

# CERT Prep

## AWS Architect Associate

# What we will cover today



- Prepping for the AWS Architect Associate Exam
- Taking the exam – what's covered – domains of knowledge
- The essential AWS core services to understand

# Steps for AWS Certification Success

- Think like a Cloud Architect
- Architects “build” (i.e. design) “construct
- Architects propose solutions based on existing building blocks
- The Associated Architect is based on common sense
- Every question is a “situation” ; current or proposed
- The correct answer is the best answer based on suggested answers to the multiple-choice question



# AWS Documentation

- AWS Certified Solutions Architect - Associate
- AWS Certified Solutions Architect – Study Guide
- AWS Certified Solutions Architect – Sample Questions

# AWS Documentation to Google

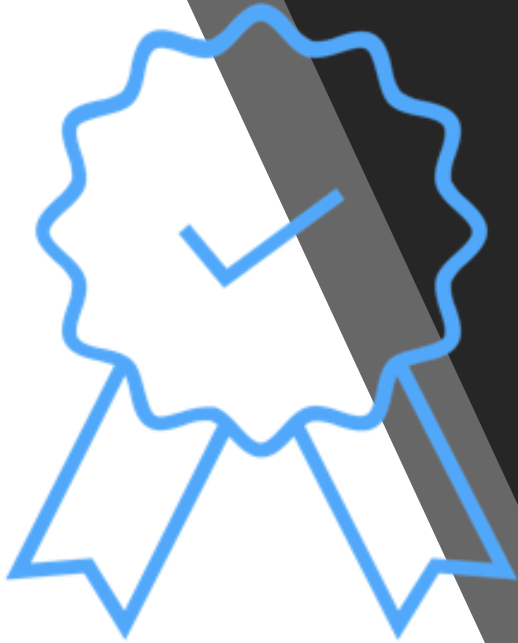
- AWS Documentation
- AWS FAQ's
- AWS Quick Starts – Automated application stacks
- Self Paced Labs – Quiklabs



# Exam Notes

---

# Re-Certification



- Every two years you must recertify
- Re-certification exam is shorter and cheaper to retake

# Domains of Knowledge

- Domain One: Designing highly available, cost-efficient, fault-tolerant, scalable systems **60% of exam**
  - Based on questions asked pick the best solution using AWS services
- Domain Two: Implementation and Deployment **10% of exam**
  - Pick the best technique and method for deploying AWS services
- Domain Three: Data Security **20% of exam**
  - Implement proper security for optimum cloud deployment
- Domain Four: Troubleshooting **10% of exam**
  - Troubleshooting questions



# How the Exam is Graded



- Questions are multiple-choice
- Both single selection and multiple selection
- No penalty for guessing
- Approximately 65 questions on the exam
- Mark questions for future review
- Answer all questions
- Sketch out your answers using the supplied plastic paper and marker



Domain **One**:

Highly available, Cost-efficient,  
Fault-tolerant, Scalable systems

What AWS  
service to use



# Domain One

---

- HA: Some AWS systems are highly available by default (ELB)
  - Cost- efficient:
    - Select the cheapest architecture
    - Don't over provision resources
  - Fault-tolerant
    - Know the difference between highly available and fault-tolerant
- Know which AWS services are designed to be fault-tolerant by default

# Domain One

---

- Scalable
  - Know which AWS services scale automatically
  - Know-how EC2 Auto Scaling works
  - Design architecture that uses independent components
  - Independent components can scale independently
- Don't design relying on the identity of individual components
  - Load balanced clusters of Web servers across multiple availability zones
  - DNS names server instead of IP addresses
  - Elastic IP addresses

Fault tolerance – the ability  
for system to remain in  
operation. Even if some of  
the components used, to build  
the system fail during  
operation

High-availability – there's no real exact definition other than a highly available service must be considered highly available at all times ( or most of the time )

Availability is defined as a  
“nines of availability”

99% - 2 nines

Downtime per year: 3.65 days

99.99% - 4 nines

Downtime per year: 4.38 hours



# Highly Available Services



Multi-AZ RDS deployments



S3 buckets – multiple objects stored in three separate physical locations



Elastic Load Balancing – highly available LB cluster

# AWS Global Infrastructure

---

# Availability Zones in Operation



- EC2 instances can launch across multiple subnets hosted in multiple availability zones
- ELB can target instances across multiple availability zones
- Auto Scaling can scale instances across multiple availability zones
- Route 53 can distribute traffic across EC2 Instances and ELB in different AZs and regions
- DynamoDB is replicated across multiple availability zones and optionally regions
- RDS solutions are replicated across multiple availability zones; Aurora can also be multi-region

# Availability Zones



- Each availability zone has at least one data center
- Each region has at least 2 availability zones
- Each availability zone contains:
  - Subnets
  - EC2 instances hosted on subnets
  - EBS storage

# Single or Multi-AZ Design

## Single - AZ

- No recovery or failover when disaster happens in a single datacenter
- No high availability for instances
- No failover in single datacenter
- All AWS regions have at least 2 availability zones
- Each AZ has at least one datacenter

## Multi - AZ

- Better high availability design options
- Designing applications hosted across AZ's provides HA options
- Load balancing (ELB) supports targeting instances in multiple availability zones
- EC2 auto scaling supports multiple AZ's
- Use Route 53 (DNS) to balance across multiple AWS regions

# Availability Zone Cheat Sheet

- Utilize 2 availability zones per region
  - If resources in one AZ fail, or are unavailable, your application should continue to work from the other AZ
- AZ's provide failover and HA design possibilities
- Designing applications using two availability zones per region is current best practice
- Note: Exam questions won't always follow best practice

## Edge Locations



- Edge locations are located outside of AWS regions
- Each user is at the user edge; with a network enabled device
- Edge locations are miniature data centers directly connected from major cities around the world into Amazon cloud resources

# AWS Services at the Edge

Caches your  
content request

## CloudFront



Delivers your  
request to closest  
edge location

## Route 53



Filters incoming  
public traffic to  
the edge

## WAF







AWS Cloud



Route 53

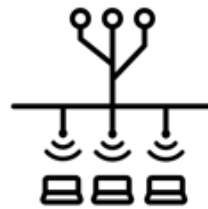


Region



VPC

IGW



Elastic Load  
Balancing



Public subnet



NAT Service



Private subnet

EC2 Instances

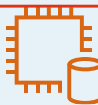
Security group



NACL



Private subnet



Master DB

Security group



Availability Zone-A



Public subnet



NAT Service



Private subnet

EC2 Instances

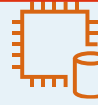
Security group



NACL



Private subnet



Standby DB

Security group



Availability Zone-B

VGW



# Fault Tolerance Services

- DynamoDB – replicate your data automatically across three physical locations within a region
  - Built-in fault tolerance with multiple pots of replicated data
- Route 53 - Designed for 100 % availability
  - Designed as an any cast network
- Amazon Simple Queue Service
  - Highly reliable distributed messaging system
- Amazon Simple Storage Service
  - Highly reliable, distributed storage across 3 physical locations within a region
- Amazon Relational Database Service
  - Master and standby database replication across multiple availability zones

# Designing with Elasticity and Scale

- Use Auto Scaling, Elastic IP's and HTTPS endpoints
- Stateless is better than stateful
- Use ELB and CloudWatch to detect the health of targeted EC2 instances
- Bootstrap your instances. Use user data at launch
- Store configuration and personal information away from Web server
  - Use DynamoDB for session state data
- Designing with elasticity helps reduce cost
  - Using EC2 auto scale minimum and maximum values: Scale out and Scale in

