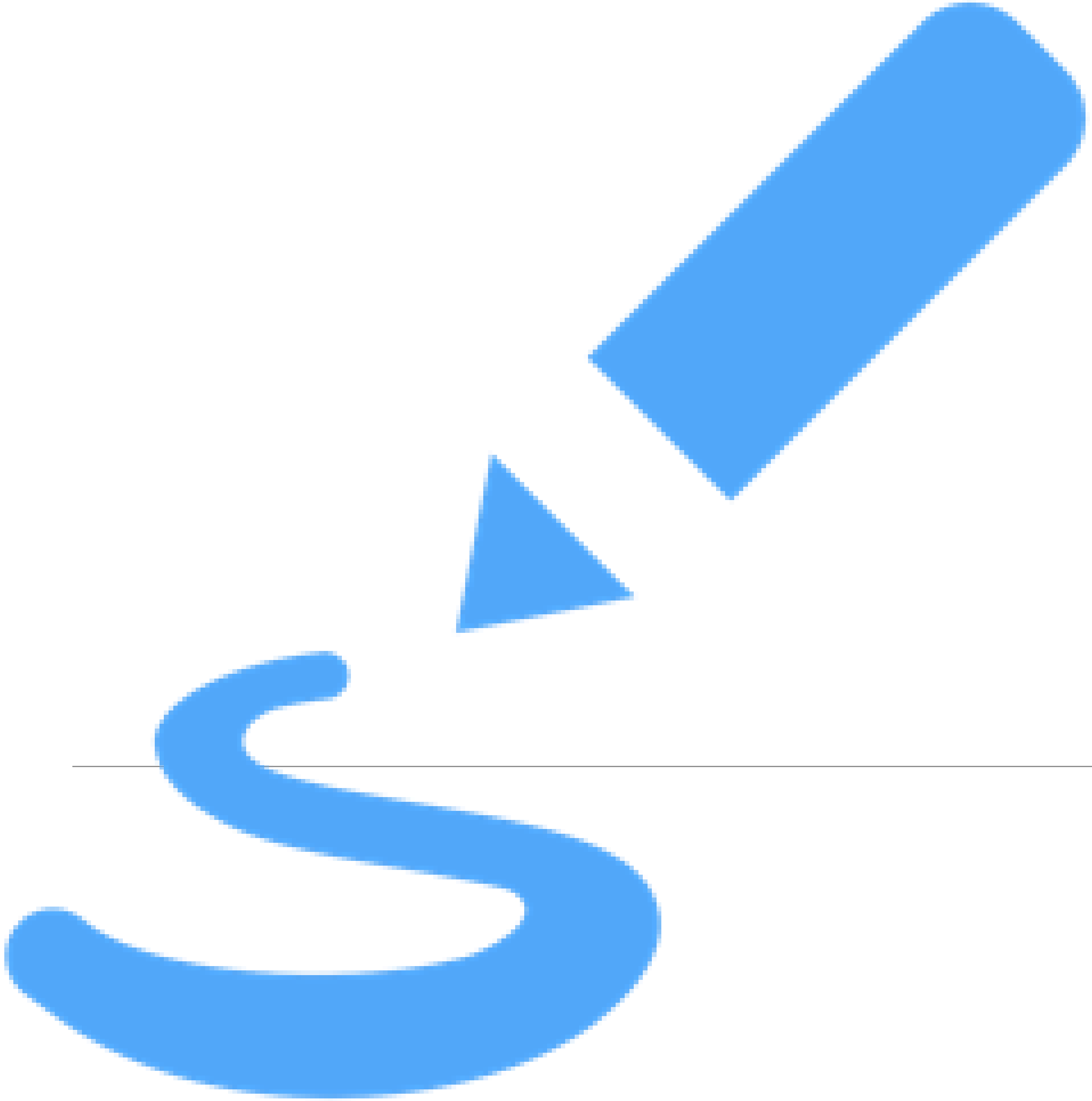
Amazon Web Services
Architect Associate Certification



AWS Core Architecture Concepts

What We will Cover

- Fundamentals of AWS: Architecture, terminology and concepts
- Virtual Private Cloud (VPC): Networking services
- Amazon Elastic Compute Cloud (EC2): Instance deployment and configuration
- Storage solutions: Elastic Block Storage (EBS) and snapshot management
- Simple Storage Service (S3): Object storage
- Glacier: Archive storage

Communication

Q and **A**

Group Chat

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
- Proposed

The correct answer is the best answer based on the suggested answers to multiple choice questions

Documentation

AWS Certified Solutions Architect - Associate

AWS Certified Solutions Architect – Study Guide

AWS Certified Solutions Architect – Sample Questions

Solutions Architect Documentation

AWS Quick Starts

- https://aws.amazon.com/quickstart/

Self Paced Labs

- https://aws.amazon.com/training/self-paced-labs/?nc2=h_l2_tr

AWS Documentation

- https://aws.amazon.com/documentation/

AWS Discussion Forums

- https://forums.aws.amazon.com/index.jspa?nc2=h_l2_su

Certification Study Guide Example:

AWS Component

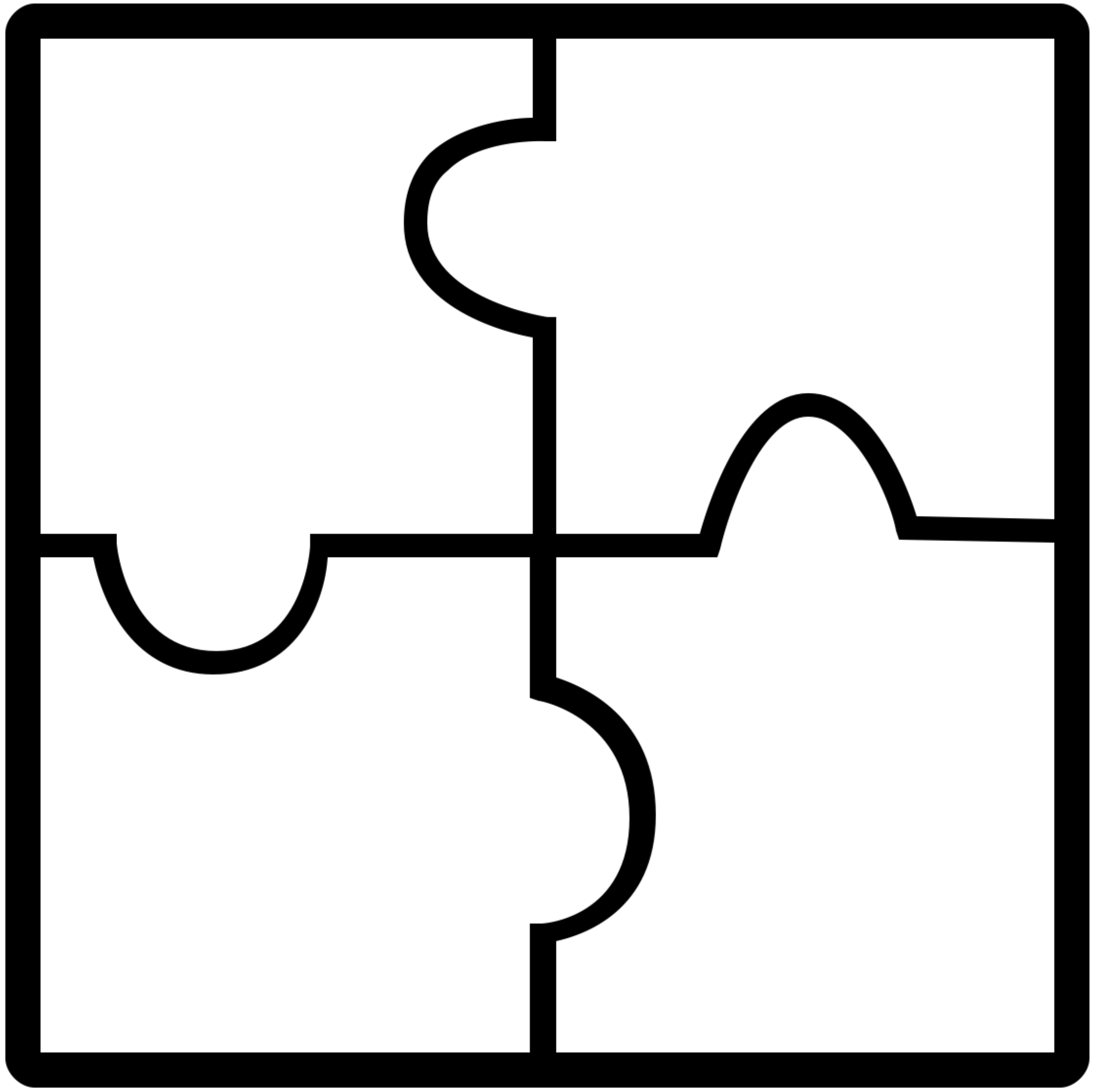
- Regions and Zones

Read FYI, documentation, or watch video

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html
- https://docs.aws.amazon.com/acm/latest/userguide/acm-regions.html

