

# AWSome Day

Getting Started on AWS

Version 4.2

# Module Layout

- Module 1: **Introduction** and History of AWS
- Module 2: **Foundational Services** – Amazon EC2, Amazon VPC, Amazon S3, Amazon EBS
- Module 3: **Security, Identity, and Access Management** - IAM
- Module 4: **Databases** – Amazon DynamoDB and Amazon RDS
- Module 5: **AWS Elasticity and Management Tools** – Auto Scaling, Elastic Load Balancing, Amazon CloudWatch, and AWS Trusted Advisor
- Module 6: Course Wrap-Up

# Module 1

# Introduction and History of AWS

# Amazon History



**1994:** Jeff Bezos incorporated the company.



**2005:** Amazon Publishing was launched.



**2007:** Kindle was launched.



**2012:** Amazon Game Studios was launched.



**2014:** Amazon Prime Now was launched.

**1995:** Amazon.com launched its online bookstore.



**2006:** Amazon Web Services (AWS) was launched.



**2011:** Amazon Fresh was launched.



**2013:** Amazon Art was launched.

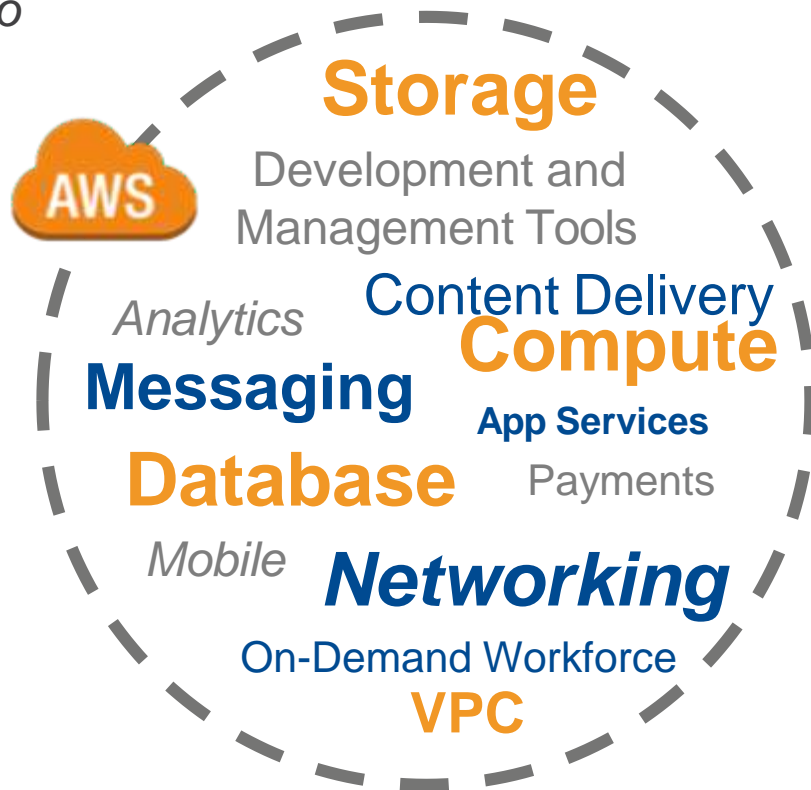


**2015:** Amazon Home Services and Amazon Echo were launched.



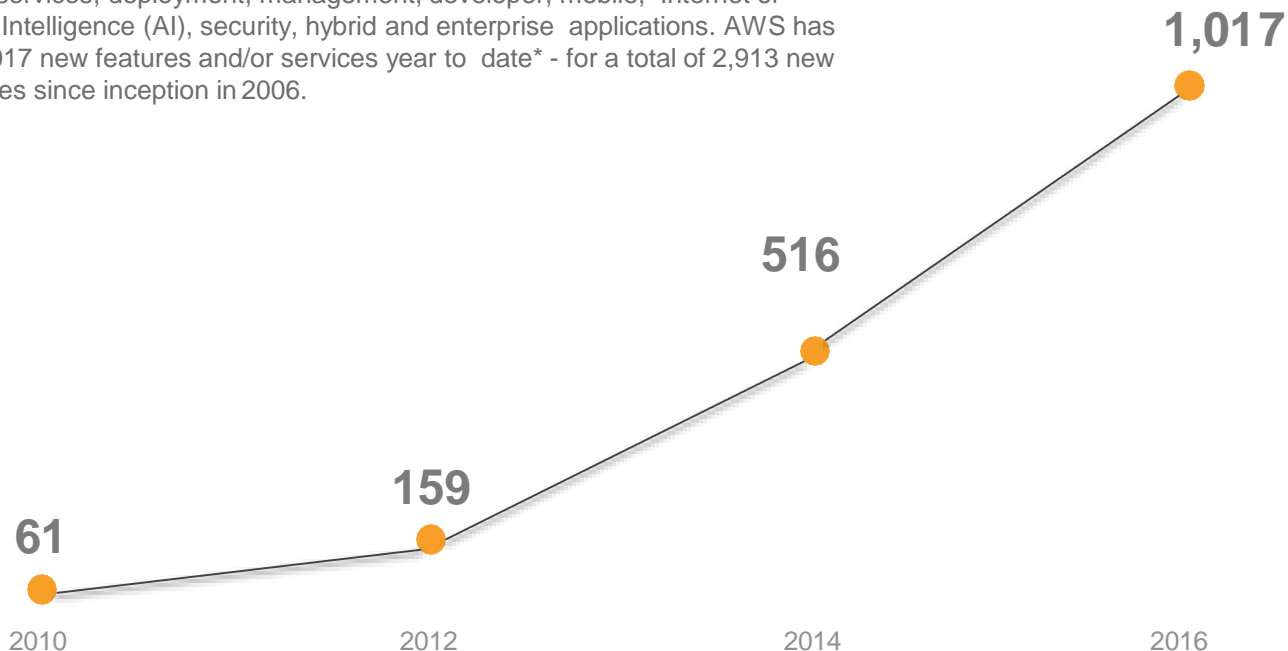
# Amazon Web Services (AWS)

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



# AWS Pace of Innovation

AWS has been continually expanding its services to support virtually any cloud workload, and it now has more than 90 services that range from compute, storage, networking, database, analytics, application services, deployment, management, developer, mobile, Internet of Things (IoT), Artificial Intelligence (AI), security, hybrid and enterprise applications. AWS has launched a total of 1,017 new features and/or services year to date\* - for a total of 2,913 new features and/or services since inception in 2006.



\*As of 1 January 2017

2,913

**Import/Export Snowball**

AWS Storage Gateway

Amazon Cognito

GovCloud  
AWS OpsWorks

CodeCommit

**EC2**

AWS CodeDeploy

Amazon  
ElastiCache

Amazon Config

Amazon CloudTrail

Amazon SES

Elastic Transcoder

**Container Service**

Amazon Kinesis

CloudHSM

Elasticsearch Service

AWS Elastic Beanstalk

**EC2 Container  
Registry**

AWS CodePipeline

Amazon Route 53

**Lambda**

AWS  
CloudFormation

AWS Device Farm

Directory  
Service

Amazon RDS  
for Aurora

AWS Mobile Hub

**RDS for MariaDB**

AWS KMS

**Amazon API  
Gateway**

WorkDocs

**AWS IoT**

CloudWatch Logs

Mobile  
Analytics

**Amazon Machine  
Learning**

AWS Direct  
Connect

Amazon Inspector

AWS Services  
Catalog



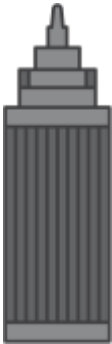
Training and  
Certification

\*As of 1 January 2017

# AWS Customers

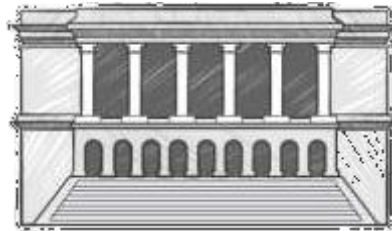
## Enterprise Customers

*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 variable expense.



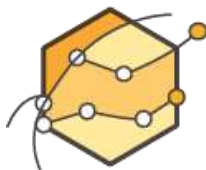
Increase speed and agility.



Benefit from massive economies of scale.



Stop spending money on running and maintaining data centers.



Stop guessing capacity.

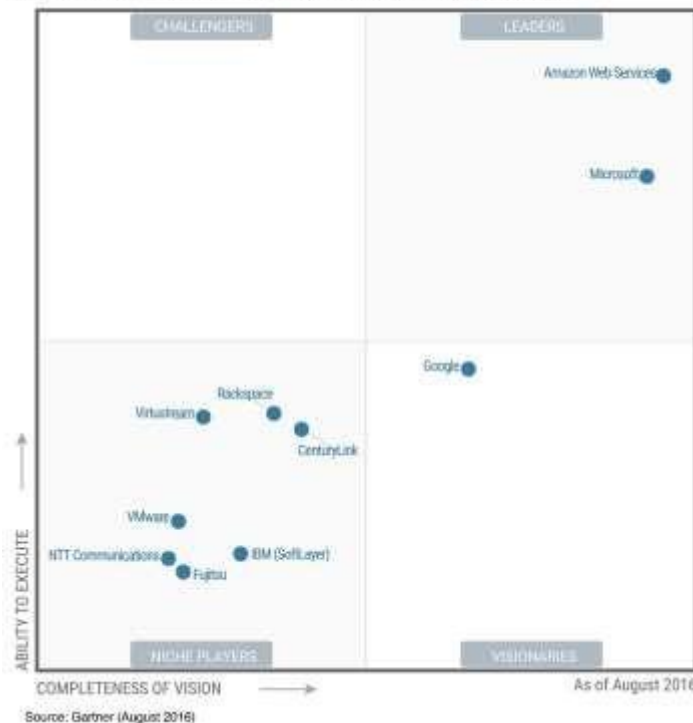


Go global in minutes.

# AWS Positioned as a Leader in the Gartner Magic Quadrant for Cloud Infrastructure as a Service, Worldwide\*

AWS is positioned highest in execution and furthest in vision within the Leaders Quadrant

Figure 1. Magic Quadrant for Cloud Infrastructure as a Service, Worldwide



\*Gartner, Magic Quadrant for Cloud Infrastructure as a Service, Worldwide, Leong, Lydia, Petri, Gregor, Gill, Bob, Dorosh, Mike, August 32016

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from AWS :

<http://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519&sl=sb>

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.



Training and  
Certification

# AWS Core Infrastructure and Services

## Traditional Infrastructure

### Security



Firewalls



ACLs



Administrators

### Security

## Amazon Web Services

### Security



Security Groups  
Security Groups



Network ACLs

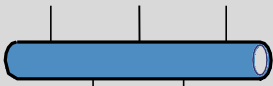


AWS IAM

### Networking



Router



Network Pipeline



Switch



ELB



VPC

### Network



On-Premises Servers

### Servers



AMI



Amazon EC2 Instances

### Storage and Database



DAS



SAN



NAS



RDBMS



Amazon  
EBS



Amazon  
EFS












Amazon  
S3








Amazon  
RDS

# AWS Foundation Services






## Compute

-  Amazon EC2
-  Amazon EC2 Container Registry
-  Amazon EC2 Container Service
-  Amazon Lightsail
-  Amazon VPC
-  AWS Batch
-  AWS Elastic Beanstalk
-  AWS Lambda
-  Elastic Load Balancing











## Network

-  Amazon CloudFront
-  Amazon Route 53
-  Amazon VPC
-  AWS Direct Connect
-  Elastic Load Balancing





## Storage

-  Amazon EFS
-  Amazon Glacier
-  Amazon S3
-  Snowball
-  AWS Storage Gateway






































## Security & Identity

-  Amazon Inspector
-  AWS Artifact
-  AWS Certificate Manager
-  AWS CloudHSM
-  AWS Directory Service
-  IAM
-  AWS KMS
-  AWS Organizations
-  AWS Shield
-  AWS WAF

## Applications

-  Amazon WorkDocs
-  Amazon WorkMail
-  Amazon AppStream
-  Amazon WorkSpaces

# AWS Platform Services

| Databases  | Analytics  | Application Services  | Management Tools  | Developer Tools  | Mobile Services   | Internet of Things  |
|--|--|---|---|--|---|---|
|  Amazon DynamoDB<br> Amazon ElastiCache<br> Amazon RDS<br> Amazon Redshift |  Amazon Athena<br> Amazon CloudSearch<br> Amazon EMR<br> Amazon ES<br> Amazon Kinesis<br> Amazon QuickSight<br> Amazon Redshift |  Amazon API Gateway<br> Amazon AppStream 2.0<br> Amazon Elastic Transcoder<br> Amazon SWF<br> AWS Step Functions |  Amazon CloudWatch<br> AWS CloudFormation<br> AWS CloudTrail<br> AWS Config<br> AWS Managed Services<br> AWS OpsWorks<br> AWS Service Catalog<br> AWS Trusted Advisor |  AWS CodeBuild<br> AWS CodeCommit<br> AWS CodeDeploy<br> AWS CodePipeline<br> AWS X-Ray |  Amazon API Gateway<br> Amazon Cognito<br> Amazon Mobile Analytics<br> Amazon Pinpoint<br> AWS Device Farm<br> AWS Mobile Hub |  AWS IoT<br> AWS Greengrass |

