Hydrosat Training Sessions
AWS Cloud Services

Reviewing AWS core Services

Abdallah Ibrahim

TECHNICAL ARCHITECT & CLOUD CONSULTANT

abdallahcoptan.github.io @ElkoptanAAZEAI

HYDROSAT

Overview

Understanding how to interact with AWS services

Examining services and best practices around security

Reviewing categories of core AWS services

Architecting fault tolerant applications with AWS services

Examining policies that govern how we can leverage AWS

Interacting with AWS Services

Interacting with AWS Services

AWS Console

Users can leverage their browser to configure resources

AWS CLI

Command line access for administering AWS resources

AWS SDK

Programmatic access to manage AWS resources

AWS SDK LANGUAGES

- Java
- .NET
- Node.js
- PHP
- Python
- Ruby
- JavaScript (Browser)
- Go
- C++

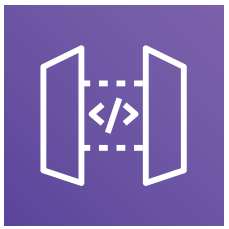
Networking & Content Delivery

Networking & Content Delivery Services

Amazon Route 53

Amazon VPC

Amazon Direct Connect



Amazon API Gateway

Amazon CloudFront

Elastic Load Balancing

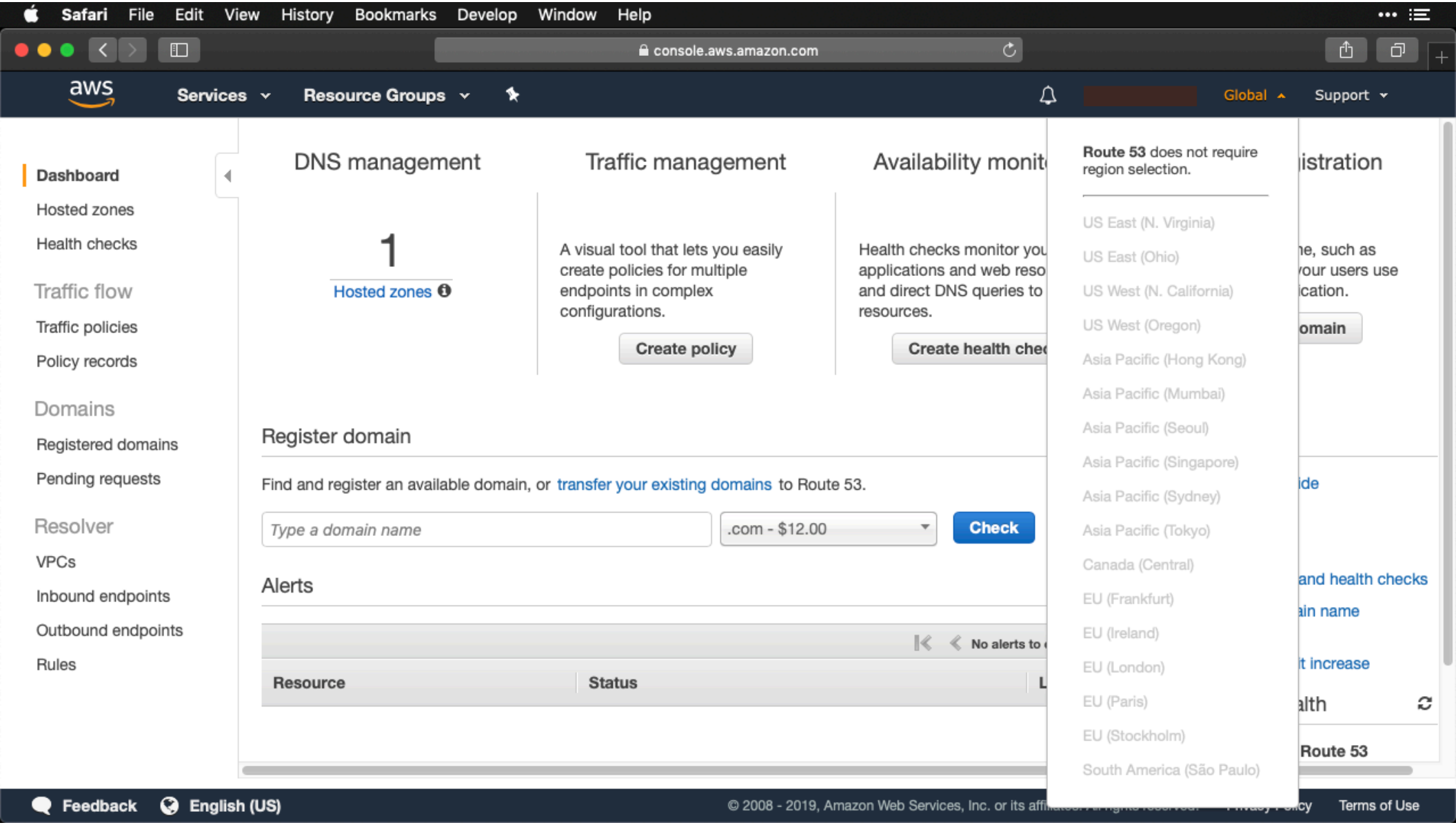
Amazon Route 53

Domain name service (DNS)