Setup component

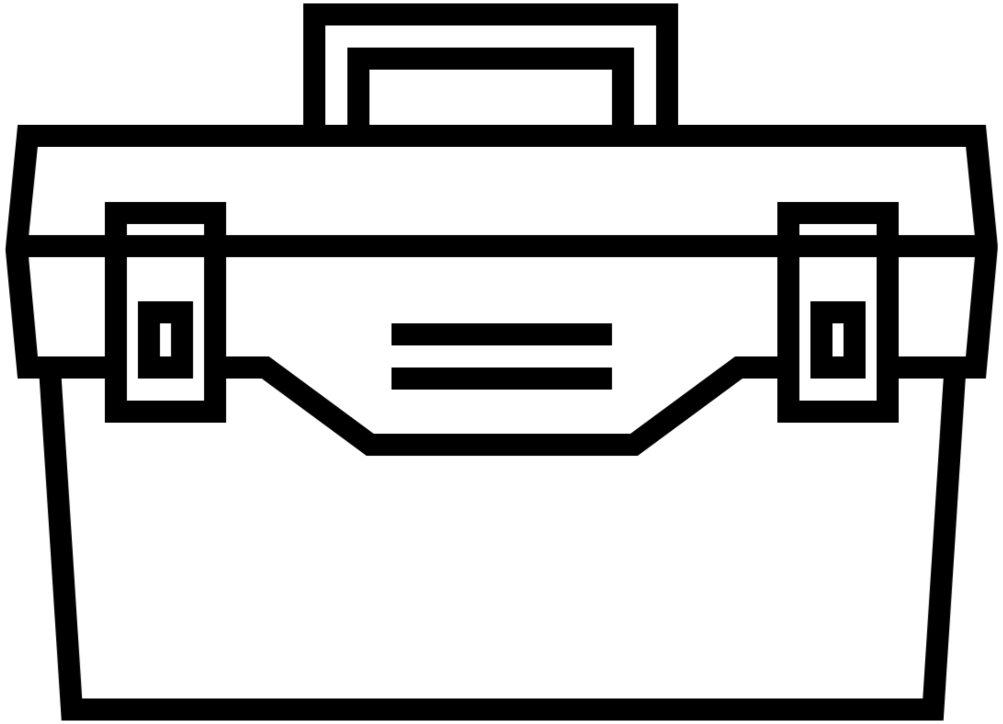
- Open EC2, CloudFront, and S3 to see the change from Region to Global location (Edge)



Core Architecture Concepts

AWS Cloud Services

- Accessing AWS – Management portal
- Compute Services – Elastic Compute Cloud
- Networking Services – Virtual Private Cloud
- Auto Scaling – Scale EC2 capacity automatically
- Elastic Load Balancing – Distribute application traffic across EC2 instances
- Elastic Block Storage – Virtual hard drives
- Simple Storage Service – Durable, scalable object storage
- Glacier – Long-term data archiving and long-term backup

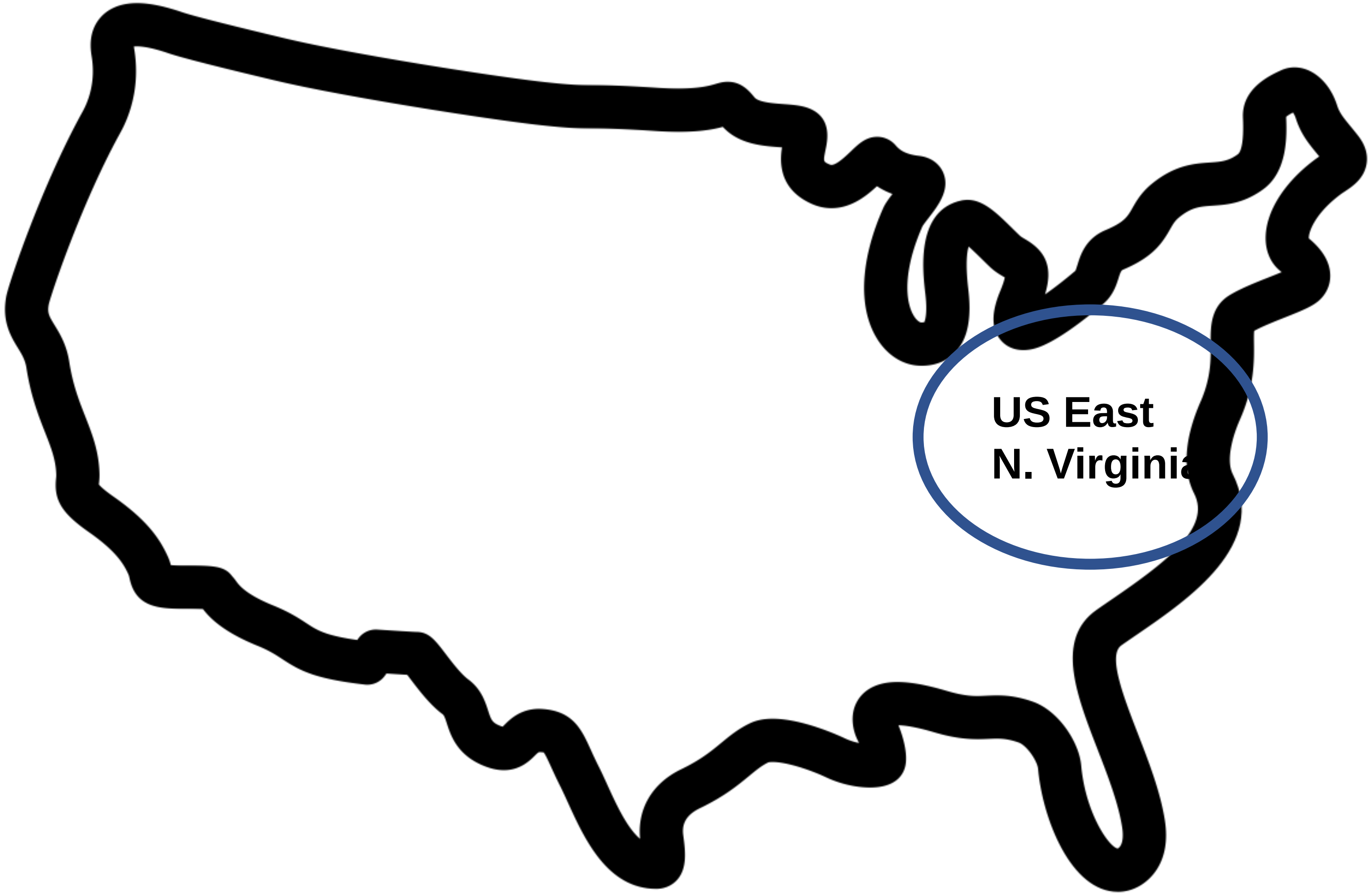


Cloud Services

- Unmanaged services: You can do whatever you want
- The bad news: You have to do most of the setup, management, and monitoring (VPC, EC2)
- Managed services: AWS does the majority of the setup
- The reality – there are no completely unmanaged services at AWS

