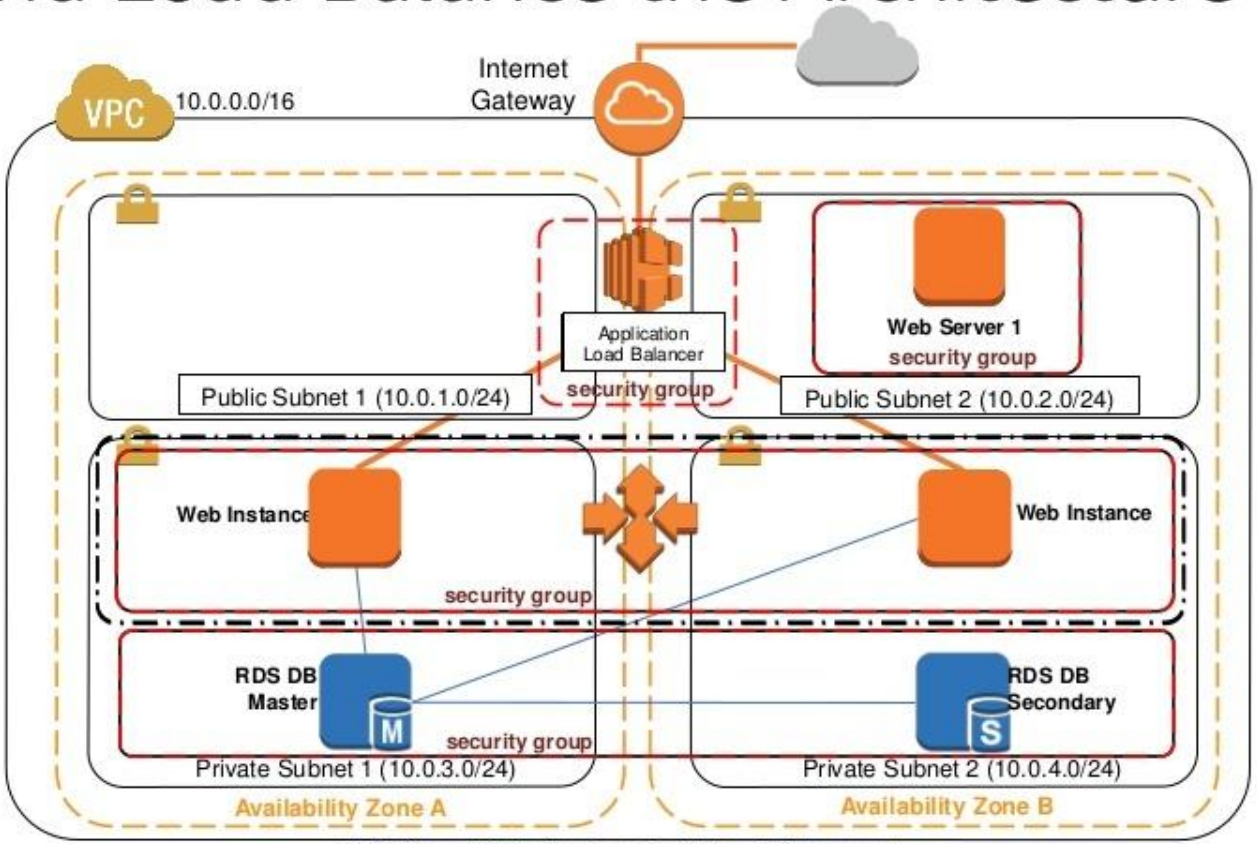
aws training and certification

AWS Support

Support Comparison

	Basic	Developer	Business	Enterprise
Customer Service and Communities	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums
Best Practices	Access to 7 core Trusted Advisor checks	Access to 7 core Trusted Advisor checks	Access to full set of Trusted Advisor checks	Access to full set of Trusted Advisor checks
Technical Support		Business hours access to Cloud Support Associates via email	24x7 access to Cloud Support Engineers via email, chat & phone	24x7 access to Sr. Cloud Support Engineers via email, chat & phone
Case Severity/ Response Times			Production system impaired: < 4 hours Production system down: < 1 hour	Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 15 minutes
Pricing	Included	Starts at $29 per month	Starts at $100 per month	Starts at $15k per month