# High Availability Cheat Sheet



- Snapshots increase availability
- EBS – Replicated within the availability zone
- S3 – Replicated multiple times within the region
- SQS – Highly available and scalable
- SNS – Highly available and scalable
- Route 53 – Global “Anycast” DNS service
- RDS – Synchronous replication between Master and Slave

# ELB Operation



- Port 80, or port 443 incoming traffic
- Targeted instances or containers
- Health checks
- ALB – security group
- ALB – WAF support
- ALB – Authentication – Cognito
- Across multiple availability zones

# Load-Balancing Choices

- Classic load balancer – operates at Layer 4
  - IP protocol data or HTTP / HTTPS
  - Supports SSL offload
- Network load balancer operates at Layer 4
  - IP protocol data
  - NLB routes connections to targets (EC2, and containers)
  - Integrates with Auto Scaling, Amazon EC2 Container service, and Route 53
- Application load balancer – operates at Layer 7
  - Routes traffic to instances and targets based on the content of the request
  - HTTP / HTTPS
  - Supports SSL offload, Authentication, and (WAF)



# ELB Cheat Sheet

- Provides high-availability by distributing traffic across multiple targets hosted in single or multiple availability zones
- Integrates with CloudWatch
- Cross-zone load-balancing supported
- Detects unhealthy targets and stops sending traffic
- Supports connection draining (deregistration)
- SSL offloading (CLB / ALB)
- Authentication (ALB)

## EC2 Auto Scaling



- Scale compute out and in based on demand
- Integrates with ELB and EC 2 Auto Scale
- Also integrates with CloudWatch



# Launch Configuration

- What EC2 instance, AMI, storage, and key pair to utilize when adding instances to auto scaling group



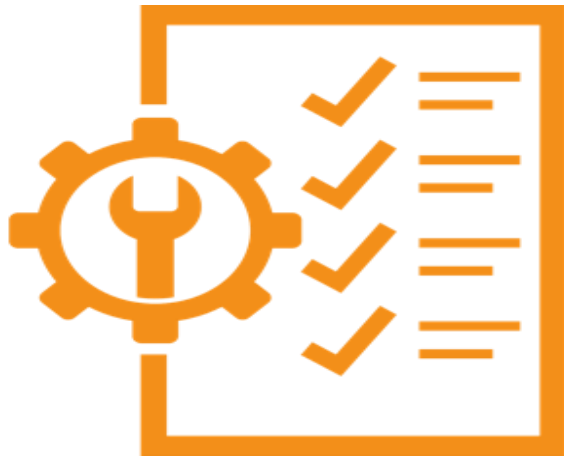
# Auto Scaling Groups



- Launch configuration is associated with specific Auto Scaling Group
- Match capacity scaling compute resources out and in

# Scaling Policy

- Maintain desired compute capacity
- Dynamically scale out using CloudWatch metrics
- Dynamically scale in using CloudWatch metrics
- Step scaling percentages out and in



# Auto Scaling Cheat Sheet

- Autoscaling scales EC2 capacity up or down based on defined rules
  - Scale out – increasing the number of Instances
  - Scale in – decreasing the number of Instances
  - Desired state – maintain state
- Launch Configuration – parameters necessary to create new EC2 instances (Instance size and type, AMI, Key pairs)
- Auto Scale Group – Max, Min, Desired state
- Policy – When and how Auto Scale responds
- Health Check – health status of each instance in auto scaling group
- Triggers – CloudWatch alarm; scaling up, and scaling down



Domain **Two**:

Identify the techniques and methods to code and implement a cloud solution

How to use the  
AWS service



# Implementation and Deployment Notes



- Focus on the commonly used services
- For each service:
  - Understand use cases
  - Know how the service works
  - Be able to sketch its use
  - Have some hands-on experience
  - Don't memorize syntax
  - Know the limits of each service
  - Read the FAQs

A large, stylized graphic of the AWS logo, consisting of a blue hexagon with a white exclamation mark inside, is positioned on the left side of the slide. The background is dark gray.

# Key AWS Services Categories

- Compute, and Networking
- Storage and Content Delivery
- Databases
- Deployment and Management
- App Services





# Key Services .... continued

- Compute, and Networking –EC2 instances, and VPC
- Storage and Content Delivery – S3 and S3 Glacier
- Databases – Relational Database Service
- Deployment and Management – CloudFormation, CloudWatch and IAM
- App Services – Simple Queue Services and the Simple Notification Service

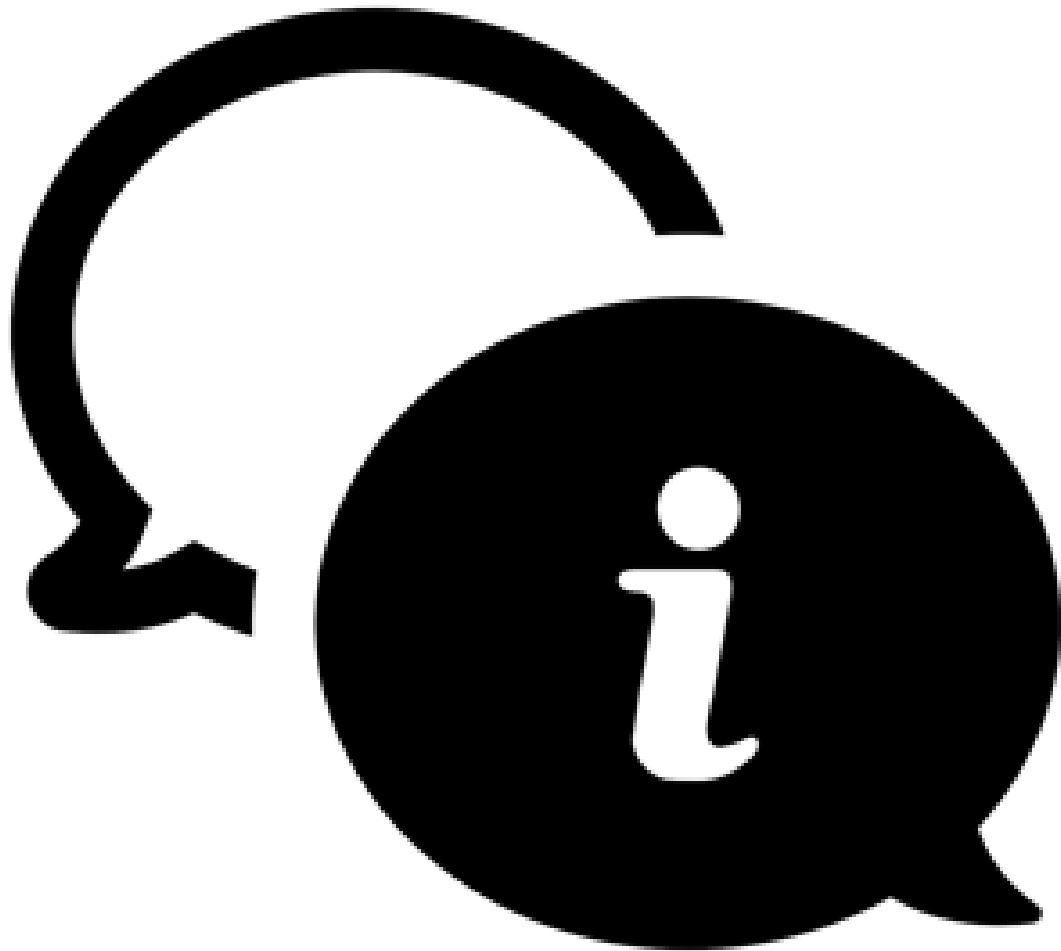
# AWS Network Infrastructure

---

VPC

- Each VPC is a completely isolated collection of subnets linked together with a local route table