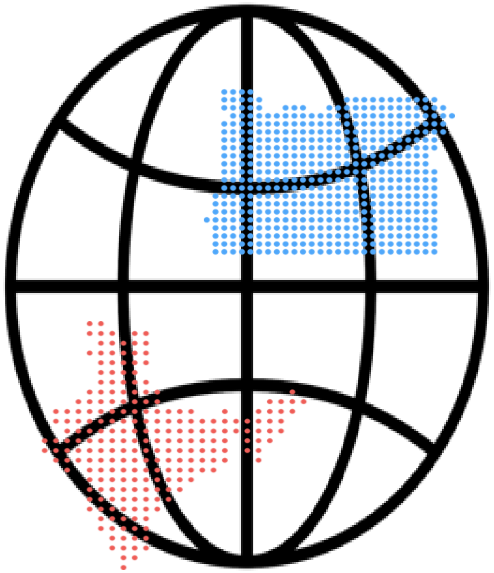
Exercise: Essential AWS Services

Regions

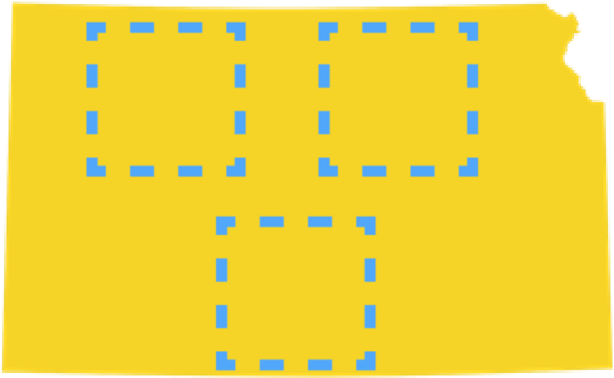


Case Study: Terra Firma

AWS Regions



Regions are Independent



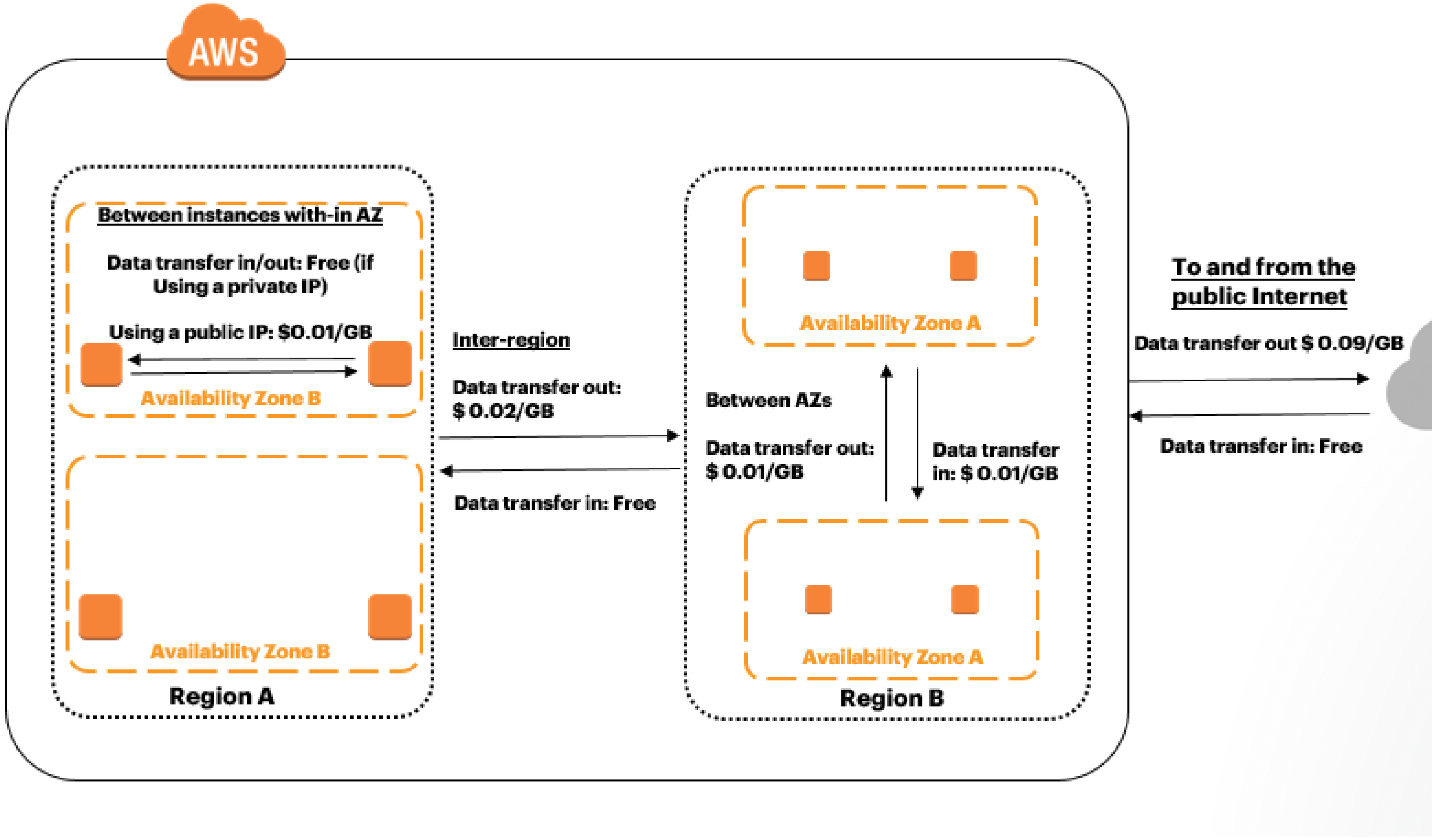
Regions have (multiple) Availability Zones

Data transfer charges between regions apply

Resources are not automatically replicated between regions

What AWS region would you suggest for Terra Firma?

AWS Costs



AWS

Between instances with-in AZ

Data transfer in/out: Free (if Using a private IP)

Using a public IP: $0.01/GB

Availability Zone B

Availability Zone B

Region A

Inter-region

Data transfer out: $ 0.02/GB

Data transfer in: Free

Availability Zone A

Between AZs

Data transfer out: $ 0.01/GB

Data transfer in: $ 0.01/GB

Availability Zone A

Region B

To and from the public Internet

Data transfer out $ 0.09/GB

Data transfer in: Free

Which Region ?

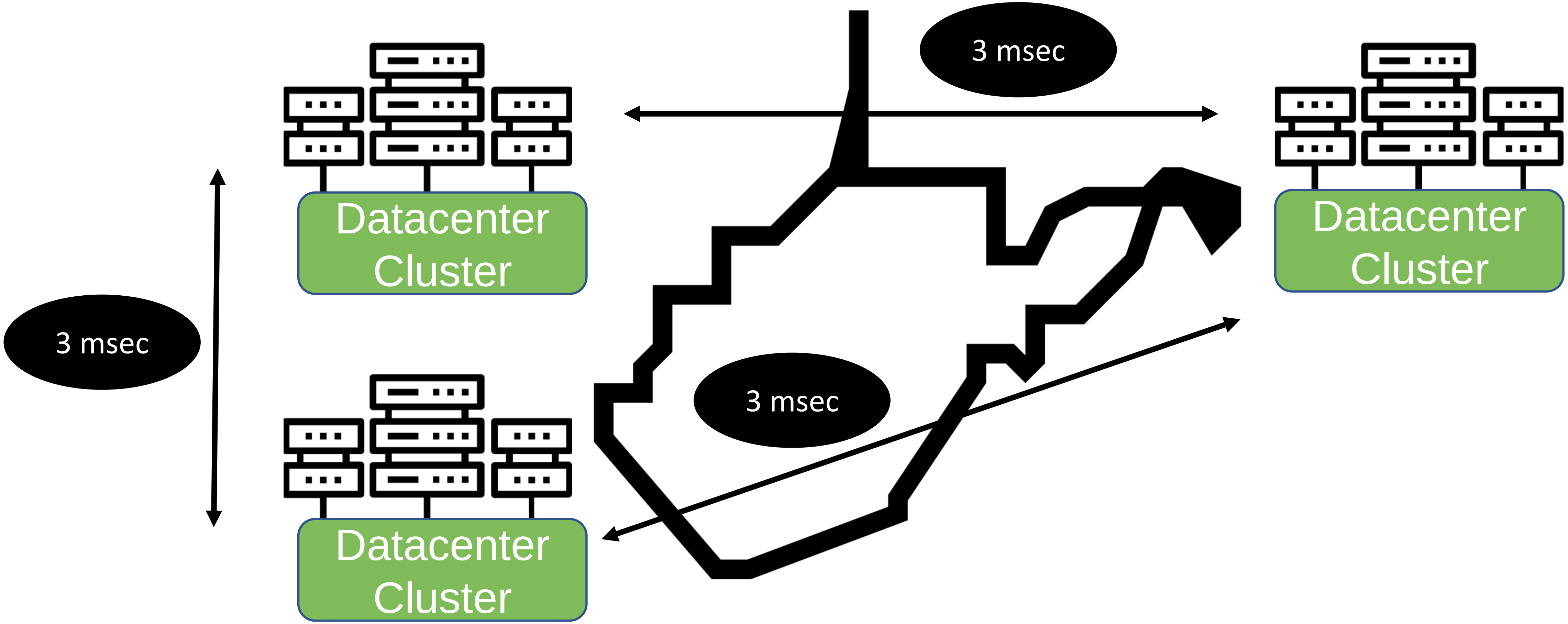
Latency – to on-prem
Customers location

Costs are different
for each region

Feature-set's are
different per region

Compliance: Industry,
Country, and business

Availability Zones (AZ)



Availability Zones (AZ)

Isolated locations

AWS account has access to multiple regions

Data transfer charges for cross AZ traffic

Connected with multiple Tier-1 transit private connections

Availability Zones are represented by a region code followed by a letter identifier

Example: us-east-1a

Workload Considerations

Select region matching compliance needs

Choose availability zones for application failover

How many AZ’s should Terra Firma use?

Single or Multi-AZ Design ?

SINGLE - AZ

- No potential recovery when disaster happens
- No high availability
- No automatic failover
- All regions have at least 2 availability zones

MULTI - AZ

- Better high availability design options
- Scalability across AZ’s provides HA
- Load balancing (ELB) can balance across availability zones
- Use Route 53 (DNS) to provide Geo-load balancing across AWS regions

Edge Locations

Edge Locations

- Provides a local entry point to AWS resources

client
dns
data

- POPs in over 55 cities across 24 countries
- Edge services (Global)
  - Route 53
  - CloudFront (113 POPs)
  - Web Application Firewall (Place in front of CDN or ALB)
  - Regional edge cache locations

AWS Resource Locations

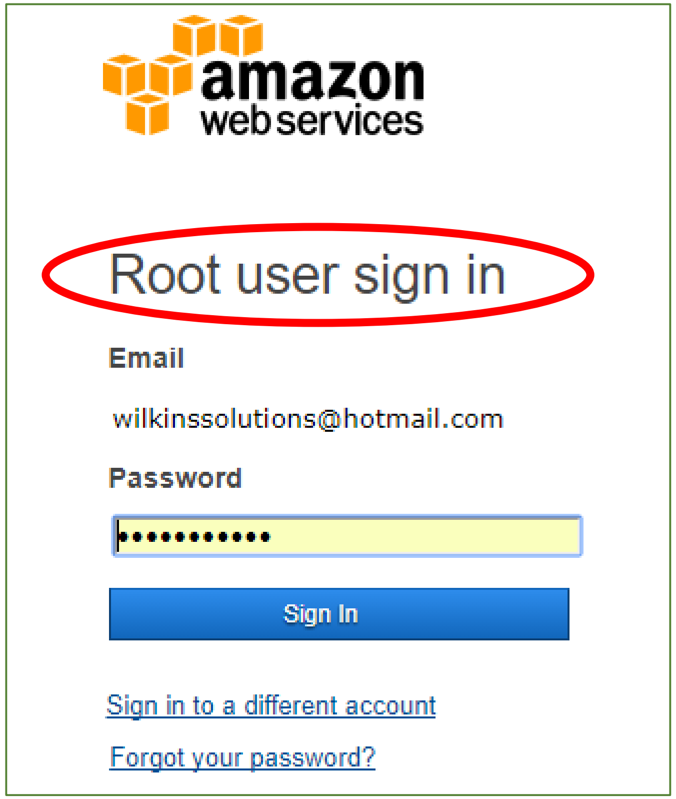
Resources are either Global, Region specific, or associated to an Availability Zone