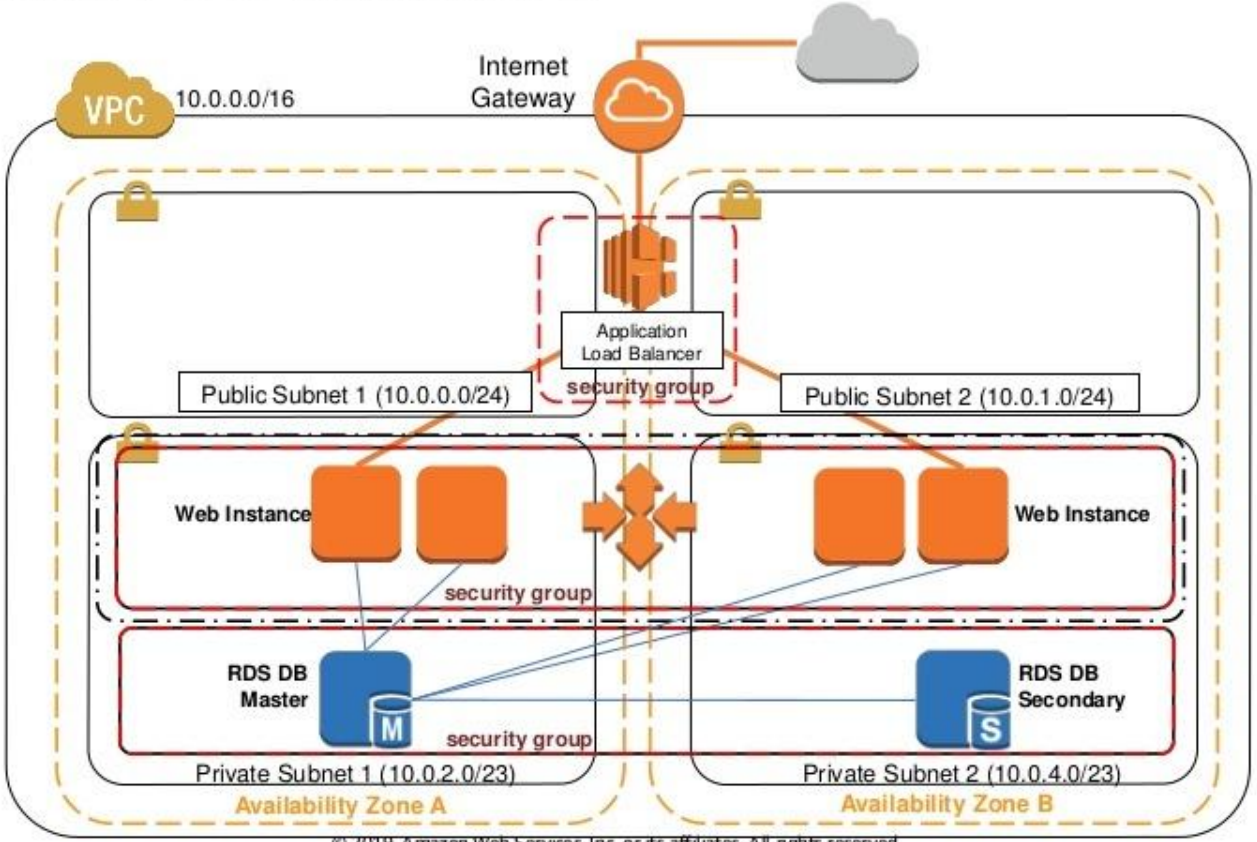
Scale and Load Balance the Architecture



Module 6
Course Wrap-Up

AWS Certification

A Scalable Architecture



Thank you!