

AWSome Day

Getting Started on AWS

Course Objectives

This course teaches you how to:

- Recognize terminology and concepts as they relate to the **AWS platform** and navigate the **AWS Management Console**.
- Understand the **foundational services**, including Amazon Elastic Compute Cloud (EC2), Amazon Virtual Private Cloud (VPC), Amazon Simple Storage Service (S3), and Amazon Elastic Block Store (EBS).
- Understand the **security** measures AWS provides and key concepts of AWS Identity and Access Management (IAM).
- Understand AWS **database** services, including Amazon DynamoDB and Amazon Relational Database Service (RDS).
- Understand AWS **management tools**, including Auto Scaling, Amazon CloudWatch, Elastic Load Balancing (ELB), and AWS Trusted Advisor.

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 7: Course Appendix

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.



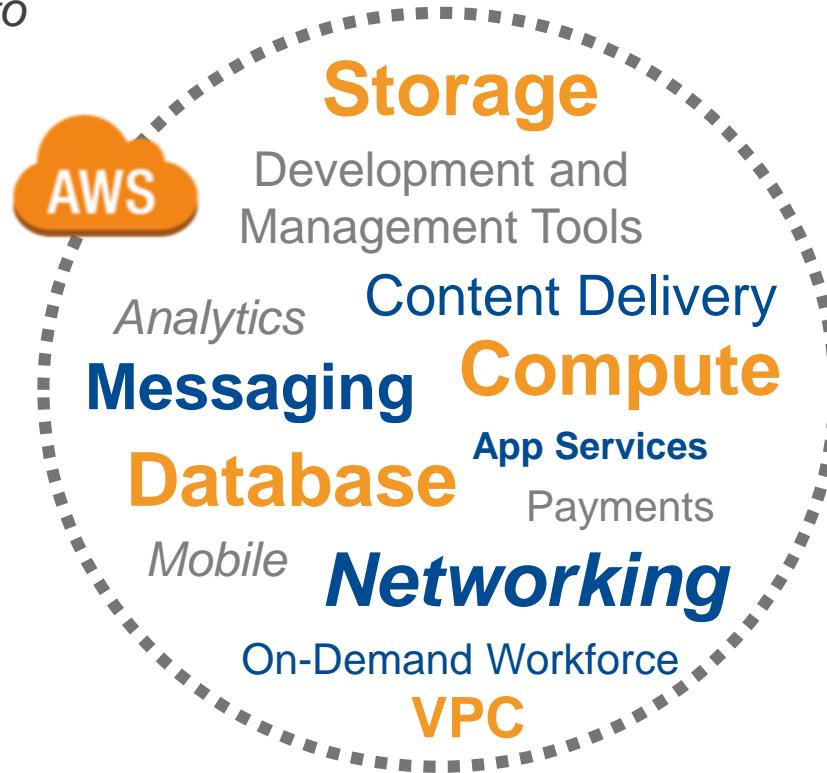
2013:
Amazon Art was launched.



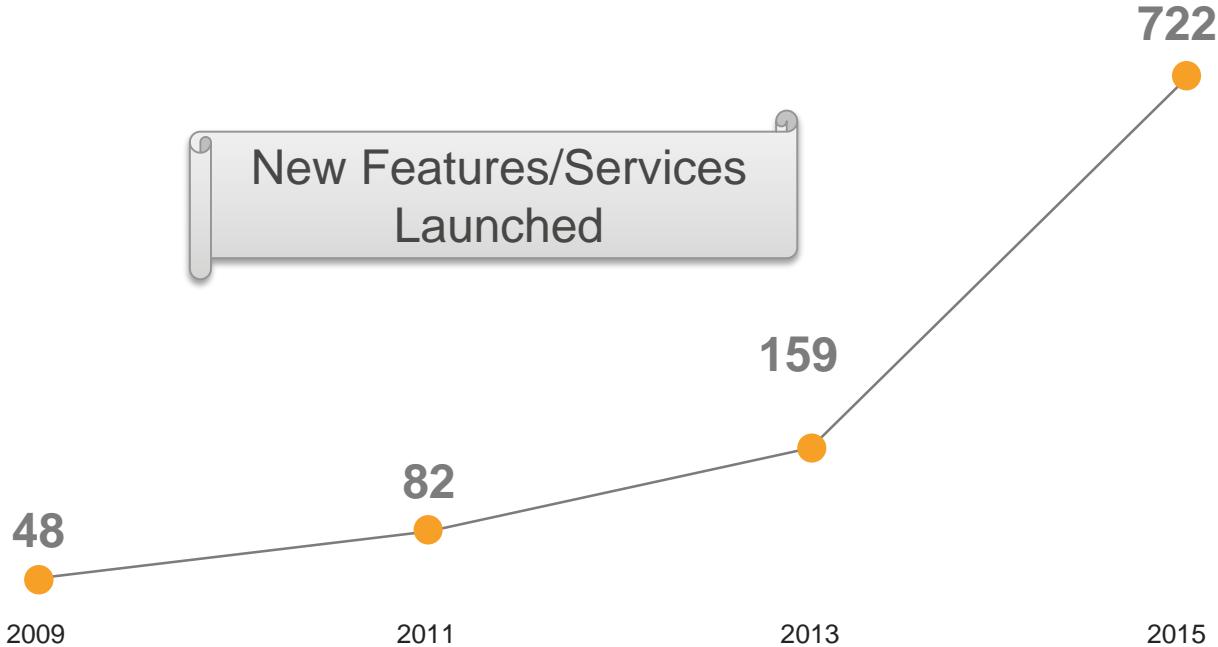
2015:
Amazon Home Services and Amazon Echo were launched.

Amazon Web Services (AWS)

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



AWS Rapid Pace of Innovation



AWS GovCloud (US)

AWS OpsWorks

AWS CodeCommit

Amazon SES

Amazon Elastic Transcoder

Amazon WorkMail

AWS Certificate Manager

Amazon EFS

Amazon Redshift

AWS Identity and Access Management

Amazon AppStream

Amazon DynamoDB

AWS Data Pipeline

Amazon QuickSight

AWS WAF

Amazon SWF

Amazon SNS

Amazon WorkSpaces

Amazon CloudSearch

Amazon Glacier

© 2016, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Import/Export

AWS CodeDeploy

Amazon EC2 Container Service

Amazon Kinesis

AWS Storage Gateway

Amazon ElastiCache

AWS CloudHSM

Amazon Cognito

AWS Config

Elasticsearch Service

AWS CloudTrail

AWS Elastic Beanstalk

Amazon EC2 Container Registry

AWS CodePipeline

Amazon Route 53

AWS Lambda

AWS CloudFormation

AWS Device Farm

Services and Features

Amazon API Gateway

AWS KMS

Amazon RDS for MariaDB

Amazon RDS for Aurora

AWS Directory Service

AWS Mobile Hub

Amazon CloudWatch Logs

Amazon Mobile Analytics

AWS IoT

AWS Service Catalog



AWS Import/Export Training and Certification

As of 1 August 2016

Amazon Machine Learning

AWS Direct Connect

Amazon WorkDocs

Amazon Inspector

AWS Customers

Enterprise Customers

Enterprise Cloud Computing with AWS

With a long history in enabling enterprises to successfully adopt cloud computing, Amazon Web Services delivers a mature set of services specifically designed for the unique security, compliance, privacy, and governance requirements of large organizations. With a technology platform that is both broad and deep, customer-obsessed Professional Services and Support organizations, robust training programs, and an ecosystem tens-of-thousands strong, AWS can help you move faster and do more.

Below are just a few of the many enterprise organizations using AWS today.

Deploy whichever architecture is right for your business



Cloud Native



Hybrid



Private

Public Sector Customers

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

Contact Public Sector Sales

Government

Education

Nonprofits

Partners

Events

Resources

Government, education and nonprofit organizations face unique challenges to accomplish complex missions with limited resources. Public sector leaders engaged in true cloud computing projects overwhelmingly turn to the power and speed of Amazon Web Services when they want to serve citizens more effectively, achieve scientific breakthroughs, reach broader constituents and put more of their time and resources into their core missions.

Amazon Web Services now serves more than 2,300 government, 7,000 education and 22,000 nonprofit organizations worldwide.



Watch the Fireside Chat With Andy Jassy, CEO and Teresa Carlson, VP WWPS at the AWS Public Sector Summit

Startup Customers

Startups and Amazon Web Services

From the spark of an idea, to the first customer, to IPO and beyond, the world's most progressive startups build and grow their businesses on Amazon Web Services. Our expansive technology platform allows startups of all sizes and kinds to run lean and free them to be fast, agile, and global while still being efficient with their IT spend. And as they evolve and become more sophisticated, they don't outgrow AWS. Instead, they plug in to AWS's continuous service and feature innovations to make their ideas realities.

The Benefits of Building and Scaling Your Startup on AWS



Startups get special AWS perks



So many ways to lower costs



Going mobile - quickly and easily

Advantages and Benefits of AWS Cloud Computing



Trade capital expense
for variable expense.



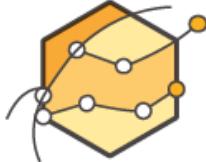
Increase speed and
agility.



Benefit from massive
economies of scale.



Stop spending money on
running and maintaining
data centers.



Stop guessing
capacity.



Go global in minutes.

Gartner Magic Quadrant for Cloud Infrastructure as a Service, Worldwide



Gartner "Magic Quadrant for Cloud Infrastructure as a Service, Worldwide." Lydia Leong, Gregor Petri, Bob Gill, Mike Dorosh, 03 August 2016. This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available at <https://aws.amazon.com/resources/analyst-reports/>. 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.

AWS Core Infrastructure and Services

Traditional Infrastructure



Firewalls



ACLs



Administrators

Security

Amazon Web Services



Security Groups



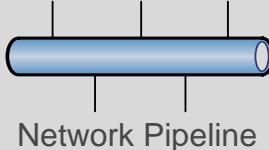
Network ACLs



AWS IAM



Router



Network Pipeline



Switch

Networking



ELB



VPC



On-Premises Servers

Servers



AMI



Amazon EC2 Instances



DAS



SAN



NAS



RDBMS

Storage and Database



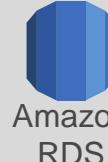
Amazon EBS



Amazon EFS



Amazon S3



Amazon RDS

AWS Cloud Computing

Applications



Virtual
Desktops



Collaboration and Sharing

Platform Services

Databases

Relational
NoSQL
Caching

Analytics

Cluster
Computing
Real-time
Data
Warehouse
Data
Workflows

App Services

Queuing
Orchestration
App Streaming
Transcoding
Email
Search

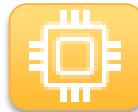
Deployment and Management

Containers
Dev/ops Tools
Resource Templates
Usage Tracking
Monitoring and Logs

Mobile Services

Identity
Sync
Mobile Analytics
Notifications

Foundation Services



Compute
(Virtual, Auto-scaling and
Load Balancing)



Networking



Storage
(Object, Block and Archive)

Infrastructure



Regions



Availability Zones



Edge Locations

AWS Foundation Services

Compute

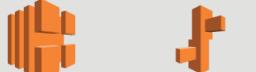
Amazon EC2 AWS Lambda



Amazon EC2 Container Service



Elastic Load Balancing AWS Elastic Beanstalk



Auto Scaling



Network

Amazon VPC Amazon Route 53



AWS Direct Connect



Storage

Amazon S3 Amazon CloudFront



Amazon Glacier



Amazon Elastic File System



AWS Storage Gateway



AWS Import/Export



Security & Identity

AWS Identity and Access Management



AWS Directory Service



AWS KMS



AWS Cloud HSM



AWS WAF



Applications

Amazon WorkDocs Amazon WorkSpaces



Amazon WorkMail



AWS Platform Services

Databases	Analytics	App Services	Management Tools	Developer Tools	Mobile Services	Internet of Things
 Amazon RDS  Amazon DynamoDB  Amazon ElastiCache  Amazon Redshift  AWS Database Migration Service	 Amazon EMR  AWS Data Pipeline  Amazon Elasticsearch Service  Amazon Machine Learning 	 Amazon SES  Amazon AppStream  Amazon SWF  Amazon Elastic Transcoder  Amazon CloudSearch  Amazon SQS 	 AWS CloudFormation  AWS Config  AWS CloudTrail  AWS Service Catalog  AWS OpsWorks  Amazon CloudWatch  Trusted Advisor  AWS Certificate Manager	 AWS CodeCommit  AWS CodeDeploy 	 Amazon Cognito  AWS Device Farm  Amazon SNS  Amazon Mobile Analytics 	 AWS IoT

AWS Global Infrastructure

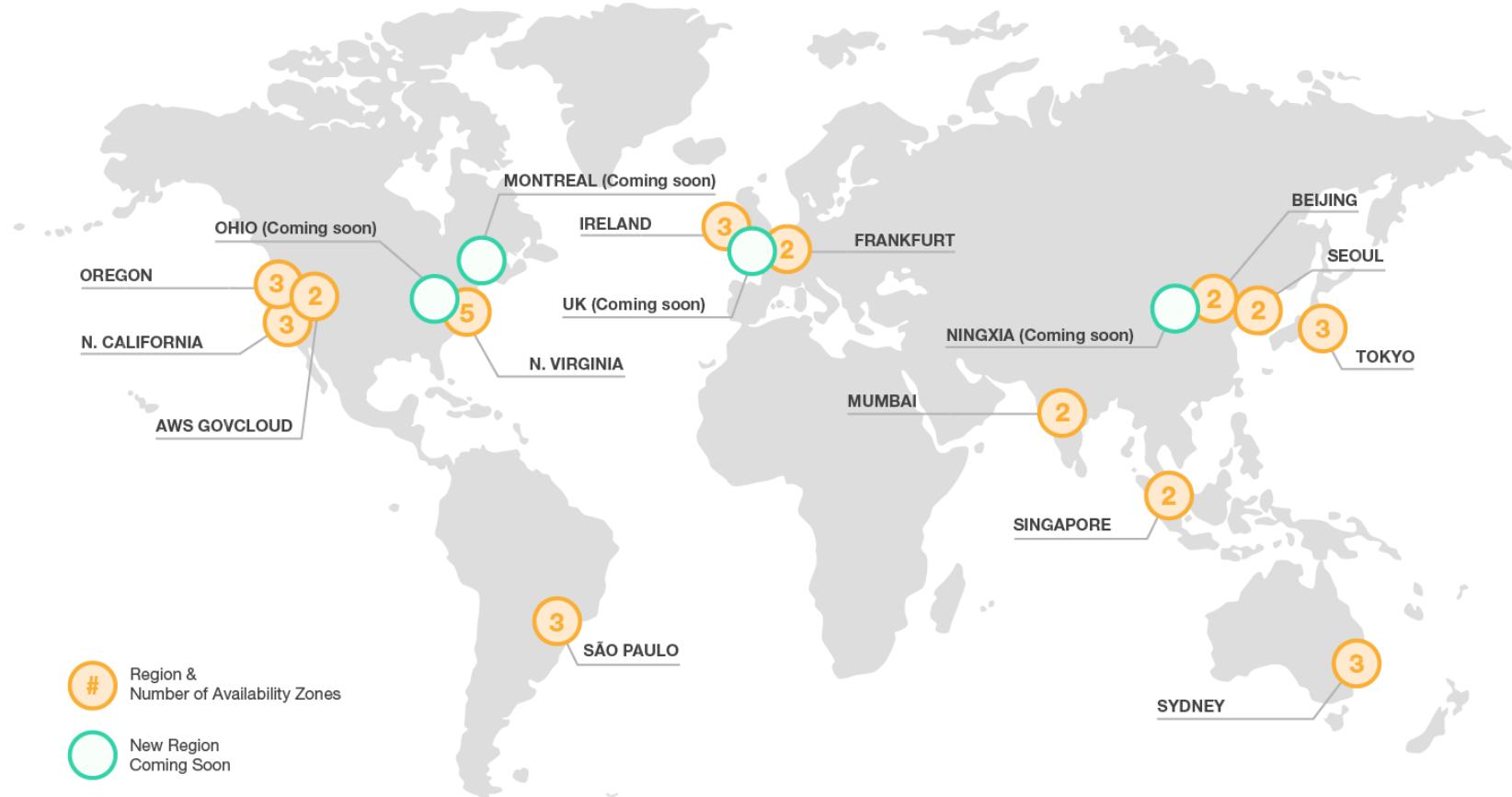
Regions

- 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

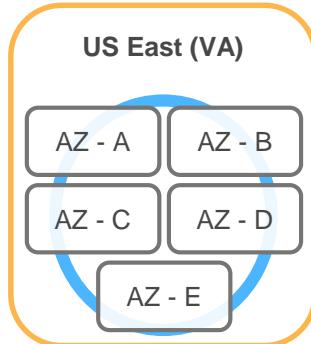


AWS Global Infrastructure

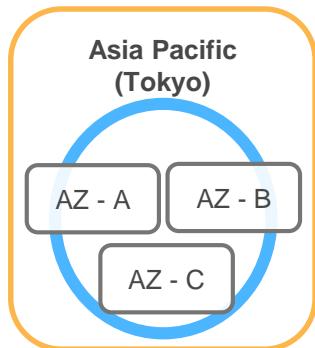
At least 2 Availability Zones per region.

Examples:

- US East (N. Virginia)
 - us-east-1a
 - us-east-1b
 - us-east-1c
 - us-east-1d
 - us-east-1e

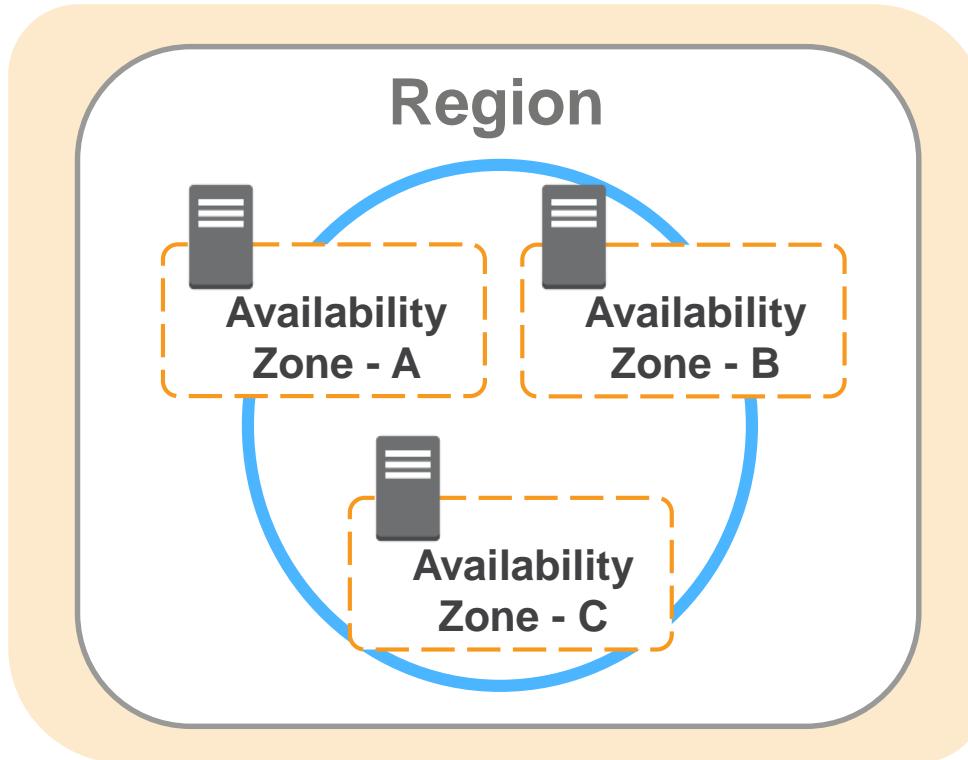


- Asia Pacific (Tokyo)
 - ap-northeast-1a
 - ap-northeast-1b
 - ap-northeast-1c



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

High Availability Using Multi-AZ Deployments



AWS Global Infrastructure

50+ AWS Edge locations - local points of presence
commonly supporting AWS services like:

- Amazon Route 53 
- Amazon CloudFront 

AWS Management Console Demonstration

Knowledge Check

Q: What is the AWS term for physically distinct groups of **data centers** within a region?

Availability Zone

True or False: There are more **Regions** than **Edge locations**.

False

True or False: AWS owns and maintains the infrastructure required for application services. You provision and use them as needed.

True

Q: How do **Availability Zones** in the same region differ?

Each Availability Zone is isolated, but the Availability Zones in a region are connected through low-latency links.

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)

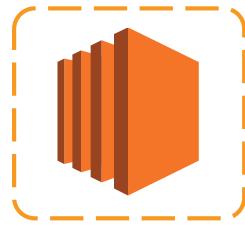
Amazon Elastic Compute Cloud (EC2)



Amazon
EC2

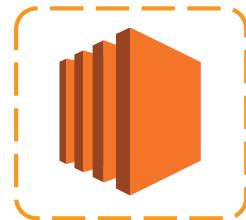
- **Resizable** compute capacity
- Complete control of your computing resources
- **Reduced time required** to obtain and boot new server instances

Amazon EC2 Facts



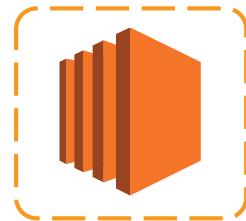
- **Scale capacity** as your computing requirements change
- Pay only for capacity that you actually use
- Choose **Linux or Windows**
- Deploy across **AWS Regions** and **Availability Zones** for reliability
- Use **tags** to help manage your Amazon EC2 resources

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.