Exercise: Regions and Availability Zones

Accessing AWS Cloud Services

- Access to all AWS services is by using a specific API call
- Application Programming Interface (API)
- Common Access Methods
  - The AWS Management Console – web-based application
  - AWS Command Line Interface (CLI) Windows, Mac, and Linux
  - AWS Tools for Windows PowerShell
  - AWS Software Development Kits (SDK)

Signing in to the AWS Console



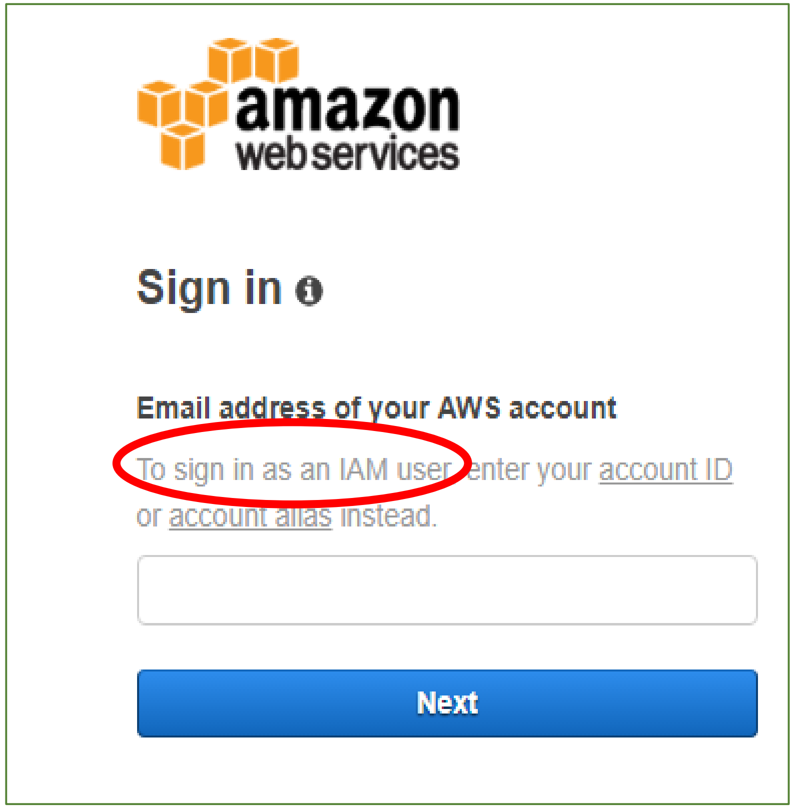
Root user sign in

Email

wilkinssolutions@hotmail.com

Password

••••••••••••



Sign in

Email address of your AWS account

To sign in as an IAM user enter your account ID or account alias instead.

Exercise: Using the Management Console

Using the CLI

- Describe existing EC2 Instance in my account:

```
$ aws ec2 describe-instances
```

- Start an EC2 Instance:

```
$ aws ec2 start-instances --instance-ids i-1348636c
```

- Get help for a service:

```
$ aws autoscaling help
```

Using PowerShell

- Launch an EC2 Instance:

```
New-EC2Instance -ImageId ami-c49c0dac -MinCount 1 -MaxCount 1
- KeyName myPSKeyPair -SecurityGroupId sg-5d293231
- InstanceType m1.small -SubnetId subnet-d60013bf
```

- Create a Security Group:

```
New-EC2SecurityGroup -VpcId "vpc-da0013b3" -GroupName
"myPSSecurityGroup" -GroupDescription "EC2-VPC Admin access"
```

Virtual Private Cloud

What’s a VPC?

- Network layer at AWS
- A logical and isolated data-center (virtual private cloud)
- Launch EC2 instances and various AWS resources into your virtual network (software data-center)
- Logically isolated from all other virtual networks hosted in the AWS cloud
- Networking platforms: EC2 - Classic and EC2 - VPC
- EC2 Classic is not available for new customers

Amazon VPC

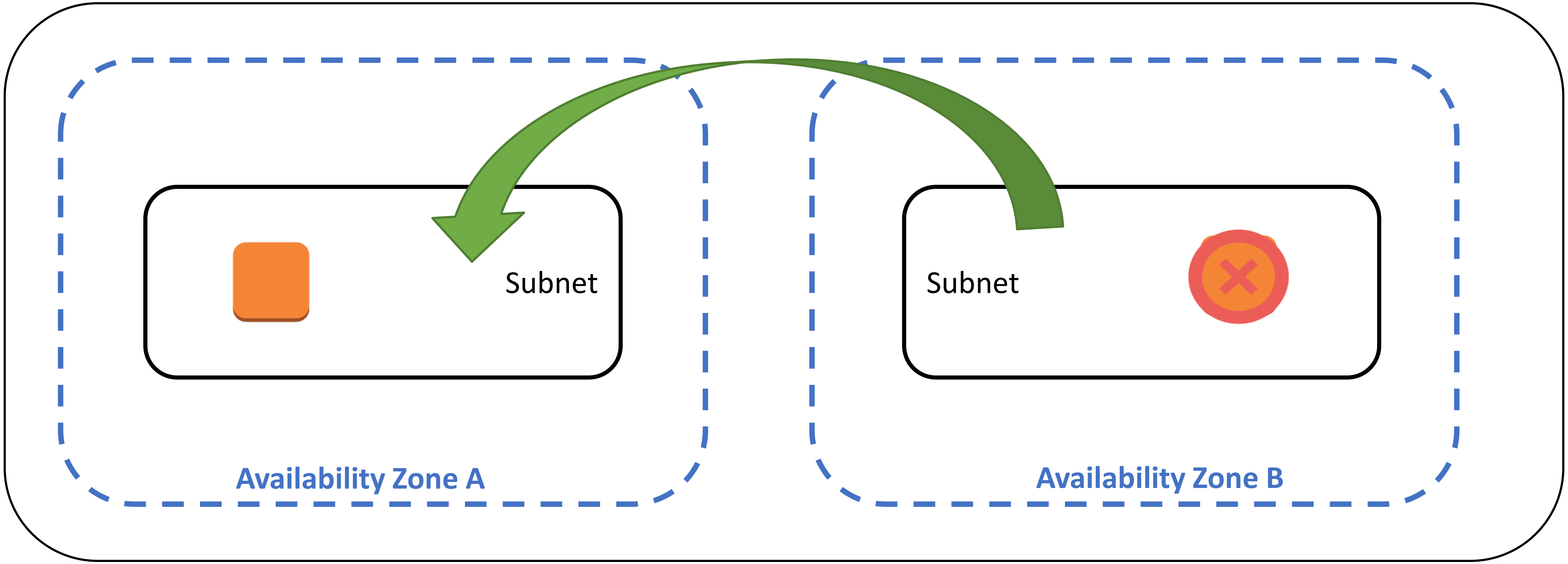
Network Platforms

- EC2 – Classic
  - The original network infrastructure for EC2 instances
  - Instances run in a single flat network that you share with other customers
  - Doesn’t support enhanced networking, multiple IP addresses, changing security groups, etc.
- EC2 – VPC
  - Instances run in a virtual private cloud that is logically isolated to your AWS account

Creating a New VPC

- When a VPC is created, it spans all the availability zones that you have defined within the selected region
- Subnets can be created in each availability zone
  - Each subnet is defined by a CIDR block which is a subset of the VPC CIDR block
- Each subnet is assigned a default route table that enables local routing throughout each VPC

VPC Design: Best Practice



VPC Design Decisions

- EC2 instance placement
- IP address range
- Subnets
- Route tables
- Network gateways
- Security settings – per instance
- Security settings – per subnet

VPC Components

- Subnets
- Route tables
- Dynamic Host Configuration Protocol option sets (DHCP)
- Security groups (SG)
- Network Access Control Lists (NACLs)

- Internet Gateways (IGW)
- Elastic IP (EIP) addresses
- Elastic Network Interfaces (ENIs)
- Endpoints
- Peering
- Network Addressed Translation (NAT) instances
- NAT Gateways
- External connectivity options (VPCs, CGWs, VPGs)

Exercise: Create a Custom VPC

How many VPC’s should Terra Firma consider?