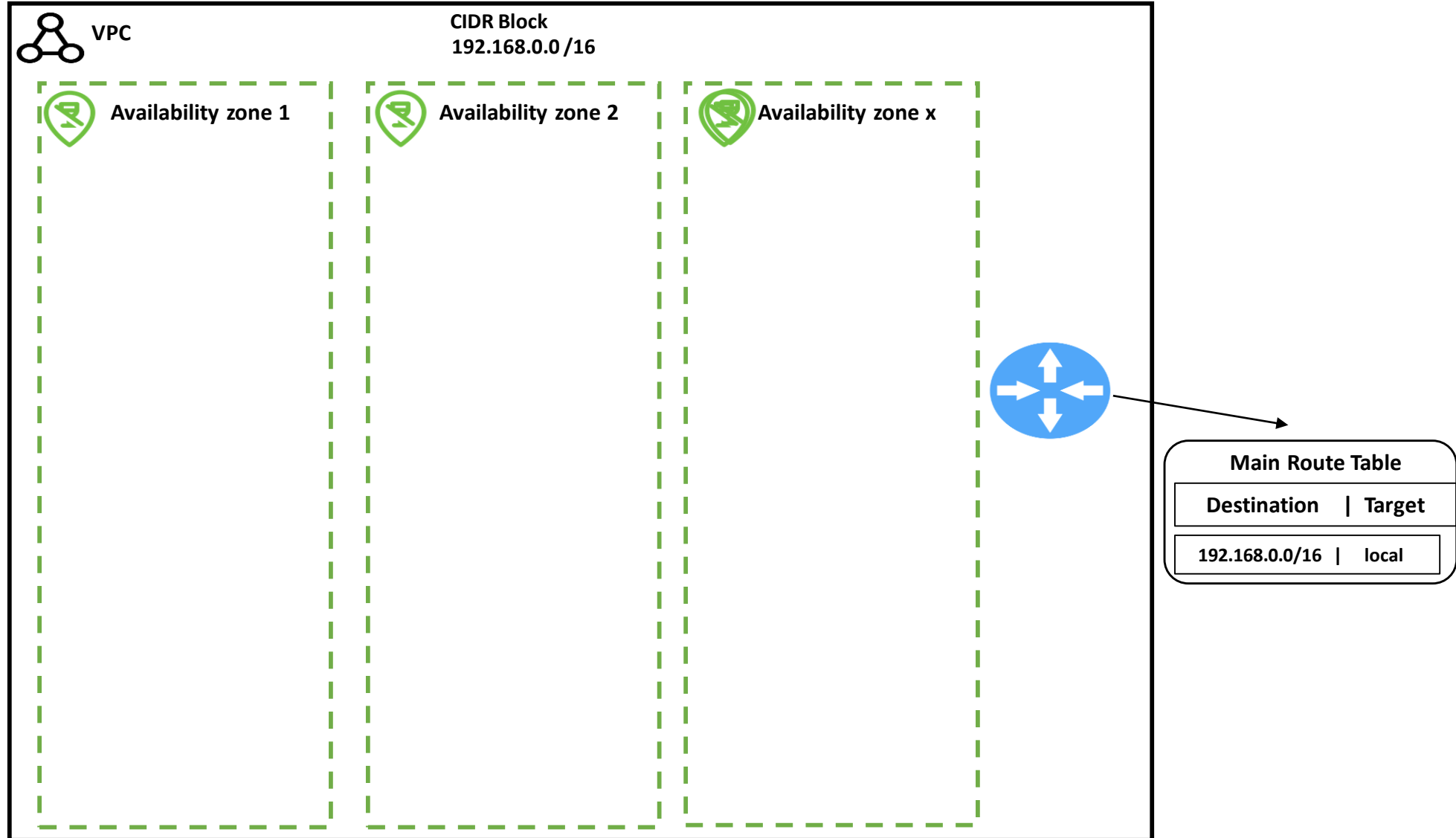




# VPC Functional Design

- VPCs span all availability zones per region
- Subnets are hosted within the selected availability zone
- EC2 instances and subnets reside within a data center (AZ)
- Route tables control subnet traffic flow

# VPC's have multiple AZ's



# Internet Gateway



- In order to have Internet connectivity to your VPC, an Internet gateway must be attached directly to the VPC
- Subnets that wish to communicate across the Internet must have a route table entry, providing a direct path to the Internet Gateway
- Only public subnets can connect with the Internet Gateway
- Only public IP addresses assigned to EC2 instances hosted on public subnets can connect to the Internet Gateway

# IP Addresses



- Public IP addresses can communicate with the Internet Gateway
- Public IP addresses cost you more money at AWS
- Public IP addresses can be assigned by AWS
- Elastic IP addresses, or static public IP address is assigned to your AWS account

# Route tables



- Associated with subnets
- Define the destination for IP traffic
- Local rules are defined by default
- Route to Internet gateway to access Internet (public subnet)
- Route to virtual private gateway for VPN connections



# Connectivity options



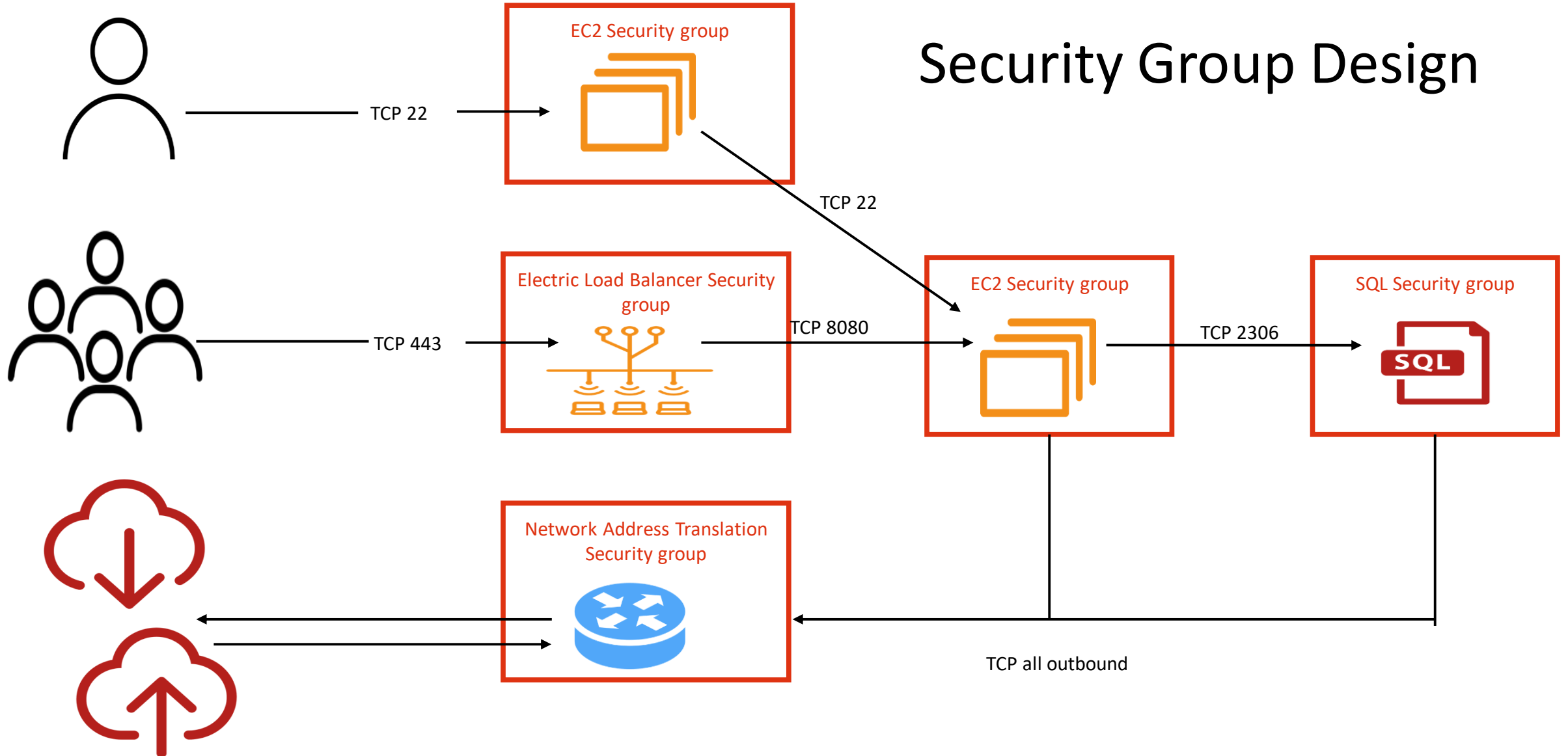
- Services to get traffic in or out of your VPC
- Internet Gateway
- Virtual Private Gateway
- Direct Connect
- VPC Peering
- Sharing