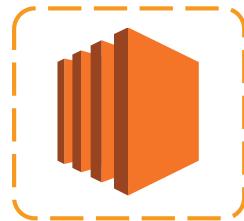
Amazon Machine Image (AMI) Details



An AMI includes the following:

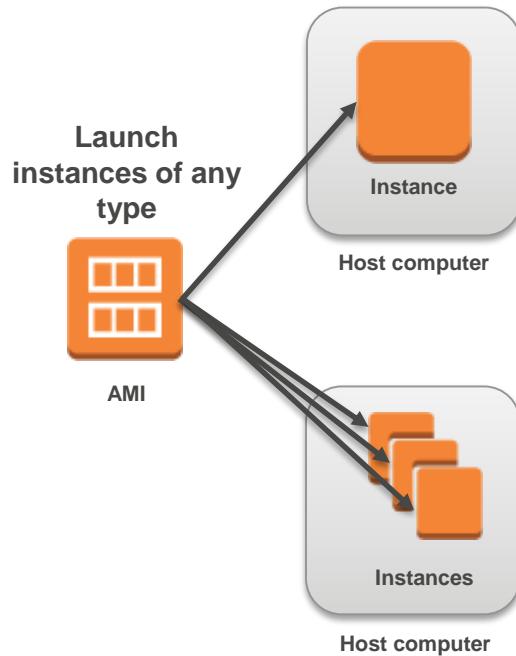
- A template for the **root volume** for the instance (for example, an operating system, an application server, and applications).
- **Launch permissions** that control which AWS accounts can use the AMI to launch instances.
- A block device mapping that specifies the **volumes to attach** to the instance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

Instances and AMIs

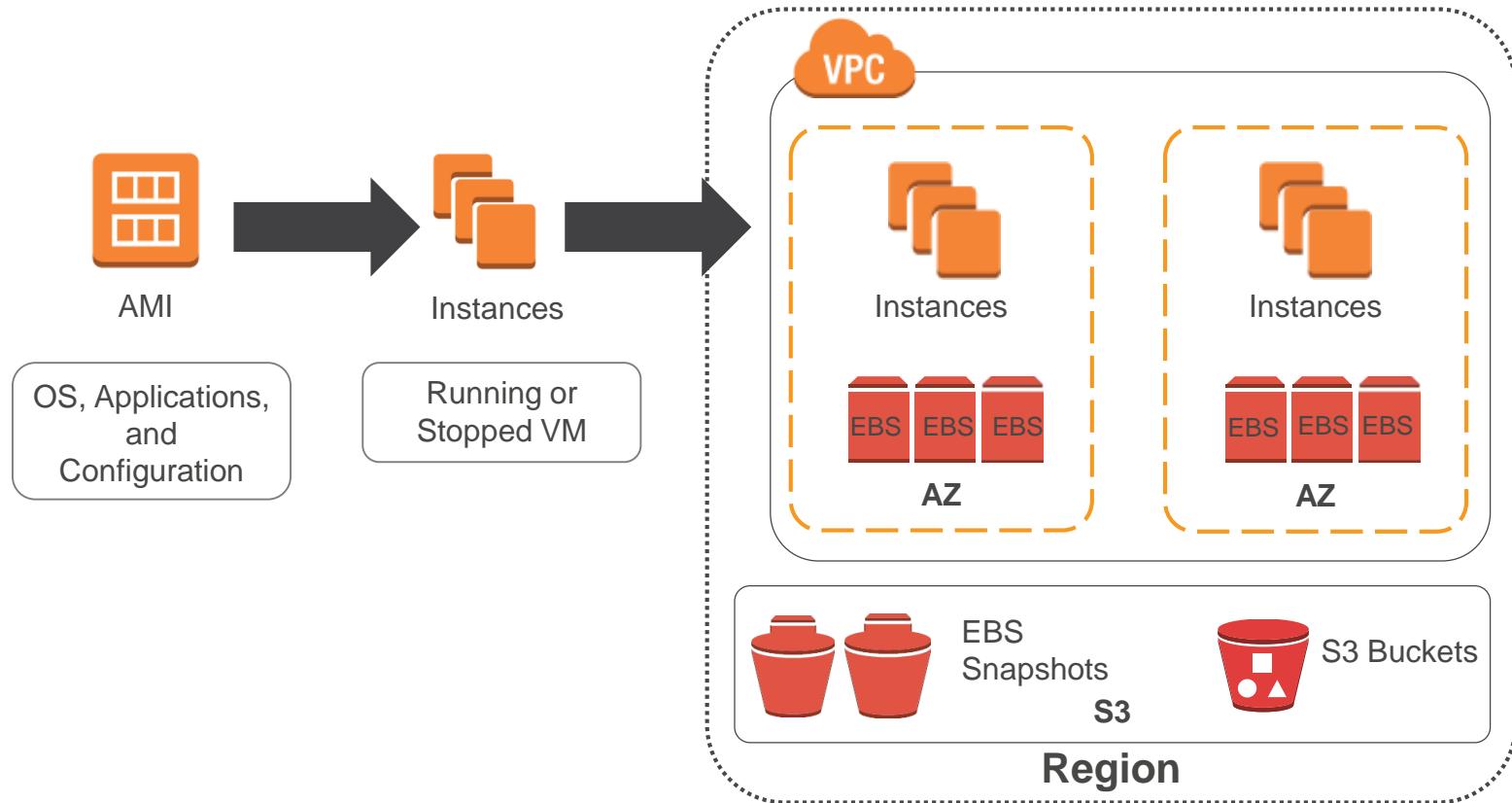
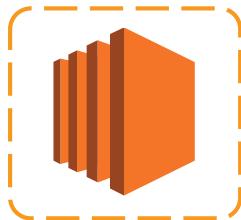


Select an AMI based on:

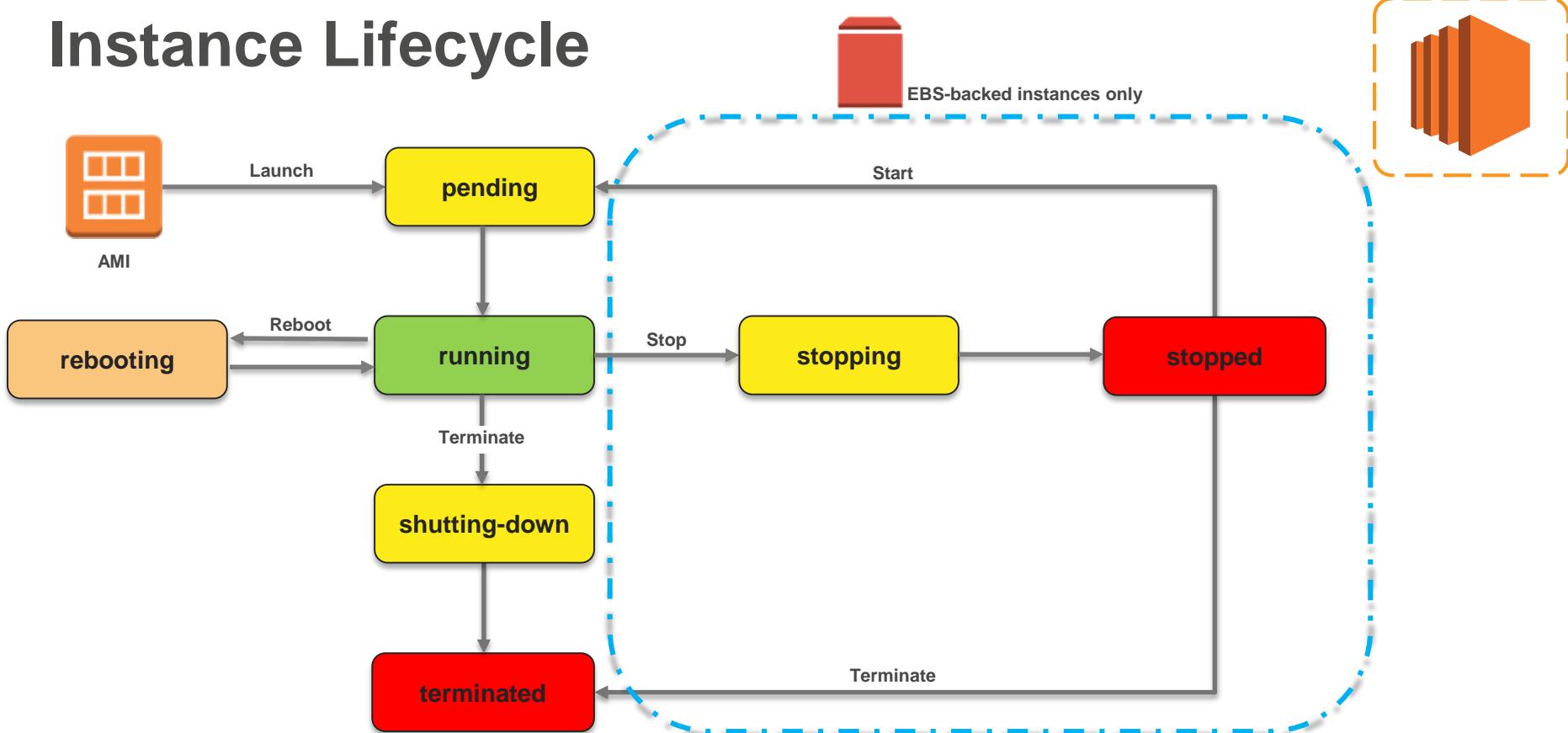
- Region
- Operating system
- Architecture (32-bit or 64-bit)
- Launch permissions
- Storage for the root device



Amazon EC2 Instances



Instance Lifecycle

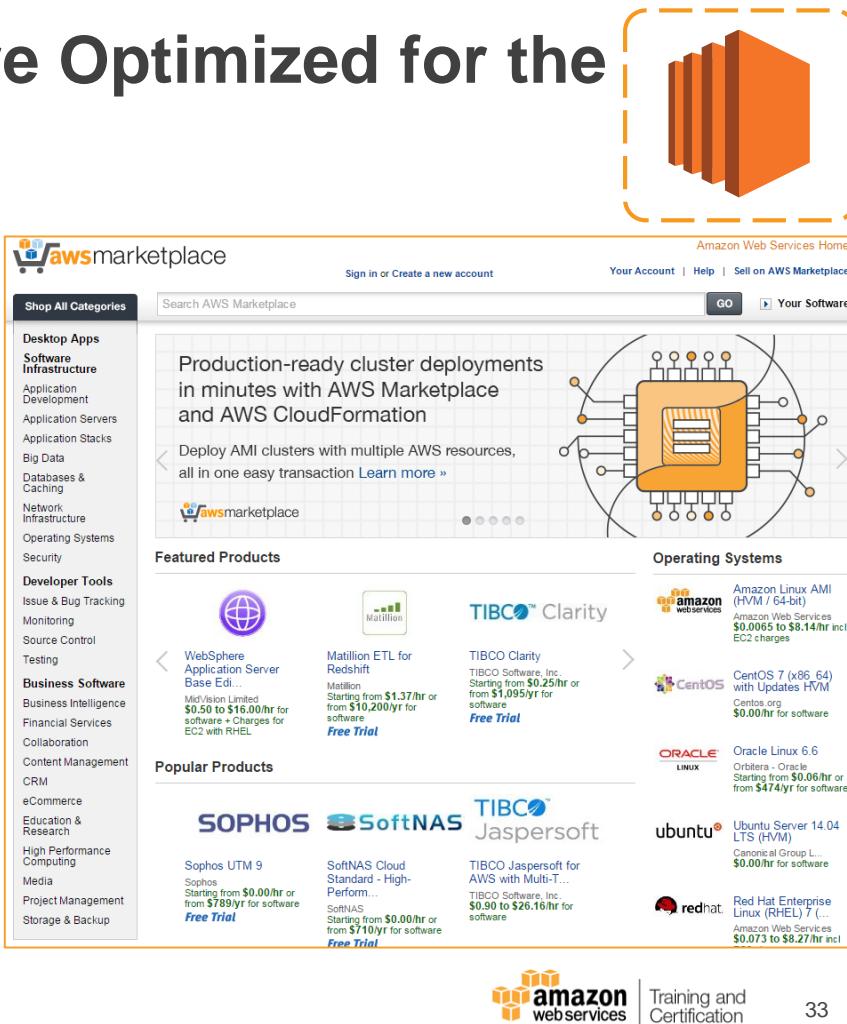


AWS Marketplace – IT Software Optimized for the Cloud

- 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>



The screenshot shows the AWS Marketplace homepage. At the top right is a large orange 3D bar chart icon. Below it is a navigation bar with links for "Sign in or Create a new account", "Your Account | Help | Sell on AWS Marketplace", and "GO | Your Software". The main content area features a search bar labeled "Search AWS Marketplace". A central banner highlights "Production-ready cluster deployments in minutes with AWS Marketplace and AWS CloudFormation" and "Deploy AMI clusters with multiple AWS resources, all in one easy transaction". Below this is a "Featured Products" section with cards for "WebSphere Application Server Red Hat Edit...", "Matillion ETL for Redshift", "TIBCO Clarity", "TIBCO Software, Inc.", "CentOS 7 (x86_64) with Updates HVM", "Oracle Linux 6.6", "Ubuntu Server 14.04 LTS (HVM)", and "Red Hat Enterprise Linux (RHEL) 7 (...)".

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



Get the Intel® Advantage

Intel's Haswell microarchitecture on new X1, C4, D2, and M4 instances, with **custom Intel® Xeon® v3** processors, provides new features:

Haswell microarchitecture can boost existing applications performance by **30% or more** for better workload performance and faster response times.

Newer **Hardware Assisted** technologies, such as **Intel® AVX2.0** instructions, can double the floating-point performance for compute-intensive workloads and provide additional instructions for compression and encryption

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.



Intel® Processor Technologies

Intel® AVX: Provides dramatically better performance for highly parallel HPC workloads such as *life science engineering, data mining, financial analysis*, or other technical computing applications. AVX also enhances *image, video, and audio processing*.

Intel® AES-NI: Enhance your security with these new encryption instructions that reduce the performance penalty associated with encrypting/decrypting data.

Intel® Turbo Boost Technology: Provides more computing power when you need it with performance that adapts to spikes in your workload.

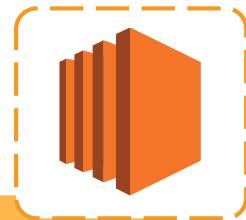
Intel Transactional Synchronization (TSX) Extensions: Enable execution of transactions that are independent to accelerate throughput.

P state & C state control: Gives you the ability to individually tune each cores performance & sleep states to improve application performance.

AWS EC2 Instances with Intel® Technologies

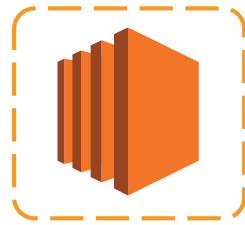
AWS Instance Type	High Memory X1	Compute-Optimized C4	Storage-Optimized D2	General Purpose M4	Memory-Optimized R3	IO-Optimized I2	Graphics-Optimized G2	Burstable Performance T2
Intel Processor	Intel Xeon E7-8880 v3	Custom Intel Xeon E5-2666 v3	Custom Intel Xeon E5-2676 v3	Custom Intel Xeon E5-2676 v3	Intel Xeon E5-2670 v2	Intel Xeon E5-2670 v2	Intel Xeon E5-2670	Intel Xeon Family
Intel AVX	AVX 2.0	AVX 2.0	AVX 2.0	AVX 2.0	Yes	Yes	Yes	Yes
Intel AES-NI	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Intel Turbo Boost	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intel TSX	Yes	No	No	No	No	No	No	No
Per core P- and C-state control	No	Yes (8xlarge only)	No	No	No	No	No	No
SSD Storage	EBS Optimized by default	EBS Optimized by default	No	EBS Optimized by default	Yes	Yes	Yes	EBS only

Current Generation Instances



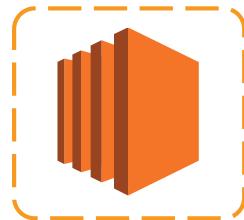
Instance Family	Some Use Cases
General purpose (t2, m4, m3)	<ul style="list-style-type: none">• Low-traffic websites and web applications• Small databases and mid-size databases
Compute-optimized (c4, c3)	<ul style="list-style-type: none">• High performance front-end fleets• Video-encoding
Memory-optimized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

Instance Metadata



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

Retrieving Instance Metadata



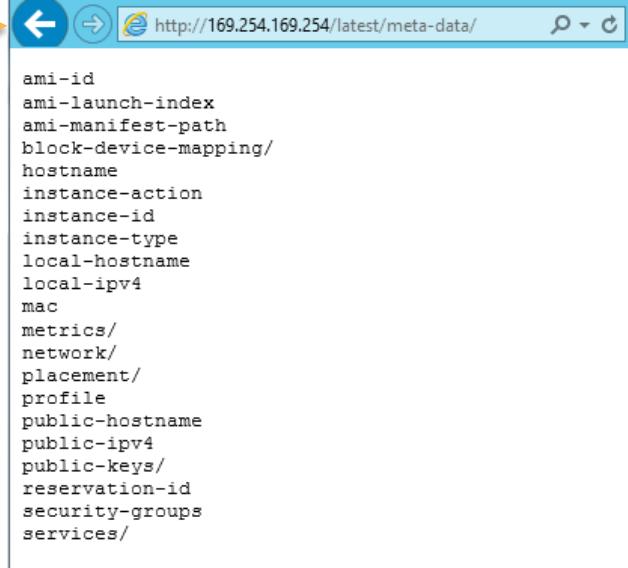
To view all categories of instance metadata from within a running instance, use the following URI:

<http://169.254.169.254/latest/meta-data/>

On a Linux instance, you can use:

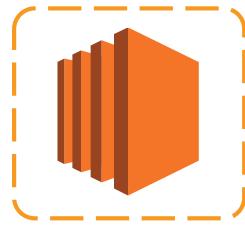
- `$ curl http://169.254.169.254/latest/meta-data/`
- `$ GET http://169.254.169.254/latest/meta-data/`

All metadata is returned as text (content type `text/plain`).



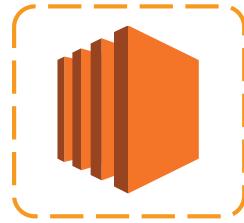
```
ami-id  
ami-launch-index  
ami-manifest-path  
block-device-mapping/  
hostname  
instance-action  
instance-id  
instance-type  
local-hostname  
local-ipv4  
mac  
metrics/  
network/  
placement/  
profile  
public-hostname  
public-ipv4  
public-keys/  
reservation-id  
security-groups  
services/
```

Instance User Data



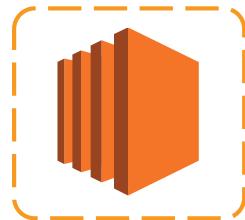
- Can be passed to the instance **at launch**.
- Can be used to perform common **automated configuration tasks**.
- Runs scripts after the instance starts.

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 **EC2Config** service
- User data scripts run once per instance ID by default.

User Data Example Linux

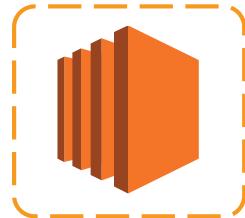


```
#!/bin/sh  
  
yum -y install httpd  
chkconfig httpd on  
/etc/init.d/httpd start
```

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.

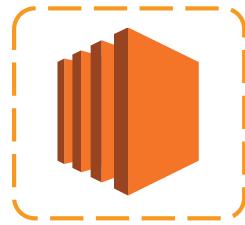
```
Install-WindowsFeature web-server, web-webserver
```

```
Install-WindowsFeature web-mgmt-tools
```

```
</powershell>
```

Install IIS
Install Web Management Tools

Retrieving User Data



To retrieve user data, use the following URI:

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

On a Linux instance, you can use:

```
$ curl http://169.254.169.254/latest/user-data/  
$ GET http://169.254.169.254/latest/user-data/
```

A screenshot of a terminal window titled "ec2-user@ip-172-31-31-72:~". The window shows the following text:

```
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"

[ec2-user@ip-172-31-31-72 ~]$ curl http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
yum install -y httpd24 php56 mysql55-server php56-mysqlnd
service httpd start
chkconfig httpd on
groupadd www
usermod -a -G www ec2-user
chown -R root:www /var/www
chmod 2775 /var/www
find /var/www -type d -exec chmod 2775 {} +
find /var/www -type f -exec chmod 0664 {} +
echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php[ec2-user@ip-172-31-31-72
~]$
```

An orange arrow points from the text "use:" in the slide content to the terminal command "curl http://169.254.169.254/latest/user-data".

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

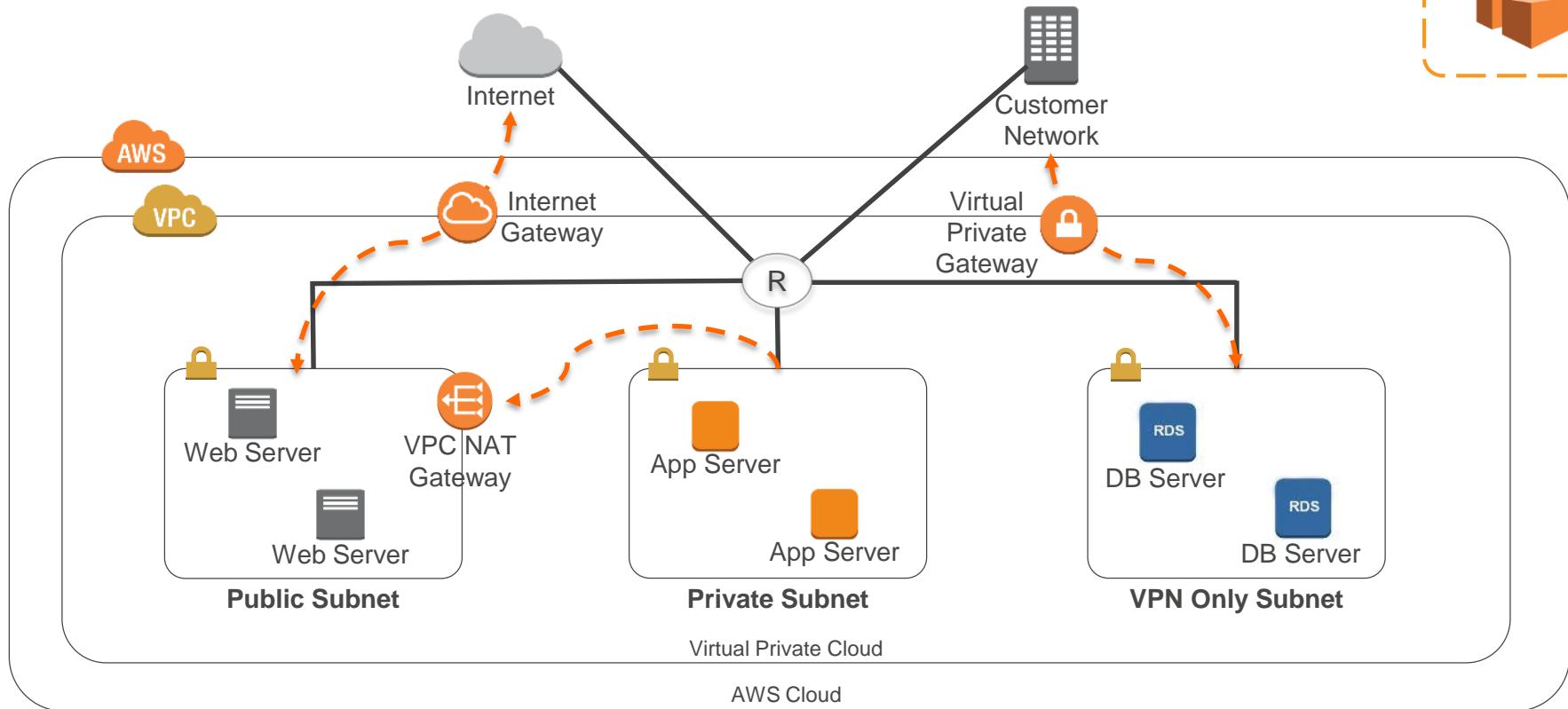
- Provision a **private, isolated virtual network** on the AWS cloud.
- Have complete control over your virtual networking environment.

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.

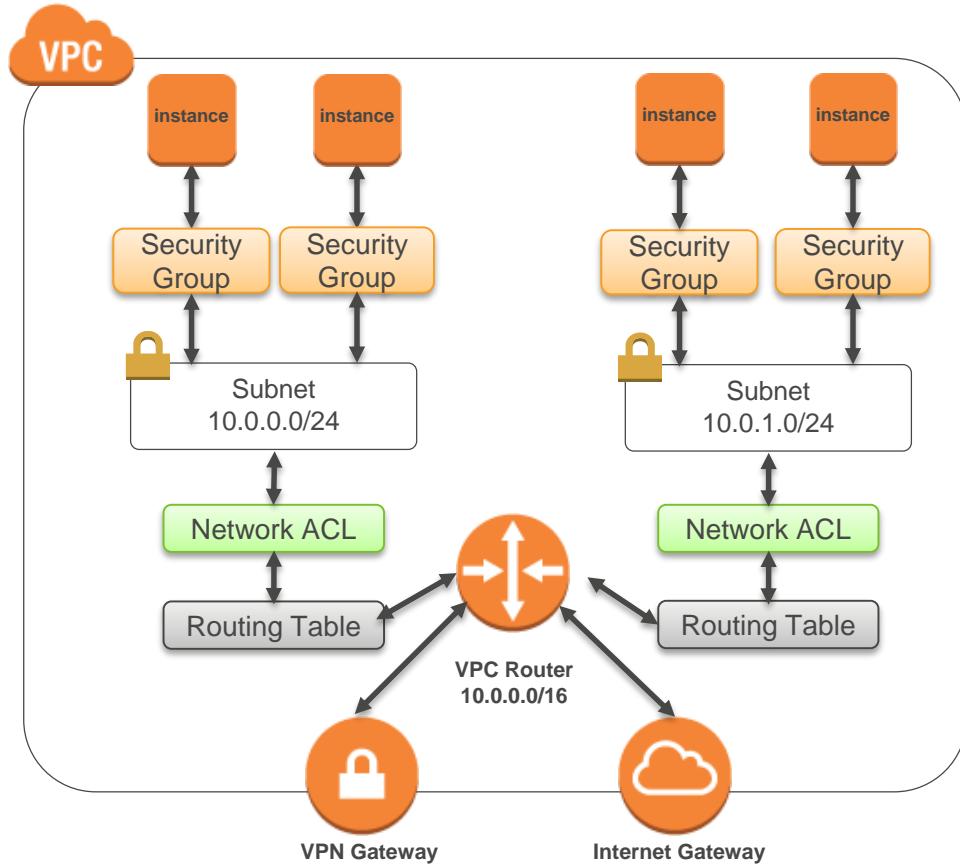
Amazon VPC Example



Security in Your VPC



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



VPN Connections

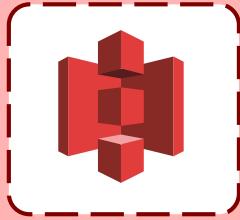


VPN Connectivity option	Description
AWS Hardware VPN	You can create an IPsec hardware VPN connection between your VPC and your remote network.
AWS Direct Connect	AWS Direct Connect provides a dedicated private connection from a remote network to your VPC.
AWS VPN CloudHub	You can create multiple AWS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

Storage Services

Amazon S3 and Amazon EBS

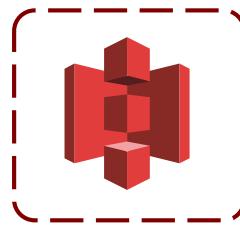
Amazon Simple Storage Service (S3)



Amazon S3

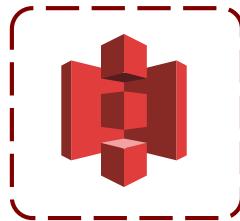
- Storage for the Internet
- Natively online, HTTP access
- Storage that allows you to store and retrieve **any amount of data**, any time, from anywhere on the web
- **Highly scalable**, reliable, fast and durable

Amazon S3 Facts



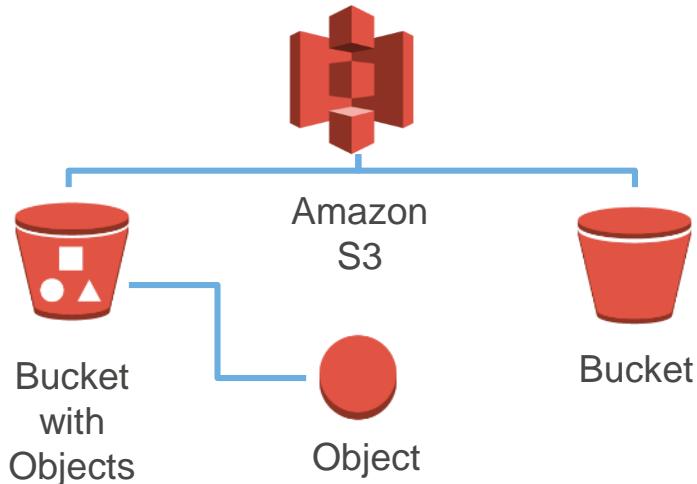
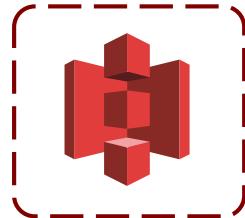
- Can store an **unlimited number of objects** in a bucket
- Objects can be **up to 5 TB**; no bucket size limit
- Designed for **99.999999999%** durability and **99.99%** availability of objects over a given year
- Can use **HTTP/S** endpoints to store and retrieve any amount of data, at any time, from 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



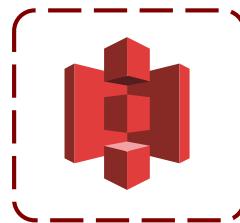
- Storage and backup
- Application file hosting
- Media hosting
- Software delivery
- Store AMIs and snapshots

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



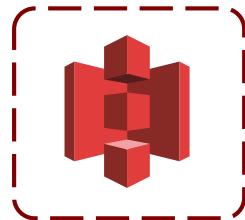
An object key is the unique identifier for an object in a bucket.