# AWS Global Infrastructure

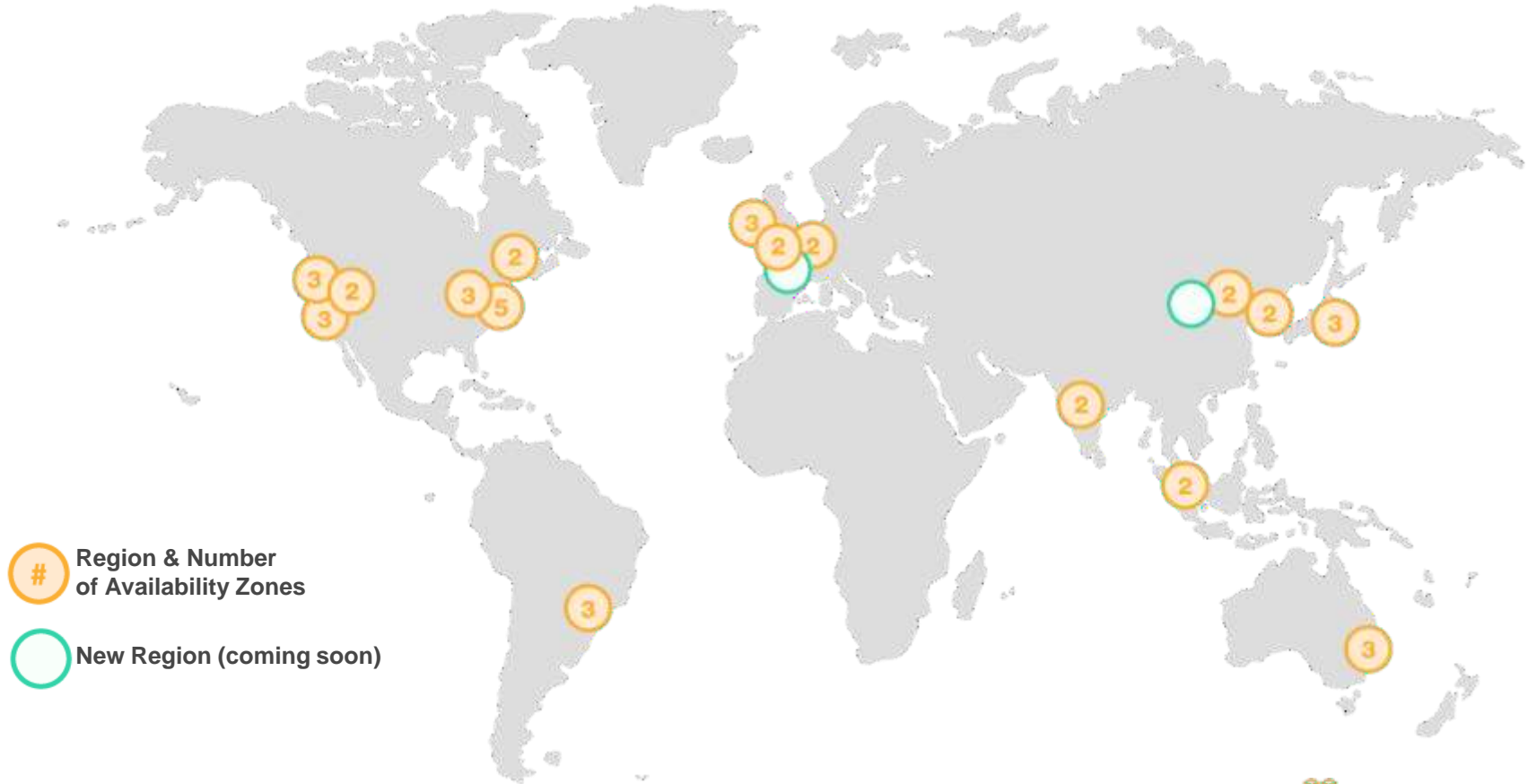
## Regions

- Geographic locations
- Consist of **at least two** Availability Zones

## Availability Zones

- Clusters of data centers
- **Isolated from failures** in other Availability Zones

# AWS Global Infrastructure



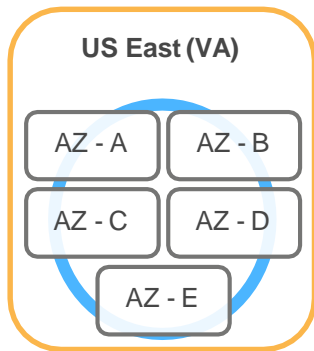
# AWS Global Infrastructure

At least 2 Availability Zones per region.

Examples:

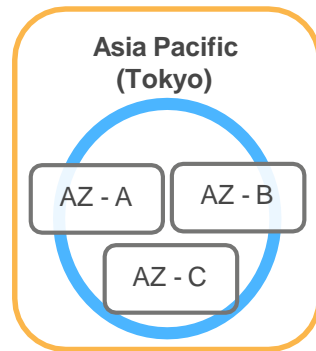
- US East (N. Virginia)

- us-east-1a
- us-east-1b
- us-east-1c
- us-east-1d
- us-east-1e



- Asia Pacific (Tokyo)

- ap-northeast-1a
- ap-northeast-1b
- ap-northeast-1c



*Note: Conceptual drawing only. The number of Availability Zones (AZ) may vary.*



# AWS Global Infrastructure – Edge Locations

- 70\* edge locations
- Local points of presence that support AWS services like:



\*as of March 2017

# **Module 2**

# **AWS Foundational Services**

# Module 2 Layout

- Amazon Elastic Compute Cloud (EC2)
- Amazon Virtual Private Cloud (VPC)
- Amazon Storage Services
  - Amazon Simple Storage Service (S3)
  - Amazon Elastic Block Store (EBS)

# Amazon Elastic Compute Cloud (EC2)

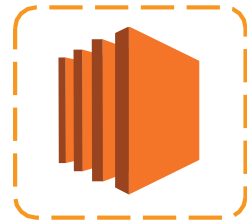
# Amazon Elastic Compute Cloud (EC2)



Amazon  
EC2

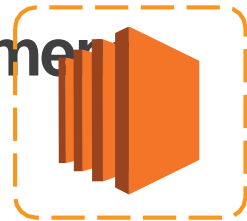
- **Resizable** compute capacity
- Complete control of your computing resources
- **Reduced time required** to obtain and boot new server instances

# Amazon EC2 Facts



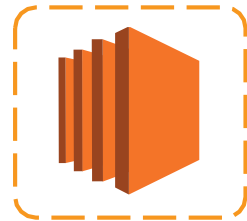
- **Scale capacity** as your computing requirements change
- Pay only for capacity that you actually use
- Choose **Linux** or **Windows**
- Deploy across **AWS Regions** and **Availability Zones** for reliability
- Use **tags** to help manage your Amazon EC2 resources

# Launching an Amazon EC2 Instance via the Management Console



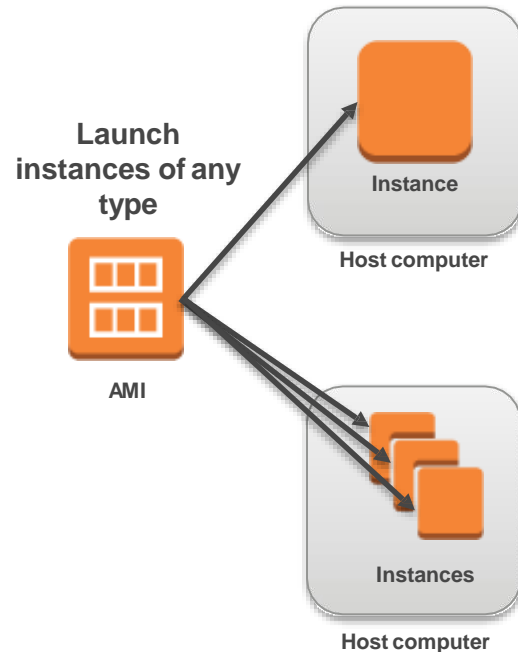
1. **Determine the AWS Region** in which you want to launch the Amazon EC2 instance.
2. **Launch** an Amazon EC2 instance from a pre-configured Amazon Machine Image (AMI).
3. **Choose an instance type** based on CPU, memory, storage, and network requirements.
4. **Configure** network, IP address, security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

# Instances and AMIs



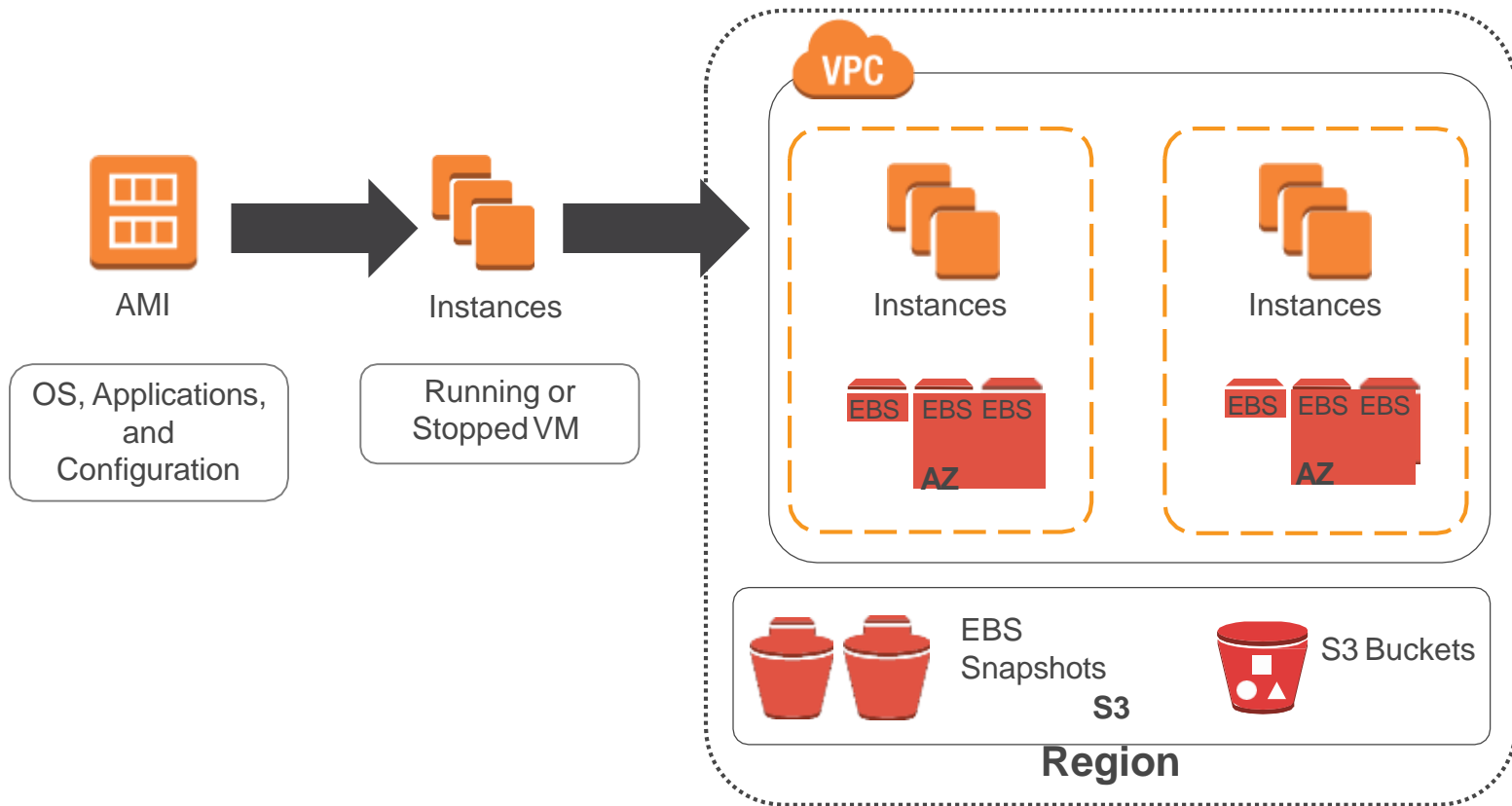
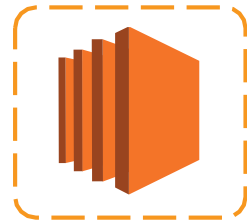
Select an AMI based on:

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

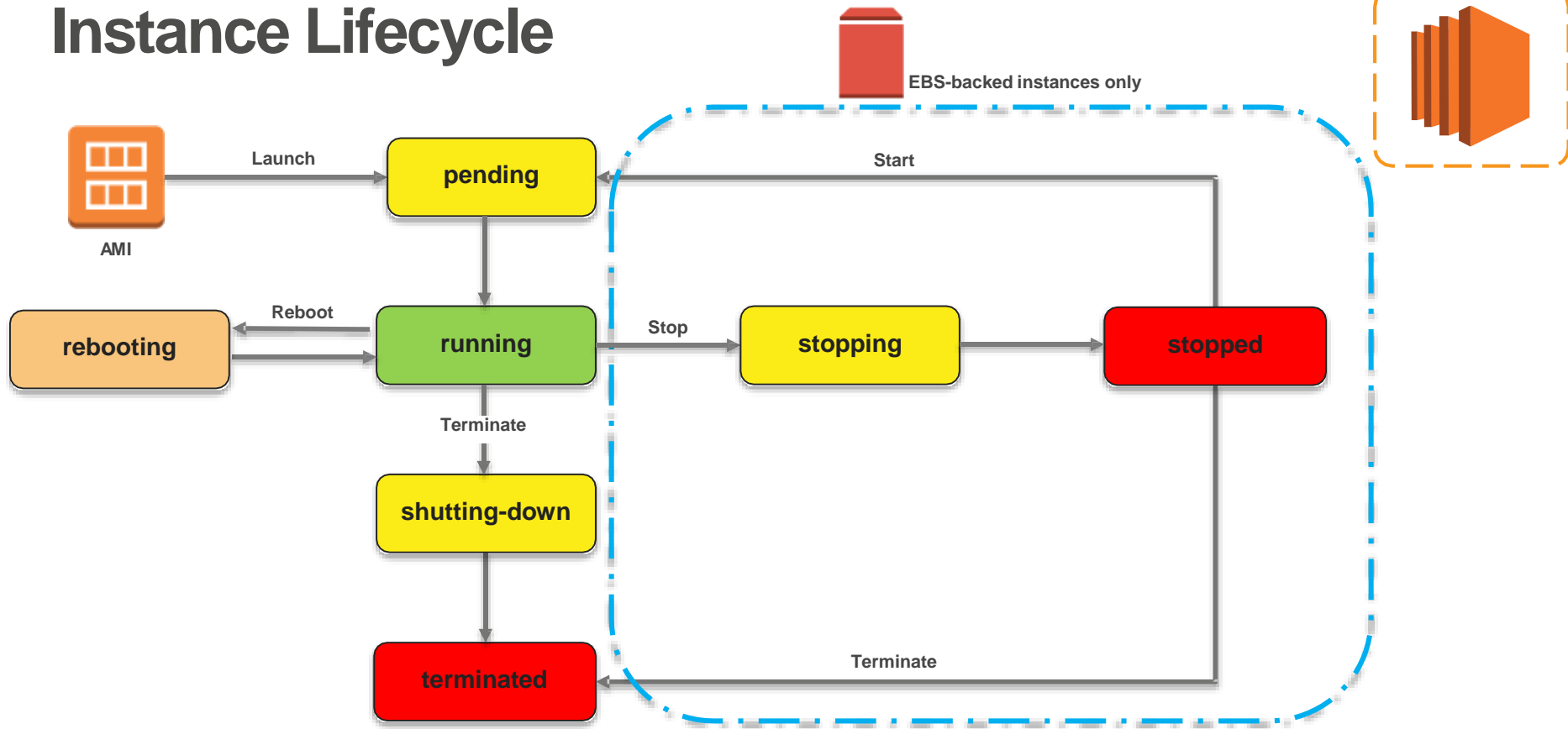




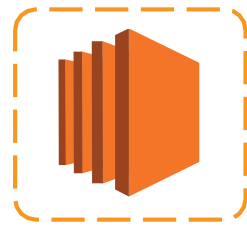
# Amazon EC2 Instances



# Instance Lifecycle



# 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 **2700+** 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>



Training and  
Certification

# Choosing the Right Amazon EC2 Instance



AWS uses Intel® Xeon® processors to provide customers with high performance and value. EC2 instance types are optimized for different use cases, 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

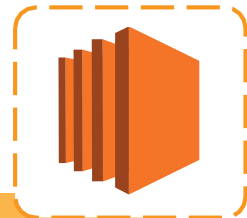
# X1 Instance - Tons of Memory

The X1 instance:

- Features up to 2TB of memory and 100 vCPU.
- Uses Intel E7 v3 Haswell processors.
- Is designed for demanding enterprise workloads, including production installations of SAP HANA, Microsoft SQL Server, Apache Spark, and Presto.