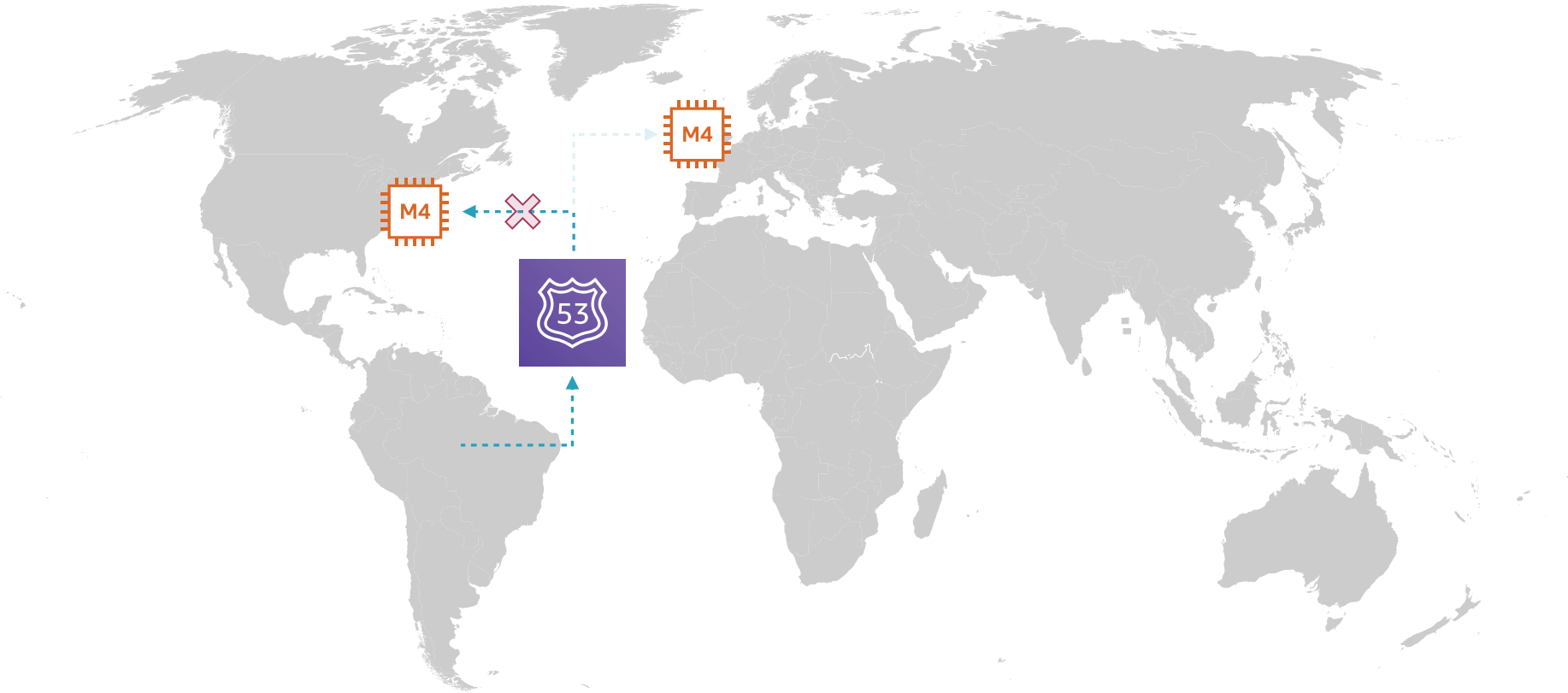
Global AWS service (not regional)

Highly available

Enables global resource routing


Safari File Edit View History Bookmarks Develop Window Help
console.aws.amazon.com
aws
Services
Resource Groups
Global
Support
Dashboard
Hosted zones
Health checks
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Pending requests
Resolver
VPCs
Inbound endpoints
Outbound endpoints
Rules
DNS management
1
Hosted zones
Traffic management
A visual tool that lets you easily create policies for multiple endpoints in complex configurations.
Create policy
Availability monit
Health checks monitor you
applications and web reso
and direct DNS queries to
resources.
Create health chec
istration
ne, such as
your users use
ication.
omain
Register domain
Find and register an available domain, or transfer your existing domains to Route 53.
Type a domain name
.com - $12.00
Check
Alerts
No alerts to
Resource
Status
Route 53 does not require region selection.
US East (N. Virginia)
US East (Ohio)
US West (N. California)
US West (Oregon)
Asia Pacific (Hong Kong)
Asia Pacific (Mumbai)
Asia Pacific (Seoul)
Asia Pacific (Singapore)
Asia Pacific (Sydney)
Asia Pacific (Tokyo)
Canada (Central)
EU (Frankfurt)
EU (Ireland)
EU (London)
EU (Paris)
EU (Stockholm)
South America (São Paulo)
ide
and health checks
ain name
t increase
alth
Route 53
Feedback
English (US)
© 2008 - 2019, Amazon Web Services, Inc. or its affi
Terms of Use