The Default VPC

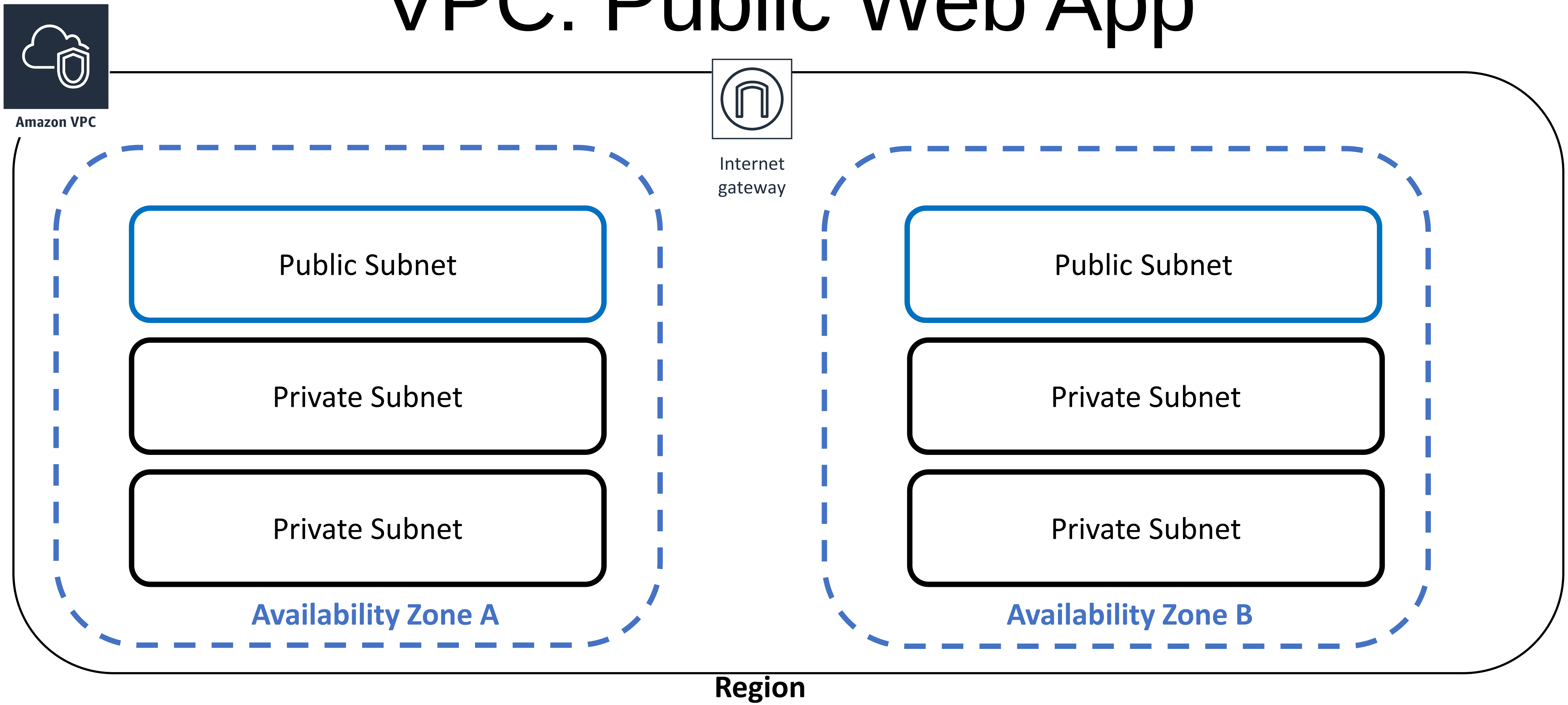
- /20 CIDR Block is assigned by default
- An Internet gateway is connected to the default VPC
- Main route table sends Internet traffic to the internet gateway
- Default security group
- Default network access control list
- Default subnets
- Instances are assigned both a private and public IPv4 address

Should Terra Firma just use the Default VPC?