# Security Groups

- Security groups are a virtual firewall that protects traffic to EC2 instances
- Security groups are associated with a VPC



# Security Group Design



# Security Groups Best Practice



- Avoid allowing incoming traffic on 0.0.0.0/0
- Control ELB ingress rules using an ELB security group
- Restrict outbound rules – all outbound ports are open by default
- Manage security groups (Trusted Advisor)
- Control security group modifications (IAM)
- Review event tracking (CloudTrail)
- Manage compliance (AWS Config)

# Security Group Cheat Sheet

- Security groups are assigned to instances
- Multiple instances can be assigned the same security group
- Security groups allow all outbound traffic by default
- Security groups process “allow rules”
- Source or destination rules can point to another security group
- Security groups are evaluated as a whole, not in order



# Network ACLs



- Network ACLs are optional subnet firewalls
- Stateless design
- Inbound traffic does not know about outbound traffic
- Outbound traffic does not know about. Inbound traffic
- Allow and deny rules

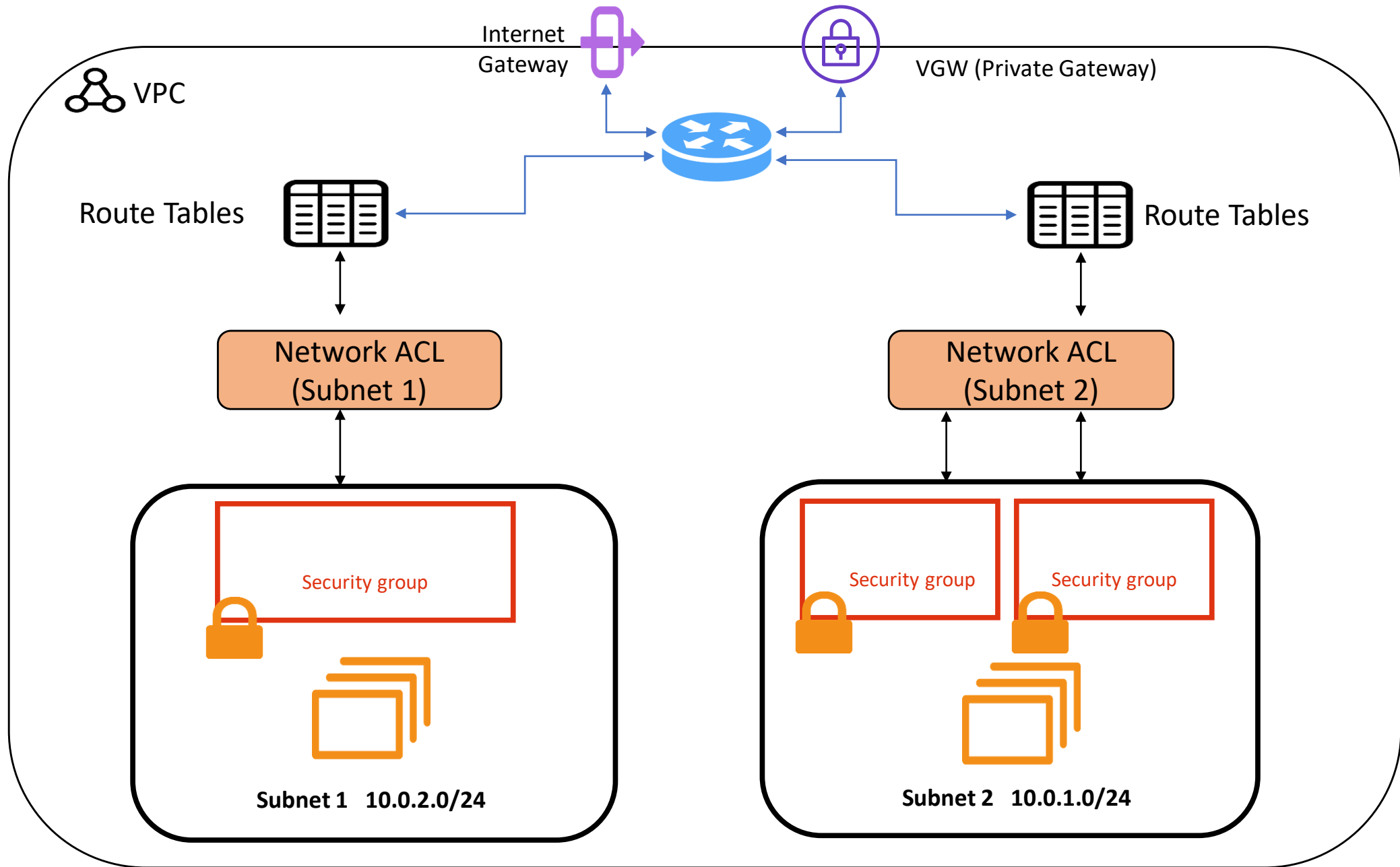
# Security Groups vs NACLs

## Security Groups

- Operates at the instance level
- Allow rules only supported
- Stateful: return traffic is automatically allowed
- All rules are processed before traffic decisions are made
- Applied to the selected instance elastic network adapter

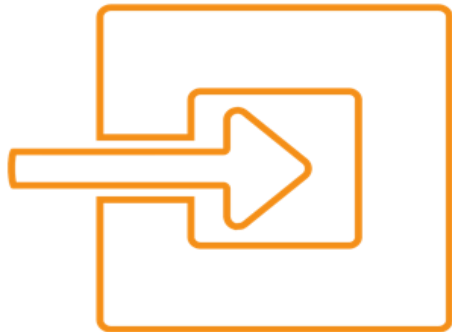
## NACLs

- Operates at the subnet level
- Allow and deny rules supported
- Stateless: return traffic must be explicitly allowed by a rule(s)
- Rules are processed in numerical order before traffic decisions are made
- Applied to the subnet





# Private Endpoints



- Interface connections – private network connections from the subnets to specific AWS services across the AWS private network
- Gateway connections – private connections from private subnets to S3 buckets or DynamoDB tables
- A gateway connection requires a route table entry

# VPC's Best Practice



- Choose two availability zones providing high-availability and disaster recovery
- Different subnet types:
  - Public subnet for external facing resources NAT, Load Balancers, Custom design
  - Private subnets for internal resources
- Use Network ACLs to control subnet traffic
- Custom routing tables for controlled traffic flow
- Use the highly available NAT gateway service

# VPC Cheat Sheet

- Internet gateway's IGW provides access to the Internet
- Virtual gateway's VGW provides access to on-premise data centers
- A VPC can have one IGW and one VGW
- NAT servers or services provide outbound Internet access for instances hosted in private subnets
- Elastic IP addresses are static persistent public IP addresses
- Security groups secure instances hosted on subnets
- NACL's secure traffic at the subnet layer