Route 53 High Availability



Amazon Virtual Private Cloud

A logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define.

Amazon Virtual Private Cloud (VPC)

Enables virtual networks in AWS

Supports IPv4 and IPv6

Allows for configuration of

- IP address range
- Subnets
- Route tables
- Network gateways

Supports public & private subnets

Can utilize NAT for private subnets

Enables a connection to your data center

Can connect to other VPC’s

Supports private connections to many AWS services

AWS Direct Connect

A cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS.

Amazon API Gateway

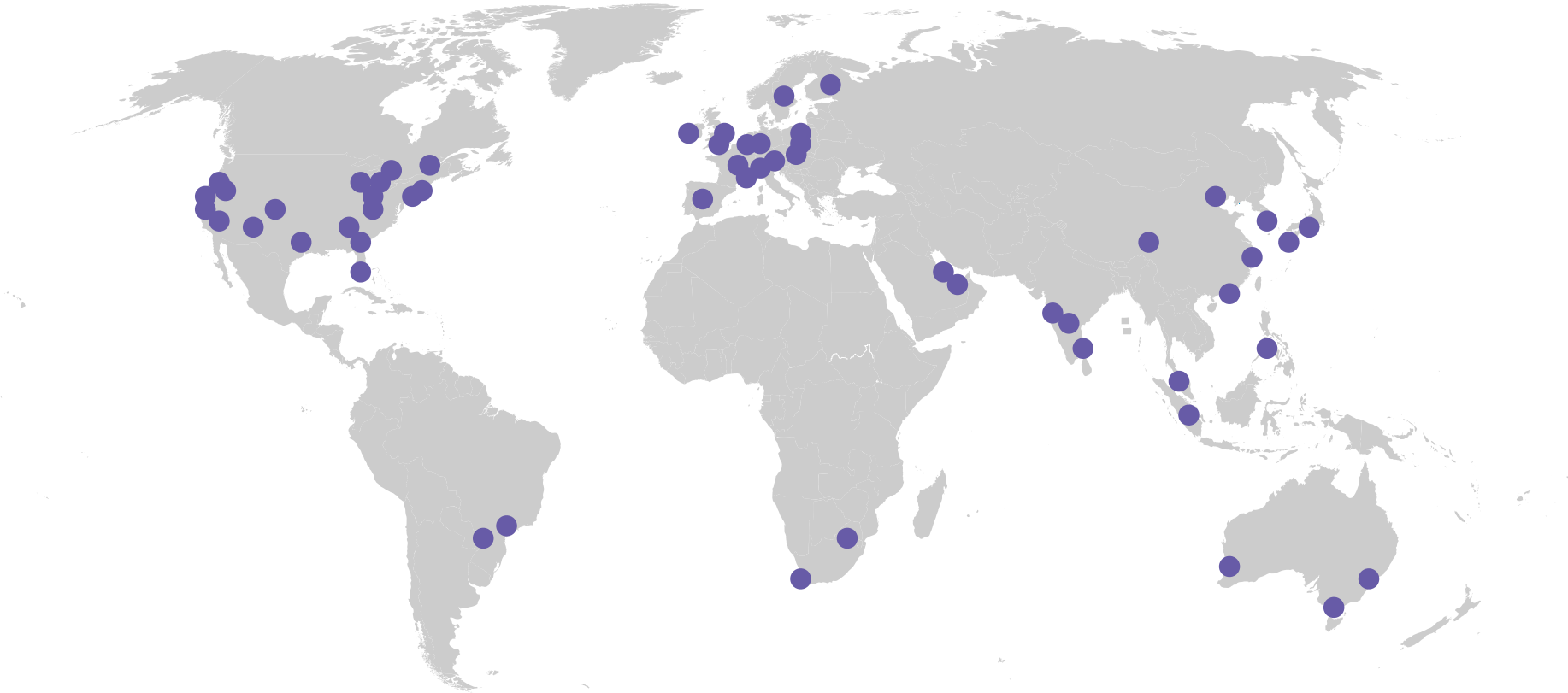
Fully managed API management service

Directly integrates with multiple AWS services

Provides monitoring & metrics on API calls

Supports VPC and on-premise private applications

AWS Edge Locations



Amazon CloudFront

Content delivery network (CDN)

Enables users to get content from server closest to them

Supports static and dynamic content

Utilizes AWS edge locations

Includes advanced security features

- AWS Shield for DDoS
- AWS WAF

Elasticity

The ability for the infrastructure supporting an application to grow and contract based on how much it is used at a point in time.