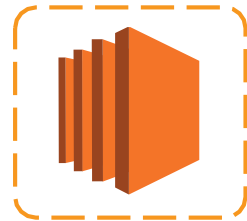


# Current Generation Instances



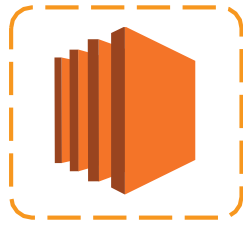
| Instance Family              | Some Use Cases   |
|------------------------------|--|
| General purpose (t2, m4, m3) | <ul style="list-style-type: none"><li>• Low-traffic websites and web applications</li><li>• Small databases and mid-size databases</li></ul> |
| Compute-optimized (c4, c3)   | <ul style="list-style-type: none"><li>• High performance front-end fleets</li><li>• Video-encoding</li></ul>                                 |
| Memory-optimized (r3)        | <ul style="list-style-type: none"><li>• High performance databases</li><li>• Distributed memory caches</li></ul>                             |
| Storage-optimized (i2, d2)   | <ul style="list-style-type: none"><li>• Data warehousing</li><li>• Log or data-processing applications</li></ul>                             |
| GPU instances (g2)           | <ul style="list-style-type: none"><li>• 3D application streaming</li><li>• Machine learning</li></ul>  |

# Instance Metadata



- Is **data** about your **instance**.
- Can be used to **configure or manage** a running instance.

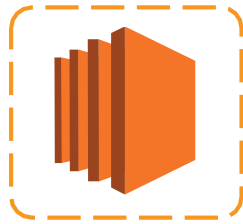
# Instance User Data



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



# User Data Example Linux



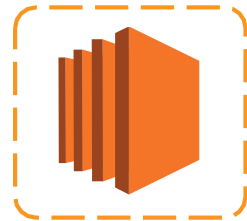
```
#!/bin/sh
```

```
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
```

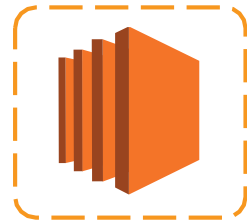
Import the Server Manager module  
for Windows PowerShell.

```
Install-WindowsFeature web-server, web-webserver  
Install-WindowsFeature web-mgmt-tools
```

```
</powershell>
```

Install IIS  
Install Web Management Tools

# Amazon EC2 Purchasing Options



## On-Demand Instances

Pay by the hour.

## Reserved Instances

Purchase, at a significant discount, instances that are always available

1-year to 3-year terms.

## Scheduled Instances

Purchase instances that are always available on the specified recurring schedule, for a one-year term.

## Spot Instances

Bid on unused instances, which can run as long as they are available and your bid is above the Spot price.

## Dedicated Instances

Pay, by the hour, for instances that run on single-tenant hardware.

## Dedicated Hosts

Pay for a physical host that is fully dedicated to running your instances.

# Networking Amazon VPC

# Amazon Virtual Private Cloud (VPC)



Amazon  
VPC

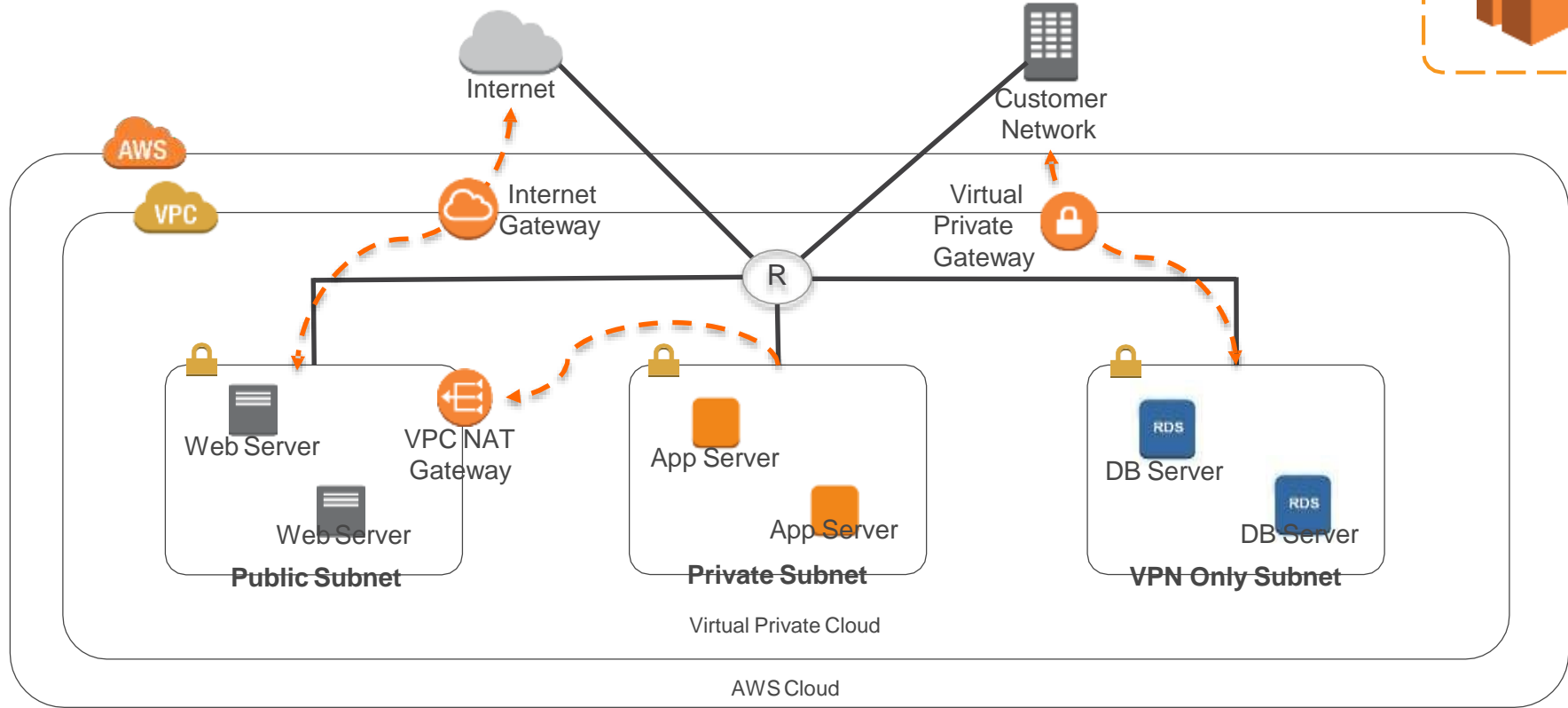
- Provision a **private, isolated virtual network** on the AWS cloud.
- Have complete control over your virtual networking environment.

# VPCs and Subnets



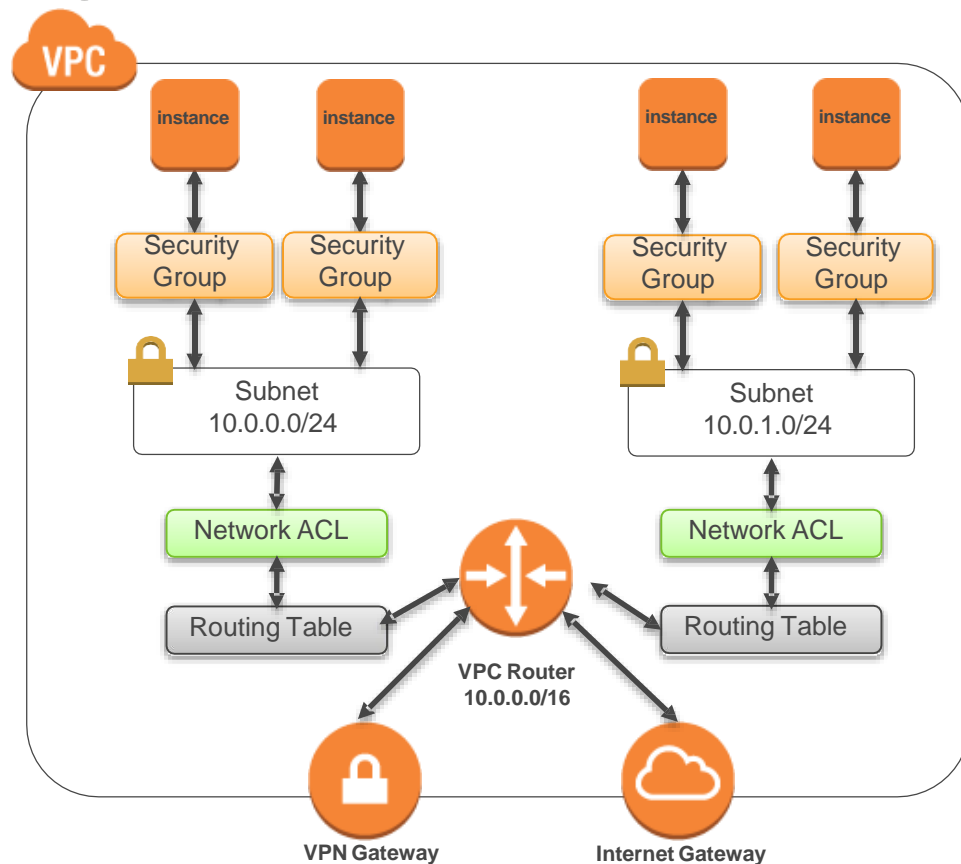
- A **subnet** defines a range of IP addresses in your VPC.
- You can launch AWS resources into a subnet that you select.
- A **private subnet** should be used for resources that won't be accessible over the Internet.
- A **public subnet** should be used for resources that will be accessed over the Internet.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

# Amazon VPC Example



# Security in Your VPC

- Security groups
- Network access control lists (ACLs)
- Key Pairs





# VPN Connections



| VPN Connectivity option   | Description   |
|---------------------------|---|
| AWS Hardware <b>VPN</b>   | You can create an <b>IPsec</b> hardware VPN connection between your VPC and your remote network.  |
| AWS <b>Direct Connect</b> | AWS Direct Connect provides a <b>dedicated private</b> connection from a remote network to your VPC.  |
| AWS <b>VPN</b> CloudHub   | You can create multiple <b>AWS hardware VPN</b> connections via your VPC to enable communications between various remote networks.                  |
| Software <b>VPN</b>       | You can create a VPN connection to your remote network by using an Amazon EC2 instance in your VPC that's running a <b>software VPN appliance</b> . |

# **Storage Services**

## **Amazon S3 and Amazon EBS**

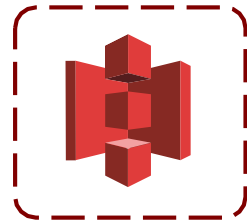
# Amazon Simple Storage Service (S3)



Amazon S3

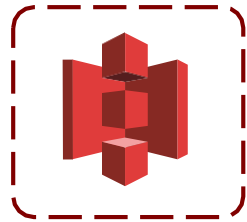
- Storage for the Internet
- Natively online, HTTP access
- Storage that allows you to store and retrieve **any amount of data**, any time, from anywhere on the web
- **Highly scalable**, reliable, fast and durable

# Amazon S3 Facts



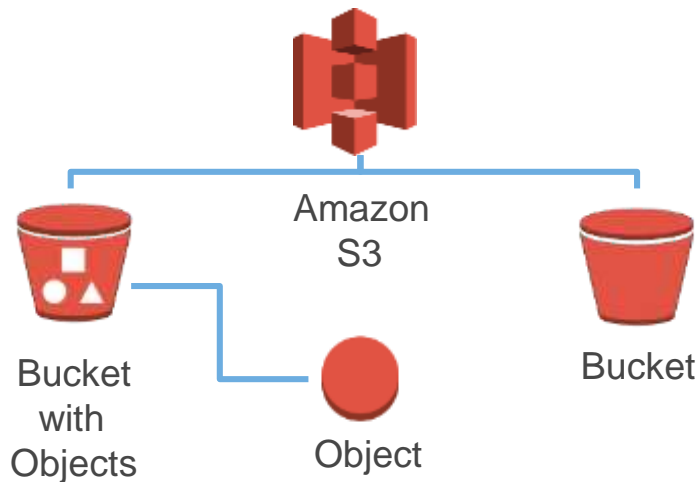
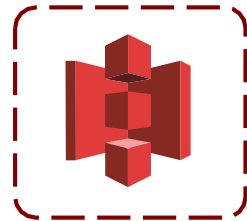
- Can store an **unlimited number of objects** in a bucket
- Objects can be **up to 5 TB**; no bucket size limit
- Designed for **99.999999999%** durability and **99.99%** availability of objects over a given year
- Can use **HTTP/S** endpoints to store and retrieve any amount of data, at any time, from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

# Common Use Scenarios



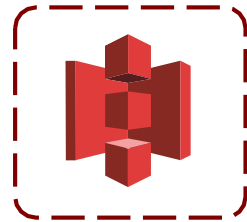
- Storage and backup
- Application file hosting
- Media hosting
- Software delivery
- Store AMIs and snapshots

# 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 can have **up to 100 buckets** in each account
- You can **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/2006-03-01/AmazonS3.html>

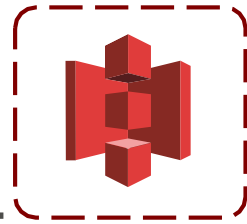
Bucket



Object/Key



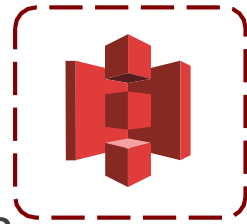
# Amazon S3 Security



- 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** encrypted endpoints.
- You can **encrypt data** using AWS SDKs.