# Subnet Cheat Sheet

- Subnets map to the availability zone where they are created
- Subnets do not span across availability zones
- CIDR Ranges in VPC can't overlap (If you want to peer later)
- Subnets must be associated with a route table
  - Route table defines traffic flow
- Public subnet – Internet Gateway (IGW) is attached
- Private subnet – Virtual Private Gateway (VGW) is attached
- Protected subnet – no connectivity from the outside world

# AWS Security Features

---

# Identity and Access Management



- IAM Users
- IAM Groups
- IAM Roles
- Access control with granular group policies
- IAM is not application authentication

# Least Privilege



- Provide permissions to allow the person or process to perform the activities they need to perform, and no more
- Person, or process is defined as an identity at AWS
- Master Account: Root Account
- IAM users

# Security Token Services



- Temporary tokens
- Grant temporary rights to process or person
- Full control over privileges granted
- Full control on how long access is allowed
- Roles
- Grant privileges to processes on EC2 instances
- No authentication keys stored on instances
- Federation
- Temporary tokens assigned based on A.D. accounts
- No personal IAM accounts needed; instead, leverage your on-premise user directory



# Root Account

- Has full privileges to entire AWS account
- Cannot be limited
- Add multifactor authentication



# Credential Report

- Report that lists details of current IAM users, password change dates, key rotation, dates and other details
- Can be downloaded from IAM console



# AWS EC2 Instances

---

# EC2 Instance



- Compute (virtual servers)
- Linux and Windows operating systems
- Hosted on subnets
- Assign a public or private IP address
- Utilizes local storage (ephemeral), or block storage (EBS)

AMI



- Amazon Machine Image
- Each EC2 instance is built using an AMI
- AMIs are region specific
- Can be copied to other regions for use

# EC2 Instances: Pricing Options



## **On-Demand**

Pay by per hour/ second  
Short-term,  
unpredictable workloads



## **Reserved Instances**

Discount for 1 - 3-year  
commitment  
Applications with  
consistent usage



## **Spot Instances**


Spare AWS capacity >  
90% discount  
Applications with flexible  
start and end times



## **Dedicated Hosts**

Physical server dedicated  
to customer  
Compliance requirements  
for applications

# EC2 Cheat Sheet

- 
- Scaling computing capacity hosted in VPC's
  - Preconfigured templates for instances called AMIs (Amazon Machine Image)
  - Persistent storage uses EBS volumes
  - Ephemeral storage uses “temporary” volumes
  - Virtual firewalls called security groups secure your instances
  - Configuration after initial installation with user data scripts
  - Metadata retrieval using 169.254.169.254 from running EC2 instance
  - Secure logon uses public / private key pairs
  - Instance types define CPU, RAM, Storage

# CloudTrail

- Built-in logging service for all AWS accounts
- Tracks all API calls to AWS account
- Tracks all authentication's
- Retains information for 90 days. By default





# Trusted Advisor



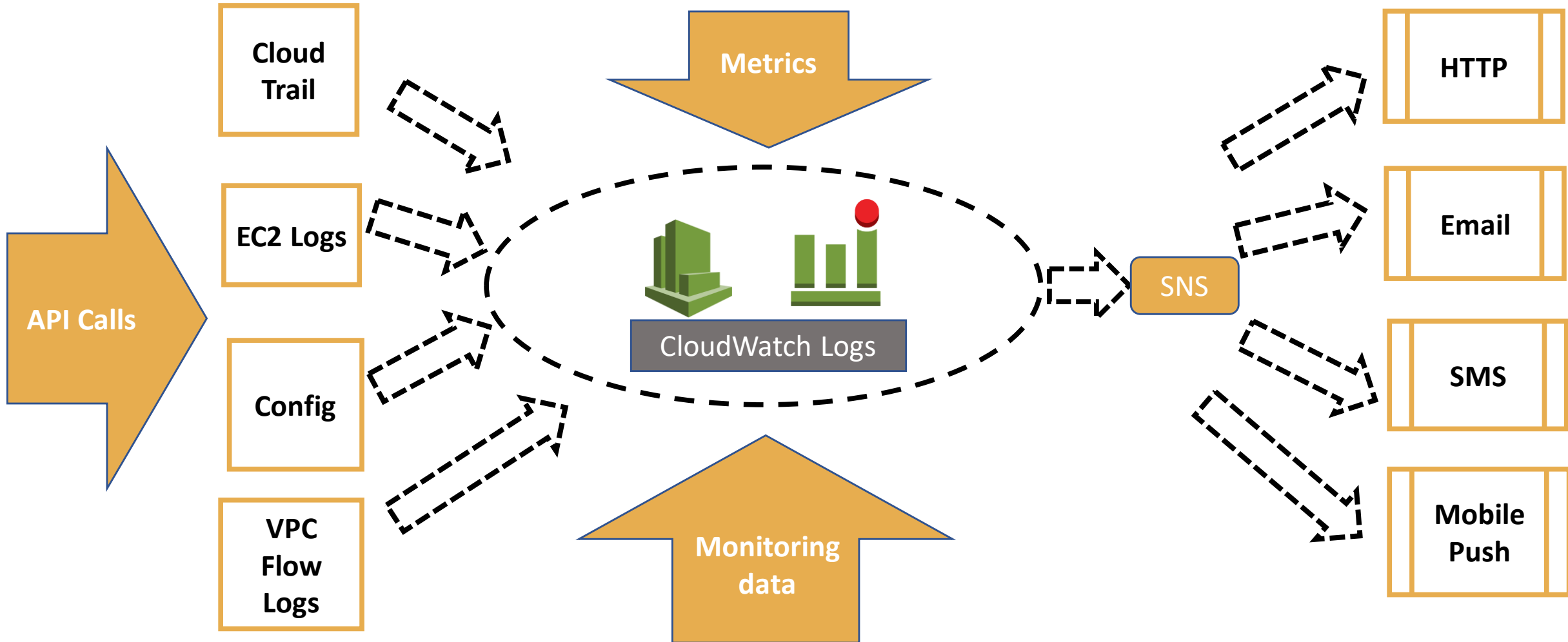
- Built-in application that analyzes your AWS account based on best practices
- Analyzes security and account service limits
- Bucket permissions, security groups, MFA on root account, EBS and RDS public snapshots

# CloudWatch



- Built-in monitoring service at AWS
- Metrics available for all AWS services
- Alarms – linked to auto scale
- Alerts – linked to each service
- Cloud watch logs – EC2 instance system logs

# CloudWatch Operation



# CloudWatch Cheat Sheet

- Collect and track metrics with CloudWatch
- Alert when Instances are under load
- Collect and monitor log files with CloudWatch logs
- Alarm when errors occur in your system logs
- Provide automated alarms with SNS
- Events trigger Lambda function



# Automation Cheat Sheet

- EC2 Auto Recovery – utilize CloudWatch alarm to monitor and recover impaired EC2 Instances
- Auto Scaling – scale healthy EC2 Instance capacity up and down, across multiple availability zones based on your defined conditions
- CloudWatch Alarms - when defined metrics, exceed defined thresholds, for a period of time.
- CloudWatch Events – near real-time system event stream describing changes in AWS resources. Rules throughout event types to Lambda functions, Kinesis streams, SNS topic
- Lambda Scheduled Events – custom Lambda functions executing on a schedule

# Scaling Cheat Sheet

- Vertically – Increase RAM, CPU, I/O, or networking speeds
- Horizontally – increase the number of resources
- Add more EBS hard drives to storage array
- Scale out: 10 GiG chunks at a time with Aurora
- Auto scale: add / remove instances to load-balancing queue
- Push - ELB, Auto Scaling, SNS, Global load-balancing with Route 53
- Pull - Message queue – Simple Queue Service