<http://doc.s3.amazonaws.com/2006-03-01/AmazonS3.html>

Bucket

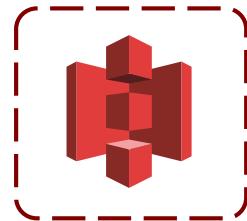
Object/Key

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 Versioning

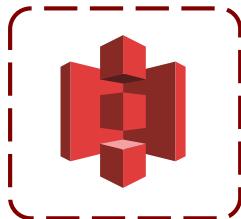


- Protects from **accidental overwrites and deletes** with no performance penalty.
- Generates a **new version with every upload**.
- Allows easily retrieval of deleted objects or **roll back** to previous versions.
- Three states of an Amazon S3 bucket
 - Un-versioned (default)
 - Versioning-enabled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



Versioning Enabled

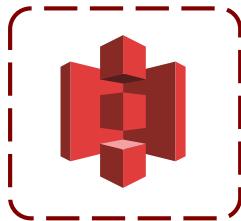
Amazon S3 Object Lifecycle



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

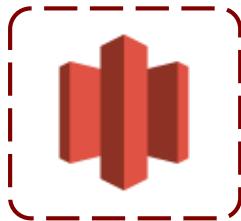
Amazon S3 Pricing



- 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 99.99999999% durability
- Three to five hours' retrieval time
- Less than \$0.01 per GB/month (depending on region)

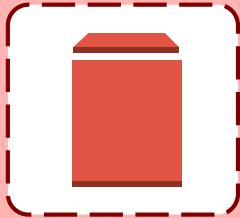
Amazon S3 Storage Classes

Storage Class	Durability	Availability	Other Considerations
Amazon S3 Standard	99.999999999%	99.99%	
Amazon S3 Standard - Infrequent Access (IA)	99.999999999%	99.9%	<ul style="list-style-type: none">• Retrieval fee associated with objects• Most suitable for infrequently accessed data
Glacier	99.999999999%	99.99% (once restored)	<ul style="list-style-type: none">• Not available for real-time access• Must restore objects before you can access them• Restoring objects can take 3-5 hours

Instructor Demo

Amazon S3

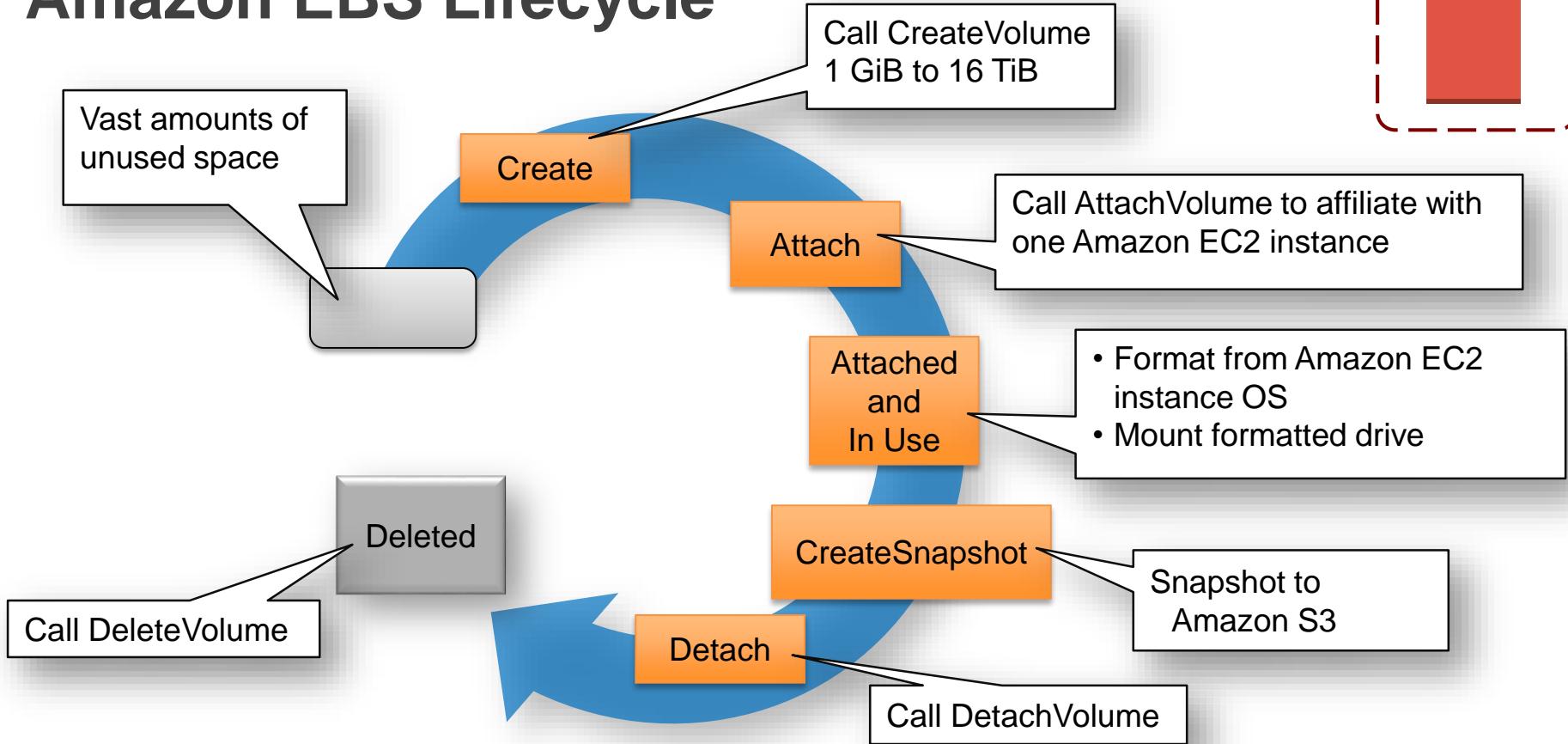
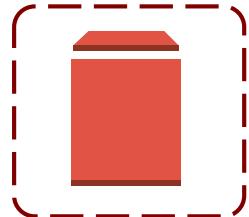
Amazon Elastic Block Store (EBS)



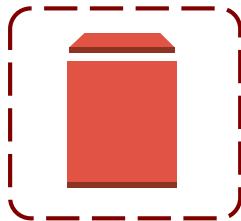
Amazon
EBS

- **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

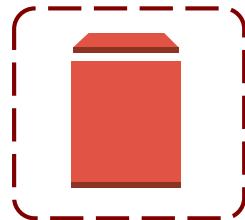


Amazon EBS Volume Types



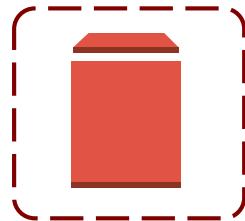
- SSD-backed volumes are
 - Optimized for **transactional** workloads that involve **frequent read/write** operations with **small I/O** size.
 - Dominant in **IOPS** performance.
- HDD-backed volumes are
 - Optimized for **large streaming** workloads.
 - Dominant in **throughput** (measured in MiB/s).

Amazon EBS Volume Types



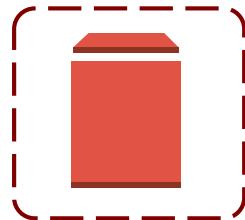
	SSD		HDD	
Volume Type	General Purpose SSD (gp2)	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	Balances price and performance for a wide variety of transactional loads.	Highest-performance SSD volume designed for mission-critical applications.	Low-cost HDD designed for frequently accessed, throughput-intensive workloads.	Lowest cost HDD designed for less frequently accessed workloads.
Volume Sizes	1 GiB – 16 TiB	4 GiB – 16 TiB	500 GiB – 16 TiB	500 GiB – 16 TiB
Dominant Performance Attribute	IOPS	IOPS	MiB/s	MiB/s

Amazon EBS Facts



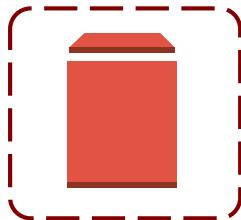
- EBS is recommended when data must be **quickly accessible** and requires **long-term persistence**.
- You can launch your EBS volumes as **encrypted** volumes – data stored at rest on the volume, disk I/O, and snapshots created from the volume are all encrypted.
- You can create **point-in-time snapshots**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

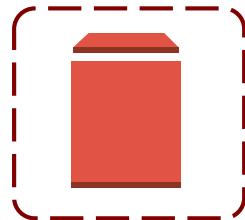


Pay for what you provision:

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

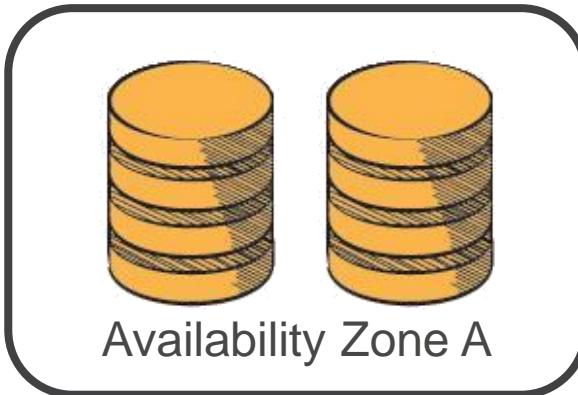
* Check Amazon EBS Pricing page for current pricing for all regions.

Amazon EBS Scope



Amazon EBS volumes are in a single Availability Zone

EBS Volume 1

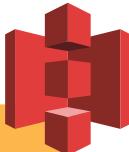


EBS Volume 2



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

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
Access from the Internet?	No (1)	Yes (2)
Typical use case	It is a disk drive	Online storage

- (1) Accessible from the Internet if mounted to server and set up as FTP, etc.
- (2) Only with proper credentials, unless ACLs are world-readable

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**.

Reboot vs. Stop vs. Terminate

Characteristic	Reboot	Stop/Start (EBS-backed instances only)	Terminate
Host computer	The instance stays on the same host computer .	The instance runs on a new host computer .	
Public IP address	No change	New address assigned	
Elastic IP addresses (EIP)	EIP remains associated with the instance.	EIP remains associated with the instance.	EIP is disassociated from the instance.
Instance store volumes	Preserved	Erased	Erased
EBS volume	Preserved	Preserved	Boot volume is deleted by default .
Billing	Instance billing hour doesn't change.	You stop incurring charges as soon as state is changed to <i>stopping</i> .	You stop incurring charges as soon as state is changed to <i>shutting-down</i> .

Knowledge Check

Q: What AWS service would help support your web application to **offload serving static assets** and **store user uploaded images and video** off-instance?

Amazon S3

Q: How would an EC2 instance find its private and public IP addresses?

Retrieve the instance metadata. <http://169.254.169.254/latest/meta-data/>

Q: What acts as an additional layer of security at the subnet level in a VPC?

Network ACLs

True or False: S3 limits the amount you can store.

False

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



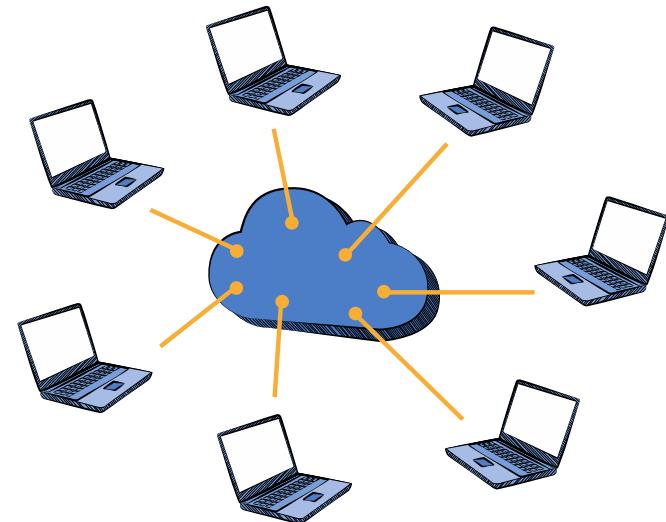
Physical Security

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

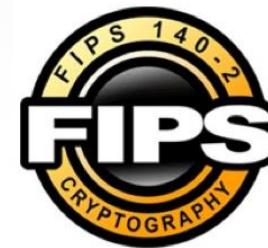


Hardware, Software, and Network

- 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

Secure Transmission

Use secure endpoints to establish secure communication sessions (HTTPS).

Security Groups

Instance Firewalls

Use security groups to configure firewall rules for instances.

VPC

Network Control

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

Secure Transmission

Use secure endpoints to establish secure communication sessions (HTTPS).

Security Groups

Instance Firewalls

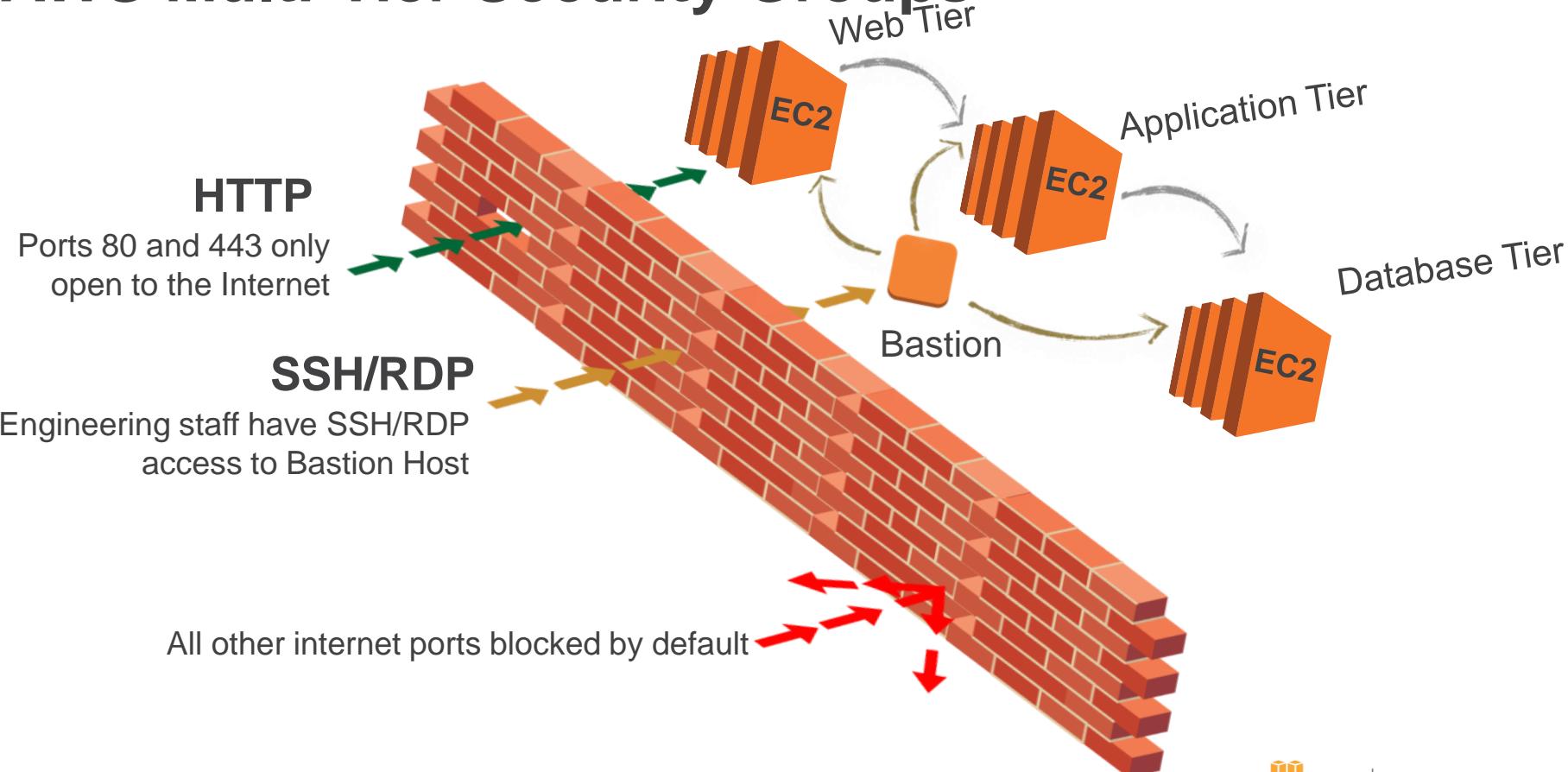
Use security groups to configure firewall rules for instances.

VPC

Network Control

Use public and private subnets, NAT, and VPN support in your virtual private cloud to create low-level networking constraints for resource access.

AWS Multi-Tier Security Groups



Amazon Virtual Private Cloud (VPC)

SSL Endpoints

Secure Transmission

Use secure endpoints to establish secure communication sessions (HTTPS).

Security Groups

Instance Firewalls

Use security groups to configure firewall rules for instances.

VPC

Network Control

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)



1

**Manage AWS IAM users
and their access**

2

**Manage AWS IAM roles
and their permissions**

3

**Manage federated users
and their permissions**

AWS IAM Authentication



- **Authentication**
- **AWS Management Console**
 - User Name and Password

Account:

User Name:

Password:

MFA users, enter your code on the next screen.

Sign In

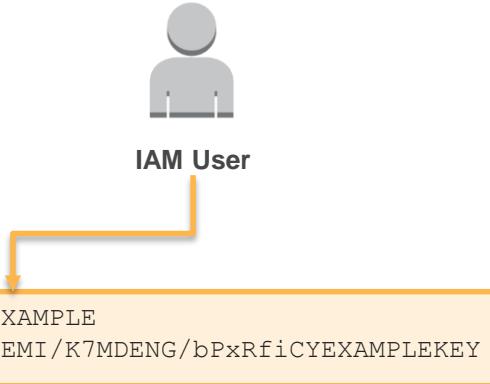


The screenshot shows the AWS Management Console with the 'IAM User' section selected. On the left, there's a sidebar with various service links like CloudWatch, Lambda, and CloudFront. The main content area displays user-related information and actions. At the bottom, there are links for Feedback, English, and other account details.

AWS IAM Authentication



- **Authentication**
- **AWS CLI or SDK API**
 - Access Key and Secret Key



AWS CLI

```
:~ $ 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

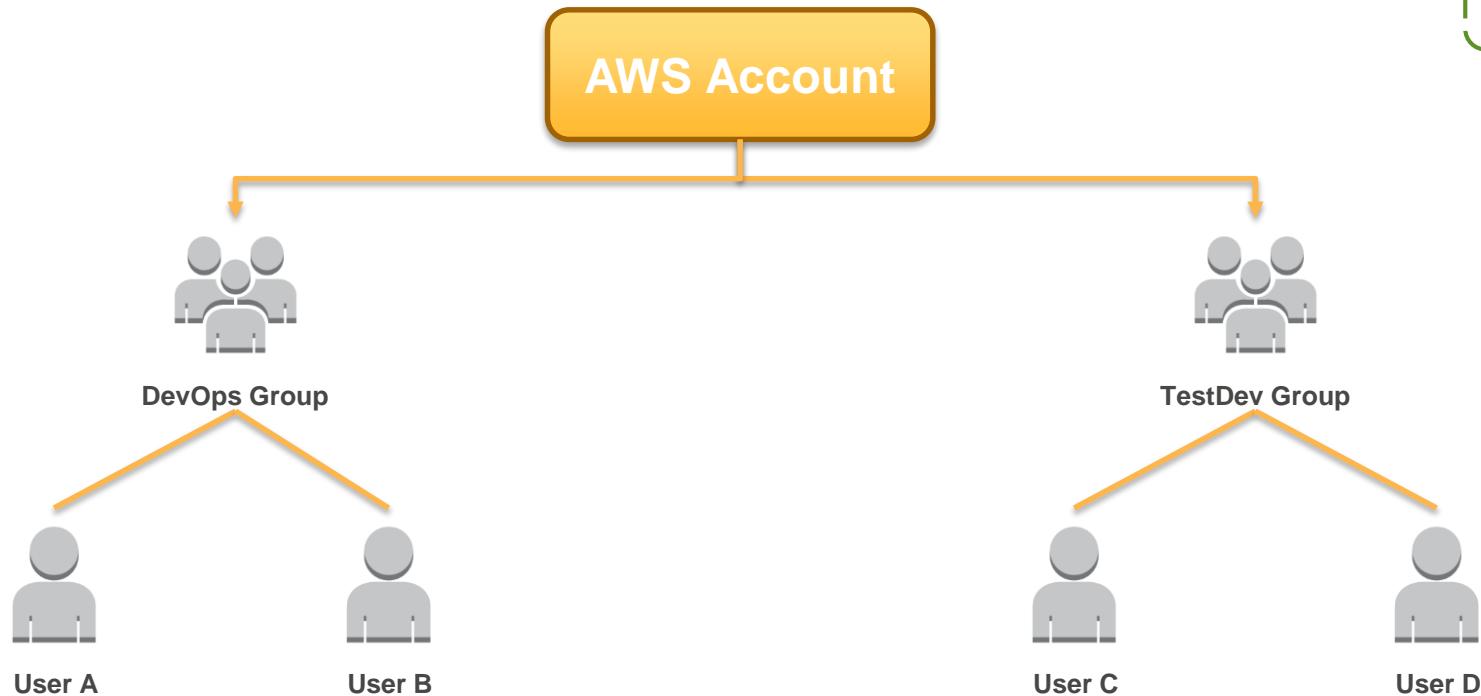


Python



.NET

AWS IAM User Management - Groups



AWS IAM Authorization



Authorization

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



IAM User



IAM Group

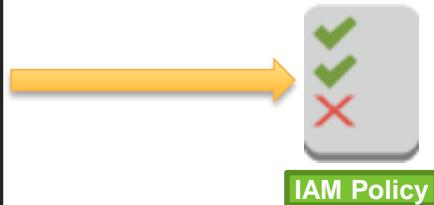


IAM Roles

AWS IAM Policy Elements



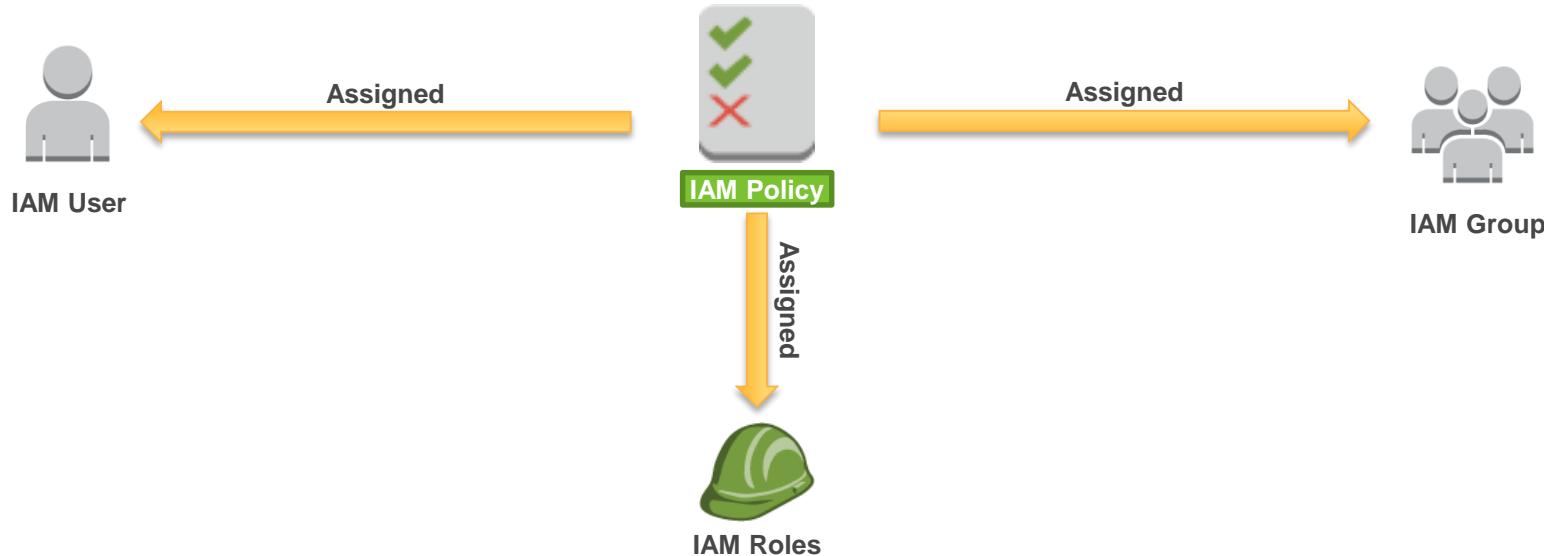
```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "Stmt1453690971587",  
            "Action": [  
                "ec2:Describe*",  
                "ec2:StartInstances",  
                "ec2:StopInstances"  
            ],  
            "Effect": "Allow",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