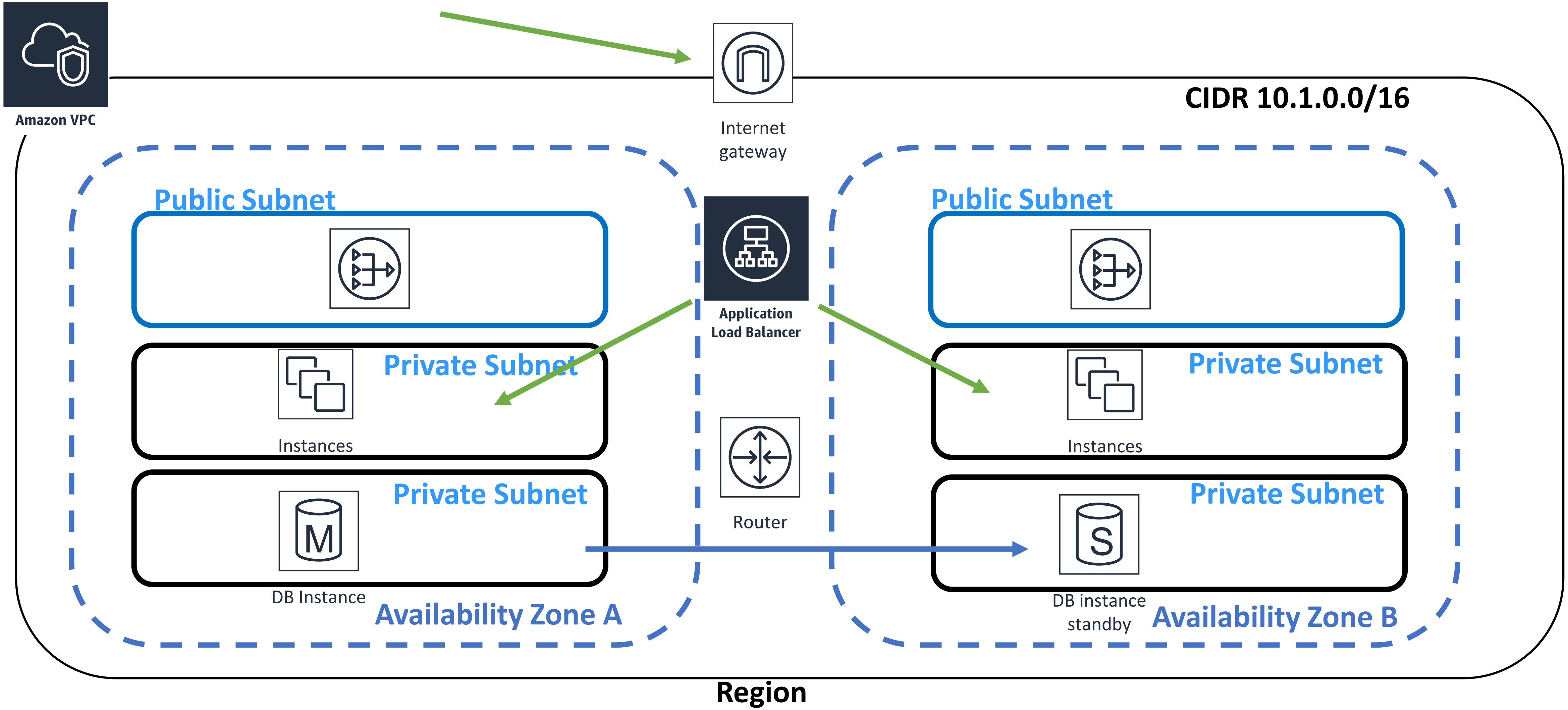
Exercise: The Default VPC

VPC Design

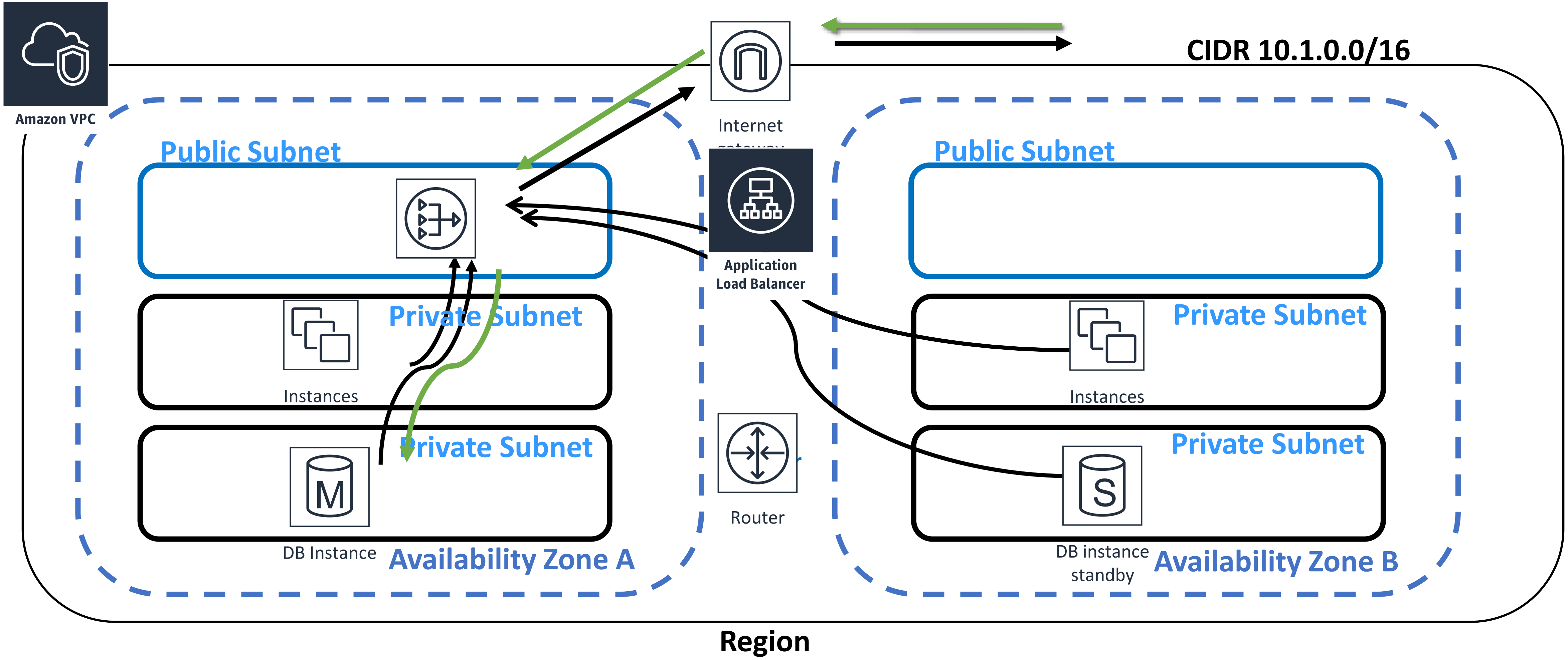
VPC: Public Web App



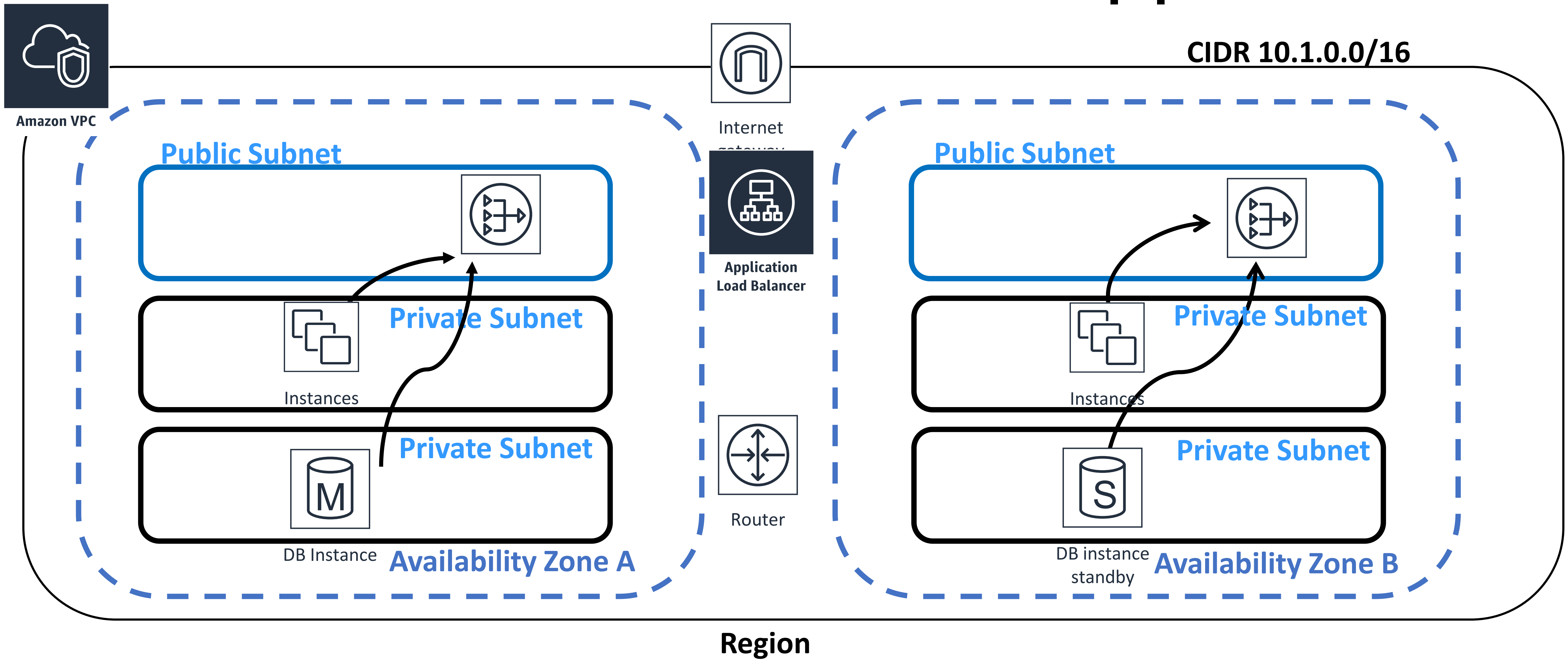
VPC: Public Web App



VPC: Public Web App



VPC: Public Web App



Subnets and Addressing

Subnets

- Public or Private subnets can be created in each availability zone
- Subnets cannot span across multiple availability zones
- If a subnet has traffic routed to an internet gateway it is defined as a **Public subnet**
- Instances in a Public subnet must have a public IPv4 address, or an Elastic IP address to be able to communicate with the Internet gateway
- A subnet that doesn’t route to an internet gateway is a **Private subnet**

Reserved Addresses

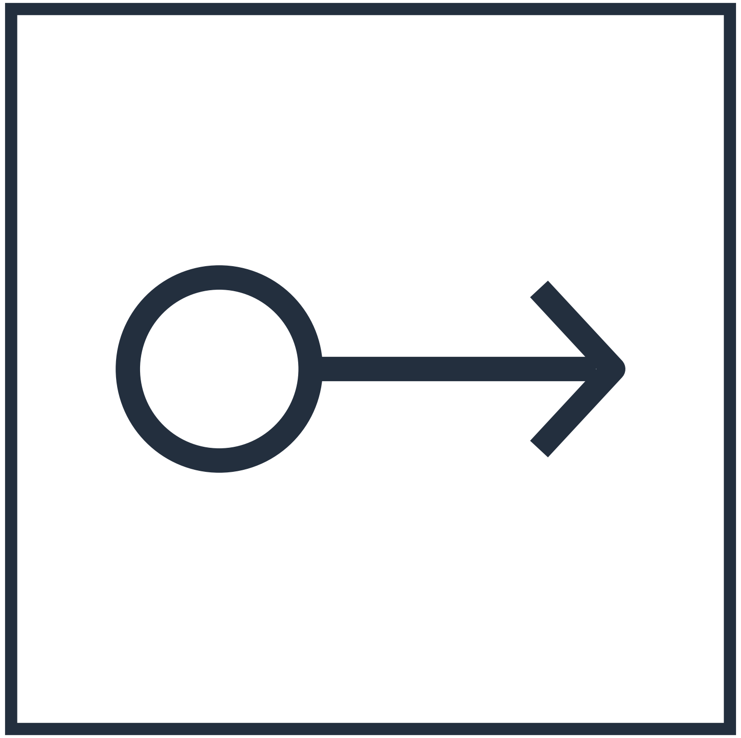
- The first four IP addresses and the last IP address in each subnet CIDR block are not available for use.
- Example: In a subnet with CIDR block 10.0.0.0/24, the following IP addresses are reserved:
  - 10.0.0.0: Network address
  - 10.0.0.1: Reserved for the VPC router (AWS)
  - 10.0.0.2: The IP address of the AWS DNS server is always the base of the VPC network range + 2
- 10.0.0.3: Reserved for future AWS use
- 10.0.0.255: Network broadcast address for the subnet
- Broadcasts are not supported across the VPC

Public IPv4 Addresses

- A subnet attribute determines whether network interfaces within a subnet automatically receive a public IPv4 address
- Public IP addresses are assigned from AWS’s pool of public IP addresses
  - These addresses are assigned and managed by AWS
  - When public IP addresses are released they are added back to the common AWS pool

Exercise: Create Subnets

How many subnets should Terra Firma use?



Elastic IP Addresses (EIPs)

- A persistent Public IP address is called an Elastic IP address
- Elastic IP addresses are assigned to your account and controlled (Assigned and removed from instances manually, or automated)
- An EIP is first allocated for use within a VPC; then assigned to a specific instance
- EIPs are specific to the region they are created in; they cannot be moved to a different region
- EIPs can be moved from one instance to another instance within the same VPC, or a different VPC within the same region

Do the Web servers need Public IP addresses?

Exercise: Order Elastic IP

Route Tables

Route Tables

- Each route table contains a default route called the “local route”
  - This enables communication within the VPC
- Each subnet created, is automatically associated with the master route table assigned to the VPC
- Each subnet must be associated with a route table
- Outbound traffic patterns are defined with a route table
- Additional routes can be created to allow VPC traffic to connect to the Internet gateway (IGW), a Virtual private gateway (VPG), a NAT service or end-point