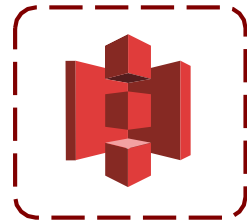
# Amazon S3 Object Lifecycle



**Lifecycle management** defines how Amazon S3 manages objects during their lifetime. Some objects that you store in an Amazon S3 bucket might have a well-defined lifecycle:

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

# Amazon S3 Pricing



- Pay only for what you use
- No minimum fee
- Prices based on location of your Amazon S3 bucket
- Estimate monthly bill using the **AWS Simple Monthly Calculator**
- Pricing is available as:
  - Storage Pricing
  - Request Pricing
  - Data Transfer Pricing: data transferred out of Amazon S3

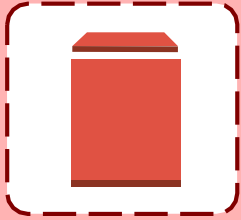


# Amazon Glacier



- Long term low-cost archiving service
- Optimal for infrequently accessed data
- Designed for 99.999999999% durability
- Three to five hours' retrieval time\*
- Less than \$0.004 per GB/month (depending on region)

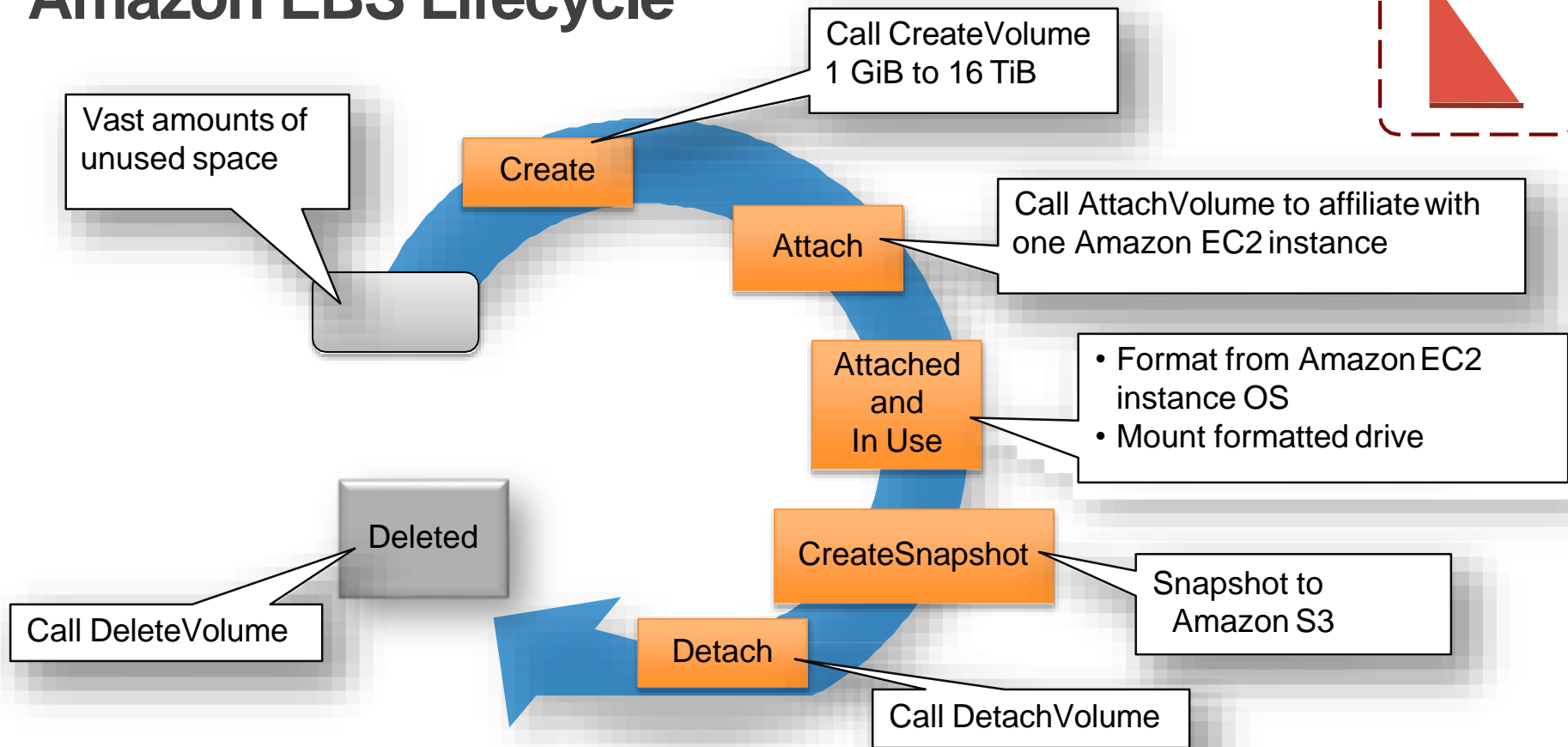
# Amazon Elastic Block Store (EBS)



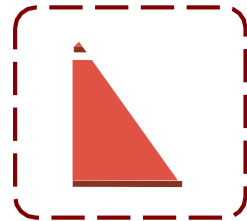
Amazon  
EBS

- **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.

# Amazon EBS Lifecycle

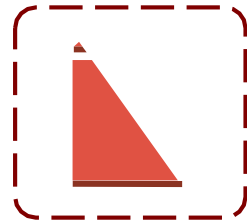


# Amazon EBS Volume Types



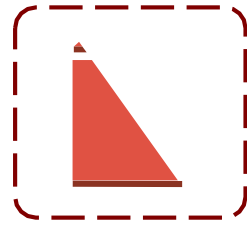
- SSD-backed volumes are
  - Optimized for **transactional** workloads that involve **frequent read/write** operations with **small I/O** size.
  - Dominant in **IOPS** performance.
- HDD-backed volumes are
  - Optimized for **large streaming** workloads.
  - Dominant in **throughput** (measured in MiB/s).

# 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.

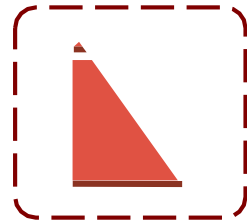
# Amazon EBS Use Cases



- **OS:** Use for boot/root volume, secondary volumes
- **Databases:** Scales with your performance needs
- **Enterprise applications:** Provides reliable block storage to run mission-critical applications
- **Business continuity:** Minimize data loss and recovery time by regularly backing up using EBS Snapshots
- **Applications:** Install and persist any application



# Amazon EBS Pricing

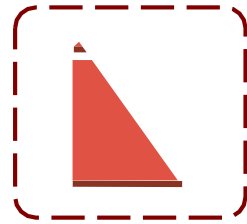


Pay for what you provision:

- Pricing based on region
- Review Pricing Calculator online
- Pricing is available as:
  - Storage
  - IOPS

*\* Check Amazon EBS Pricing page for current pricing for all regions.*

# Amazon EBS Scope



**Amazon EBS volumes are in a single Availability Zone**



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

# Amazon EC2 Instance Storage

- Is local, complimentary **direct attached block storage**.
- Includes availability, number of disks, and size **based on EC2 instance type**.
- Is optimized for **up to 365,000 Read IOPS** and 315,000 First Write IOPS.
- Is SSD or magnetic.
- 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 alive.
- Storage is **ephemeral**.

# **Module 3**

# **Security, Identity, and Access Management**

# AWS Shared Responsibility Model

Customers

Customer Applications & Content

Platform, Applications, Identity, and Access Management

Operating System, Network, and Firewall Configuration

Client-side Data  
Encryption

Server-side Data  
Encryption

Network Traffic  
Protection

Customers are responsible for security **IN** the cloud

AWS Foundation Services

Compute

Storage

Database

Networking

AWS Global  
Infrastructure

Availability Zones

Regions

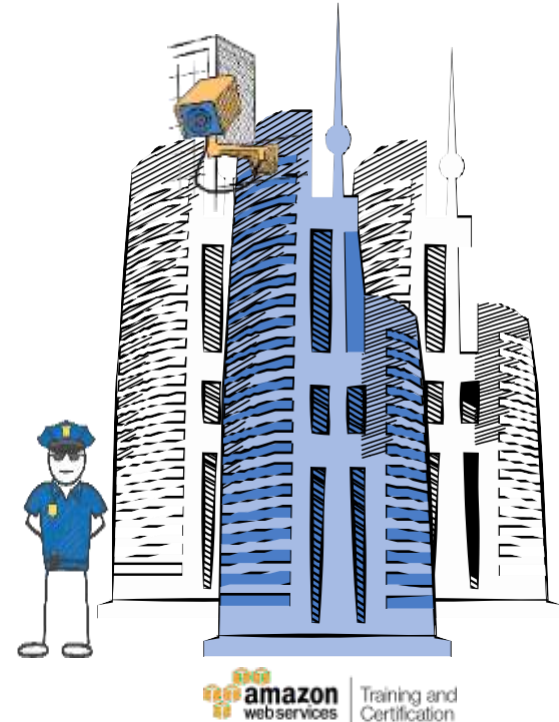
Edge Locations

AWS is responsible for the security **OF** the cloud



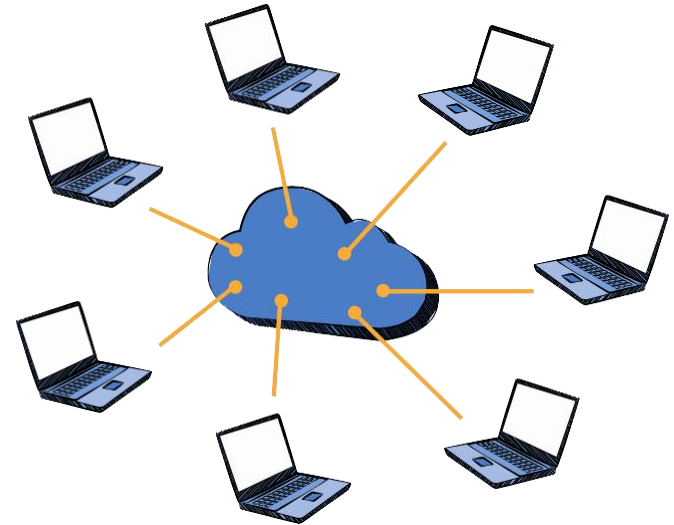
# Physical Security

- 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





# Certifications and Accreditations



ISO 9001, ISO 27001, ISO 27017, ISO 27018, IRAP (Australia), MLPS Level 3 (China), MTCS Tier 3 Certification (Singapore) and more ...

# SSL Endpoints

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

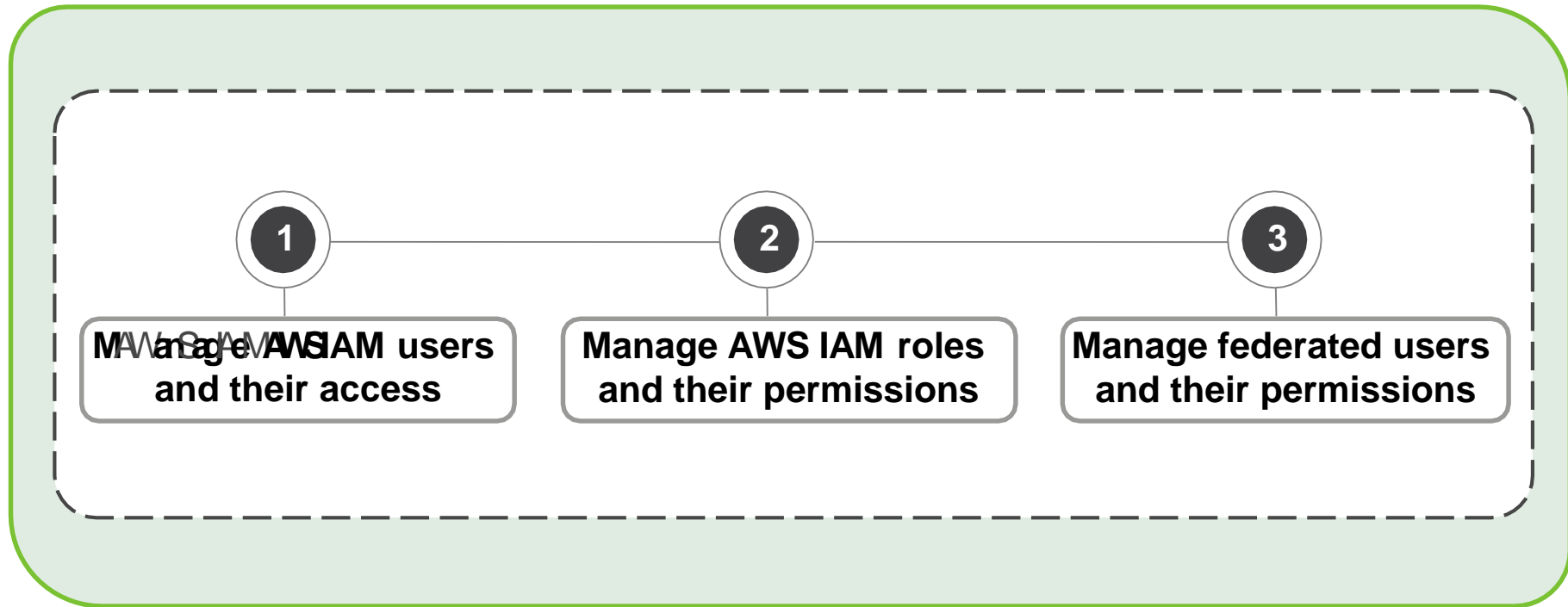
# Security Groups

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

# Amazon Virtual Private Cloud (VPC)

| SSL Endpoints  | Security Groups   | VPC  |
|--|---|--|
| <b>Secure Transmission</b><br><br>Use secure endpoints to establish secure communication sessions (HTTPS). | <b>Instance Firewalls</b><br><br>Use security groups to configure firewall rules for instances. | <b>Network Control</b><br><br>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



- Authentication
- AWS Management Console
  - User Name and Password



IAM User

**Account:**

**User Name:**

**Password:**

MFA users, enter your code on the next screen.