AWS IAM Policy Assignment



AWS IAM Policy Assignment



AWS IAM Roles

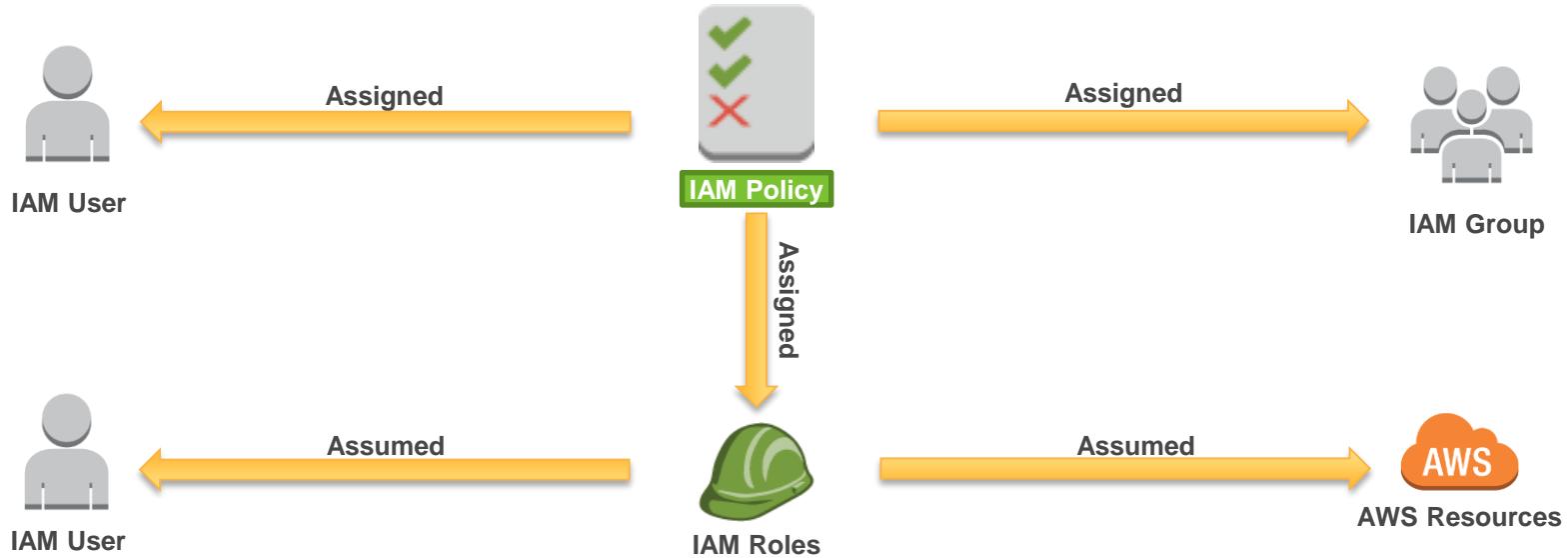


- An IAM role uses a policy.
- An IAM role has no associated credentials.
- IAM users, applications, and services may assume IAM roles.



IAM Roles

AWS IAM Policy Assignment



Example: Application Access to AWS Resources



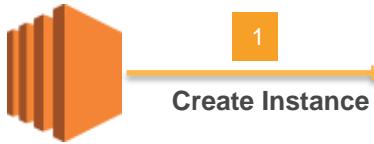
- Python application hosted on an Amazon EC2 Instance needs to interact with Amazon S3.
- AWS credentials are required:
 - Option 1: ~~Store AWS Credentials on the Amazon EC2 instance.~~
 - Option 2: Securely distribute AWS credentials to AWS Services and Applications.



IAM Roles

AWS IAM Roles - Instance Profiles

Amazon EC2



Select IAM Role

App &



Screenshot of the AWS EC2 instance creation wizard, Step 3: Configure Instance Details. The 'IAM role' dropdown menu is open, showing several options: None, aws-elasticbeanstalk-ec2-role, EMR_EC2_DefaultRole, and PythonInEC2AccessS3. The PythonInEC2AccessS3 option is highlighted with a red box.

3

EC2 MetaData Service

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

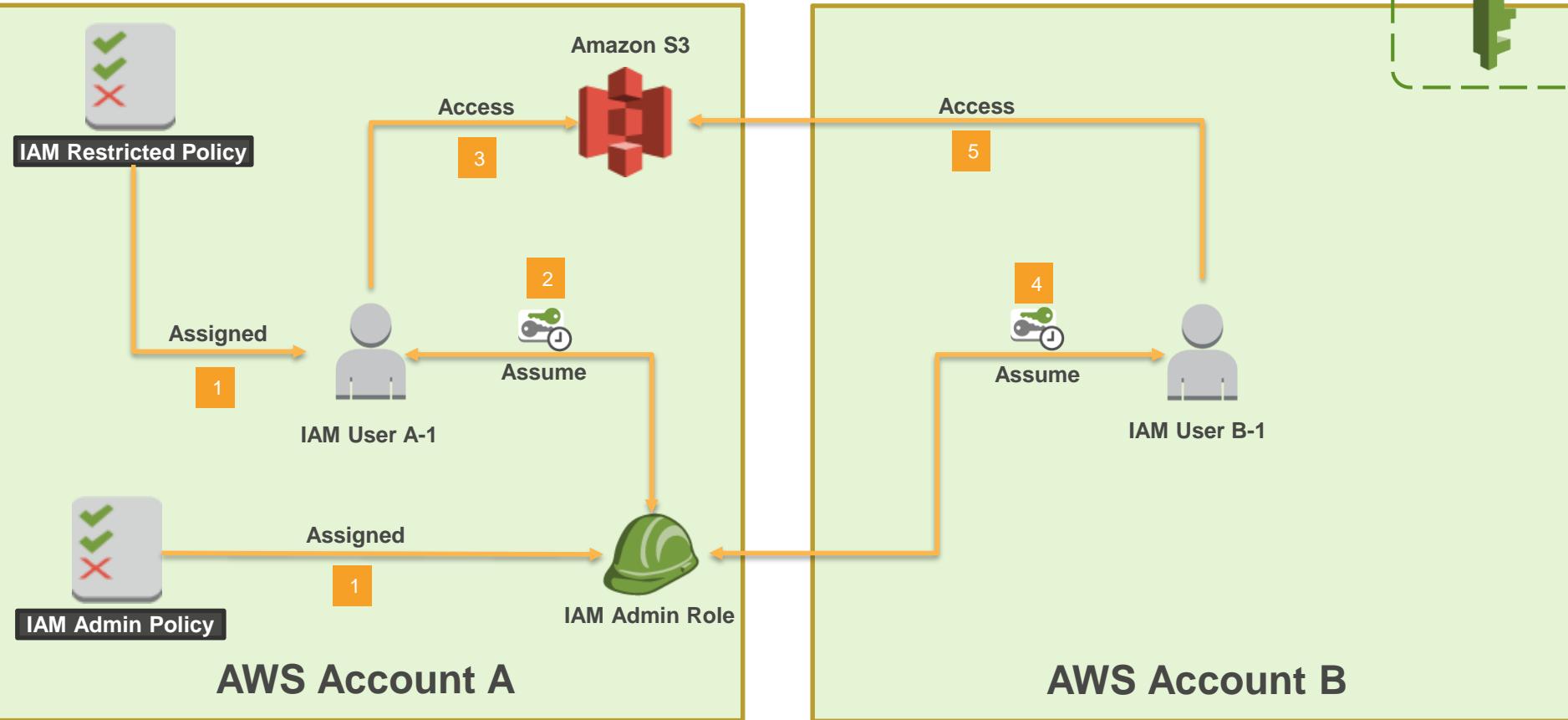
Amazon S3



Application interacts with S3

4

AWS IAM Roles – Assume Role



Temporary Security Credentials (AWS STS)



Session
Access Key ID
Secret Access Key
Session Token
Expiration

Temporary Security Credentials
15 minutes to 36 hours



Use Cases

- Cross account access
- Federation
- Mobile Users
- Key rotation for Amazon EC2-based apps

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



IAM User



IAM Group



IAM Roles

Authorization

- Policies

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.**



AWS IAM Best Practices (cont.)

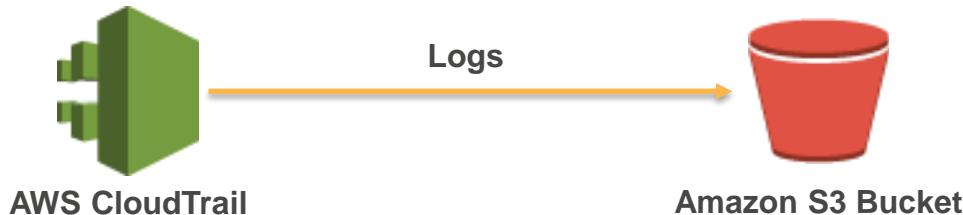


- Use **roles for applications** that run on Amazon EC2 instances.
- Delegate by **using roles** instead of by sharing credentials.
- **Rotate credentials** regularly.
- **Remove unnecessary** users and credentials.
- Use **policy conditions** for extra security.
- **Monitor activity** in your AWS account.

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.



Knowledge Check

Q: Your **web application** needs to **read/write** an Amazon DynamoDB table and an Amazon S3 bucket. This operation requires **AWS credentials** and **authorization to use AWS services**. What IAM entity should be used?