Elastic Load Balancing

Distributes traffic across multiple targets

Integrates with EC2, ECS, and Lambda

Supports one or more AZ's in a region

Three types of load balancers

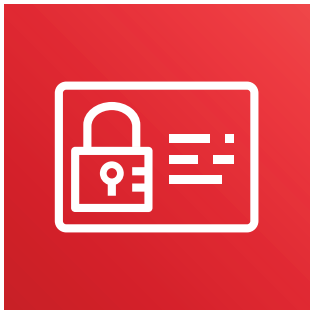
- Application Load Balancer (ALB)
- Network Load Balancer (NLB)
- Classic Load Balancer

Security on AWS

“Security and Compliance is a shared responsibility between AWS and the customer.”

Amazon Web Services, Shared Responsibility Model

AWS Identity & Access Management (IAM)



Service that controls access to AWS resources

Using the service is free

Manages both authentication and authorization

Supports identity federation

AWS IAM Identities

Users

Account for a single individual to access AWS resources

Groups

Allows you to manage permissions for a group of IAM users

Roles

Enables a user or AWS service to assume permissions for a task

Policies in AWS IAM

A JSON document that defines permissions for an AWS IAM identity (principal)

Defines both the AWS services that the identity can access and what actions can be taken on that service

Can be either customer managed or managed by AWS

AWS IAM Best Practices

Multi-factor Authentication

Provides additional security with either a physical or virtual device that generates a token for login

Least Privilege Access

Users should only be granted access to AWS resources that are required for their current tasks

Security in Amazon VPC

Security groups

Enables firewall-like controls for resources within the VPC

Network ACL's

Controls inbound and outbound traffic for subnets within the VPC

Flow logs

Captures the information around traffic within your VPC

Additional Security Services on AWS

AWS CloudTrail

Enables logging of all actions taken within your AWS account

AWS Shield

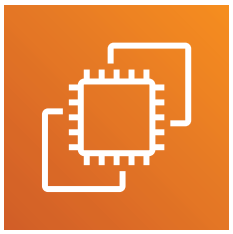
Provides detection and mitigation of DDoS attacks

AWS WAF

Protects your web application from common exploits

Compute on AWS

Compute Services on AWS



Amazon EC2

Provides secure and resizable virtual servers on AWS (IaaS)

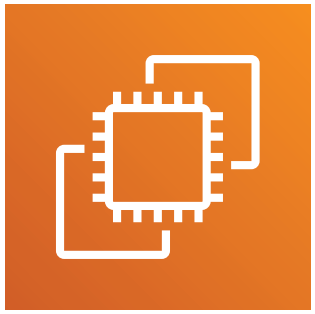
AWS Lambda

Enables compute without managing servers (FaaS)

Amazon ECS

Manages and scales containerized applications (CaaS)

Amazon Elastic Compute Cloud (EC2)



Operating system and additional software are provided in an AMI

Resources are provided by Instance Type

Instances can store data in two ways

- Instance store
- Elastic Block Store (EBS)

Launched into a VPC

Secured by a VPC security group and key pair

Amazon EC2 Instance Types

Defines the processor, memory, and storage type

Cannot be changed without downtime

Provided in the following categories

- General Purpose
- Compute, Memory, and Storage Optimized
- Accelerated Computing

Scaling on Amazon EC2

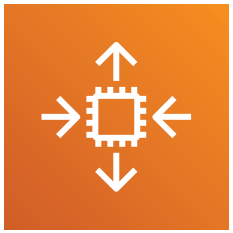
Vertical Scaling

You “scale up” your instance type to a larger instance type with additional resources

Horizontal Scaling

You “scale out” and add additional instances to handle the demand of your application