**Sign In**



# AWS IAM Authentication



- 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

```
~$ aws configure
AWS Access Key ID [*****Q22A]:
AWS Secret Access Key [*****4m8i]:
Default region name [ap-southeast-1]:
Default output format [json]:
```

## AWS SDK & API



Java

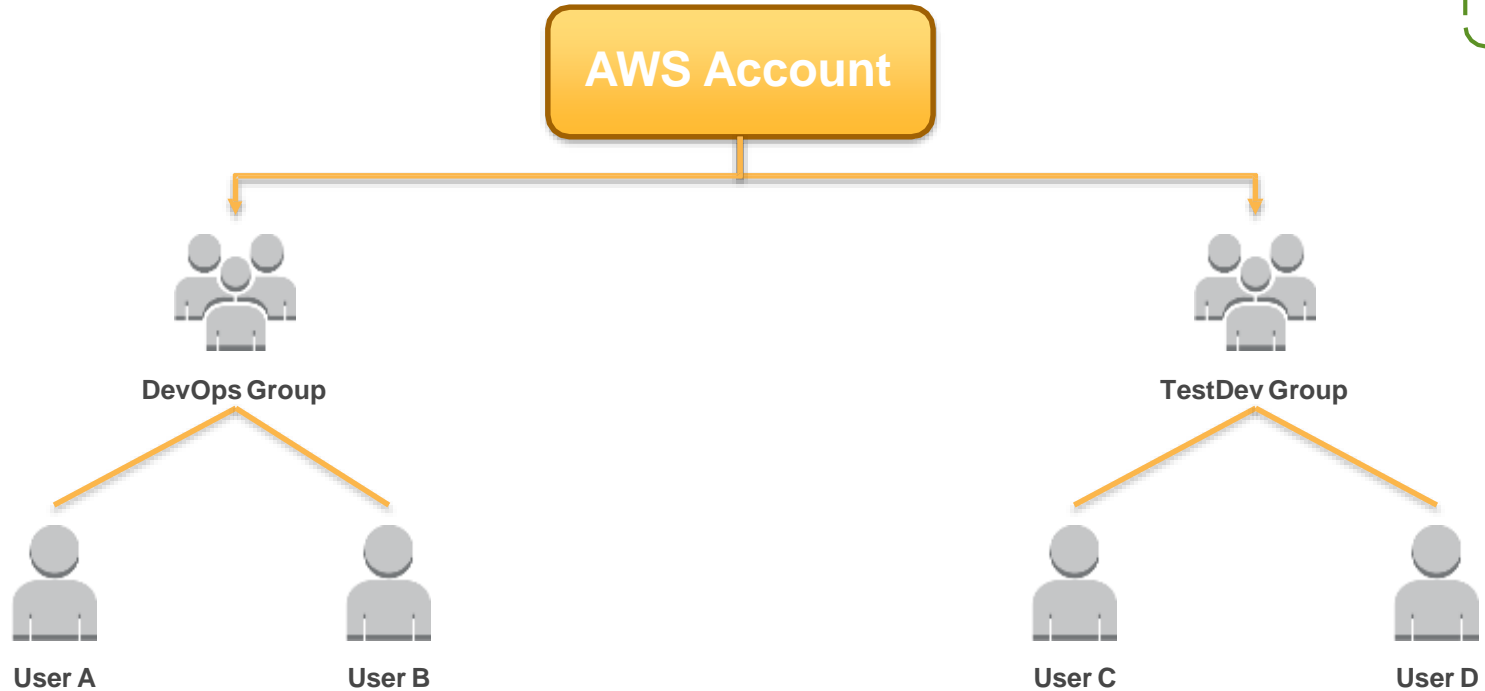


Python



.NET

# AWS IAM User Management - Groups





# AWS IAM Authorization

## Authorization

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



IAM User



IAM Group



IAM Roles



# 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/*"
    }
  ]
}
```

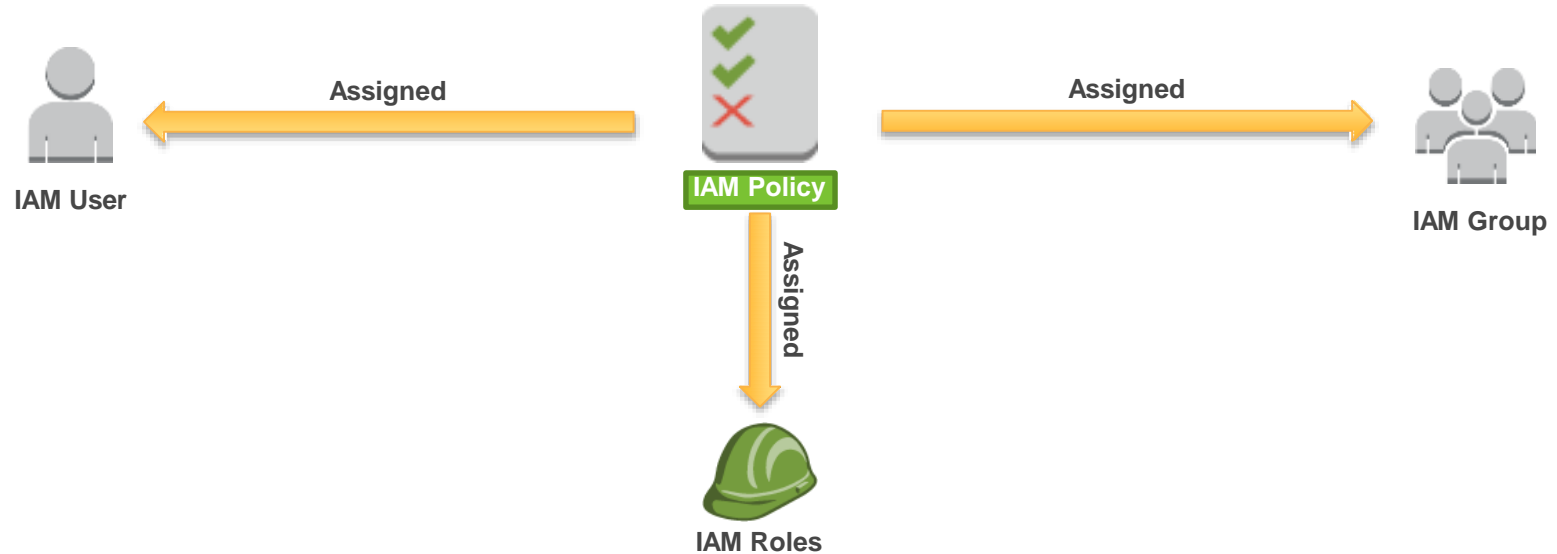


IAM Policy

# AWS IAM Policy Assignment



# AWS IAM Policy Assignment



# AWS IAM Roles

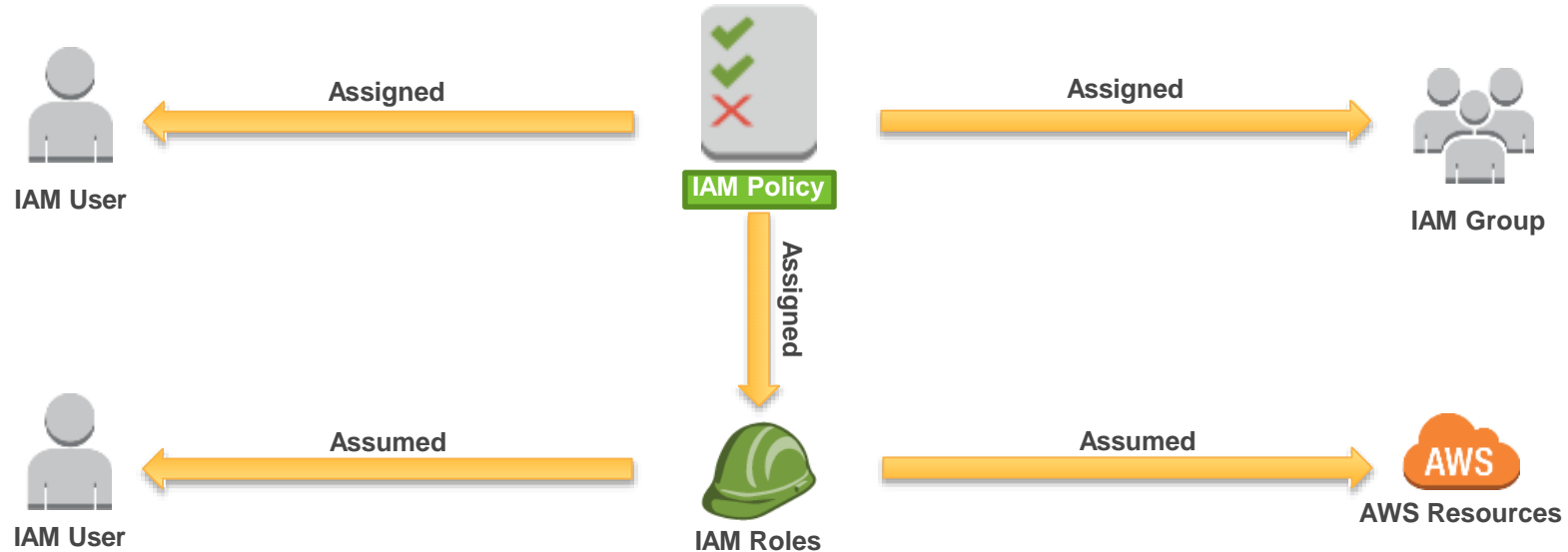


- An IAM role uses a policy.
- An IAM role has no associated credentials.
- IAM users, applications, and services may assume IAM roles.



**IAM Roles**

# AWS IAM Policy Assignment



# 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

Amazon EC2



1

Create Instance

Select IAM Role

2

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: ☐ On-Demand Instances ☐ Request Spot Instances

Network:  (172.31.0.0/16) (default) Create new VPC

Subnet:  Create new subnet

Auto-assign Public IP:

Domain join directory:  Create new directory

IAM role:  Create new IAM role

Shutdown behavior:

Enable termination protection: ☐

Monitoring: ☐ Enable CloudWatch detailed monitoring. Additional charges apply.

Tenancy:  Additional charges will apply for dedicated tenancy.

3



App &



EC2 MetaData Service  
<http://169.254.169.254/latest/meta-data/iam/security-credentials/rolename>

Amazon S3



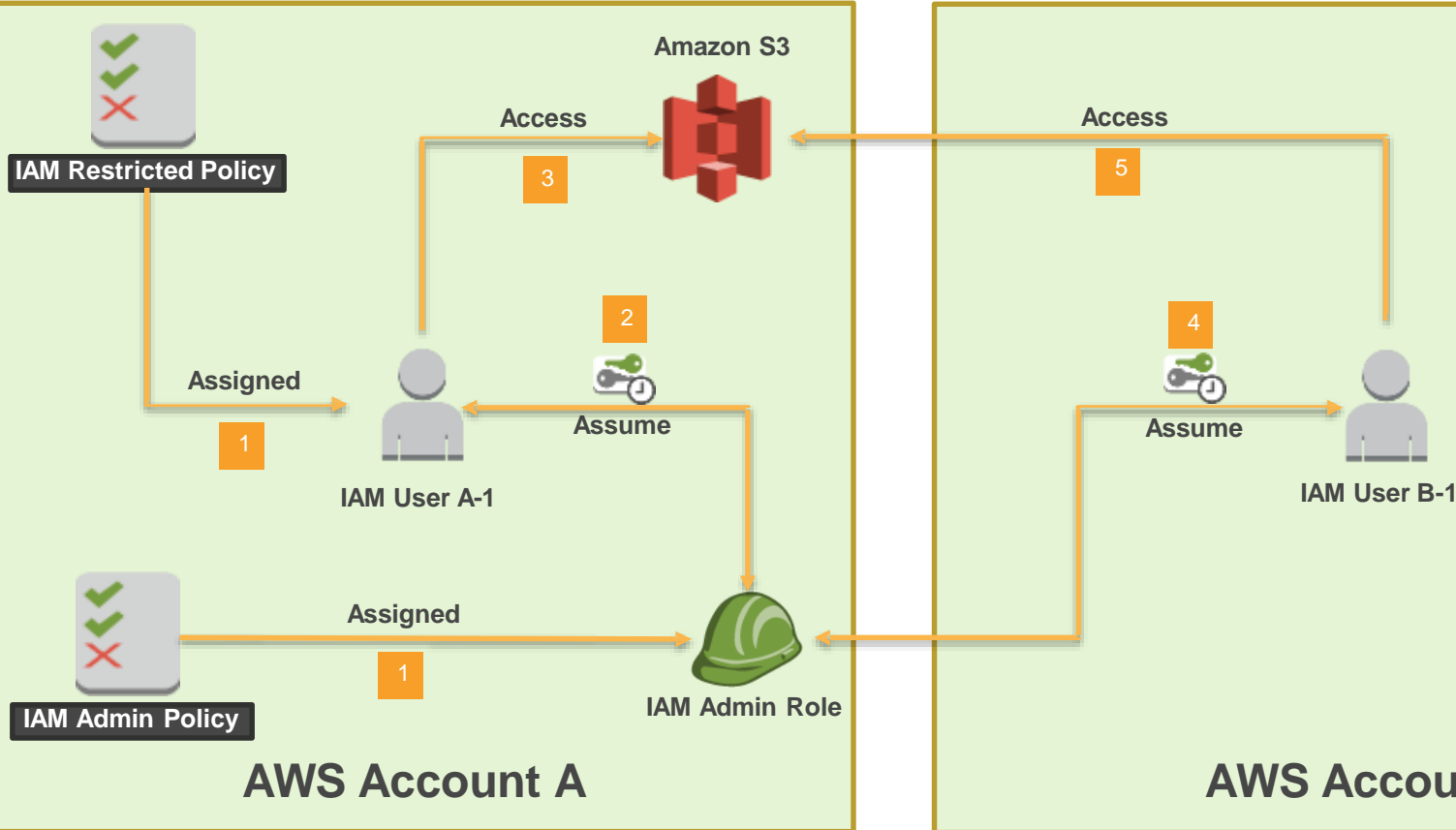
Application interacts with S3

4





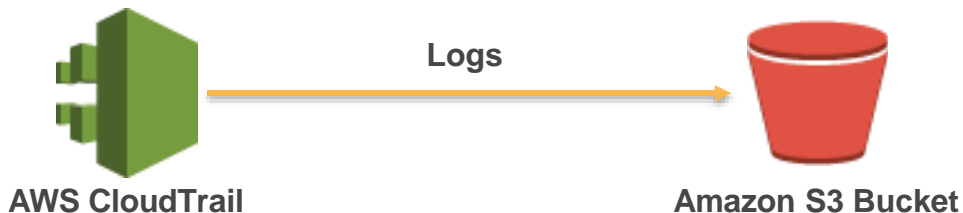
# AWS IAM Roles – Assume Role



# AWS CloudTrail



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



# Module 4: Databases

# SQL and NoSQL Databases

|              | SQL              | NoSQL                              |
|--------------|------------------|------------------------------------|
| Data Storage | Rows and Columns | Key-Value                          |
| Schemas      | Fixed            | Dynamic                            |
| Querying     | Using SQL        | Focused on collection of documents |
| Scalability  | Vertical         | Horizontal                         |

## SQL

| ISBN          | Title                    | Author       | Format    |
|---------------|--------------------------|--------------|-----------|
| 9182932465265 | Cloud Computing Concepts | Wilson, Joe  | Paperback |
| 3142536475869 | The Database Guru        | Gomez, Maria | eBook     |

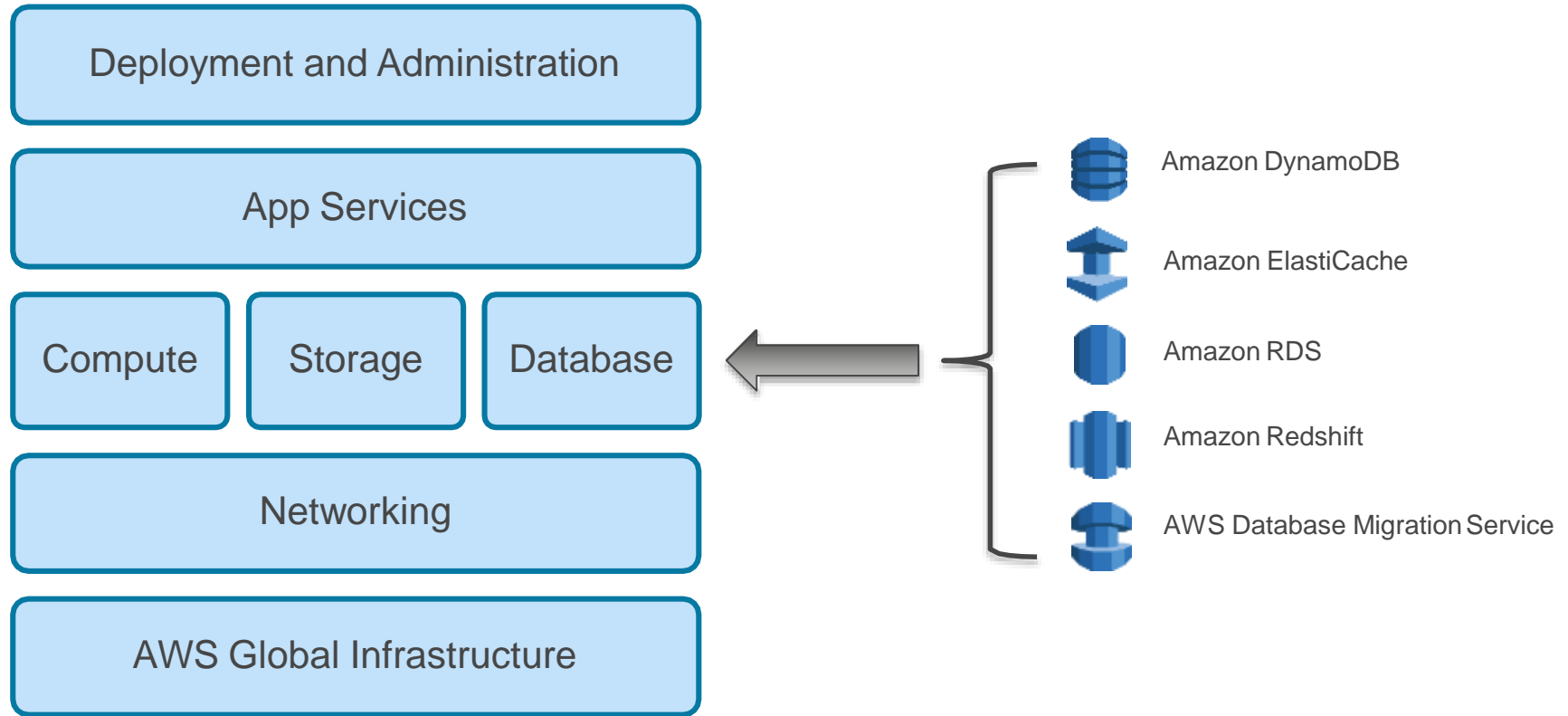
## NoSQL