User

Group

Role

Policy

Instructor Demo

IAM

Module 4

Databases

2



Training and
Certification

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

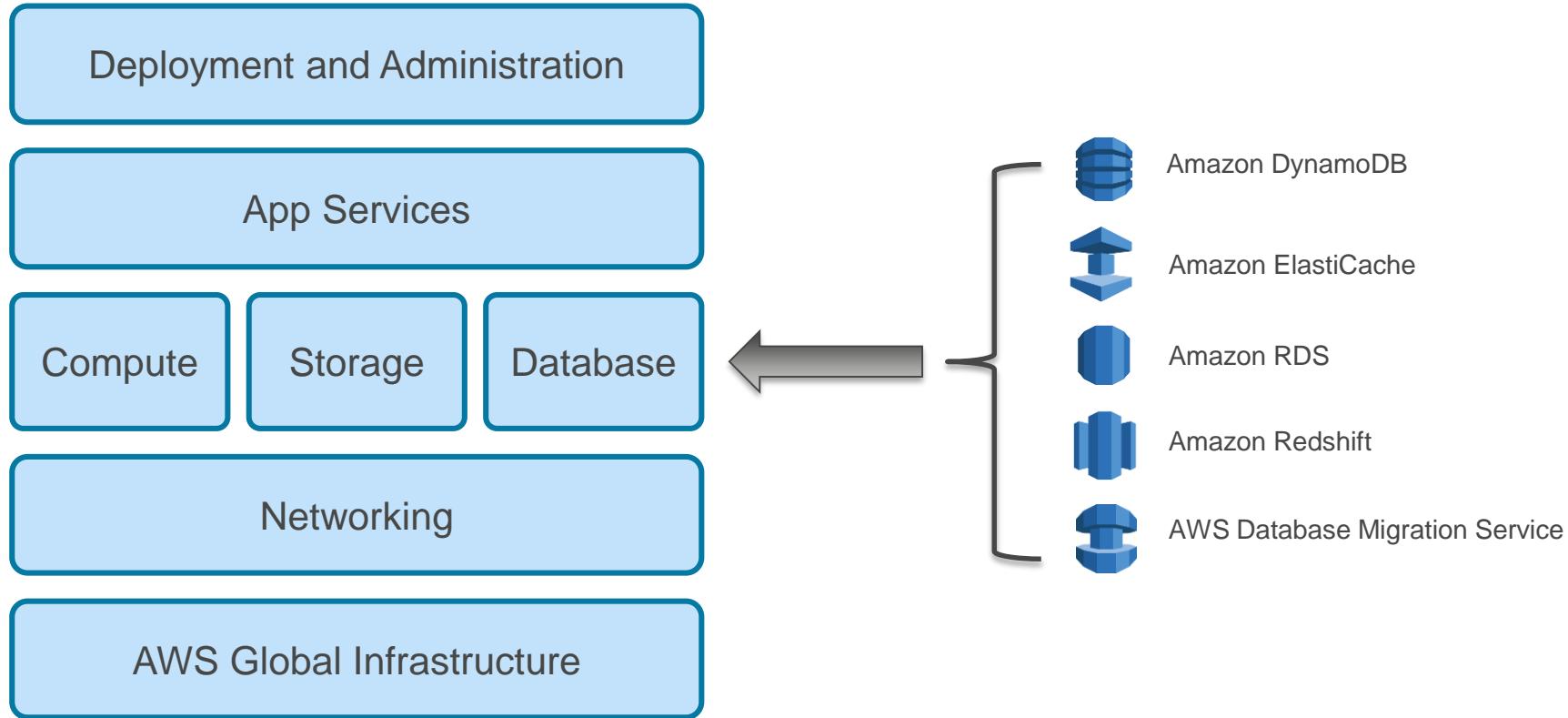
NoSQL

```
{  
    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



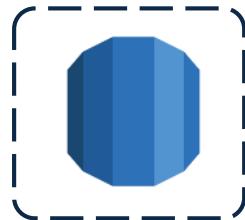
Amazon Relational Database Service (RDS)



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

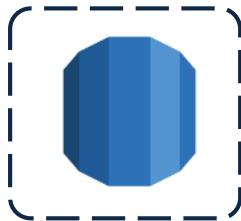
Amazon RDS



- 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

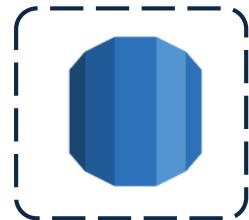


DB Instances



- 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:

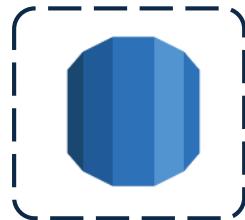
- Restore your database to a point in time.
- Are enabled by default.
- Let you choose a retention period up to 35 days.



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.

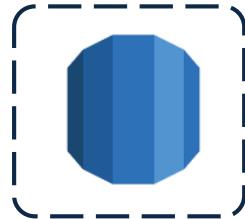
Cross-Region Snapshots



- 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.

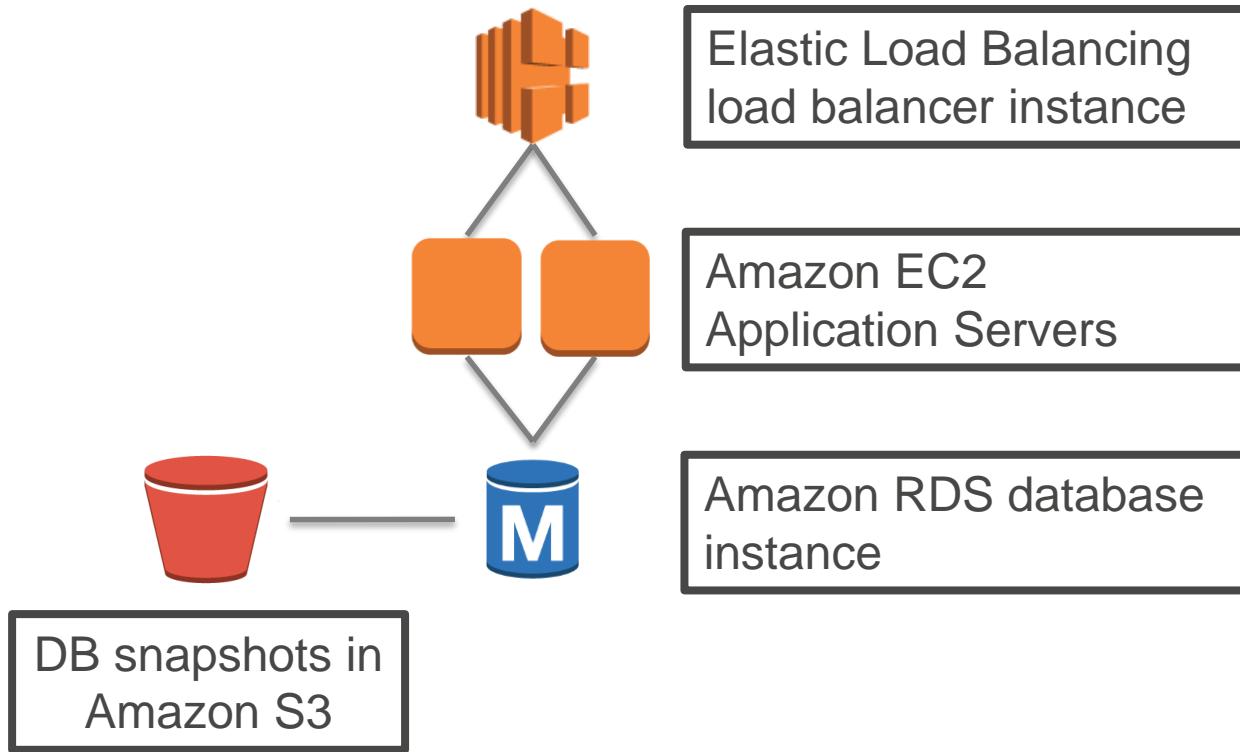
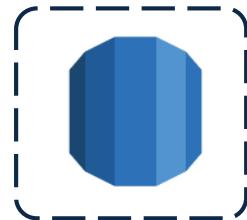


Amazon RDS Security

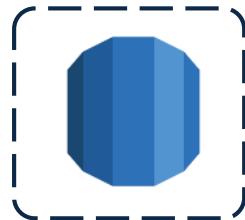


- Run your DB instance in an **Amazon VPC**.
- Use **IAM policies** to grant access to Amazon RDS resources.
- Use **security groups**.
- Use Secure Socket Layer (**SSL**) connections with DB instances (Amazon Aurora, Oracle, MySQL, MariaDB, PostgreSQL, Microsoft SQL Server).
- Use Amazon RDS **encryption**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

A Simple Application Architecture

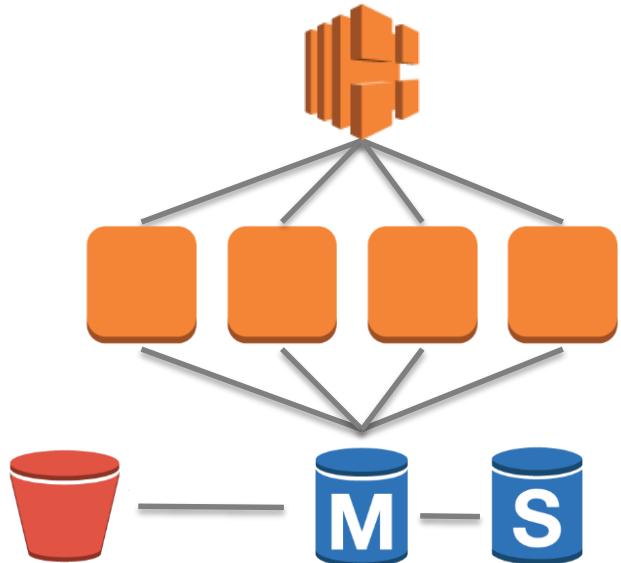
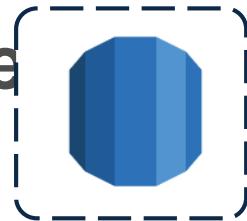


Multi-AZ RDS Deployment



- 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



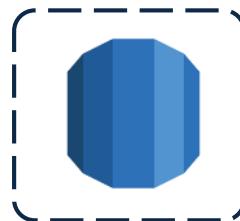
DB snapshots in
Amazon S3

Elastic Load Balancing
load balancer instance

Application, in Amazon
EC2 instances

Amazon RDS database instances:
Master and Multi-AZ standby

Amazon RDS Best Practices



- **Monitor** your memory, CPU, and storage usage.
- Use **Multi-AZ** deployments to automatically provision and maintain a synchronous standby in a different Availability Zone.
- 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).
- If your client application is caching the DNS data of your DB instances, set a TTL of less than 30 seconds.
- **Test failover** for your DB instance.

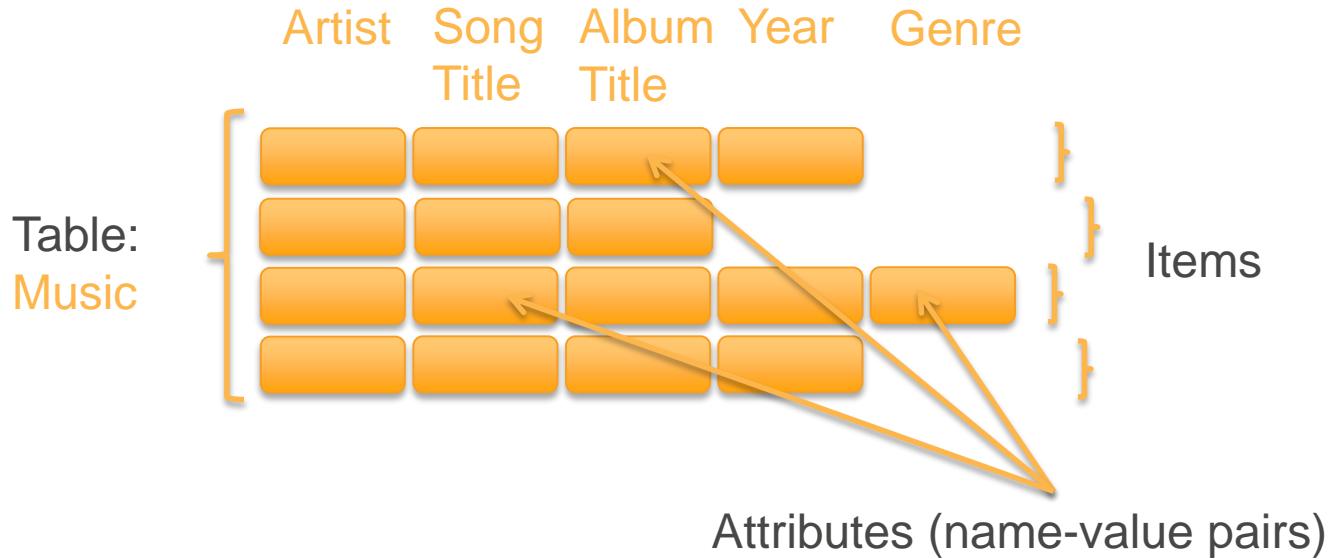
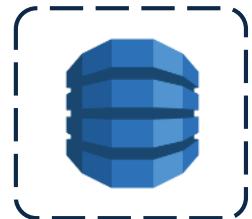
Amazon DynamoDB



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

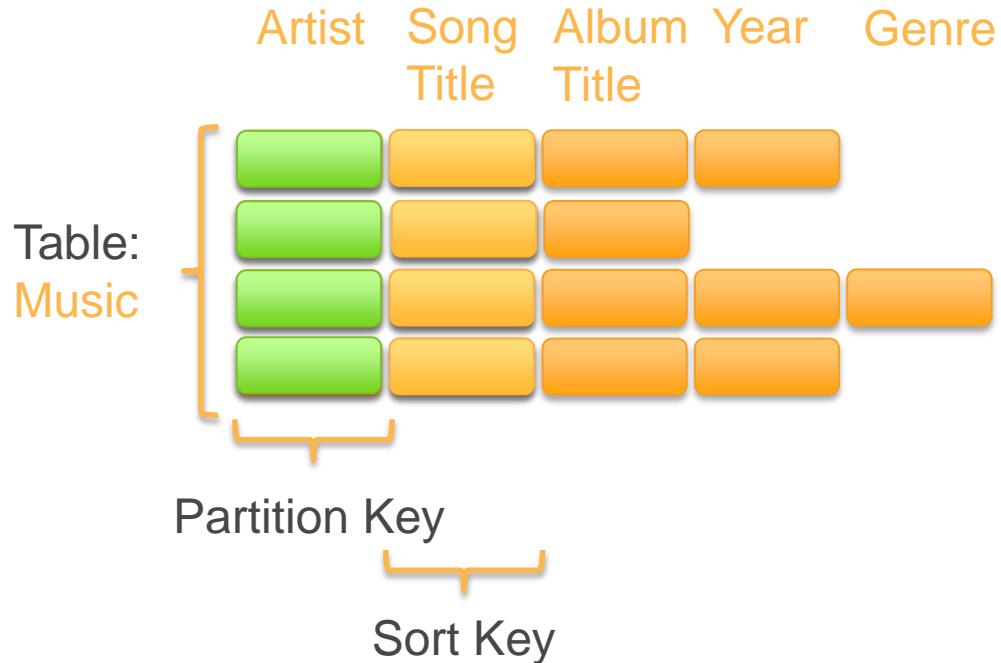
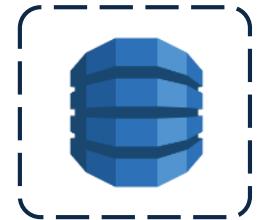


Table: Music
Partition Key: Artist
Sort Key: Song Title

(DynamoDB maintains a sorted index for both keys)

Provisioned Throughput



You specify how much **provisioned throughput capacity** you need for reads and writes.

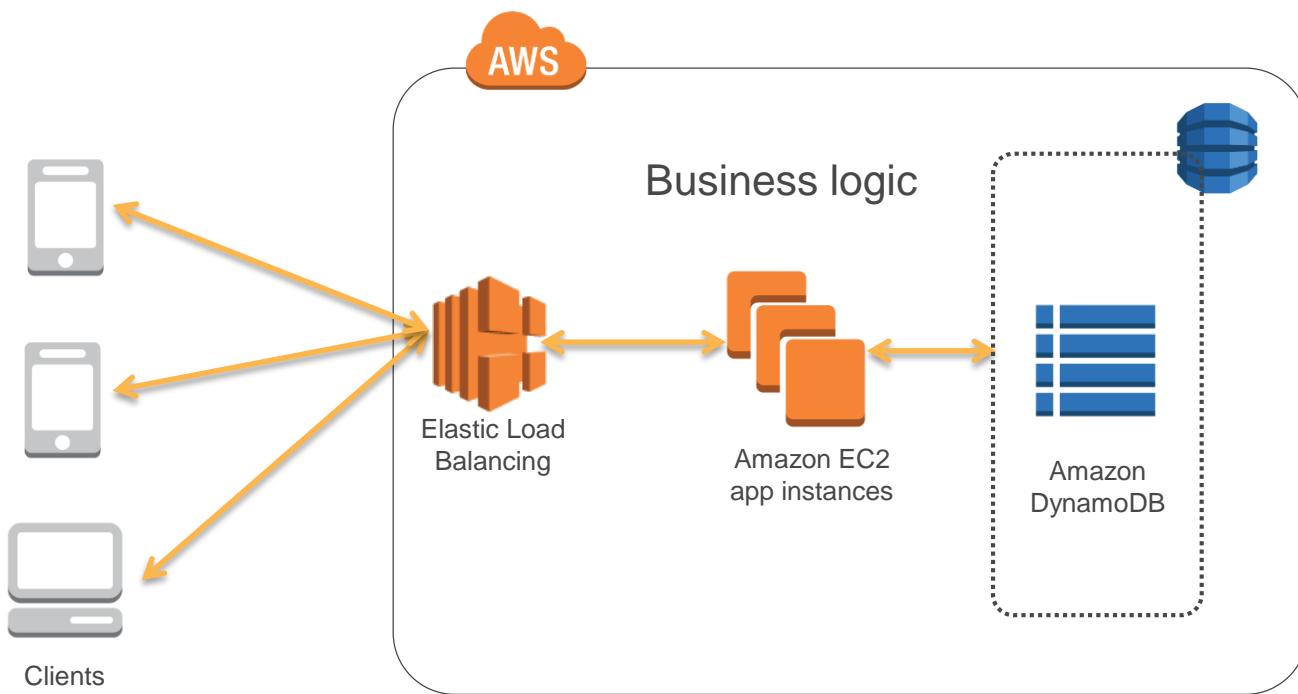
Amazon DynamoDB allocates the necessary machine resources to meet your needs.

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**.
- You can use conditional expressions in both Query and Scan operations.

Simple Application Architecture



Amazon RDS and Amazon DynamoDB

Factors	Relational (Amazon RDS)	NoSQL (Amazon DynamoDB)
Application Type	<ul style="list-style-type: none">Existing database appsBusiness process–centric apps	<ul style="list-style-type: none">New web-scale applicationsLarge number of small writes and reads
Application Characteristics	<ul style="list-style-type: none">Relational data models, transactionsComplex queries, joins, and updates	<ul style="list-style-type: none">Simple data models, transactionsRange queries, simple updates
Scaling	Application or DBA–architected (clustering, partitions, sharding)	Seamless, on-demand scaling based on application requirements
QoS	<ul style="list-style-type: none">Performance—depends on data model, indexing, query, and storage optimizationReliability and availabilityDurability	<ul style="list-style-type: none">Performance—Automatically optimized by the systemReliability and availabilityDurability

Database Considerations

If You Need	Consider Using
A relational database service with minimal administration	Amazon RDS <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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 Amazon EBS that provide scale compute and storage, complete control over instances, and more.

Knowledge Check

Q: What are the basic building blocks of Amazon Relational Database Service (RDS)?

DB Instances

True or False: Amazon DynamoDB allows you to store any amount of data with no limits.

True

True or False: Scan is the most efficient way to retrieve items from a DynamoDB table.

False

Q: You are creating a resilient, durable application using Amazon RDS. In addition to Amazon RDS's automatic backups, what feature should you use to ensure that your backups are durable retained?

Manual Snapshots

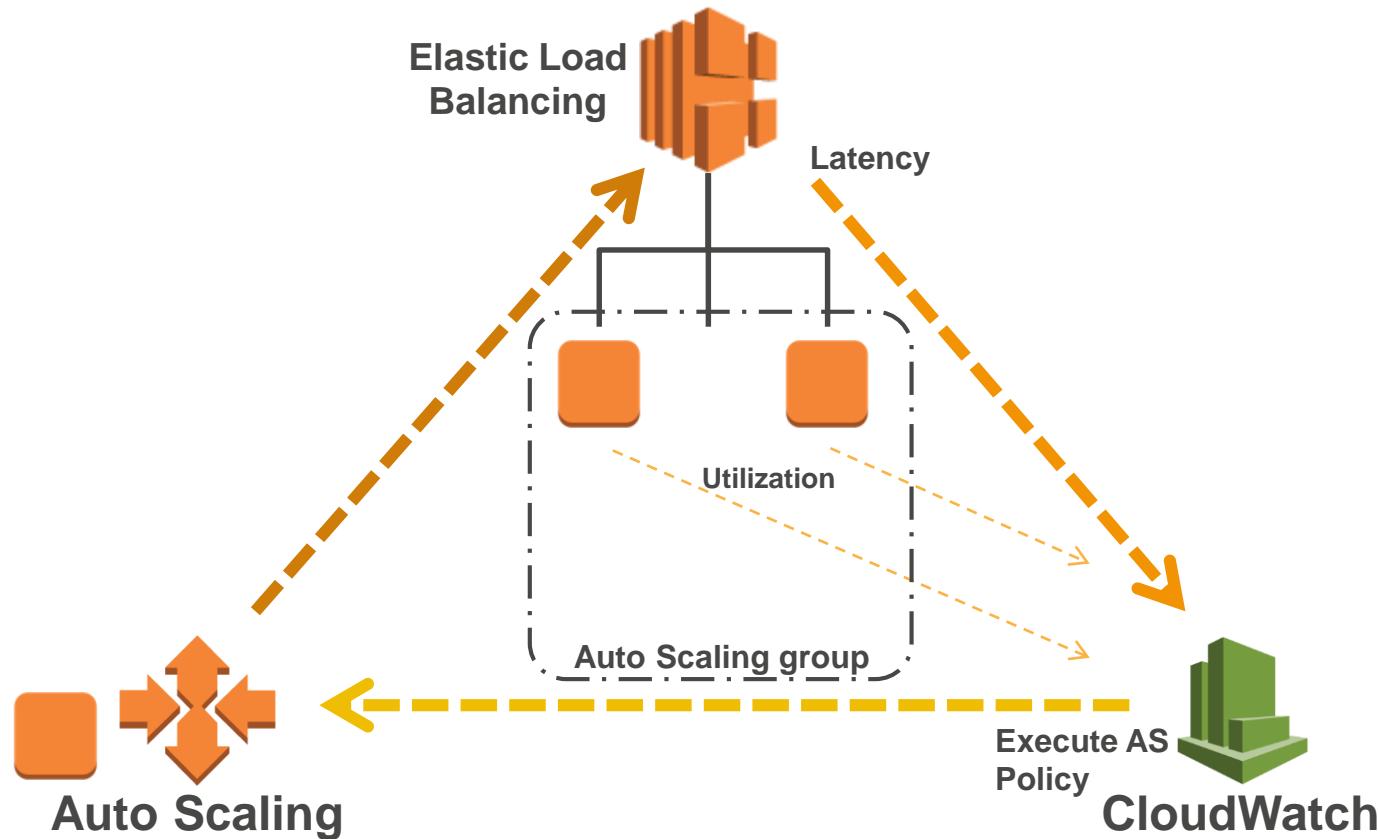
Module 5

AWS Elasticity and Management Tools



Training and
Certification

Triad of Services



Elastic Load Balancing



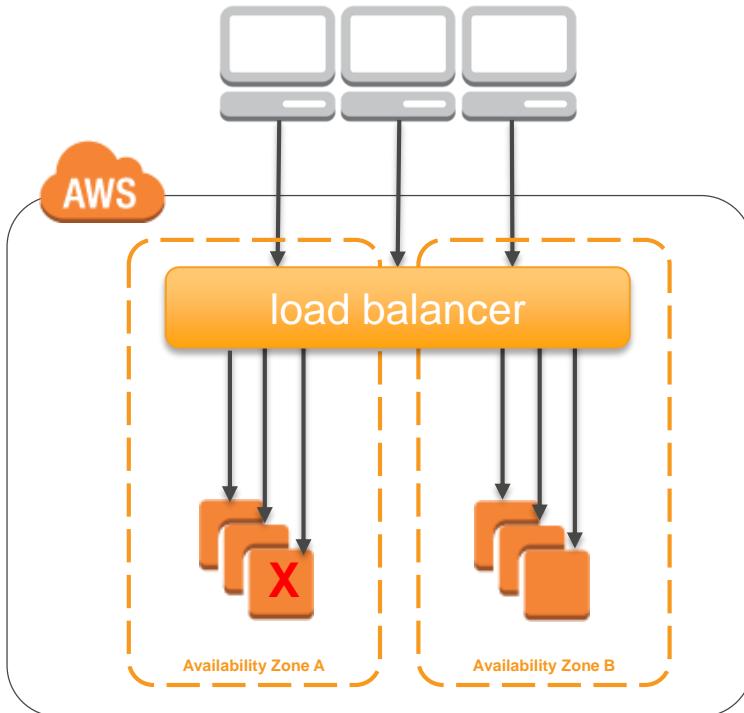
Elastic Load
Balancing

- **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



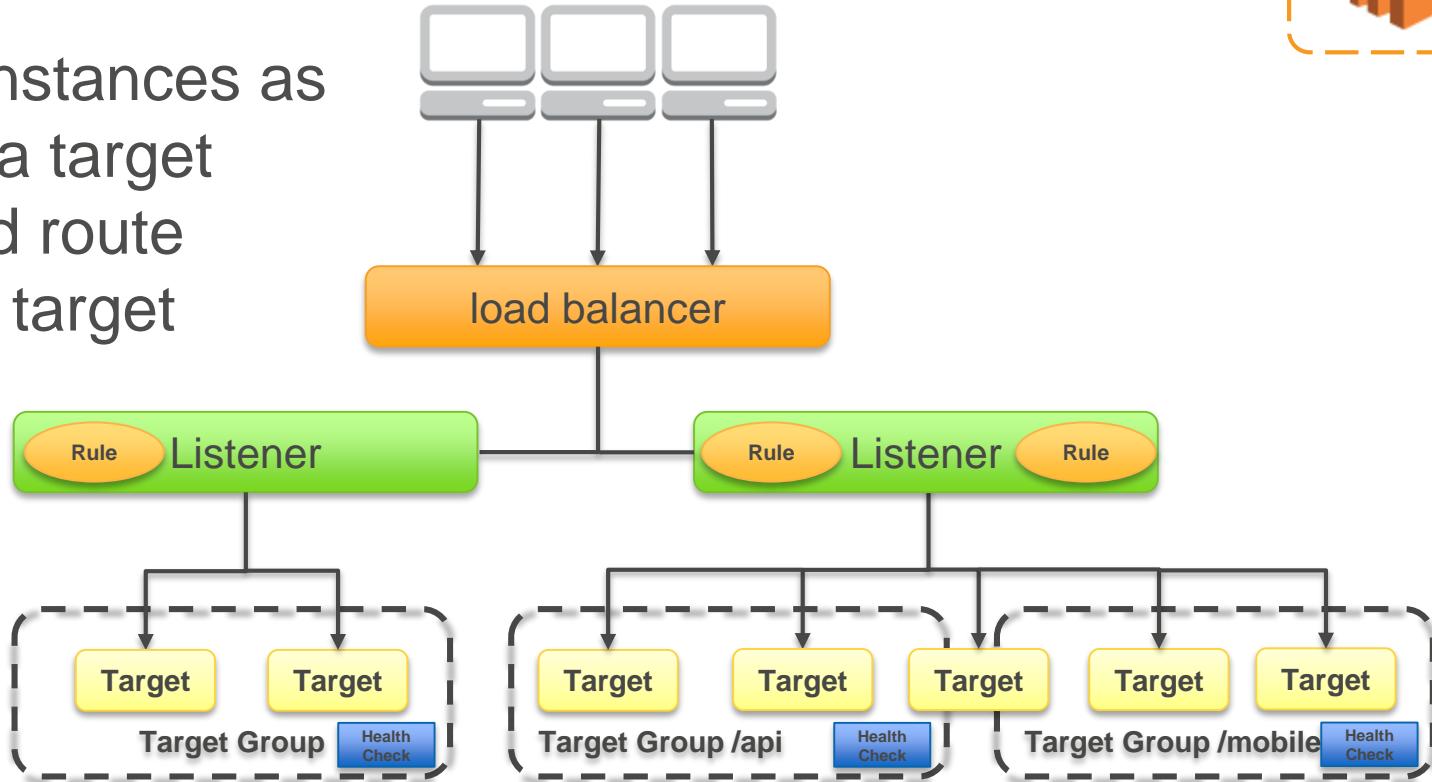
Register instances with your load balancer.



Application Load Balancer – How It Works



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



Load Balancer Comparison



Classic Load Balancer
benefits include support for:

- EC2-Classic.
- VPC.
- TCP and SSL listeners.
- Sticky sessions.

ALB benefits include support for:

- Path-based routing.
- Routing requests to multiple services on a single EC2 instance.
- Containerized applications.
- Monitoring the health of each service independently.

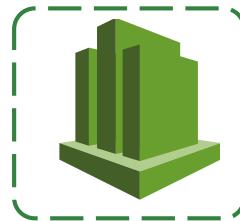
Amazon CloudWatch



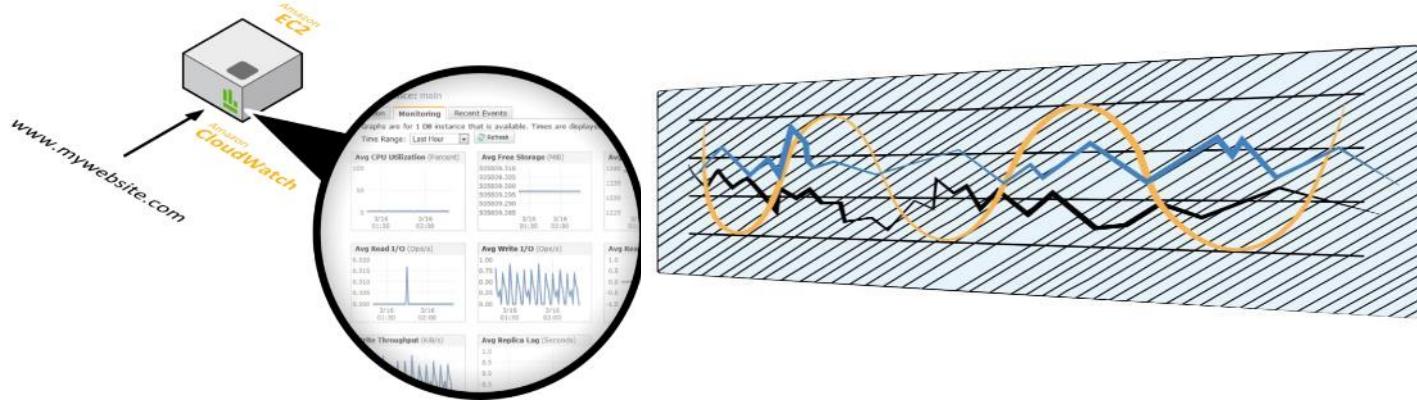
Amazon
CloudWatch

- 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

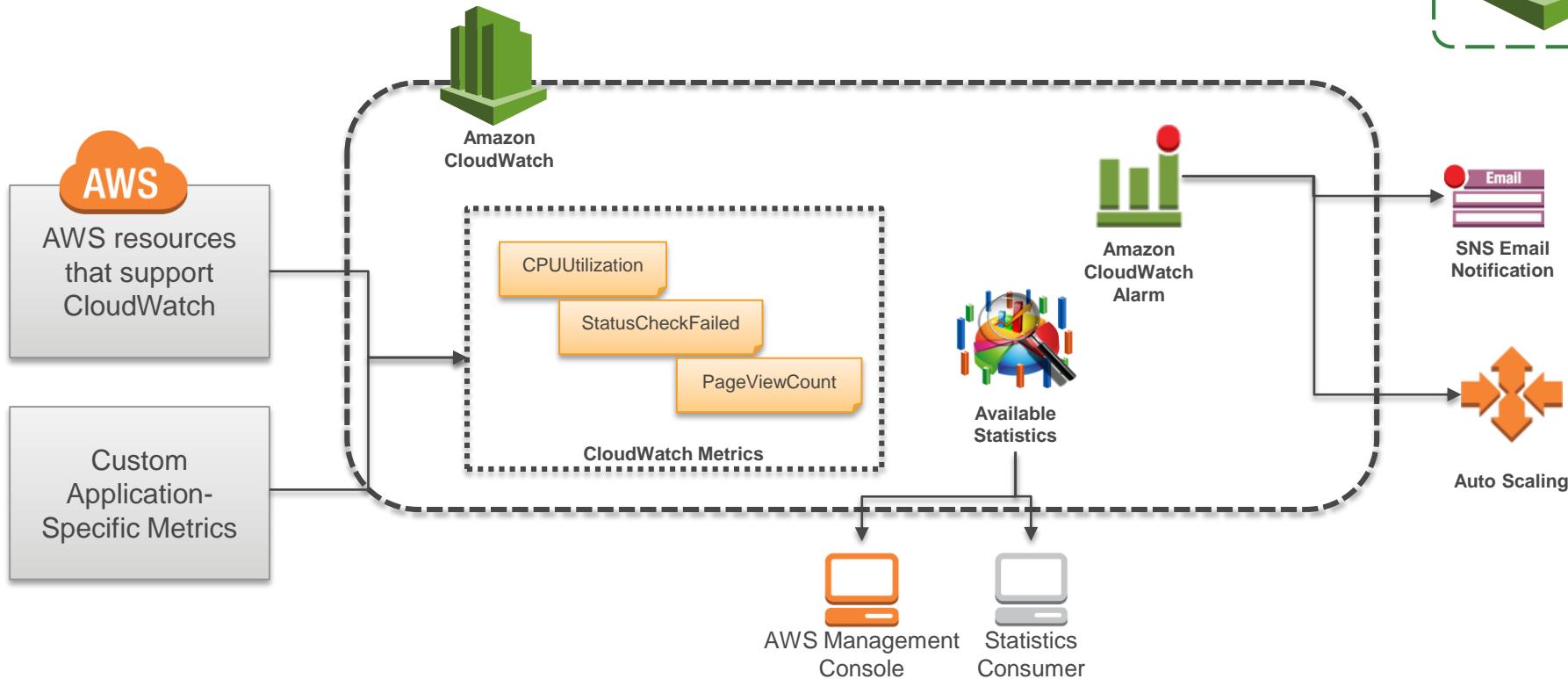
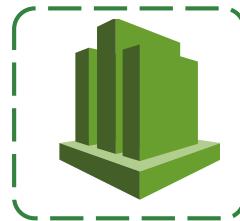
Amazon CloudWatch Facts



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



Amazon CloudWatch Architecture



CloudWatch Metrics Examples



CloudWatch Metrics by Category

Your CloudWatch metric summary has loaded. Total metrics: 97

EBS Metrics: 24