Security Groups

Security Group Details

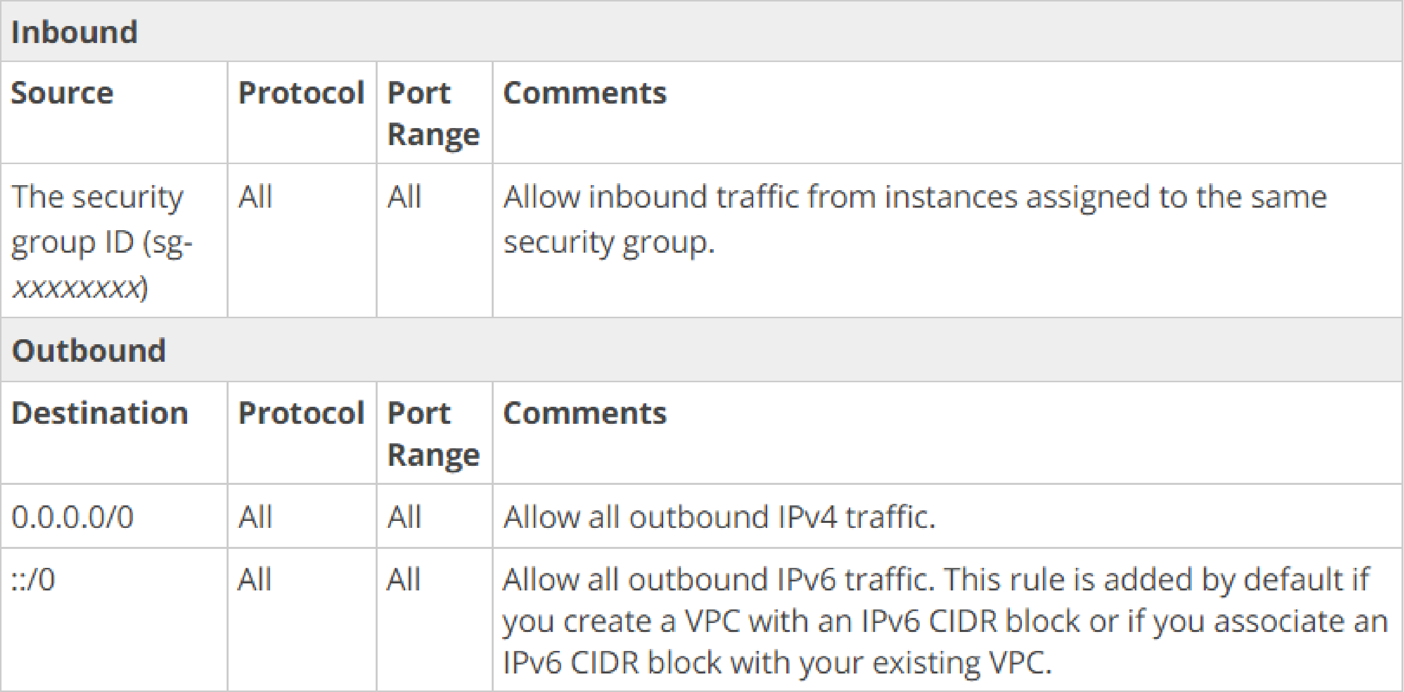
- Security groups work at the instance level
- Security groups are defined as “virtual firewall’ protecting EC2 instance’s inbound and outbound traffic
- Security groups contain rules that control the inbound and outbound traffic to Instances
- Each instance launched into a VPC can have up to 5 security groups
- Each SG can have 50 inbound / outbound rules
- Each VPC can have up to 500 Security Groups
- When security groups are created they are linked to your account for re-use

Security Group Rules

- Rules apply to either inbound traffic (ingress) or outbound (egress) traffic
- Allow rules **can** be specified
- Deny rules **can’t** be specified
- Inbound rules – the source of the traffic, and the destination port or port range
- Outbound rules – the destination for the traffic and the destination port or security group
- Any protocol that is defined with a standard protocol and number is supported
- Separate rules can be defined for both inbound and outbound traffic

Default Security Group

- Each EC2 Instance created in a VPC is associated with a default security group
- However you can change the association or the default security group



Inbound			
Source	**Protocol**	**Port Range**	**Comments**
The security group ID (sg-*xxxxxxxx*)	All	All	Allow inbound traffic from instances assigned to the same security group.
Outbound			
Destination	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	All	All	Allow all outbound IPv4 traffic.
::/0	All	All	Allow all outbound IPv6 traffic. This rule is added by default if you create a VPC with an IPv6 CIDR block or if you associate an IPv6 CIDR block with your existing VPC.

Security Group Operation

- Security groups are **stateful** – if a request is made to an instance flowing inbound, the response traffic for that request is allowed to flow out
- Responses to allowed inbound traffic are allowed to flow out
- Security groups are associated with the network interface(s) of the EC2 instance
- Security groups associated with an instance can be changed after the instance has been launched

Exercise: Create Security Groups

NACLs

Network ACLs

- NACLs operate at the subnet level of the VPC
- NACLs are an **optional security control**
- NACLs act as an “subnet firewall” for controlling traffic in and out of each subnet
- The default Network ACL for a VPC allows all inbound and outbound IPv4 traffic
- A subnet can be associated with only one network ACL at a time
- A network ACL can be associated with multiple subnets

Network ACL Rules

- Inbound Rule
  - Allow or deny for the specified traffic pattern
- Outbound Rule
  - Allow or deny for the specified traffic pattern
- Each subnet within a VPC must be associated with a network ACL

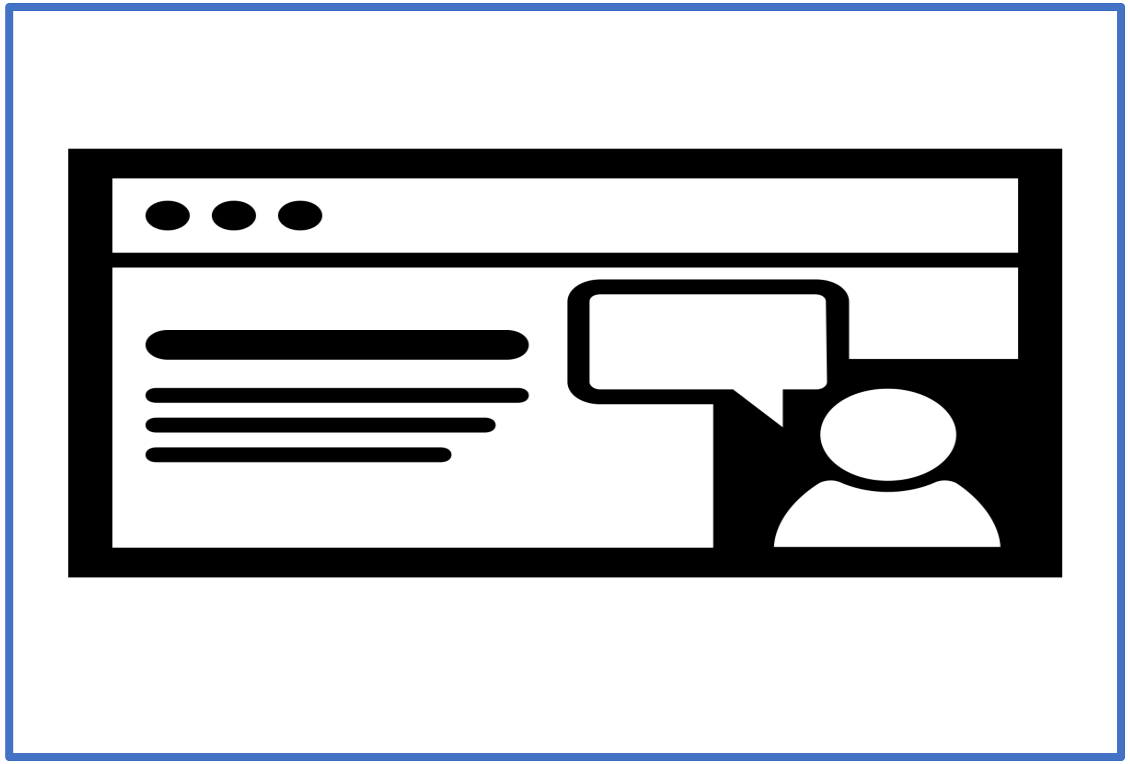
Network ACL Operation

- NACL rules are defined as **stateless**
- Rules are evaluated in order until a match is found
- Evaluation starts with the lowest numbered rule to determine if traffic is allowed in or out of the subnet associated with the network ACL
- Best practice: Create rules in multiples of 10, so adding new rules doesn't cause problems in the future

Security Groups vs NACLs

SECURITY GROUPS	NACLS
Operates at the instance level	Operates at the subnet level
Allow rules only supported	Allow and deny rules supported
Stateful: return traffic is automatically allowed	Stateless: return traffic must be explicitly allowed by a rule(s)
All rules are processed before traffic decisions are made	Rules are processed in numerical order before traffic decisions are made
Applied to the selected instance elastic network adapter	Applied to the subnet

Exercise: Configure Network ACLs



VPC Options

Endpoints

- A private direct gateway connection between a VPC and S3 storage, or Dynamo DB table
- A private direct interface connection between an AWS service

Endpoint Creation Steps:

1. Specify the VPC
2. Select S3 bucket, DynamoDB table, or AWS resource
3. Define the IAM policy
4. Specify the route table

Peering VPC’s

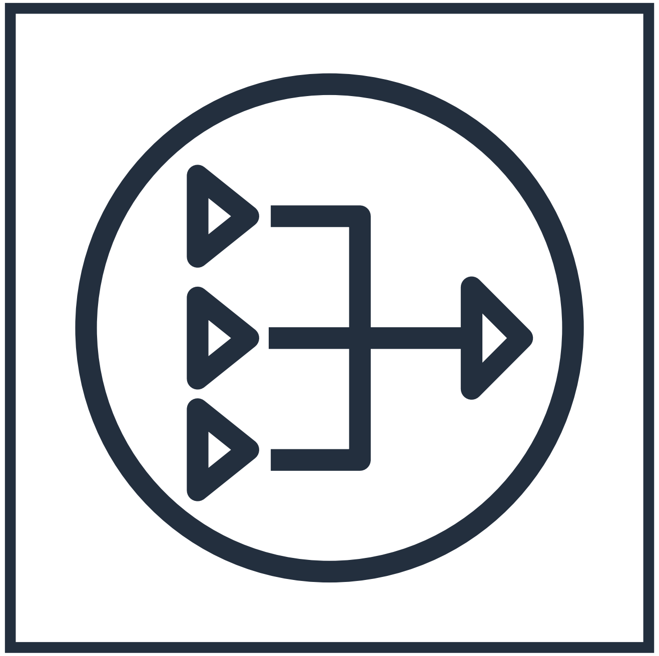
- Networking connection between two VPC’s
- Peer your VPC’s or between other account holders VPC’s
- Peering is a one-to-one relationship
- Peering connections are not transitive
- CIDR blocks can’t overlap in a peering relationship
- Peering connections can be created between VPCs in the same region
- Peering connections can be created between VPCs in different regions