```
{  
  ISBN: 9182932465265,  
  Title: "Cloud Computing Concepts",  
  Author: "Wilson, Joe",  
  Format: "Paperback"  
}
```

# 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

# AWS Managed Database Services



# 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

# 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





# 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.

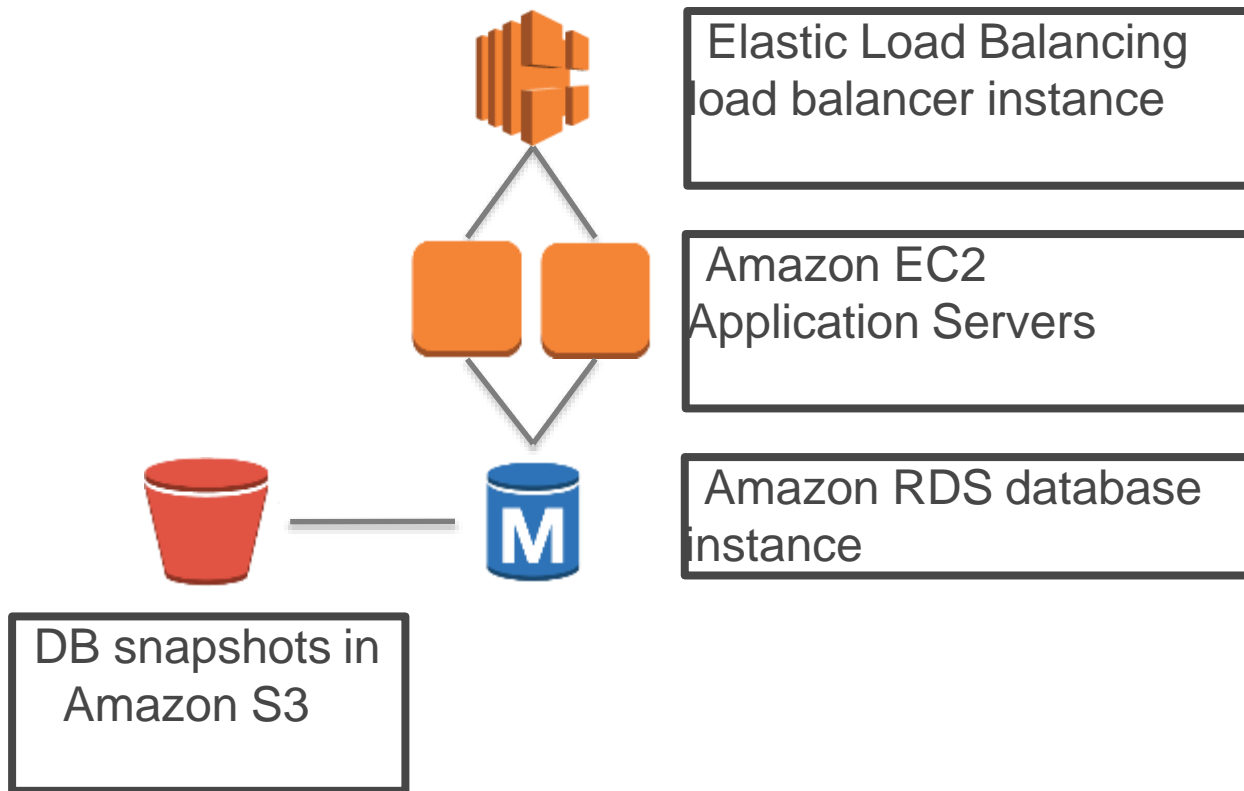


# Amazon RDS Security



- Run your DB instance in an **Amazon VPC**.
- 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

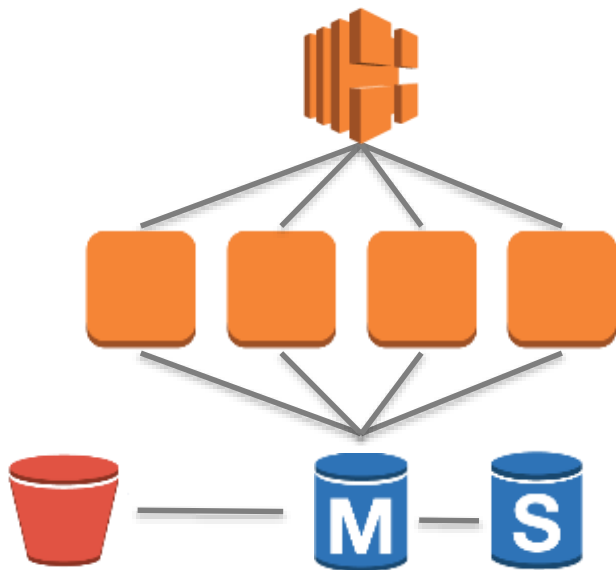


# Multi-AZ RDS Deployment



- 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



Elastic Load Balancing  
load balancer instance

Application, in Amazon  
EC2 instances

Amazon RDS database instances:  
Master and Multi-AZ standby

DB snapshots in  
Amazon S3

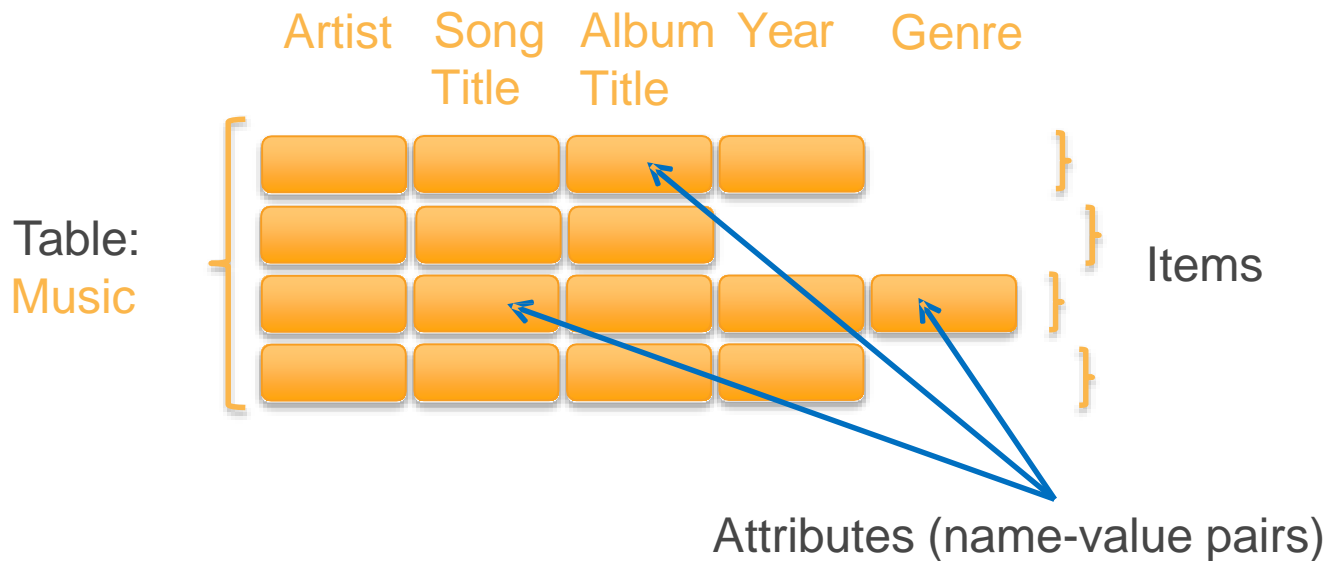
# Amazon DynamoDB



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



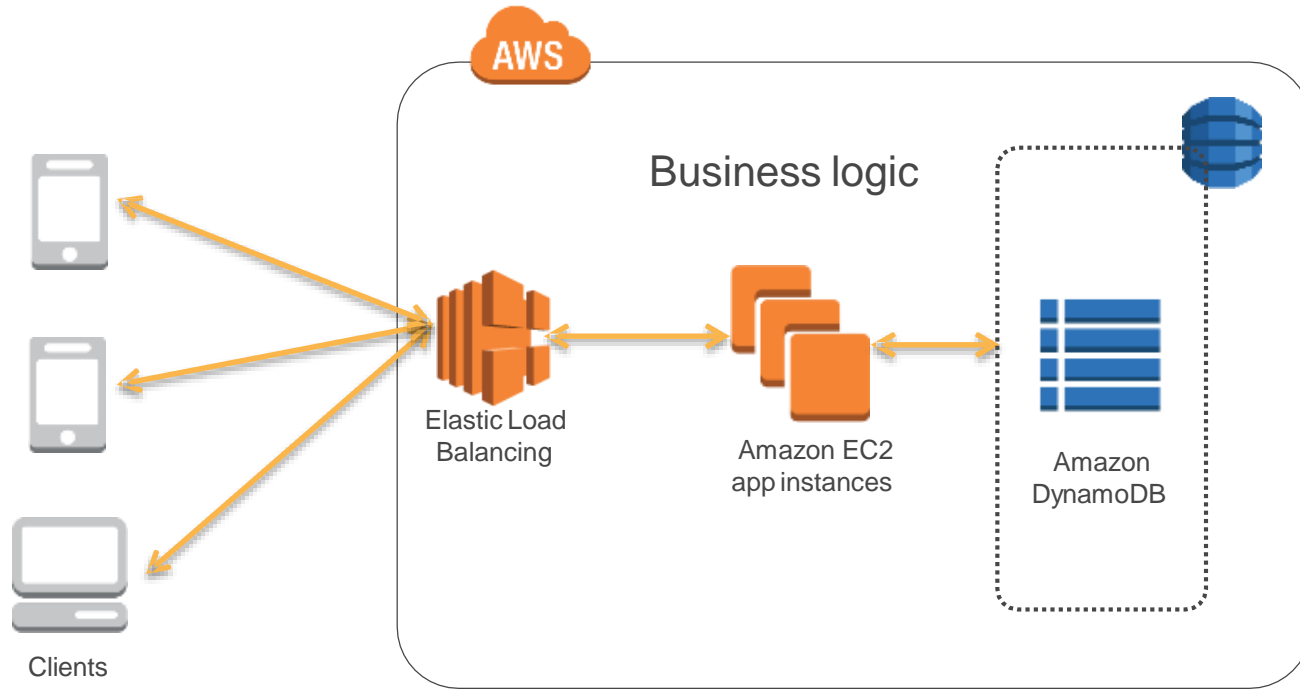


# Provisioned Throughput






- You specify how much **provisioned throughput capacity** you need for reads and writes.
- Amazon DynamoDB allocates the necessary machine resources to meet your needs.

# Simple Application Architecture



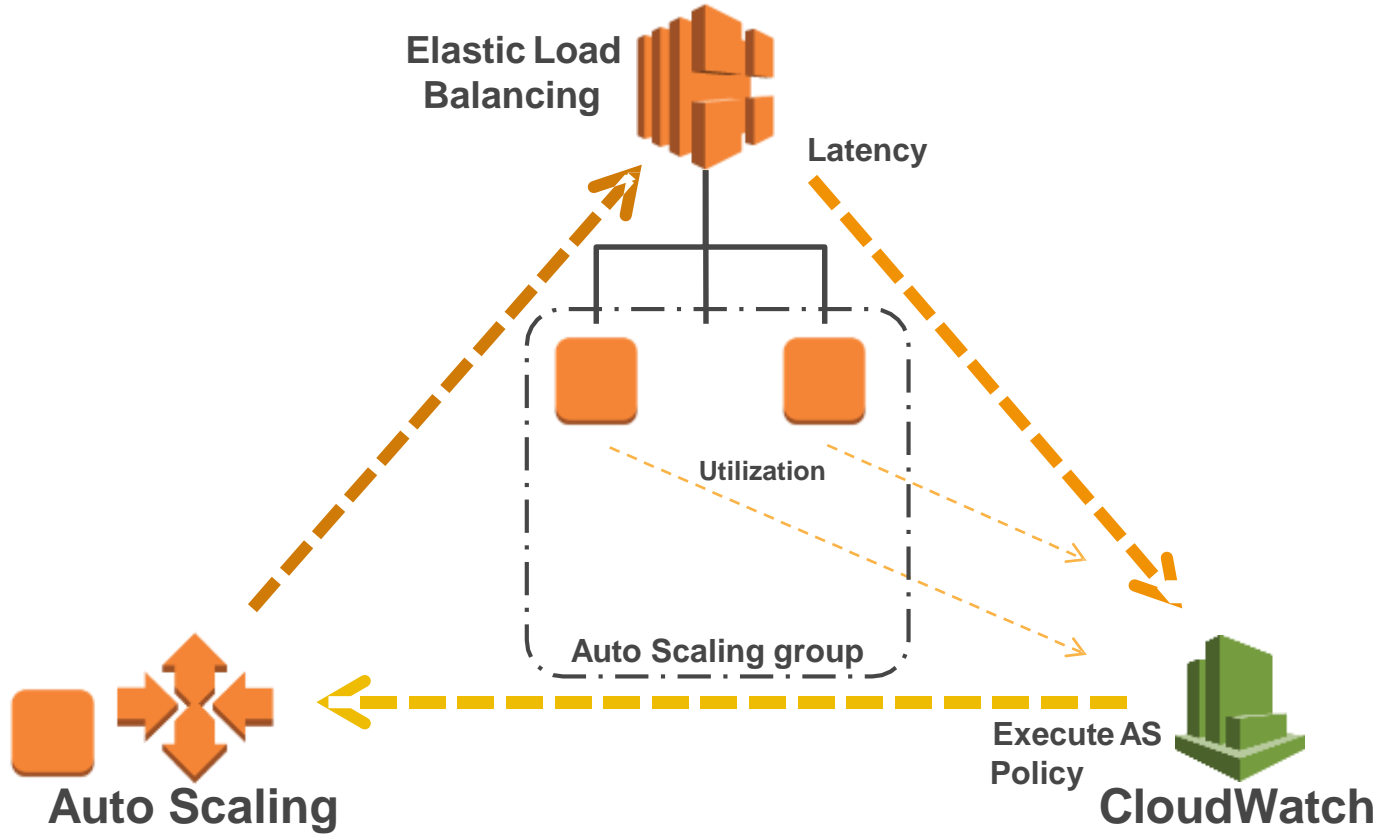
# Database Considerations

| If You Need   | Consider Using  |
|---|---|
| A relational database service with minimal administration | <b>Amazon RDS</b> <ul style="list-style-type: none"><li>• Choice of Amazon Aurora, MySQL, MariaDB, Microsoft SQL Server, Oracle, or PostgreSQL database engines</li><li>• Scale compute and storage</li><li>• Multi-AZ availability</li></ul>  |
| A fast, highly scalable NoSQL database service            | <b>Amazon DynamoDB</b> <ul style="list-style-type: none"><li>• Extremely fast performance</li><li>• Seamless scalability and reliability</li><li>• Low cost</li></ul>    |
| A database you can manage on your own                     | Your choice of <b>AMIs</b> on Amazon EC2 and Amazon EBS that provide scale compute and storage, complete control over instances, and more.   |

# **Module 5**

# **AWS Elasticity and Management Tools**

# Triad of Services



# Elastic Load Balancing



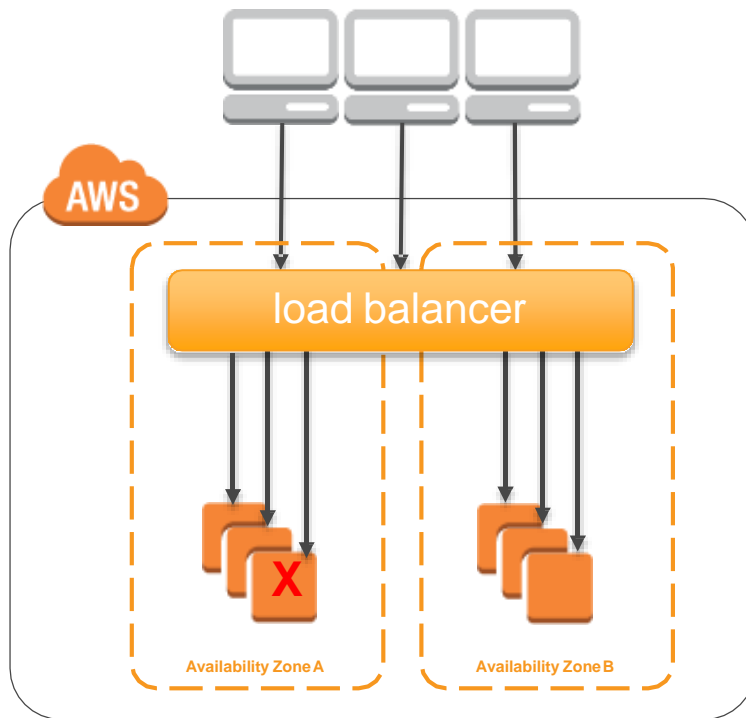
Elastic Load  
Balancing

- **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

# Classic Load Balancer - How It Works



Register  
instances with  
your load  
balancer.



# Amazon CloudWatch



Amazon  
CloudWatch

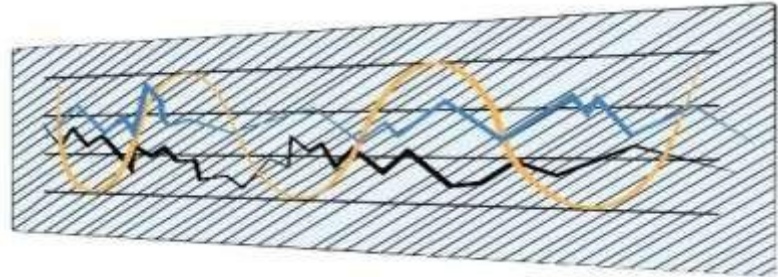
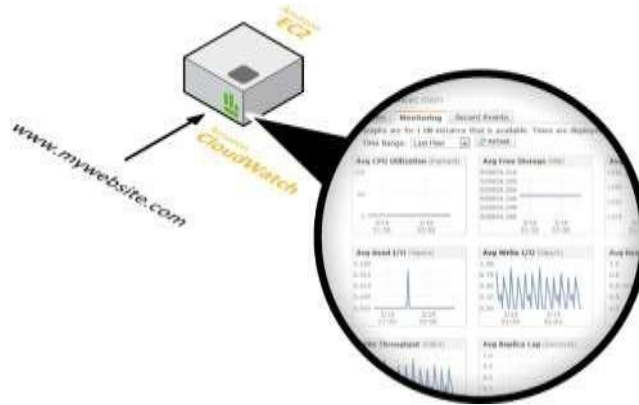
- A **monitoring service** for AWS cloud resources and the applications you run on AWS
- **Visibility into** resource utilization, operational performance, and overall demand patterns
- **Custom application-specific** metrics of your own
- **Accessible** via AWS Management Console, APIs, SDK, or CLI



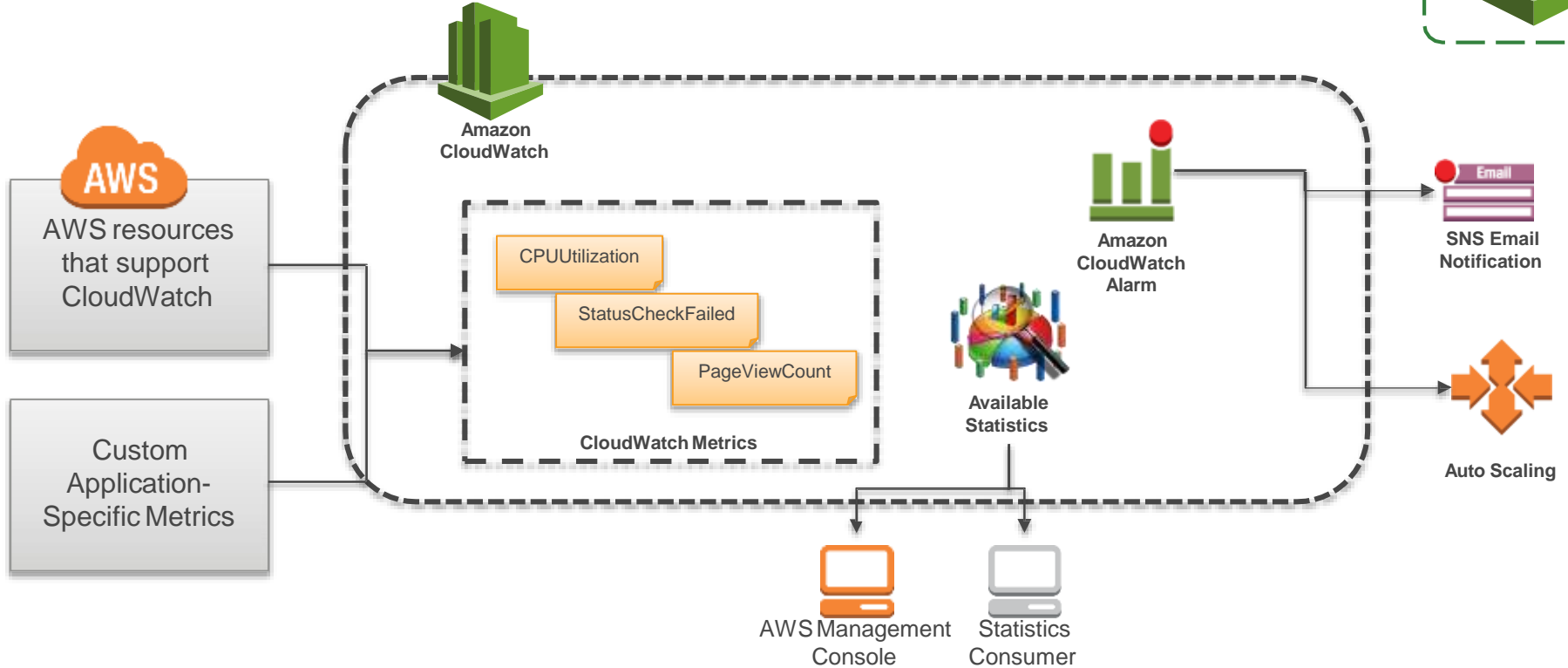
# Amazon CloudWatch Facts



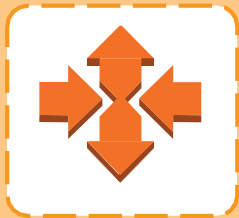
- Monitor other AWS resources
  - View graphics and statistics
- Set Alarms



# Amazon CloudWatch Architecture



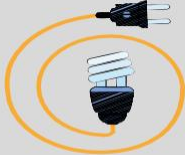
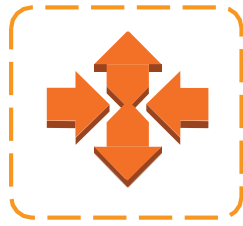
# Auto Scaling



Auto  
Scaling

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

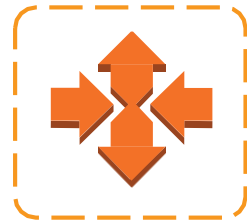
# Auto Scaling Benefits



**Better  
Availability**



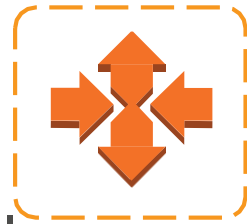
# Launch Configurations



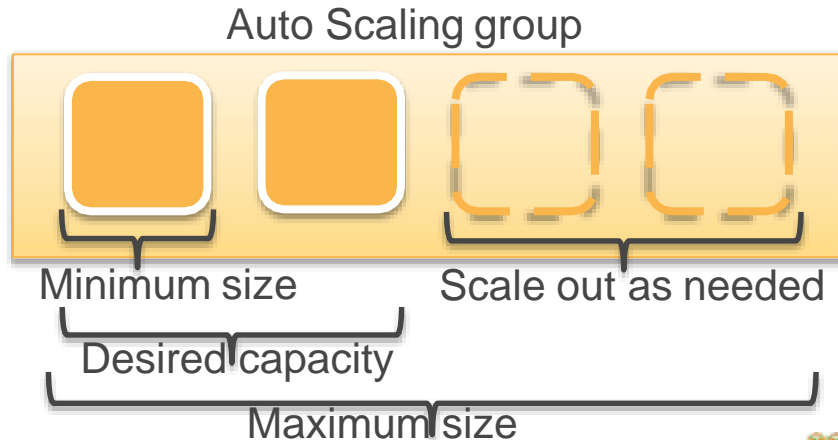
- A **launch configuration** is a template that an Auto Scaling group uses to launch EC2 instances.
- When you create a launch configuration, you can specify:
  - AMI ID
  - Instance type
  - Key pair
  - Security groups
  - Block device mapping
  - User data