# Cloud Formation

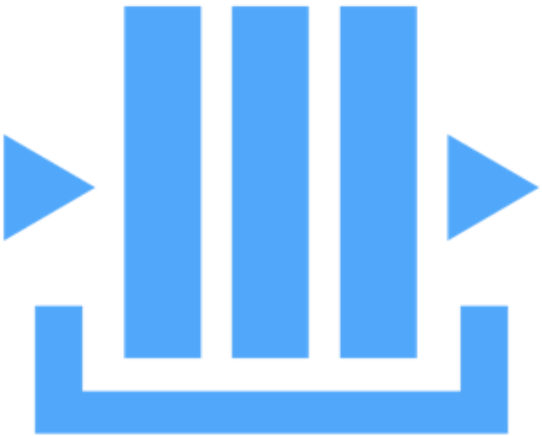


- Automation service for deploying AWS resources
- Supports JSON and YAML scripts
- The scripted describes all the AWS resources to deploy for your stack
- Deploy, modify, update, compare, and delete stacks



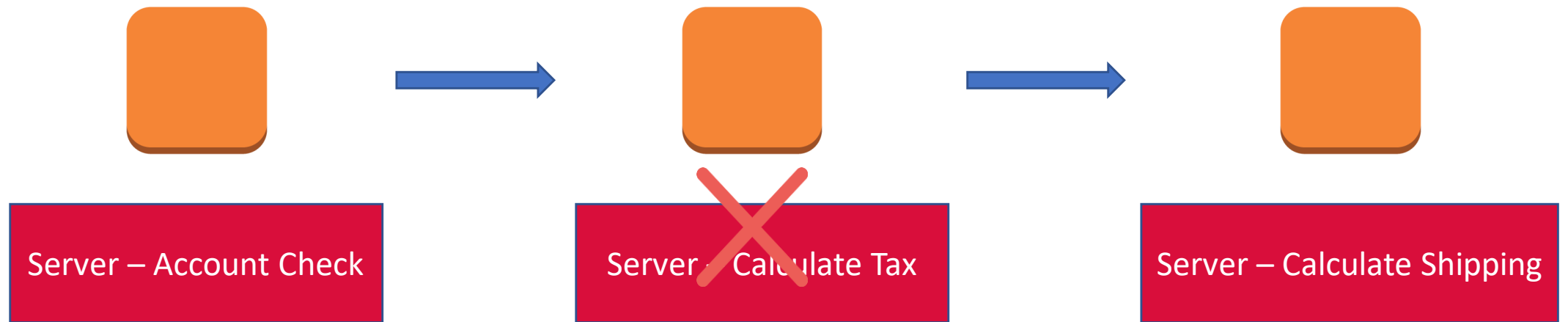
SQS

- Simple Queue Service
- Polling modes: Push, Pull
- Text-only
- Message lifecycle
- Asynchronous work queues