Per-Volume Metrics: 24

EC2 Metrics: 38

Per-Instance Metrics: 38

S3 Metrics: 18

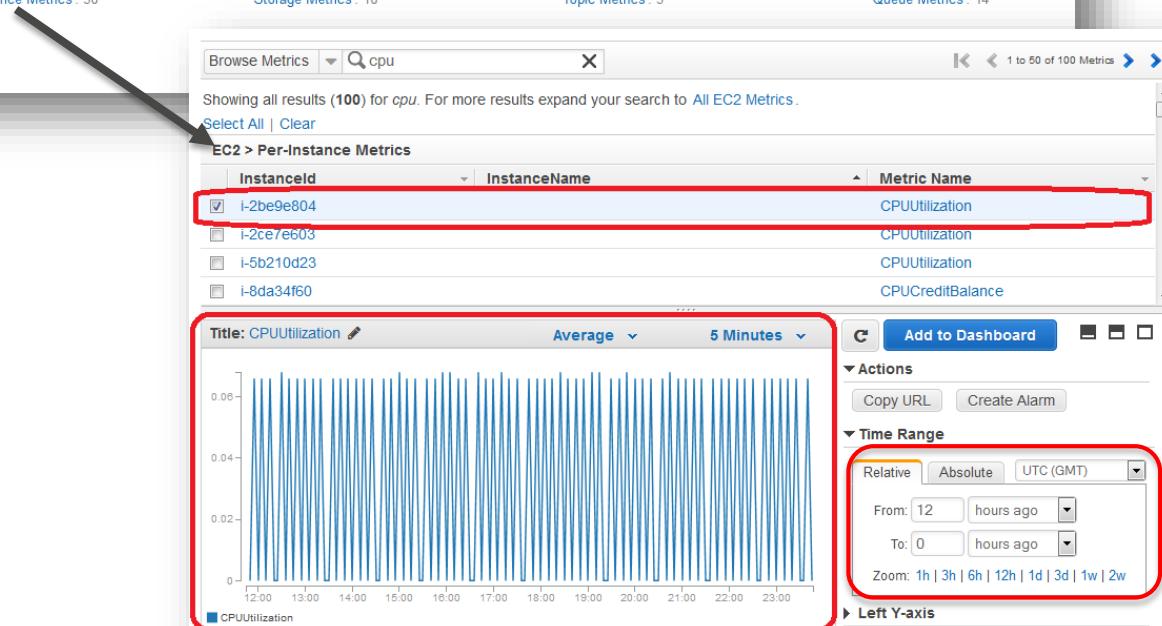
Storage Metrics: 18

SNS Metrics: 3

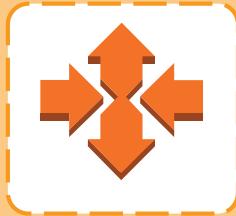
Topic Metrics: 3

SQS Metrics: 14

Queue Metrics: 14



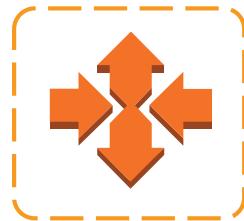
Auto Scaling



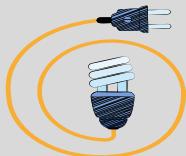
Auto
Scaling

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

Auto Scaling Benefits



Better Fault Tolerance



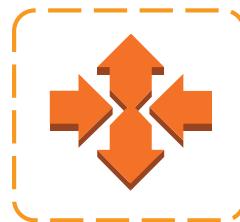
Better Availability



Better Cost Management



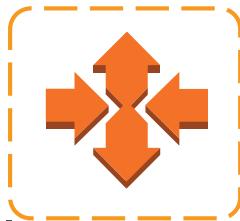
Launch Configurations



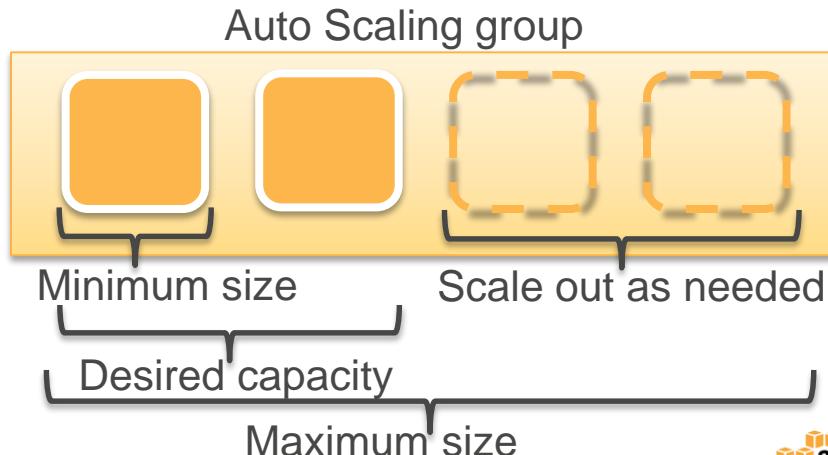
- A **launch configuration** is a template that an Auto Scaling group uses to launch EC2 instances.
- When you create a launch configuration, you can specify:
 - AMI ID
 - Instance type
 - Key pair
 - Security groups
 - Block device mapping
 - User data



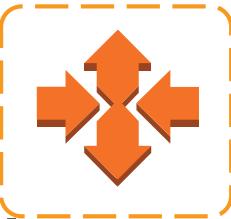
Auto Scaling Groups



- 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.

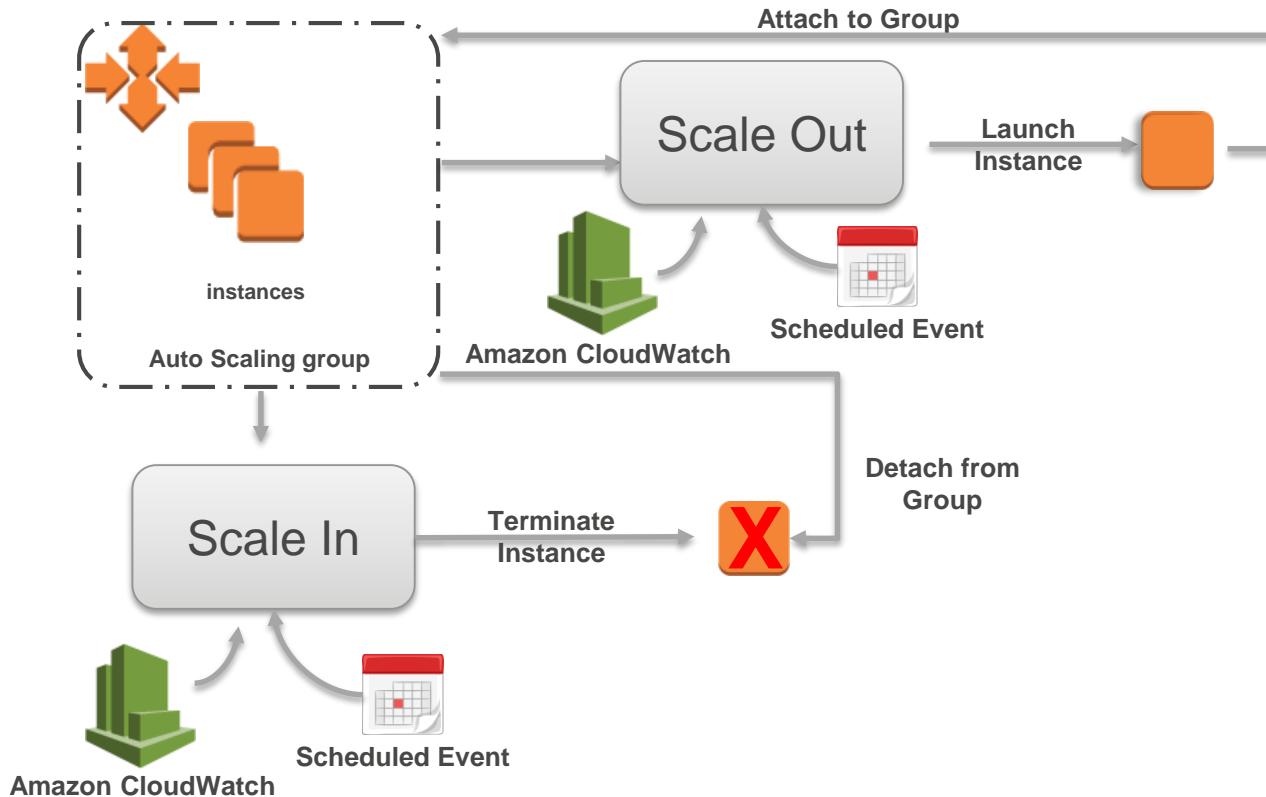
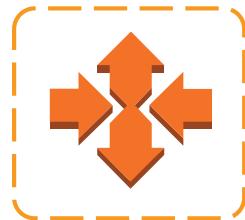


Dynamic Scaling



- 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 toot 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

Knowledge Check

True or False: Auto Scaling helps you ensure that you have the correct number of EC2 instances available to handle the load for your application.

True

Q: What feature would you use with an auto scaling policy to determine when your auto scaling group should scale out/in?

Amazon CloudWatch alarms

Q: You have an application composed of individual services and need to route a request to a service based on the content of the request. What type of load balancer should you use?

Application Load Balancer

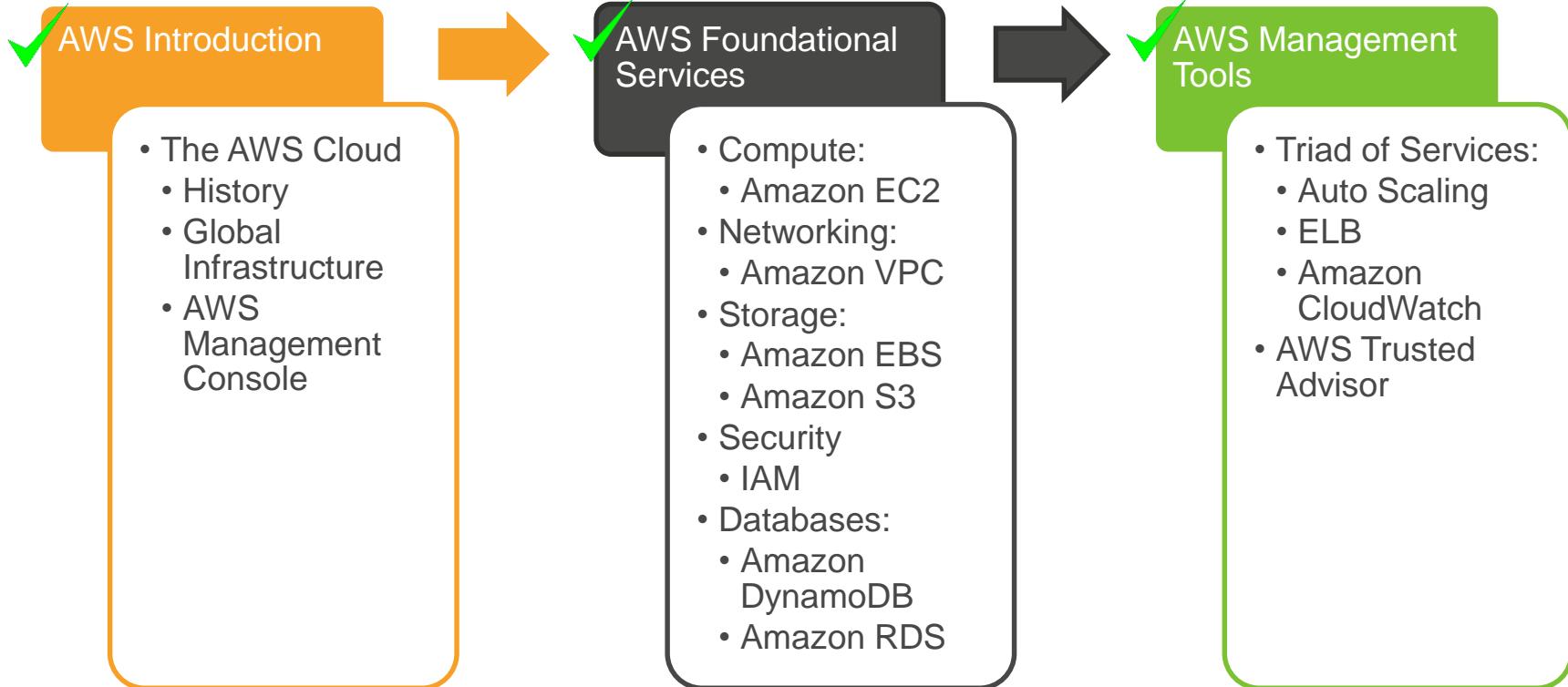
Q: Which AWS service serves as a best practice and recommendation engine?

AWS Trusted Advisor

Module 6

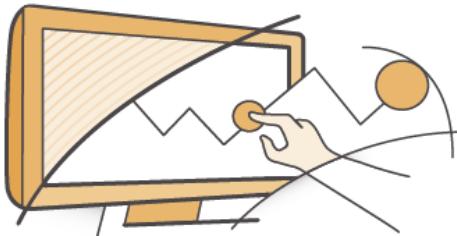
Course Wrap-Up

Learning Path



Expand Your Cloud Skills with AWS

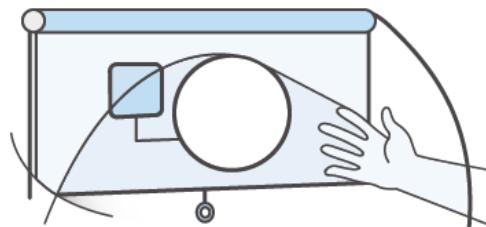
Online videos and labs



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)

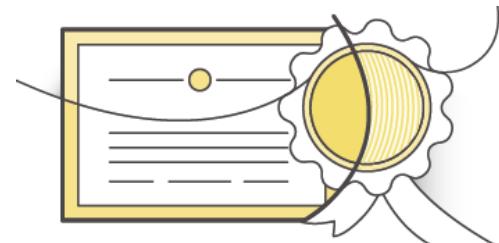
Instructor-led courses



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

aws.amazon.com/training

Certification



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

aws.amazon.com/certification

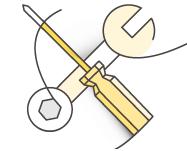
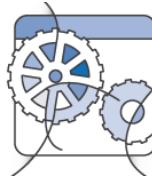
Self-Paced Labs

- 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/.

AWS ILT Training Courses



Introductory
courses

AWS Technical Essentials

1 day

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

Data Warehousing on AWS

3 days

Big Data on AWS

3 days

Taking AWS Operations to the Next Level

1 day

Securing Next-Gen Applications at Cloud Scale

1 day

Building a Recommendation Engine on AWS

1 day

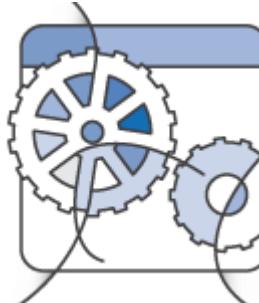
Running Container-Enabled Microservices on AWS

1 day

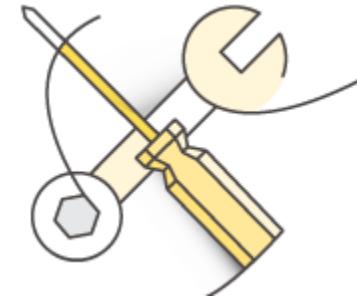
AWS Certification



AWS Certified Solutions
Architect - Associate



AWS Certified
Developer - Associate



AWS Certified SysOps
Administrator- Associate

AWS Certified Solutions
Architect - Professional

AWS Certified DevOps Engineer - Professional

For more information, see aws.amazon.com/certification.

Benefits of AWS Certification

Individual

- Demonstrate expertise
- Stand out
- Industry visibility
- Customer visibility
- Peer recognition
- Credibility with customers

Employer

- Baseline bar on AWS skills
- Identify expert talent
- Leverage best practices
 - Reduce operational risk
 - Increase business advantage
 - Maximize AWS efficiencies
- Common vocabulary
- Accelerate time to cloud

Preparing for AWS Certification

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

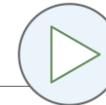
AWS Support

Support Options



The Technical Account Manager provides...

- ✓ A dedicated **voice within AWS** to serve as your **advocate**.
- ✓ **Proactive guidance** and **insight** into ways to optimize AWS through business and performance reviews.
- ✓ Orchestration and access to the full **breadth and depth of technical expertise** across the full range of AWS.
- ✓ Access to resources and **best practice recommendations**.



Infrastructure Event Management provides...

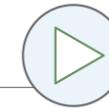
- ✓ A common understanding of event objectives and use cases through **pre-event planning and preparation**.
- ✓ Resource **recommendations** and deployment **guidance** based on anticipated capacity needs.
- ✓ **Dedicated attention** of the your AWS Support team during your event.
- ✓ The ability to immediately **scale down resources** to normal operating levels post-event.

Support Options



The Concierge Service provides...

- ✓ A primary contact to help **manage AWS resources.**
- ✓ **Personalized handling** of billing inquiries, tax questions, service limits, and bulk reserve instance purchases.
- ✓ Direct access to an agent to help **optimize costs**, and identify **underutilized resources**.



AWS Trusted Advisor provides...

- ✓ Insight into how and where you can get the **most impact for your AWS spend.**
- ✓ Opportunities to **reduce your monthly spend** and retain or **increase productivity.**
- ✓ Guidance on getting the **optimal performance and availability** based on your requirements.
- ✓ Confidence that your environment is **secure.**

Cost Optimization



0 0 0

Performance



1 0 0

Security



0 2 0

Fault Tolerance



0 0 0

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 Urgent: < 1 hour High: < 4 hours Normal: < 12 hours Low: < 24 hours	Urgent: < 1 hour High: < 4 hours Normal: < 12 hours Low: < 24 hours	Normal: < 12 hours Low: < 24 hours				
Architecture Support	Application Architecture	Use case guidance	Building blocks				
Best Practice Guidance	✓	✓	✓				
Client-Side Diagnostic Tools	✓	✓	✓				
AWS Support API	✓	✓	Available at additional cost				
Third-Party Software Support	✓	✓					
Infrastructure Event Management	✓						
AWS Concierge	✓						
Direct access to Technical Account Manager (TAM)	✓						
Prioritized Case Routing	✓						
Management Business Reviews	✓						