Amazon EC2 Horizontal Scaling Services



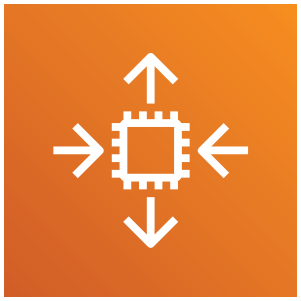
Auto-Scaling Group

Set of EC2 instances with rules for scaling & management

Elastic Load Balancer

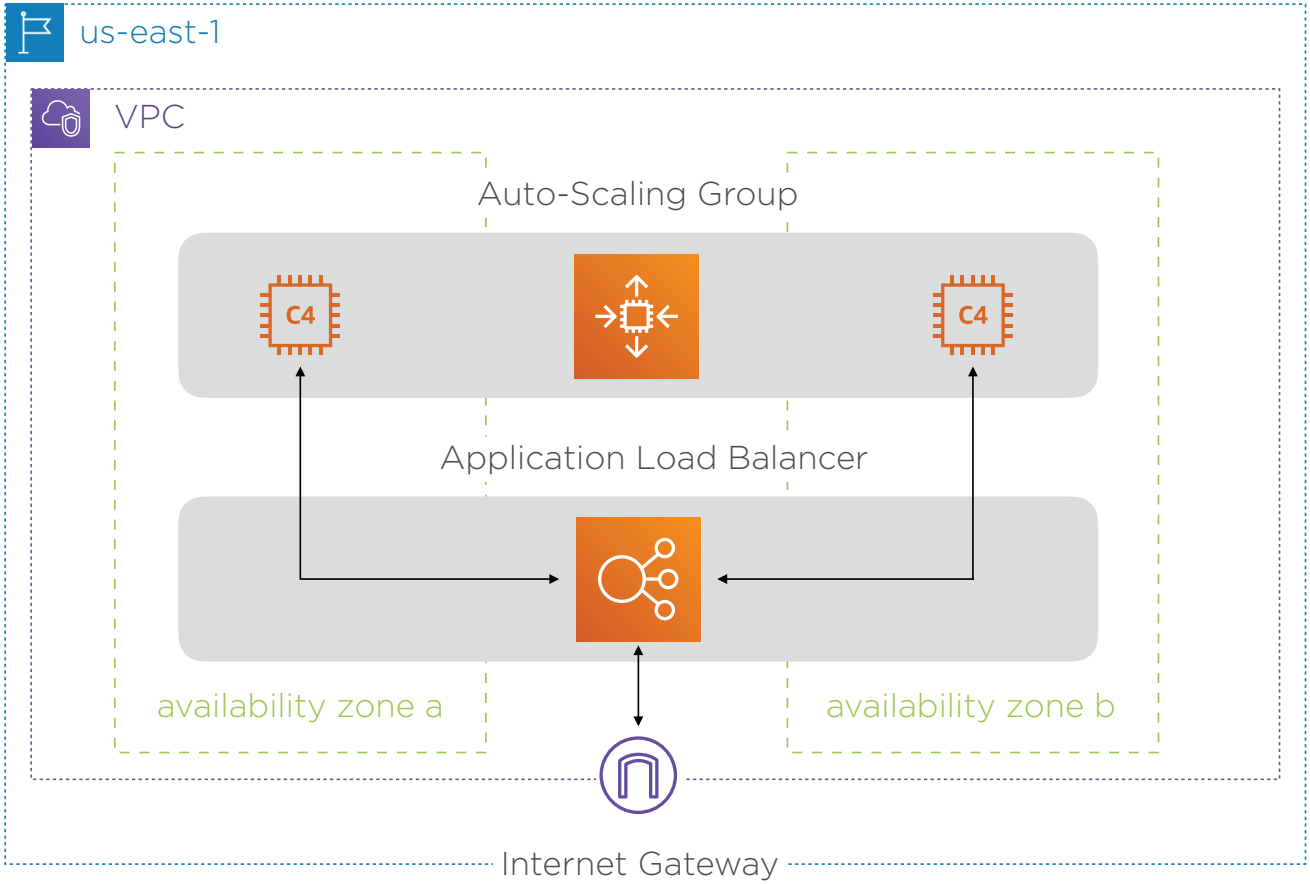
Distributes traffic across multiple targets

Amazon EC2 Auto-scaling Group



- **Launch configuration defines the instance template for the group**
- **Defines the minimum, maximum, and desired number of instances**
- **Performs health checks on each instance**
- **Includes scaling policies that define scaling behavior**
- **Exists within 1 or more availability zones in a single region**

Amazon EC2 Horizontal Scaling Example



Amazon EC2 Purchase Options

On-demand

You pay by the second for the instances that are launched

Reserved

You purchase at a discount instances in advance for 1-3 years

Spot

You can leverage unused EC2 capacity in a region for a large discount

Amazon EC2 Purchase Options

If you have an instance that is consistent and always needed, you should purchase a Reserved Instance.

If you have batch processing where the process can start and stop without affecting the job, you should leverage Spot Instances.

If you have an inconsistent need for instances that cannot be stopped without affecting the job, leverage On-demand Instances.