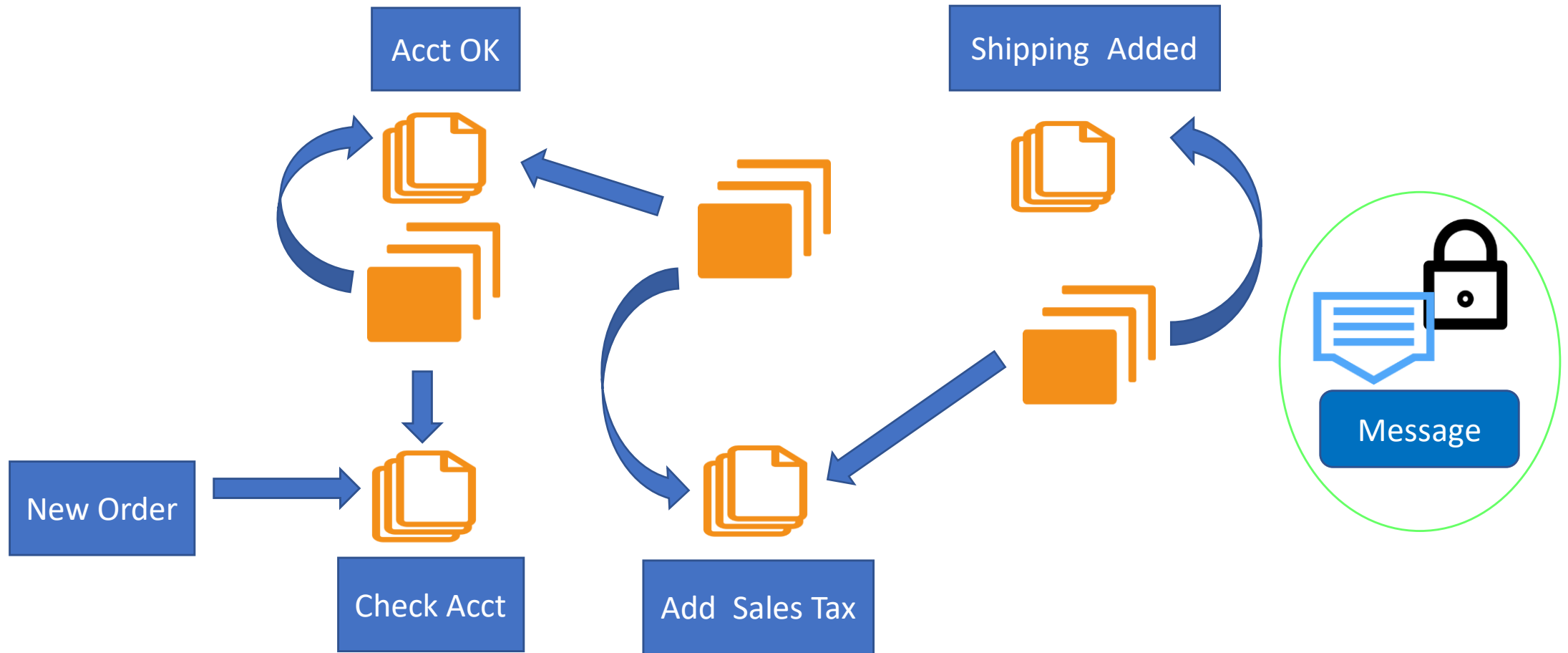




# Tight Coupling



# Loose Coupling

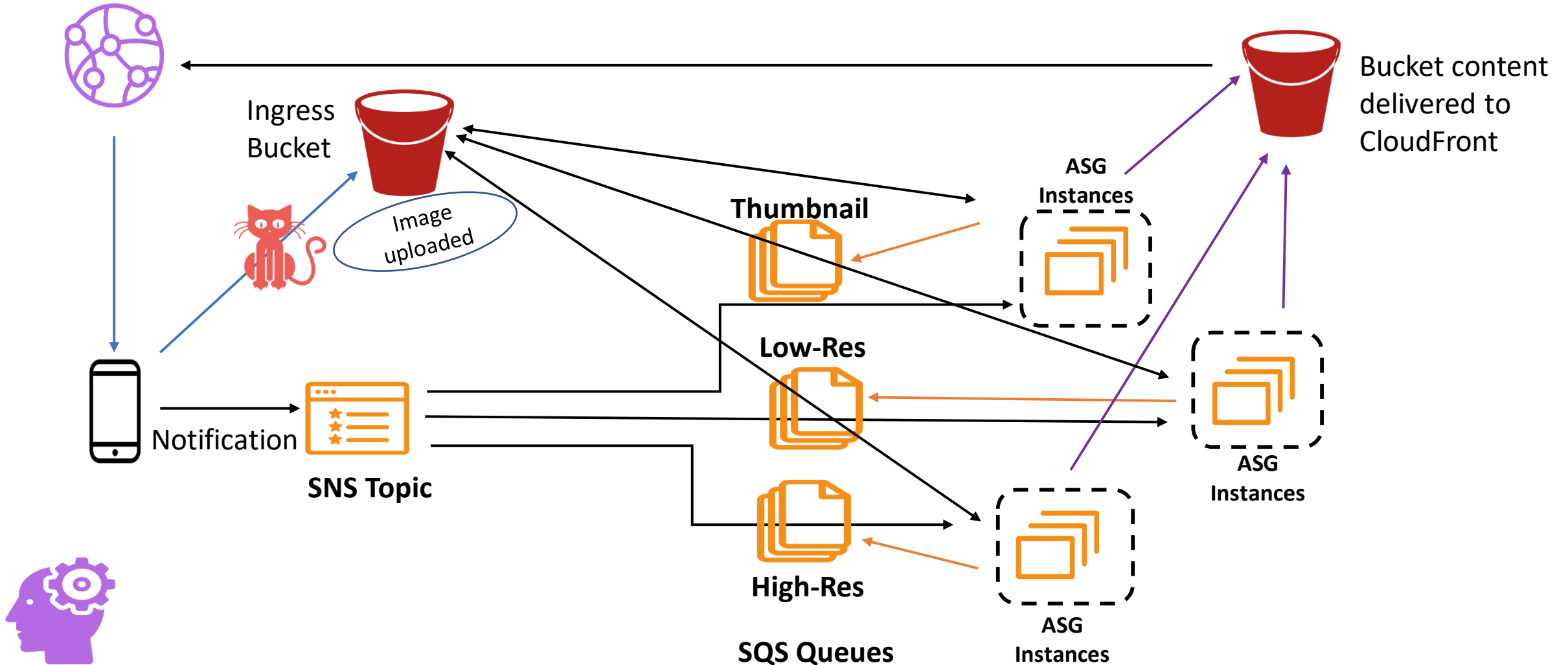


SNS

- Push model
- Subscribe to topics
- Delivery mechanisms: HTTP / HTTPS, SQS, SMS, Email
- SQS with CloudWatch alarms



# Design Project: Image Processing





Domain **Three**:

Data Security

# Data Security



Read resources found here:



<http://aws.amazon.security>

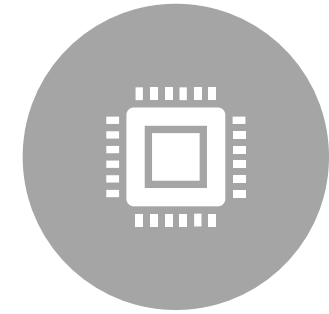


<http://aws.amazon.com/compliance>

# Build Security in Every Layer



INFRASTRUCTURE  
LAYER



COMPUTE /  
NETWORK LAYER



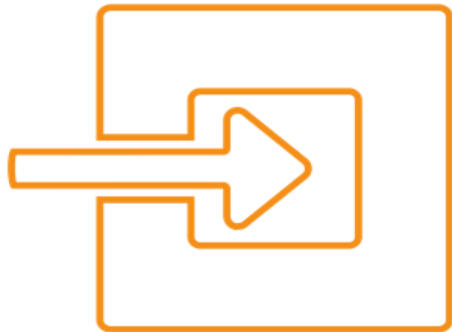
DATA LAYER



APPLICATION  
LAYER

## Data in Transit

- In and out of your AWS infrastructure
- SSL over web – use HTTPS endpoints
- VPN for IPsec - VPG connections
- Direct Connect – private high-speed fiber connection; from 1 to 10 gig speeds





# AWS S3 Storage

---

# Object Storage



- Can be any file type
- Complete file must be replaced when changes are made
- 5 TB size limit
- No limit on bucket contents overall size

# Durability

- 11 nines durability (99.9999999999)
- 4 nines availability (99.99)
- Stored in 3 physical locations within each region



# S3 Storage Classes

An orange document icon with a folded top-right corner. A white rectangular label is positioned on the lower-left part of the document, containing the word "CLASS" in orange, bold, uppercase letters.

**CLASS**

- S3 Standard – no minimum storage time
- S3 Intelligent-tiering – monitor and move after 30 days
- S3 Standard-1A – min 30 days
- S3 One Zone-1A – one AZ – min 30 days
- S3 Glacier – min 90 days
- S3 Glacier Deep Archive – min 180 days

# Versioning



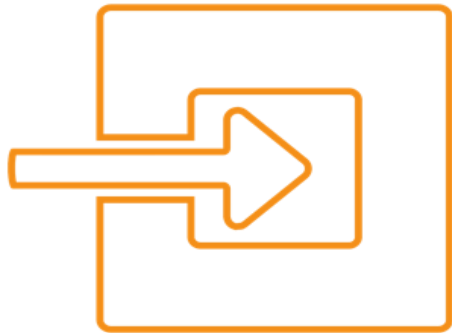
- Versioning can be enabled at the root of the S3 bucket
- Ensures that all files remain even the original copy
- When files are uploaded and changed, the new copy has a separate version number from the original object

# Lifecycle Policies



- Versioning must be enabled to take advantage of lifecycle policies
- Lifecycle policies control retention and movement of S3 data
- Transition actions – move to another storage class
- Expiration actions – when objects expire, i.e. are deleted

## Data at Rest on S3



- IAM Policies
- Bucket Policies
- Access control lists
- Temporary credentials; used for signed URL's
- Encryption
  - Server-side – AWS managed keys
  - Server-side – customer managed keys
  - Client-side encryption – client code encrypted decrypts

# S3 Storage Cheat Sheet

- Versioning allows preserving and retrieving every stored object
- Integrated with CloudTrail, CloudWatch, SNS, and Lambda for event notifications
- Lifecycle policies control the archiving of S3 data to Glacier vaults
- Glacier data is automatically encrypted; secure with vault lock policies





# S3 Storage Cheat Sheet

- Object level storage providing high durability; objects stored on three facilities within a region
- Storage tiers include Standard, Standard IA, Reduced Redundancy
- Pre-signed URLs can be used for sharing without requiring AWS security credentials
- Security provided by OAI User, signed URL's for RTMP distribution, or signed cookies



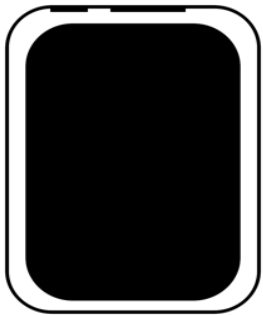
# S3 Glacier



- Archive storage
- Archives can be up to 40 TB
- Unlimited number of archives in S3 Glacier
- Archives cannot be updated
- Vaults store archives
- Vault lock controls – Write Once Read Many
- Expedited, standard, and bulk data retrieval options
- Snowball devices integrate with S3 Glacier

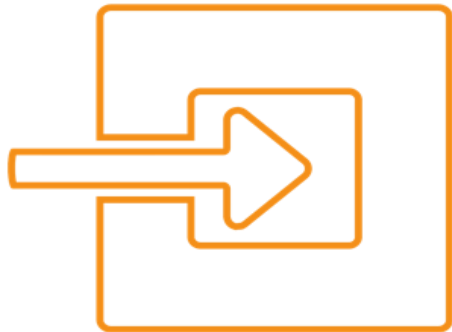


EBS



- Virtual Hard Drives
- Attached to EC2 instances directly
- Can be backed up with point in time, snapshots
- General purpose SSD drives
- IOPS performance up to 64,000
- Scalable
- Cold storage hard drives
- Throughput storage hard drives

## Data at Rest EBS



- Encrypted, EBS volumes - AWS managed keys
- Encrypted file systems on EBS volumes
- Encrypted data at the application layer
  - Apps encrypt/decrypt data on client side
  - Customer managed keys
  - Transparent Data Encryption in some databases TDE