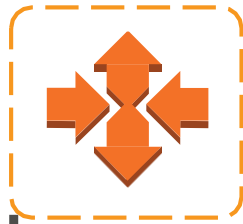
# Auto Scaling Groups



- 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.

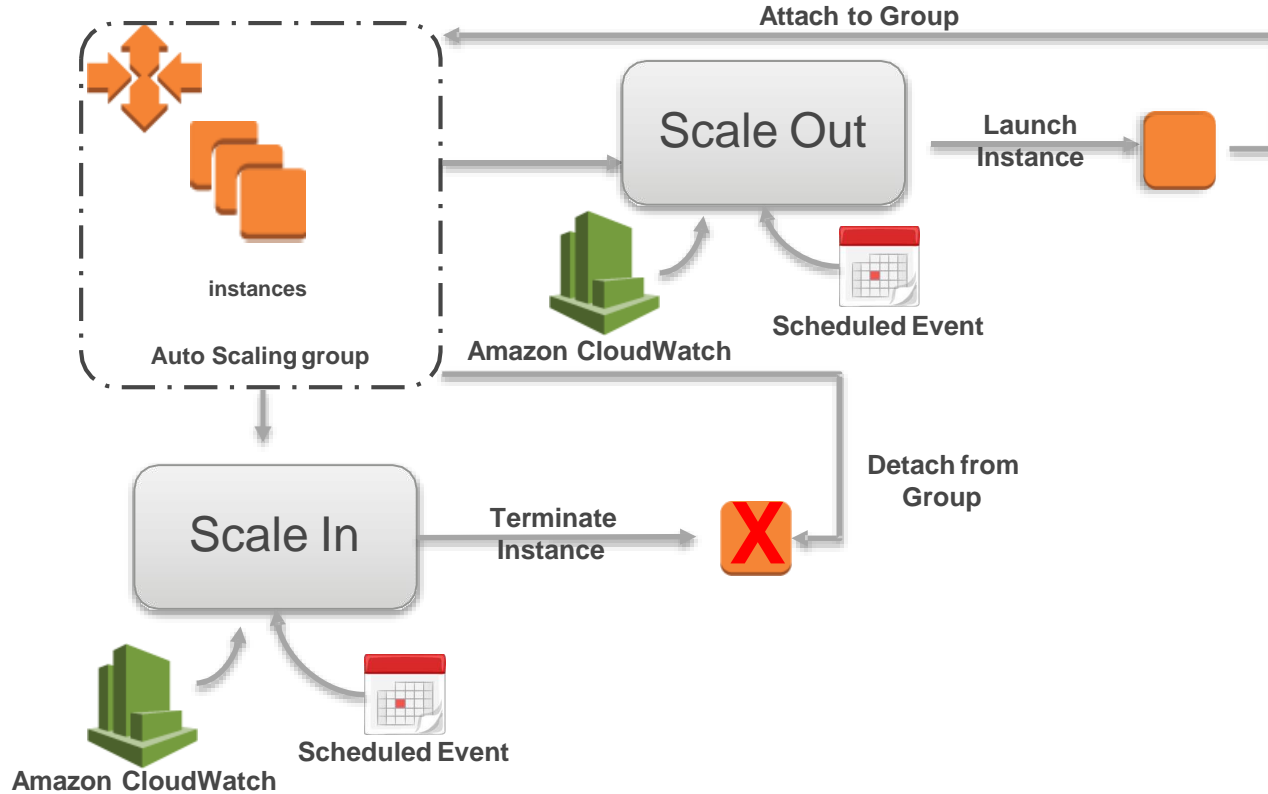
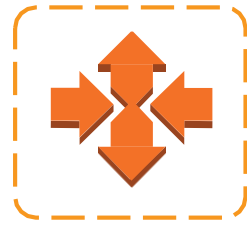


# Dynamic Scaling



- You can create a scaling policy that uses **CloudWatch alarms** to determine:
  - When your Auto Scaling group should **scale out**.
  - When your Auto Scaling group should **scale in**.
- You can use alarms to monitor:
  - Any of the metrics that AWS services send to Amazon CloudWatch.
  - Your own **custom metrics**.

# Auto Scaling Basic Lifecycle





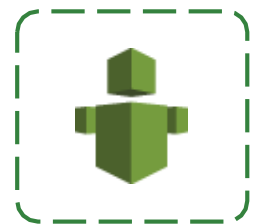
# AWS Trusted Advisor



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.**

# Cost Optimization



- Amazon EC2 Reserved Instance Optimization
- Low-utilization Amazon EC2 Instances
- Idle load balancers
- Underutilized Amazon EBS volumes
- Unassociated Elastic IP addresses
- Amazon RDS idle DB instances

## Cost Optimization



2  4 

0 

0 excluded items

# Security



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

Security



4  2 

3 

1 excluded items

# Fault Tolerance



- Amazon EBS Snapshots
- Load balancer optimization
- Auto Scaling Group Resources
- Amazon RDS Multi-AZ
- Amazon Route 53 name server delegations
- ELB connection draining

## Fault Tolerance

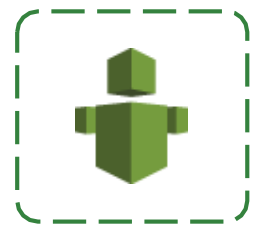


9 ✓ 2 ⚠

2 ⚠

1 excluded items

# Performance Improvement



- High-utilization Amazon EC2 instances
- Service limits
- Large number of rules in EC2 security group
- Over-utilized Amazon EBS magnetic volumes
- Amazon EC2 to EBS throughput optimization
- Amazon CloudFront alternate domain names

Performance



8  0 

0 

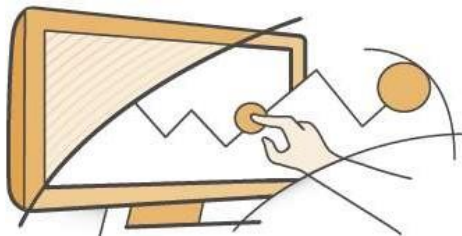
0 excluded items

# Module 6

## Course Wrap-Up

# Expand Your Cloud Skills with AWS

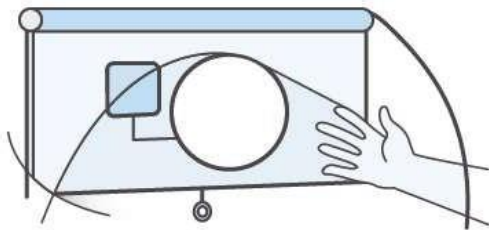
## Online videos and labs



Start working with an AWS service in minutes with free online instructional videos and labs

[aws.amazon.com/training/self-paced-labs](https://aws.amazon.com/training/self-paced-labs)

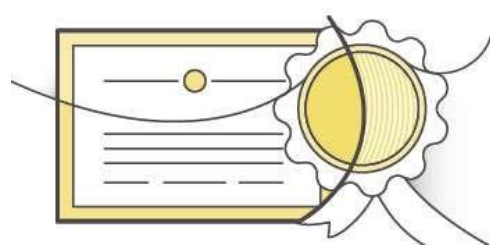
## Instructor-led courses



Learn how to design, deploy, and operate highly available, cost-effective, and secure applications on AWS

[aws.amazon.com/training](https://aws.amazon.com/training)

## Certification



Validate your proven technical expertise with the AWS platform and gain recognition for your skills

[aws.amazon.com/certification](https://aws.amazon.com/certification)

# Self-Paced Labs

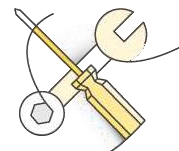
- Learn an individual [AWS Service topic](#)
- [Follow a Learning Quest by AWS Service Area or Use Case](#)
- Practice working with AWS as you [prepare for an exam](#)



For more information, see [aws.amazon.com/training/self-paced-labs/](https://aws.amazon.com/training/self-paced-labs/).



# AWS ILT Training Courses



## Introductory courses

### AWS Technical Essentials

1 day

## Intermediate courses

### Architecting on AWS

3 days

### Developing on AWS

3 days

### Systems Operations on AWS

3 days

## Advanced courses

### Advanced Architecting on AWS

3 days

### DevOps Engineering on AWS

3 days

### Security Operations on AWS

3 days

## Specialty courses

### Migrating to AWS

2 days

### Big Data on AWS

3 days

### Data Warehousing on AWS

3 days

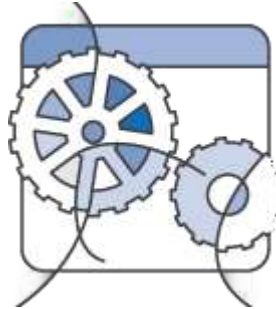
<https://aws.amazon.com/training/>

# AWS Certification



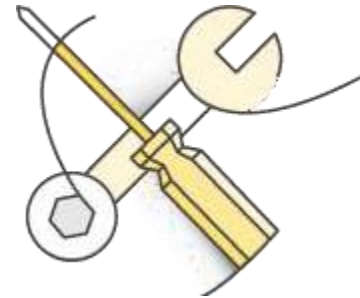
AWS Certified Solutions  
Architect - Associate

AWS Certified Solutions  
Architect - Professional



AWS Certified  
Developer - Associate

AWS Certified DevOps Engineer - Professional



AWS Certified SysOps  
Administrator- Associate