Container Management Services for AWS

Amazon ECS

Provides a container orchestration service on AWS

AWS Fargate

Enables containerized applications without managing servers

Amazon ECS for Kubernetes (EKS)

Manages Kubernetes applications in AWS

AWS Lambda

- Enables the running of code without provisioning infrastructure
- Only charged for usage based on execution time
- Can configure available memory from 128 MB to 3008 MB
- Integrates with many AWS services
- Enables event-driven workflows
- Primary service for serverless architecture

AWS Elastic Beanstalk

- **Automates the process of deploying and scaling workloads on EC2**
- **Supports a specific set of technologies**
- **Leverages existing AWS services**
- **Only pay for the other services you leverage**
- **Handles provisioning, load balancing, scaling, and monitoring**

File Storage on AWS

General File Storage Services

Amazon S3

Scalable, secure, and durable object storage service

Amazon S3 Glacier

Object storage service targeted at long-term and low-cost storage

Amazon Simple Storage Service (S3)

- Stores files in buckets
- Provides different storage classes for different use cases
- Stores data across multiple availability zones
- Enables URL access for files
- Can provide transfer acceleration for uploads using AWS edge locations
- Offers configurable rules for data lifecycle

Amazon S3 Non-archival Storage Classes

S3 Standard is the default storage class and is for frequently accessed data.

S3 Intelligent-Tiering will move your data to the correct storage class based on usage.

S3 Standard-IA is for infrequently accessed data with the standard resilience.

S3 One Zone-IA is for infrequently access data that is only stored in one AZ.

Amazon S3 Glacier

Designed for archiving of data within S3 as separate storage classes

Offers configurable retrieval times

Can send files directly or through lifecycle rules in S3

Provides two different storage classes

- S3 Glacier
- S3 Glacier Deep Archive

Amazon S3 Glacier Storage Classes

S3 Glacier

Designed for archival data

90 day minimum storage duration change

Can be retrieved in either minutes or hours

You pay a retrieval fee per GB retrieved

Over 5 times less expensive than S3 Standard storage class

S3 Glacier Deep Archive

Designed for archival data

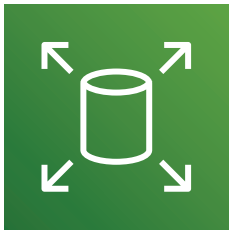
180 day minimum storage duration change

Can be retrieved in hours

You pay a retrieval fee per GB retrieved

Over 23 times less expensive than S3 Standard storage class

Amazon EC2 File Storage Services



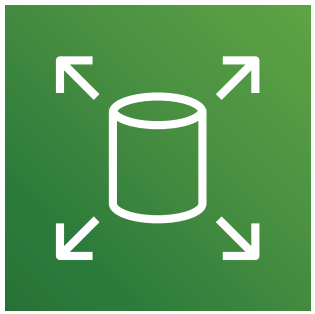
Amazon EBS

Persistent block storage for use with Amazon EC2

Amazon EFS

Elastic file system for use with Linux-based workloads

Amazon Elastic Block Store (EBS)



Enables redundancy within an AZ

Allows users to take snapshots of its data

Offers encryption of its volumes

Provides multiple volume types

- General purpose SSD
- Provisioned IOPS SSD
- Throughput optimized HDD
- Cold HDD

Amazon EBS Volume Types

General Purpose SSD is a cost effective type designed for general workloads.

Provisioned IOPS SSD high performance volume for low latency applications.

Throughput Optimized HDD is designed for frequently accessed data.

Cold HDD is designed for less frequently accessed workloads.

Amazon Elastic File System (EFS)

Fully managed service

Designed for Linux workloads

Supports up to petabyte scale

Stores data across multiple AZ's

Provides two different storage classes

- Standard
- Infrequent access

Provides configurable lifecycle data rules

Databases on AWS

AWS Databases & Related Services

Amazon RDS

Amazon Aurora

Amazon DynamoDB

Amazon Redshift

Amazon Elasticache

AWS Database Migration Service

Amazon Relational Database Service (RDS)

Fully managed service for relational databases

Handles provisioning, patching, backup, and recovery of your database

Supports deployment across multiple availability zones (multi-AZ)

Some platforms support read replicas

Launches into a VPC

Provides both general purpose SSD and provisioned IOPS SSD drive options

Amazon RDS Platforms

MySQL

PostgresSQL

MariaDB

Oracle Database

SQL Server

Amazon Aurora

Amazon DynamoDB

- **Fully managed NoSQL database service**
- **Provides both key-value and document database**
- **Enables extremely low latency at virtually any scale**
- **Supports automated scaling based on configuration**
- **Offers in-memory cache with the DynamoDB Accelerator (DAX)**

“DynamoDB can handle more than 10 trillion requests per day and can support peaks of more than 20 million requests per second.”