Module 7

Course Appendix

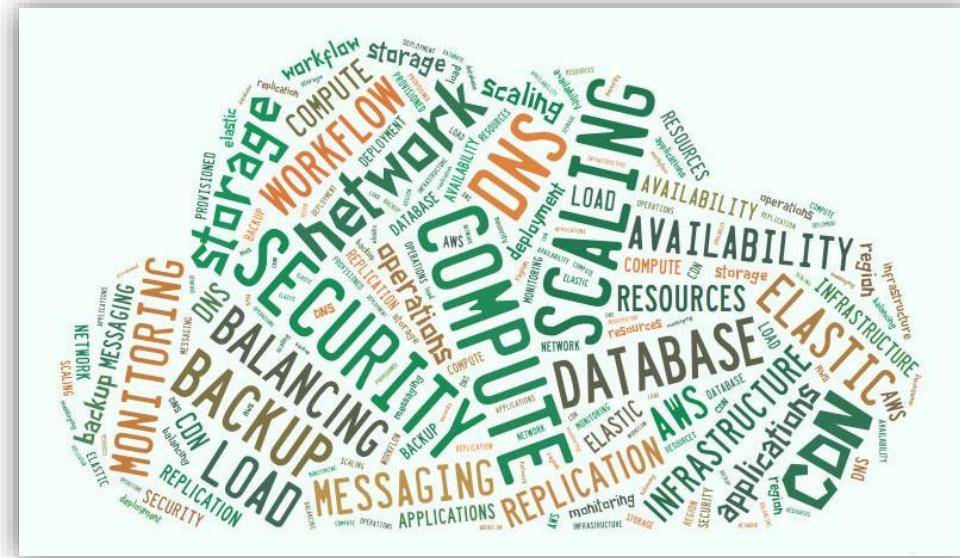
Module 1 Appendix

AWS Introduction and History

Cloud Computing Concepts

What is cloud computing?

Cloud computing is on-demand delivery of IT resources and applications via the Internet with pay-as-you-go pricing.



Essential Characteristics of Cloud Computing

On-Demand Self Services

Broad Network Access

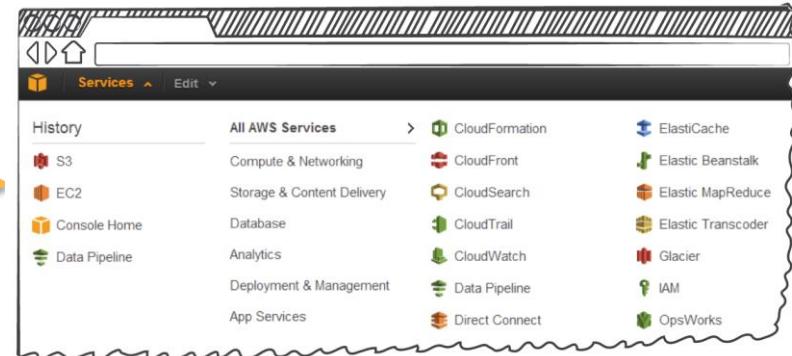
Resource Pooling

Rapid Elasticity

Measured Service

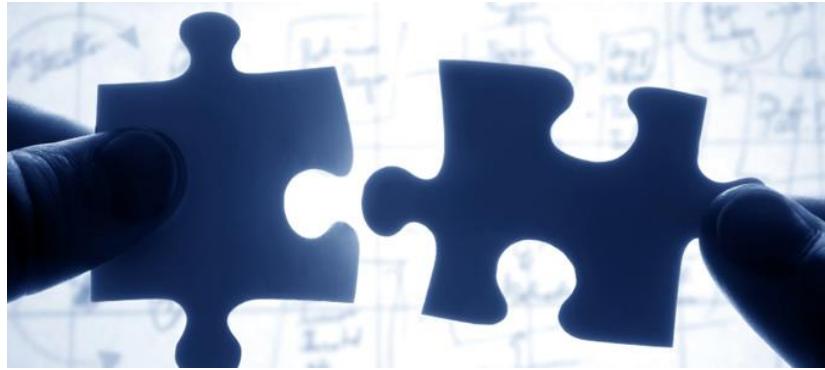
On-Demand Self Services & Broad Network Access

- User provisions computing resources as needed.
- User interacts with cloud service provider through an online control panel.
- Clear solutions are available through a variety of network-connected devices and over varying platforms.



Resource Pooling

Securely separate resources to service multiple customers.



Rapid Elasticity

Resources are quickly scalable and flexible based on business needs.



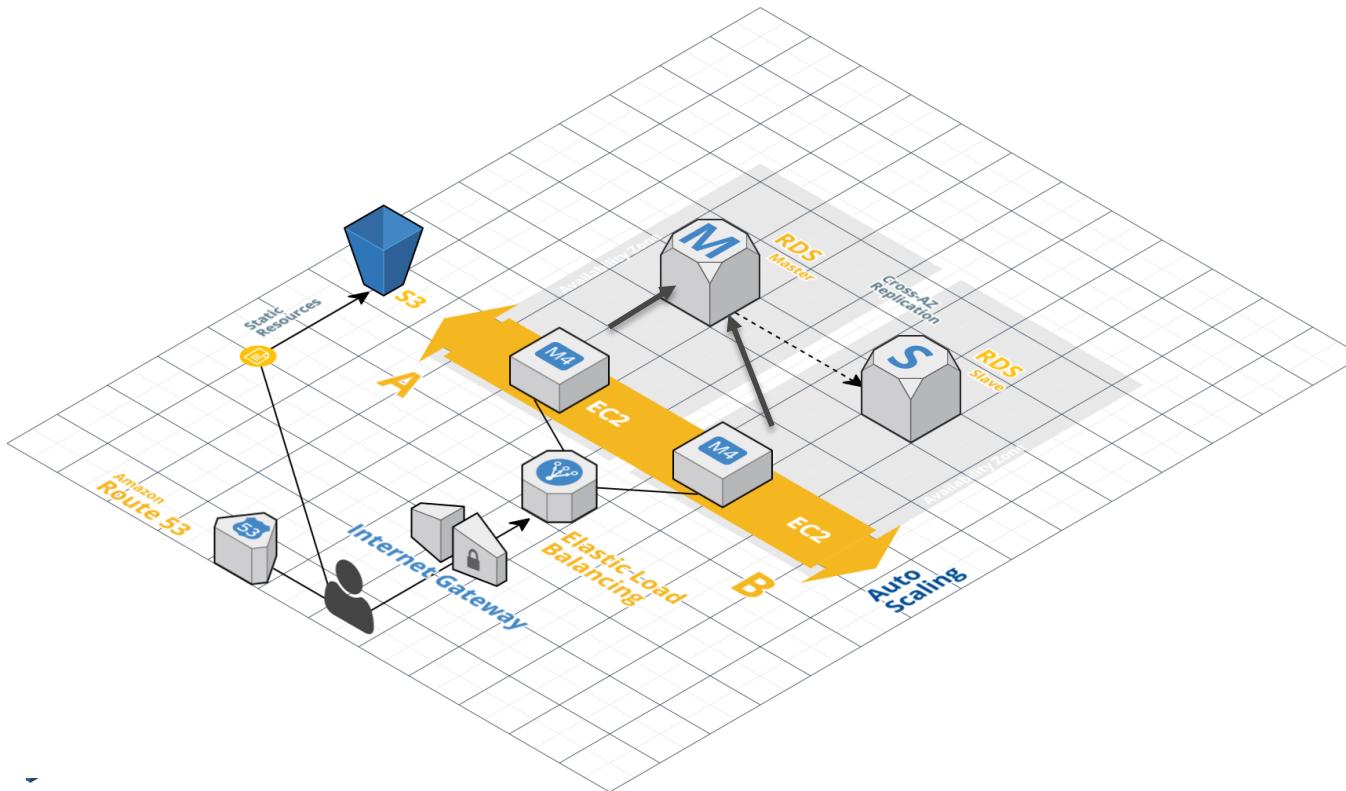
Measured Service

Pay for services as you go.



Electrical services
analog

What Does My AWS Cloud Look Like?



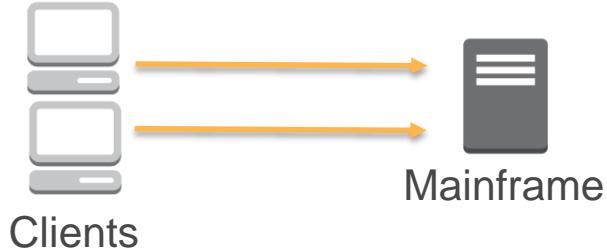
Module 2 Appendix

AWS Foundational Services

Data Center Design Models

Application Design Model

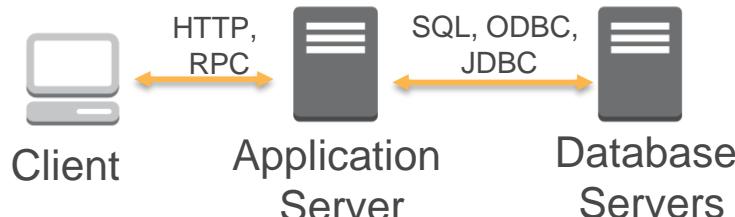
One-Tier Model



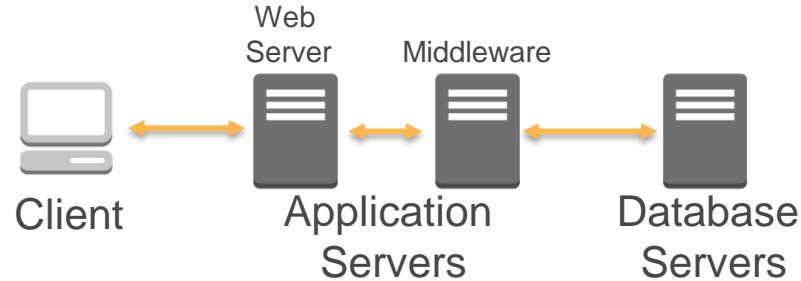
Two-Tier Model



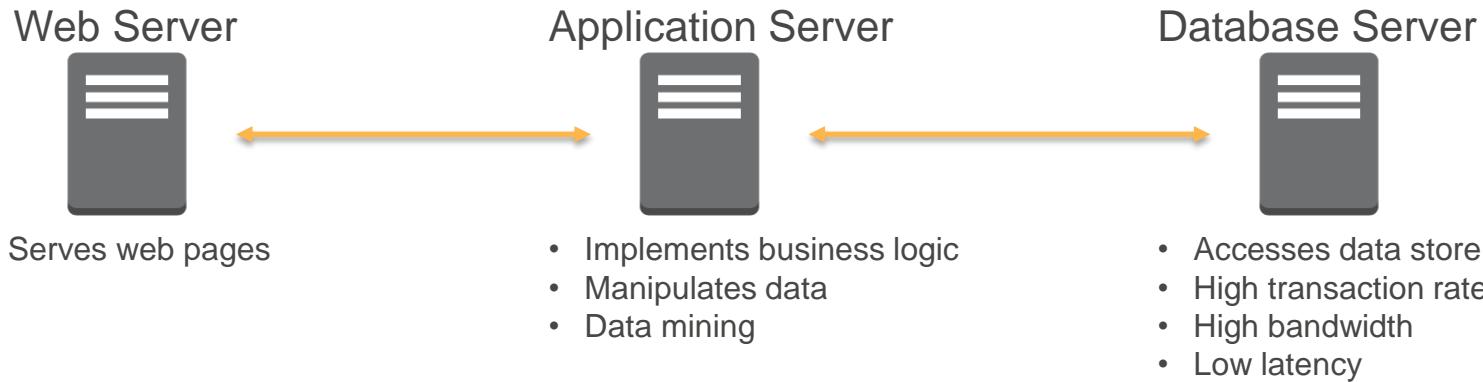
Three-Tier Model



N-Tier Model

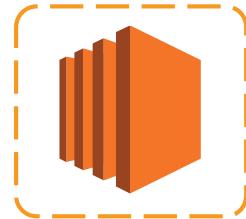


Web Services Model



Amazon EC2

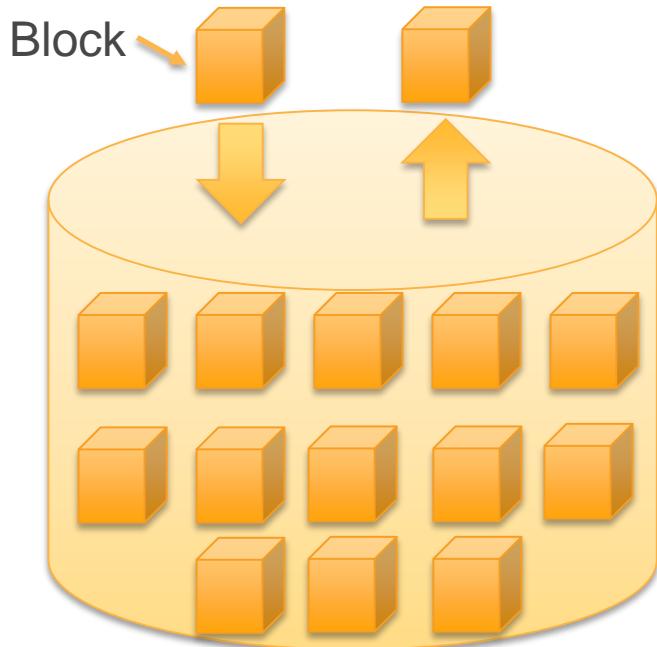
AMI Types - Storage for the Root Device



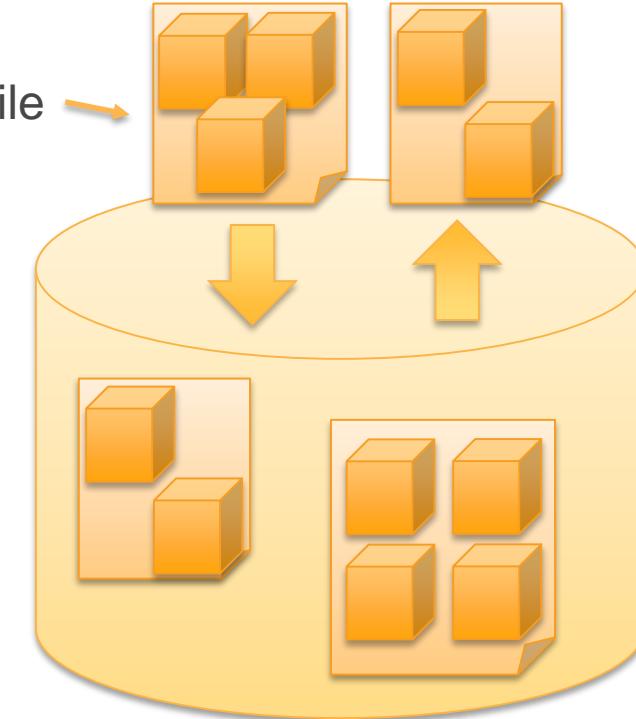
Characteristic	Amazon EBS-Backed	Amazon Instance Store-Backed
Boot time	Usually < 1 minute	Usually < 5 minutes
Size limit	16 TiB	10 GiB
Data persistence	The root volume is deleted when the instance terminates. Data on any other Amazon EBS volumes persists after the instance is terminated.	Data on any instance store volumes persists only during the life of the instance.
Charges	Instance usage, Amazon EBS volume usage, and storing your AMI as an Amazon EBS snapshot.	Instance usage and storing your AMI in Amazon S3.
Stopped state	Can be stopped.	Cannot be stopped.

Storage Concepts and Solutions

Block and File Level Storage

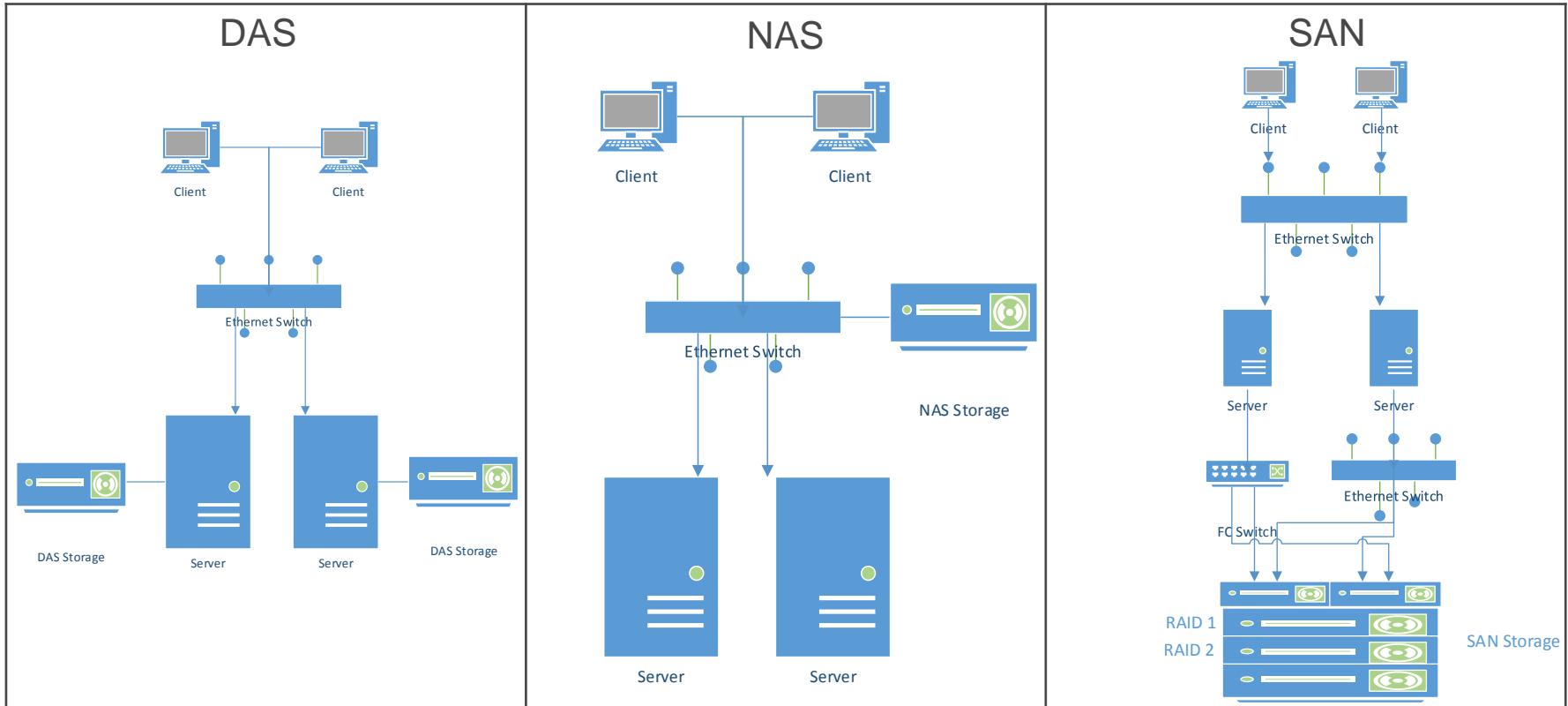


Block Level Storage



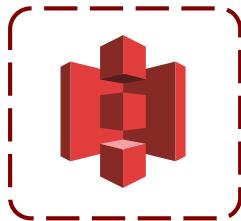
File Level Storage

Storage Technologies



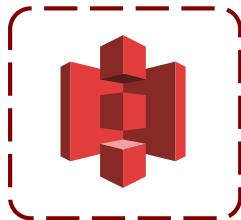
Amazon S3

Amazon S3 Buckets



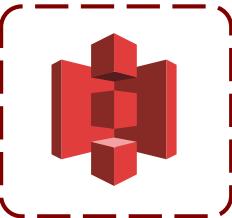
- Organize the Amazon S3 namespace at the highest level.
- Identify the account responsible for storage and data transfer charges.
- Play a role in access control.
- Serve as the unit of aggregation for usage reporting.
- Have globally unique bucket names, regardless of the AWS region in which they were created.

Amazon S3 Region Considerations



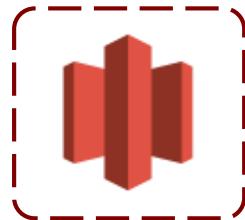
- Amazon S3 creates a bucket in the region you select.
- You can choose a region to:
 - Optimize latency
 - Minimize costs
 - Address regulatory requirements
- Objects stored in a region never leave the region unless you explicitly transfer them to another region.

Amazon S3 Objects

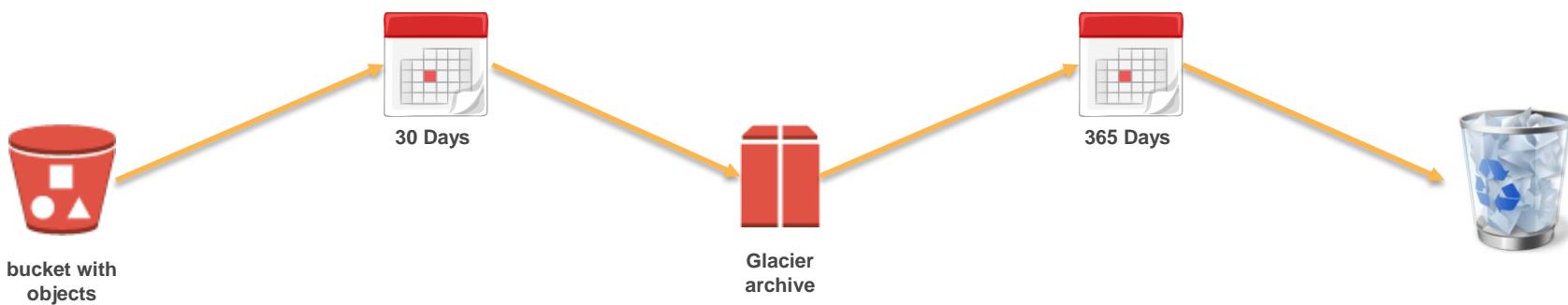


- Objects are the fundamental entities stored in Amazon S3.
- When using the console, you can think of them as files.
- **Objects consist of data and metadata.** The data portion is opaque to Amazon S3. The metadata is a set of name-value pairs that describe the object.
 - Default metadata such as the date last modified
 - Standard HTTP metadata such as Content-Type
 - Custom metadata at the time the object is stored
 - A key that uniquely identifies as object within its bucket

Amazon S3 + Amazon Glacier

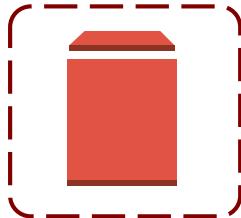


S3 Lifecycle policies allow you to delete or move objects based on age and set rules per S3 bucket.



Amazon EBS

EBS Performance



EBS Magnetic

- 40-200 IOPS

EBS General Purpose SSD

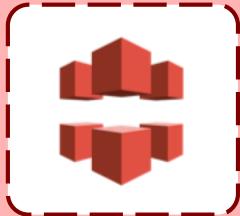
- SSD backed
- 3 IOPS / GB
- Burstable to 3,000 IOPS and up to 10,000 IOPS

EBS Provisioned IOPS SSD

- SSD backed
- Up to 20,000 IOPS consistently
- Up to 320 MB/s throughput

Amazon CloudFront

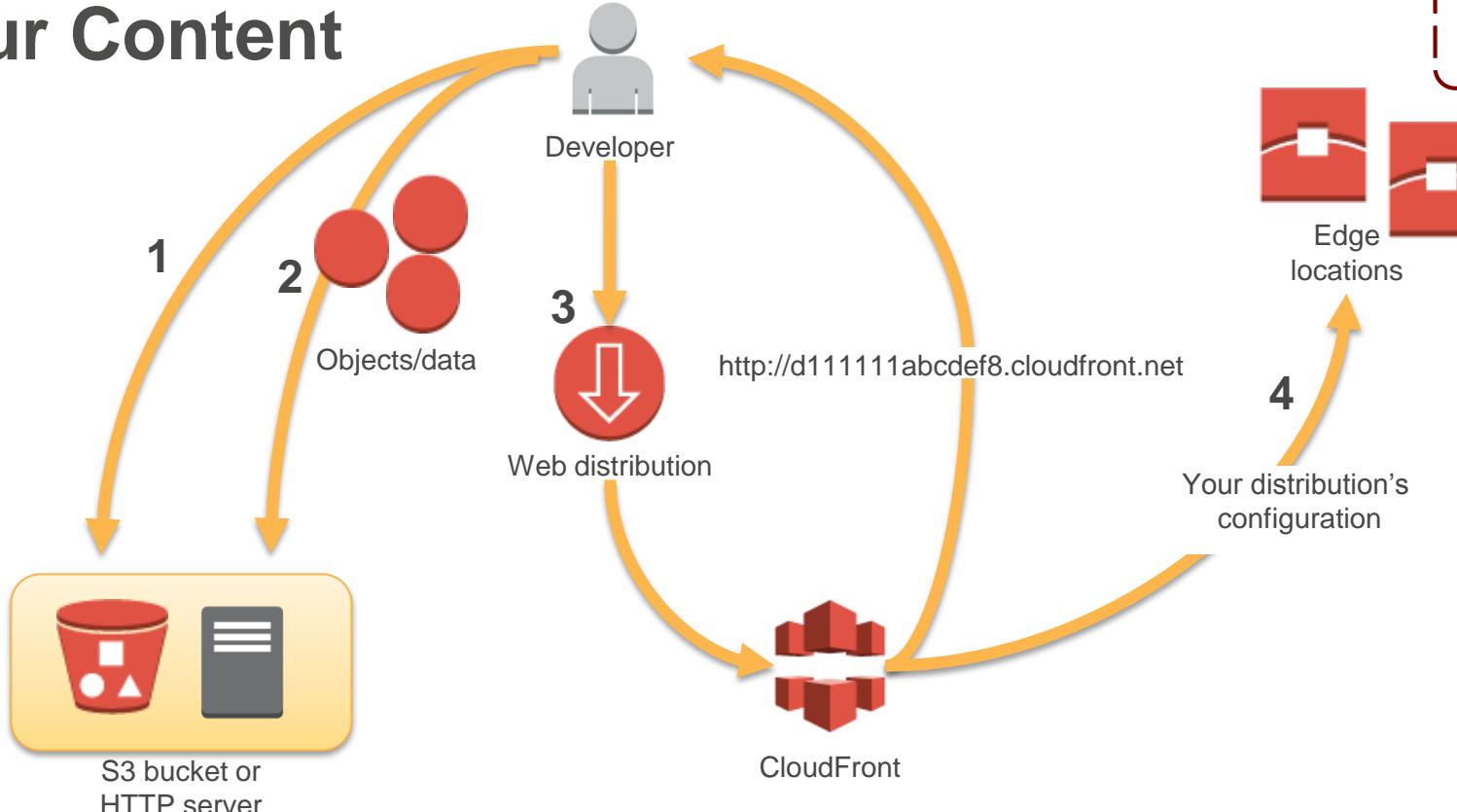
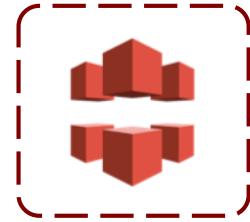
Amazon CloudFront



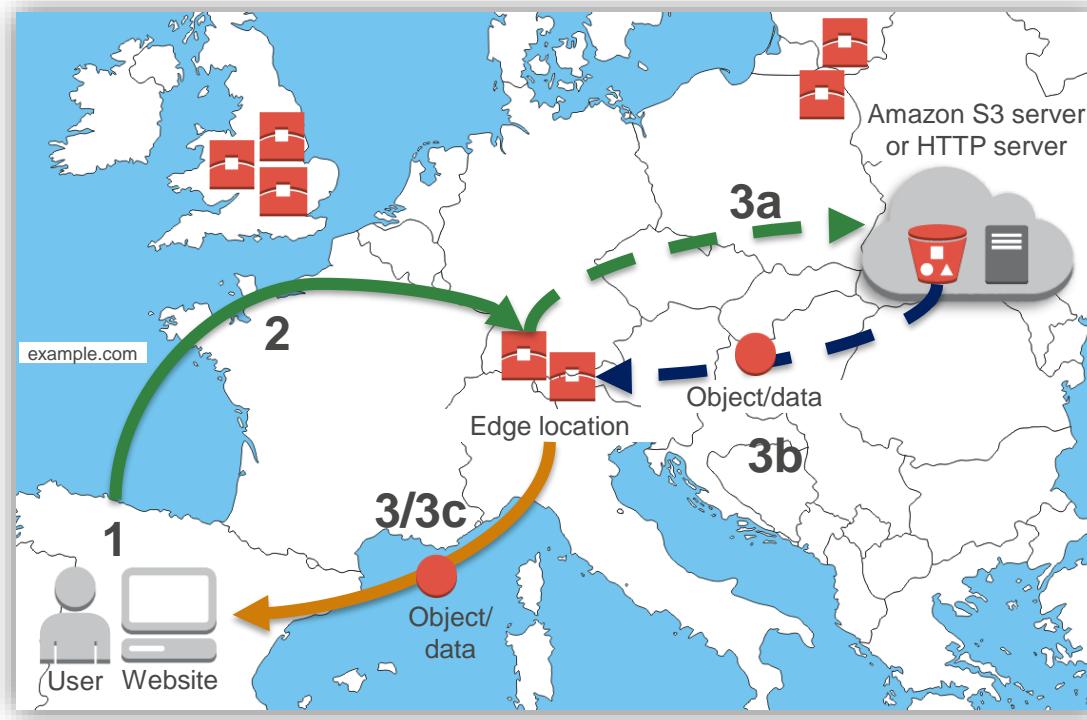
Amazon
CloudFront

- Easy and cost effective way to **distribute content** to end users
- **Low latency, high data transfer speeds**
- Deliver your entire website, including static, dynamic, and streaming content using a global network of edge locations

How You Configure CloudFront to Deliver Your Content



How CloudFront Delivers Content to Your Users



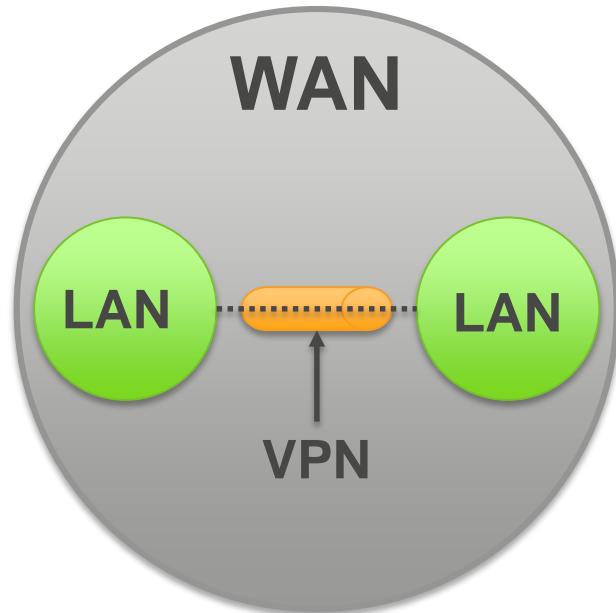
Networking Concepts

What is a Network?

A network is two or more computers linked to share resources, exchange files, or allow electronic communications.

Network Types:

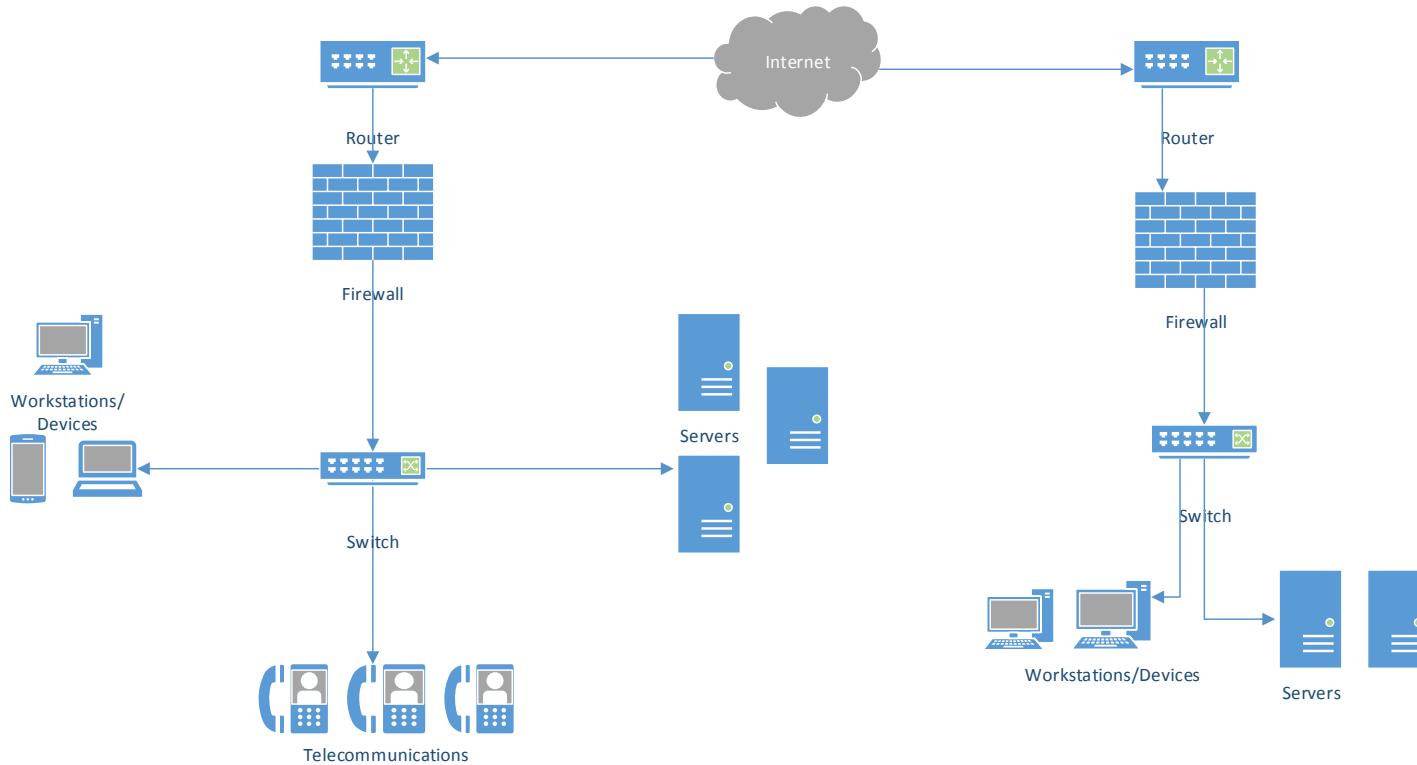
- Local Area Network (LAN)
- Wide Area Network (WAN)
- Virtual Private Network (VPN)



Physical vs. Logical Topology

- A physical topology defines how the systems are physically connected.
- A logical topology defines how the systems communicate across the physical topologies.

Physical Network Hardware/Devices



Amazon VPC

Networking in Your VPC



You can use the following components to configure networking in your VPC:

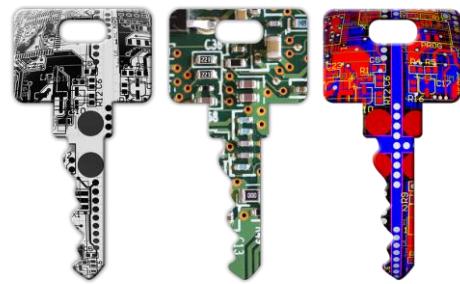
- IP addresses
- Elastic network interfaces
- Route tables
- Internet gateways
- Network Address Translation (NAT)
- Dynamic Host Configuration Protocol (DHCP) options sets
- Domain Name System (DNS)
- VPC peering
- VPC endpoints
- VPC flow logs

Module 3 Appendix

Security, Identity, and Access Management

Data Center Security

Physical & Environmental Security



- Lock your data center.
- Only provide access to those who need it.
- Keep track of access.
- Mount servers on racks with locks.
- Have redundant utilities.
- Build your data center with security in mind.

Network Security

- Identification & Authentication
- Firewalls
- Patching
- Virus Protection
- Encryption

AWS IAM

Advanced Concepts