For more information, see [aws.amazon.com/certification](https://aws.amazon.com/certification).

# Preparing for AWS Certification

For resources to help you prepare for the certification exam, see

[aws.amazon.com/certification](https://aws.amazon.com/certification).

**Exam Guides &  
Sample Questions**

**AWS-Authored Study Guide**

**Self-Paced Labs on qwikLABS**

**AWS Technical Training**

**AWS Whitepapers &  
FAQs**

**AWS Documentation &  
Reference Architectures**

**Practice Exams**

# AWS Support

# Support Comparison

|   | Enterprise  | Business   | Developer                             | Basic                                |
|---|---|--|---------------------------------------|--------------------------------------|
| Customer Service 24x7x365                         | ✓   | ✓  | ✓                                     | ✓                                    |
| Support Forums                                    | ✓   | ✓  | ✓                                     | ✓                                    |
| Documentation, White Papers, Best Practice Guides | ✓   | ✓  | ✓                                     | ✓                                    |
| AWS Trusted Advisor                               | Full Checks   | Full Checks  | Basic Checks                          | Basic Checks                         |
| Access to Technical Support                       | Phone, chat, email, live screen sharing, TAM(24/7)  | Phone, chat, email, live screen sharing                                    | Email (local business hours)          | Support for Health Checks            |
| Primary Case Handling                             | Sr. Cloud Support Engineer  | Cloud Support Engineer   | Cloud Support Associate               | Technical Customer Service Associate |
| Users who can create Technical Support cases      | Unlimited (IAM supported)   | Unlimited (IAM supported)  | 1 (account credentials only)          |                                      |
| Case Severity/Response Times                      | Critical: < 15 minutes<br>Urgent: < 1 hour<br>High: < 4 hours<br>Normal: < 12 hours<br>Low: < 24hours | Urgent: < 1 hour<br>High: < 4hours<br>Normal: < 12 hours<br>Low: < 24hours | Normal: < 12 hours<br>Low: < 24 hours |                                      |
| Architecture Support                              | Application Architecture  | Use case guidance  | Building blocks                       |                                      |
| Best Practice Guidance                            | ✓   | ✓  | ✓                                     |                                      |
| Client-Side Diagnostic Tools                      | ✓   | ✓  | ✓                                     |                                      |
| AWS Support API                                   | ✓   | ✓  |                                       |                                      |
| Third-Party Software Support                      | ✓   | ✓  |                                       |                                      |
| Infrastructure Event Management                   | ✓   | Available at additional cost   |                                       |                                      |
| AWS Concierge                                     | ✓   |  |                                       |                                      |
| Direct access to Technical Account Manager (TAM)  | ✓   |  |                                       |                                      |
| Prioritized Case Routing                          | ✓   |  |                                       |                                      |
| Management Business Reviews                       | ✓   |  |                                       |                                      |