Amazon Web Services

Amazon Redshift

- Scalable data warehouse service
- Supports petabyte scale warehousing of data
- Leverages high performance disks and columnar storage
- Offers the ability to fully encrypt contents
- Provides isolation with a VPC
- Enables querying of exabytes of data in Amazon S3 using Redshift Spectrum

Amazon Elasticache

Fully managed in-memory data stores

Supports both Memcached and Redis

Provides low latency in response times

Enables scaling and replicas to meet application demand

Handles common use cases including

- Database layer caching
- Session storage

AWS Database Migration Service

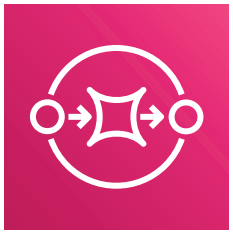
Enables you to securely migrate data into AWS in an efficient manner for both homogeneous and heterogeneous migrations either all at once or in a continual manner.

App Integration Services

AWS App Integration Services

Amazon SNS

Managed pub/sub messaging service



Amazon SQS

Managed message queue service

Amazon Simple Notification Service (SNS)

Fully managed pub/sub messaging service

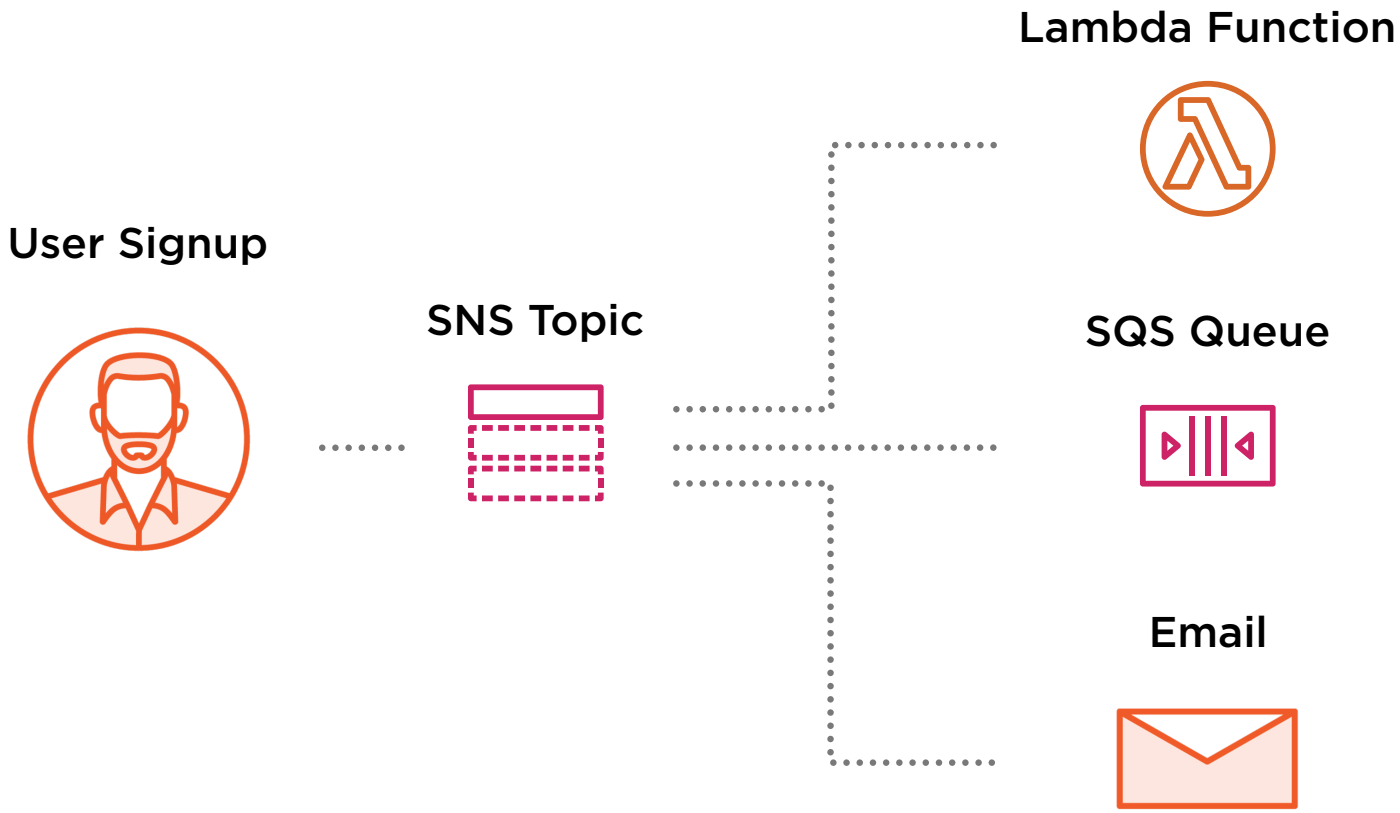
Enables you to create decoupled applications

Organized according to topics

Integrates with multiple AWS services

Provides end user notifications across SMS, email, and push notifications

Example Amazon SNS Architecture



Amazon Simple Queue Service (SQS)