AWS Resource-Based Policies

- Are an alternative to IAM and supported by some services.
- Grant cross-account access to your resources.
- Use a principal to uniquely identify accounts in the policy.
- Supported AWS services include :
 - Amazon S3 Bucket Policy
 - Amazon SNS Topic Policy
 - Amazon SQS Queue Policy
 - Amazon Glacier Vault Policy
 - AWS OpsWorks Stack Policy
 - AWS Lambda Function Policy

Access to AWS Resources



Temporary Security Credentials

- Security Token Service
- AssumeRole
- AssumeRoleWithSAML
- AssumeRoleWithWebIdentity

AWS Services support for IAM Roles

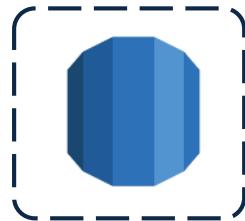


- AWS CLI on Amazon EC2
- AWS CloudTrail logs to Amazon S3
- Amazon Elastic Transcoder access to Amazon S3
- AWS Elastic Beanstalk access to AWS services
- AWS Lambda code access to AWS services
- Many more ...

Module 4 Appendix

Databases

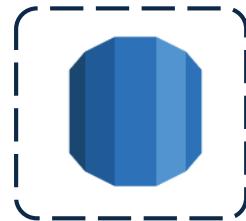
Security Groups



Allow access to IP address ranges or Amazon EC2 instances you specify.

Use VPC security groups to control access to a DB instance inside a VPC.

DB Parameter & Option Groups



DB parameter groups:

- Contain engine configuration values that can be applied to one or more DB instances of the same instance type.
- Are applied by Amazon RDS by default when you create DB instance, which contains defaults for the specific database engine and instance class of the DB instance.

DB option groups:

- Tools that simplify database management.
- Currently available for Oracle, Microsoft SQL Server, and MySQL 5.6 DB instances.

Configuration Details

Engine:	sqlserver-web (11.00.2100.60.v1)
DB Name:	[REDACTED]
Username:	[REDACTED]
Option Group(s):	default:sqlserver-web-11-00 <i>(in-sync)</i>
Parameter Group:	sqsvr-web11-parms (pending-reboot)

Supported Operations



Table Operations:

- Create, update, and delete tables.
- After creation, you can increase or decrease provisioned throughput.
- Retrieve the table's status, the primary key, and when the table was created.
- List all tables in your account for a region.

Item Operations:

- Add, update, and delete items from a table.
- Add, update, and delete existing attributes from an item.
- Perform conditional updates.
- Retrieve a single item or multiple items.

Local Secondary Index

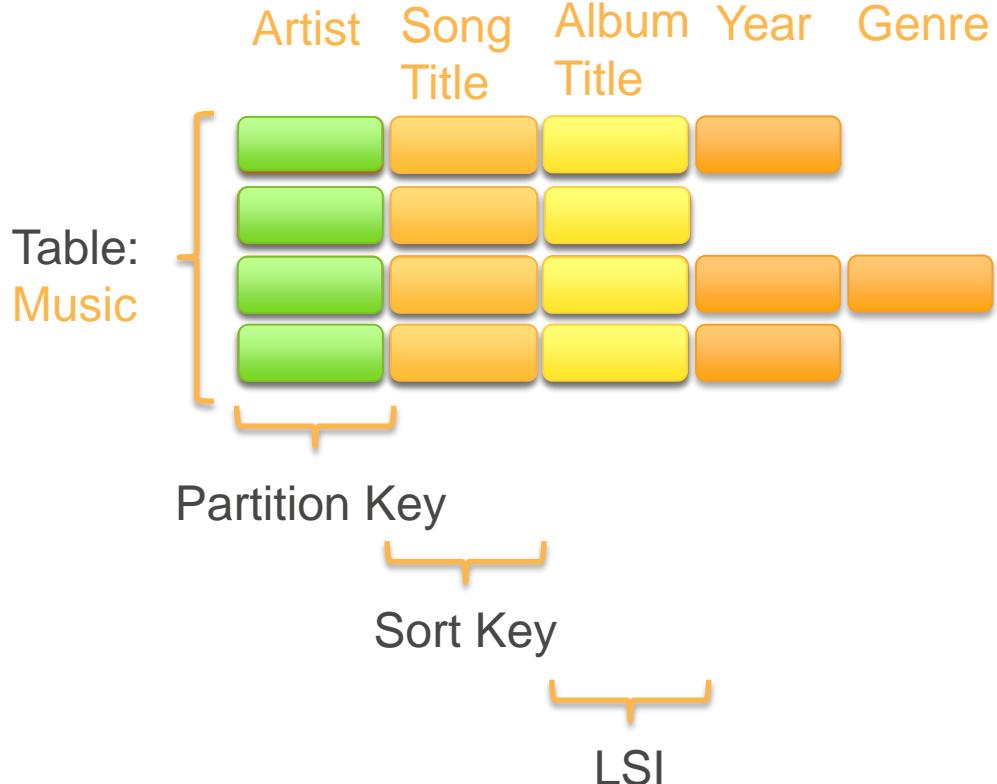


Table: Music
Partition Key: Artist
Sort Key: Song Title
LSI: Album Title

Global Secondary Index

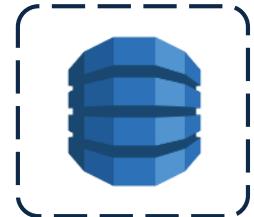


Table:
Music

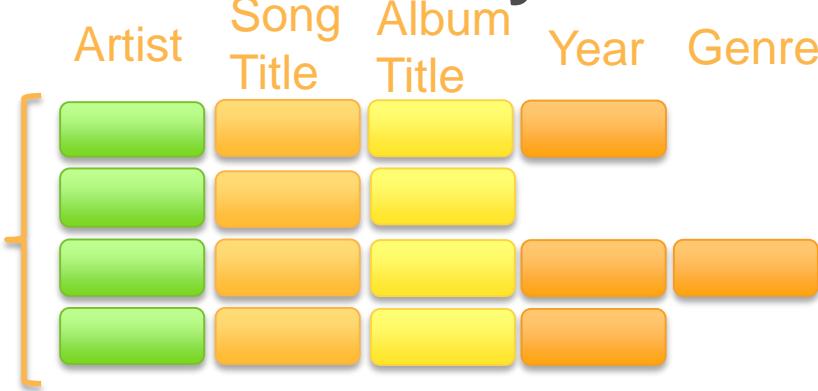
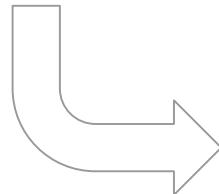


Table: Music
Partition Key: Artist
Sort Key: Song Title



Choose which attributes
to project (if any)

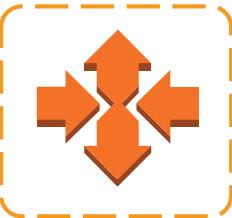
GSI: MusicGSI
Partition Key: Genre
Sort Key: Year

Module 5 Appendix

AWS Elasticity and Management Tools

AutoScaling Advanced Concepts

Scaling Plans



Auto Scaling Minimum

Health Check monitors running instances within an Auto Scaling group.

If an unhealthy instance is found, it can be replaced.

Manual Scaling

Specify a new minimum for your Auto Scaling group.

Manually invoke Auto Scaling policies.

Scheduled Scaling

Scaling functions are performed as a function of time and date.

On Demand Scaling

You create a policy to scale your resources.

Define when to scale using CloudWatch Alarms.

Elastic Load Balancing

Advanced Concepts

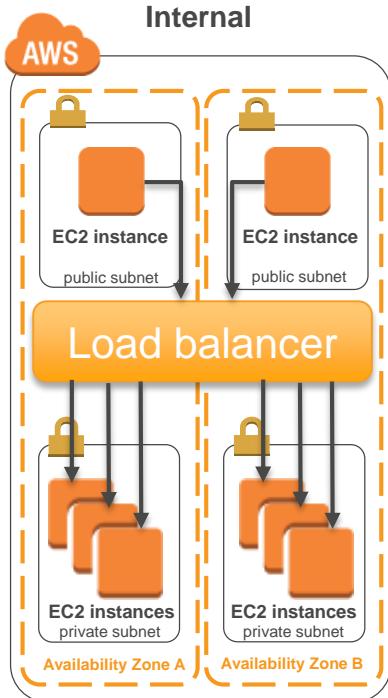
Load Balancer Types



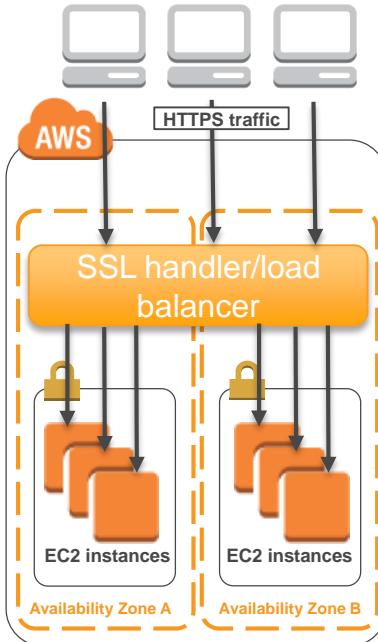
Internet-Facing



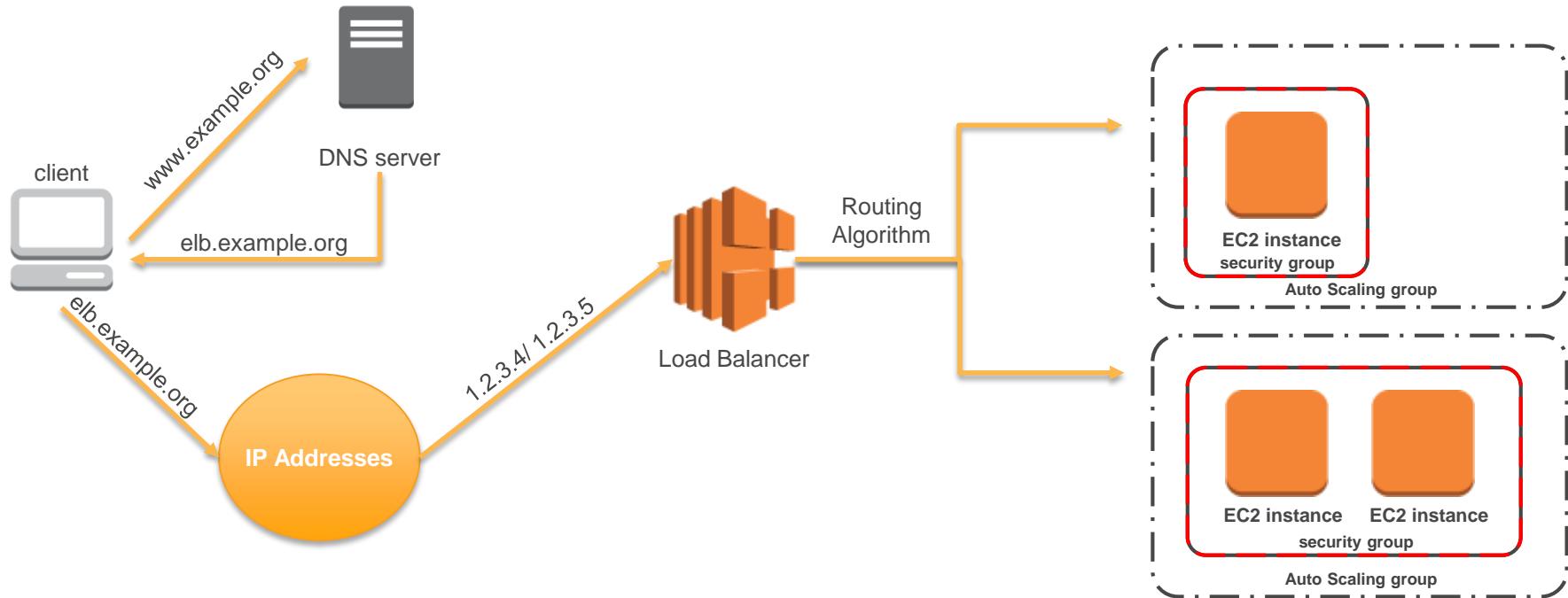
Internal



HTTPS



Request Routing



Listeners



- A listener is a process that checks for connection requests.
- Front-end connections are:
 - Client to load balancer connections.
 - Configured with a protocol and a port.
- Back-end connections are:
 - Load balancer to back-end instance connections.
 - Configured with a protocol and a port .
- ELB supported protocols:
 - HTTP
 - HTTPS
 - TCP
 - SSL

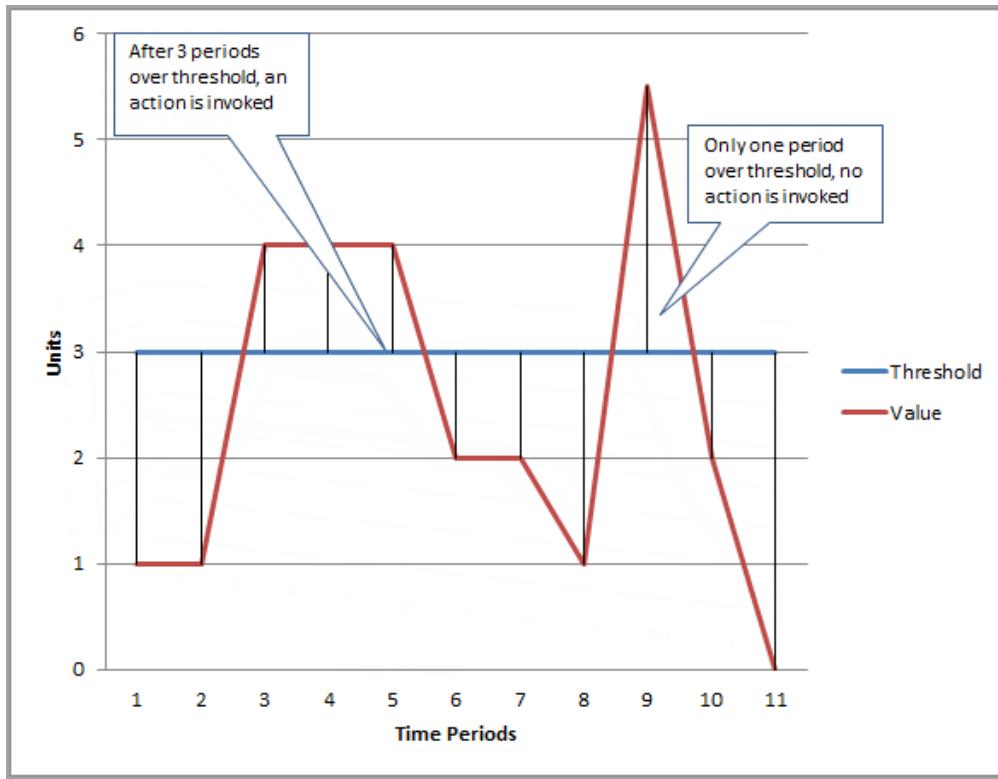
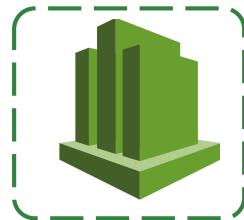
Back-end Instances for Your Load Balancer



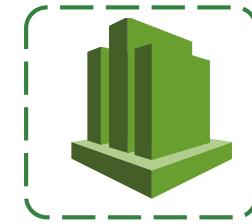
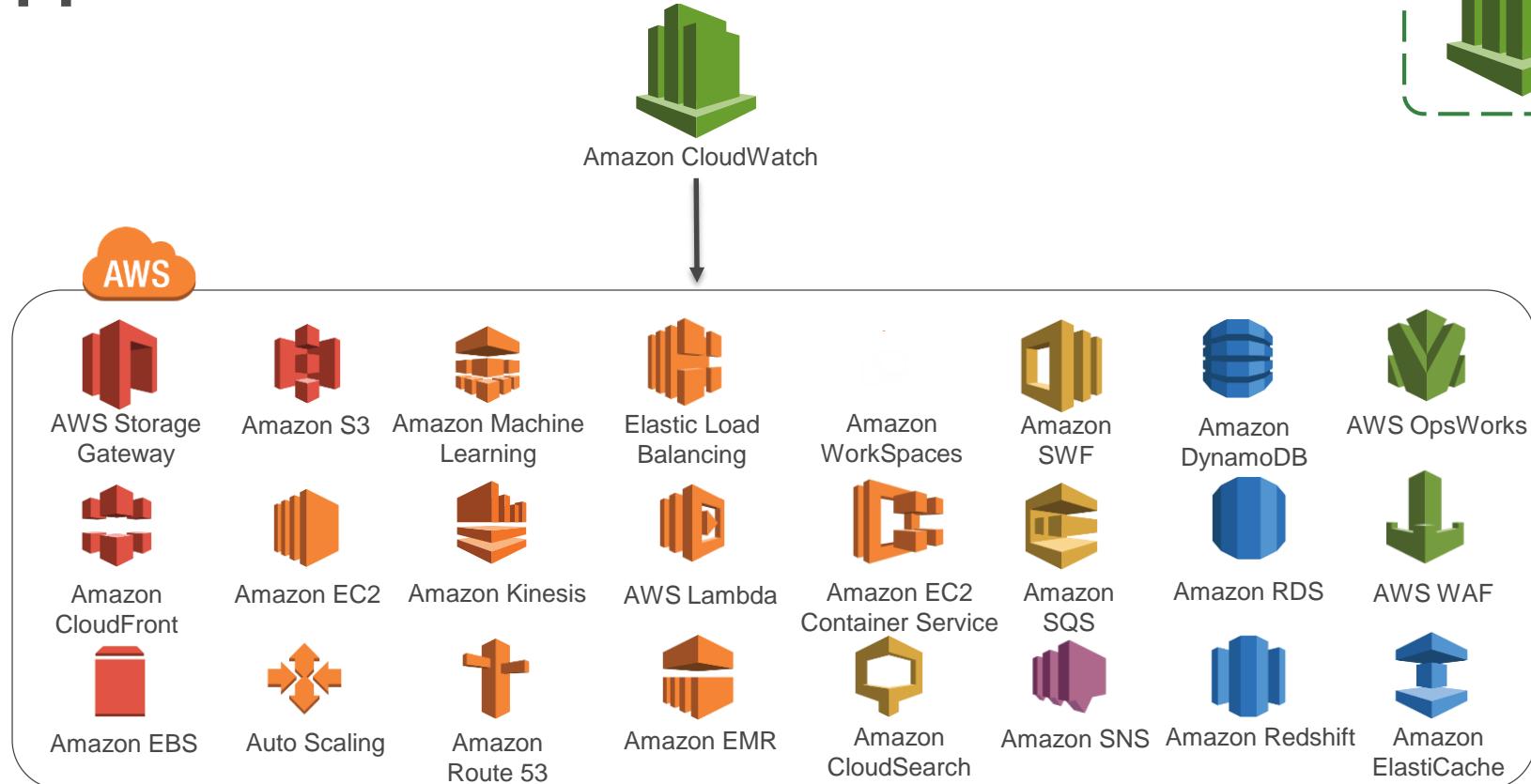
- Health checks
- Security groups
- Subnets
- Register
- De-register instances

CloudWatch Advanced Concepts

CloudWatch Alarms



Supported AWS Services



Module 6 Appendix

Course Wrap-Up

AWS Support

Case Severity & Response Times

	Critical	Urgent	High	Normal	Low
Enterprise Plan (24 x 7)	15 minutes or less	1 hour or less	4 hours or less	12 hours or less	24 hours or less
Business Plan (24 x 7)		1 hour or less	4 hours or less	12 hours or less	24 hours or less
Developer Plan (Business hours)				12 hours or less	24 hours or less

Pricing

Basic	Developer	Business	Enterprise
Included	\$29/month -or- 3% of monthly AWS spend	Greater of \$100 -or- 10% of monthly AWS usage for the first \$0-\$10K 7% of monthly AWS usage from \$10K-\$80K 5% of monthly AWS usage from \$80K-\$250K 3% of monthly AWS usage over \$250K	Greater of \$15,000 -or- 10% of monthly AWS usage for the first \$0-\$150K 7% of monthly AWS usage from \$150K-\$500K 5% of monthly AWS usage from \$500k-\$1M 3% of monthly AWS usage over \$1M

Pricing Examples

Business Pricing Example

For \$85K in AWS monthly usage:

$$\$10,000 \times 10\% = \$1,000$$

(10% of the first \$0 - \$10K of usage)

$$+ \$70,000 \times 7\% = \$4,900$$

(7% of usage from \$10K - \$80K)

$$+ \$5,000 \times 5\% = \$250$$

(5% of usage from \$80K - \$250K)

$$+ \$0 \times 3\% = \$0$$

(3% of usage over \$250K)

Total: \$6,500

Enterprise Pricing Example

For \$1.2M in AWS monthly usage:

$$\$150,000 \times 10\% = \$15,000$$

(10% of the first \$0 - \$150K of usage)

$$+ \$350,000 \times 7\% = \$24,500$$

(7% of usage from \$150K - \$500K)

$$+ \$500,000 \times 5\% = \$25,000$$

(5% of usage from \$500K - \$1M)

$$+ \$200,000 \times 3\% = \$6,000$$

(3% of usage over \$1M)

Total: \$70,500

© 2016 Amazon Web Services, Inc. or its affiliates. All rights reserved.

This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.

Errors or corrections? Email us at aws-course-feedback@amazon.com.

For all other questions, contact us at:

<https://aws.amazon.com/contact-us/aws-training/>.

All trademarks are the property of their owners.