# EBS Storage Cheat Sheet

- EBS network attached block storage
- EBS volumes cannot be shared with multiple EC2 Instances
- Multiple volumes can be attached to a single EC2 Instance
- Volumes can be detached and attached to another EC2 Instance only in the same AZ
- Snapshots cannot span across regions
- Snapshots can be restored to a new volume in the region
- Snapshots can be copied to a different region and restored as a volume in the new region



# AWS RDS

---

# RDS Platforms

- Amazon RDS is a managed relational database service
- Six database engines to choose from: Aurora, MySQL , MariaDB, Oracle, Microsoft SQL, Postgre SQL



# RDS features



- Use AWS Database Migration Service for migration to RDS
- Scalable compute and storage
- Multi-AZ deployment
- Automatic software patching
- Automatic backups and failover
- Point in time recovery
- Amazon RDS supports Transparent Data Encryption in SQL Server and Oracle database engines



# Read Replicas

- Asynchronous copies of master database instance
- Allows read-only connections
- Choose regions to deploy
- Takes query load off master database instance
- Read replicas can be promoted to become standalone DB instances
- Available for MySQL, MariaDB, PostgreSQL, and Oracle



# Aurora

- MySQL and PostgreSQL compatible
- Auto scales to 64 TB per database instance
- Up to 15 read replicas





# Database Options: Aurora

- Relational database engine with 5 times the performance of MySQL
- Fully managed – 6-way replication across 3 availability zones
- MySQL and PostgreSQL compatible
- Database engine integrated with SSD Virtual SAN
- Minimal database storage is 10 GB; can scale to 64 TB in 10 GB chunks

# Database Options: DynamoDB

- Document data model supports using JSON on documents stored in Dynamo DB tables
- Dynamo DB is designed with automatic synchronous data replication across three facilities in a region
- DynamoDB table can be Local or Global (Across regions)

# Understanding Durability

Data replication updated the redundant copies of data  
S3 – multiple copies within the region, versioning, cross region replication within and across regions

EBS – multiple copies within the facility, manual snapshots, manual copy snapshots across regions

## Database Durability

- Synchronous replication – the transaction is complete only after it has been durably stored in both the primary and secondary replicas
- Synchronous replication has strong consistency
- Asynchronous replication – changes performed on the primary node are not immediately performed on the replicas



# Database Scalability

- Relational databases scale well vertically
- Upgrade to a larger RDS instance
  - Add faster storage
  - IOPS
- Horizontally scale using read replicas
- Multi-AZ deployment – synchronously replicated standby instance in a different AZ
  - Failure invokes automatic failover to the standby without the need for manual intervention
- Sharding – data split across multiple database schemas each running in its own autonomous primary database instance (A-E, F-J, etc.)



Domain **Four**:

Troubleshooting

# Troubleshooting topics



EC2 instance connectivity



EC2 instance recoverability



EBS volume recovery



Service limits



# Why can't I connect to my instance?



Is an IGW or VPG attached?



Do my route tables have entries pointing to the resources I need to connect to?



Do I have an EIP or public IP address on instance for public communication?



Are NACLs defined on the subnet?

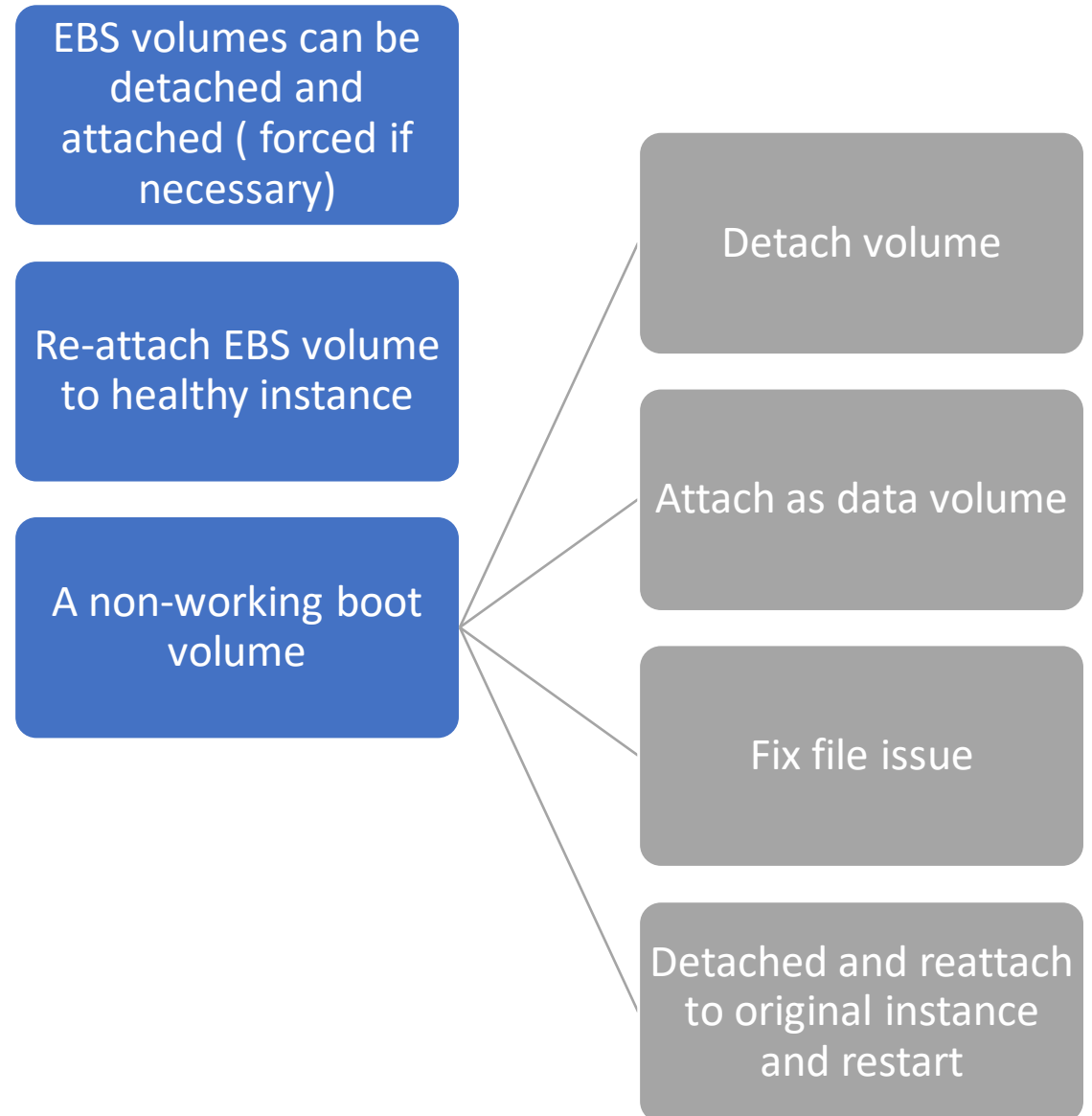


Is the Security Group set properly for inbound rules?



Is an operating system level firewall installed?

# Troubleshooting, EBS volumes



# Soft and Hard Limits

Many soft limits

A few hard limits – 100 S3 buckets per account

Limits can mask problems

EC2 instances can't be launched because EBS limit has been reached

Remember to use Trusted Advisor to check soft limits for account

Limits to  
know....but  
not memorize

20 instances per account

5 EIPs per region

100 security groups per VPC

20 load balancers

20 auto scaling groups

# What we covered today



- Prepping for the AWS Architect Associate Exam
- Taking the exam – what's covered – domains of knowledge
- The essential AWS core services to understand