Fully managed message queue service

Enables you to build decoupled and fault tolerant applications

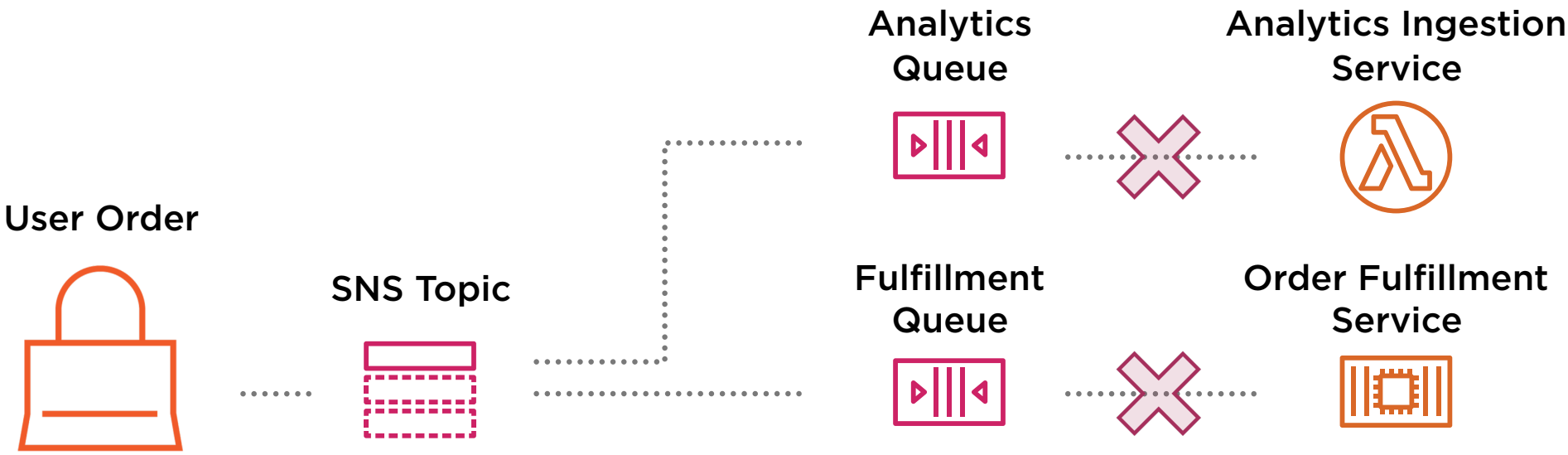
Supports up to 256 KB data payload

Allows messages to be store up to 14 days

Provides two types of queues

- Standard queue
- FIFO queue (first in first out)

Example Amazon SNS & SQS Architecture



Management & Governance Services

Management Services for AWS

AWS CloudTrail

Enables operational auditing of your AWS account

AWS CloudFormation

Provides infrastructure as code capabilities for AWS

AWS CloudWatch

Enables monitoring and metrics on your AWS resources

AWS CloudFormation

- Managed service for provisioning infrastructure based on templates
- No additional charge
- Templates can be YAML or JSON
- Enables infrastructure as code
- Manages dependencies between resources
- Provides drift detection to find changes in your infrastructure

```
Description: Creates an S3 bucket

Resources:
  SampleS3Bucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: sample-s3-bucket
```

Example CloudFormation YAML

The code above if placed within a full CloudFormation template would create a single S3 bucket

Amazon CloudWatch

Monitoring and management service

Collects logs, metrics, and events from most AWS services

Enables alarms based on metrics

Provides visualization capabilities for metrics

Allows for custom dashboards based on collected metrics

Additional Topics

AWS Acceptable Use Policy

The AWS Acceptable Use Policy defines prohibited uses of the services offered by AWS. All users of the platform are bound by this policy.

AWS Marketplace

Curated catalog of third-party solutions for customers to run on AWS

Provides AMI's, CloudFormation stacks, and SaaS based solutions

Enables different pricing options to overcome licensing in the cloud

Charges appear on your AWS bill

AWS Large Scale Data Transfer Services

AWS Snowball

Service to physically migrate petabyte scale data to AWS

AWS Snowmobile

Service to physically migrate exabyte scale data onto AWS

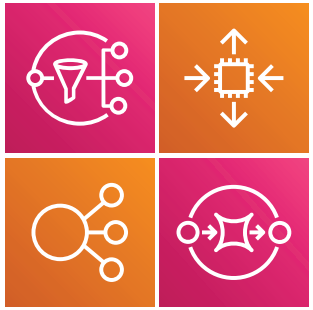
Summary

AWS Service Categories

Analyzed AWS services across the major categories

Security Services & Best Practices

Examined the services that secure AWS infrastructure



Fault Tolerant Approach & Services

Reviewed decoupled and fault tolerate app services