VPC Flow Logs

- Flow logs can be created for a VPC, a subnet, or a network interface
- Shows IP traffic to and from network interfaces in a VPC (accepted / rejected)
- Each NIC has a unique log stream
- Flow log data is published to a log group stored as a CloudWatch log group or S3 Bucket
- Does not capture DNS, license, metadata, or default VPC router traffic

Exercise: Enable Flow Logs

NAT Gateway



- The NAT Gateway service accepts traffic from instances hosted on a private subnet
  - Translate the source IP address to the Elastic IP address of the NAT Gateway service
  - Forward the traffic request to the IGW
  - Returns incoming traffic to the private instance that made the request
- NAT Gateway creation steps:

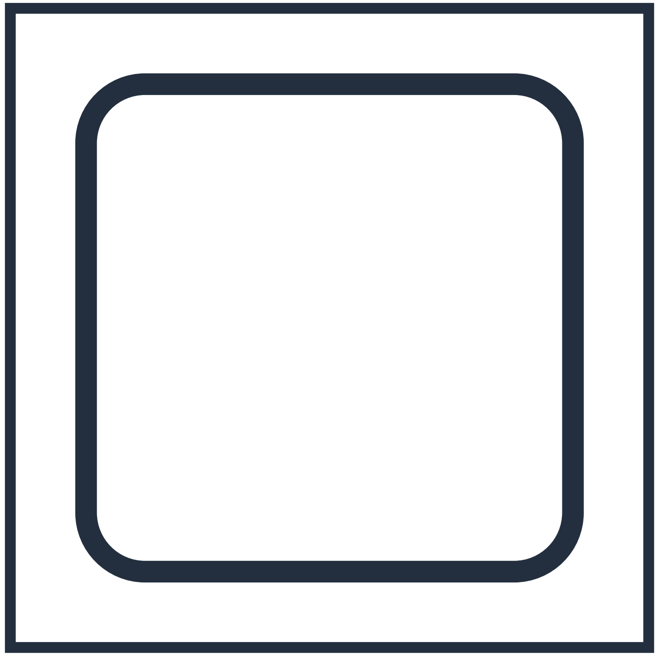
1. Order a NAT Gateway service
2. Associate an EIP with the NAT instance

Exercise: Order NAT Gateway Service

Are NAT Services required for Terra Firma?

EC2 Instances

EC2 Instances



- Virtual servers are called instances
  - Instance types – vCPU’s, memory, storage (type and size), network speed
  - Low, moderate, high
  - Enhanced networking
- Performance Builds

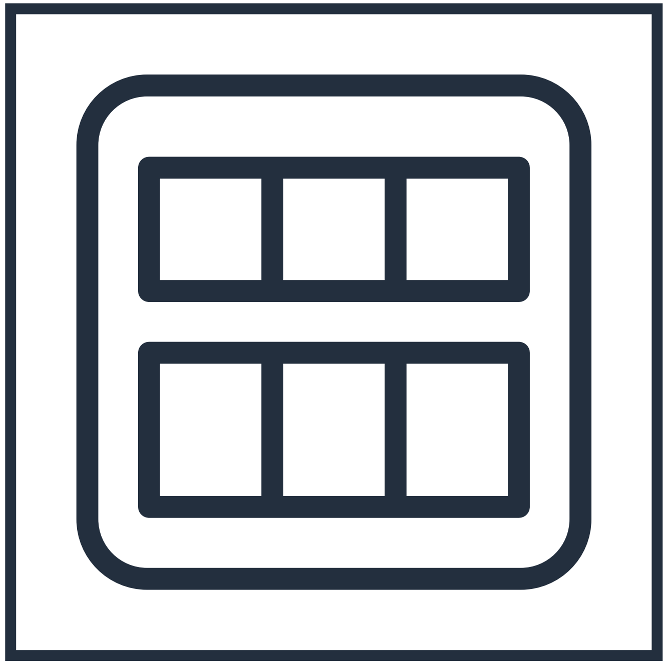
Compute	c4	Extreme processing
Memory	r3	Memory intense
Storage	i2	Fast SSD storage
GPU	g2	Graphic workloads

What type of instances should be considered for the human resources software?

Compute, Memory, or Storage performance builds?

Amazon Machine Images

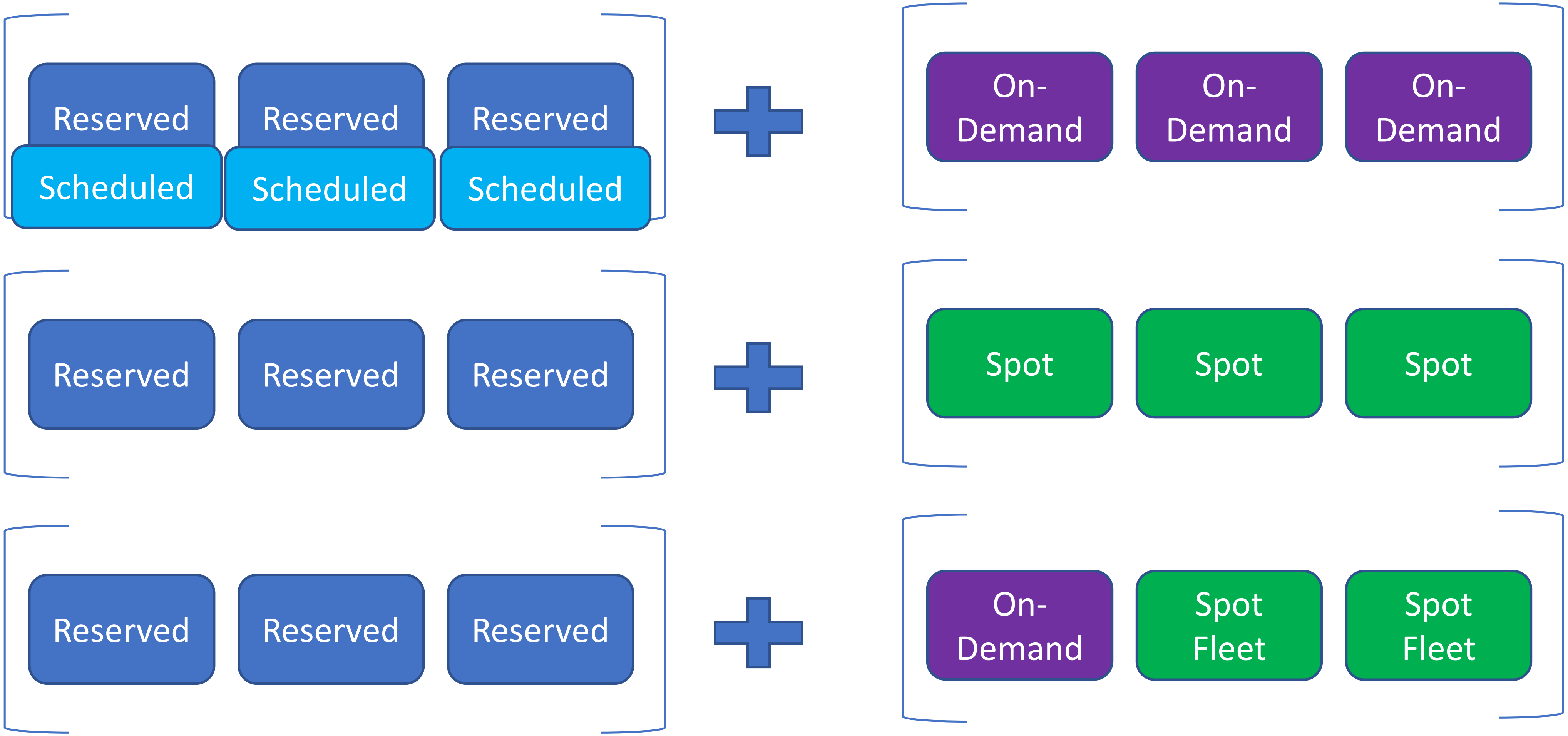
- AMI - Amazon Machine Images
- Defines initial s/w installed on instance when launched
  - O/S, state, system software
  - Launch parameters
- AMI Types
  - Published – Marketplace
  - Published by AWS – Linux and Window versions / variants
  - VM Import / Export service for on premise VMs
  - Generated from existing Instances – Create image
- Access after launch
  - Across the Internet – Public IP Address, or Elastic IP
  - Behind a Load Balancer



EC2 Pricing Options

- On-Demand – Billed by the second (for Linux instances)
  - Minimum 1 minute charge
- Reserved – All upfront, No upfront, Partial upfront (1, and 3 year)
  - Can also be purchased as “convertible”
- Scheduled – Example: Monday, Wednesday, Friday 1-7PM
  - Capacity reservations – 1 or 3 year, fixed schedule
- Spot Instances
  - Spot price (2 minute warning)
  - Hibernate – until price decreases
  - Up to 6 hour fleets
- Spot Fleets
  - A mixture of spot pools and on-demand instances

Pricing Scenarios



Reserved Reserved Reserved
Scheduled Scheduled Scheduled
+
On-Demand On-Demand On-Demand

Reserved Reserved Reserved
+
Spot Spot Spot

Reserved Reserved Reserved
+
On-Demand Spot Fleet Spot Fleet

What type of purchasing option should be considered for the human resources SQL database instances?

Exercise:

Simple Pricing Calculator

EC2 Tenancy Options

- Shared tenancy (Default)
  - VPC can be set to dedicated tenancy
  - Dedicated instances – no sharing
- Dedicated Host – Whole host CPU core control
- Bare Metal
- Placement groups – instances on the same subnet within a single AZ

Golden Image Maintenance

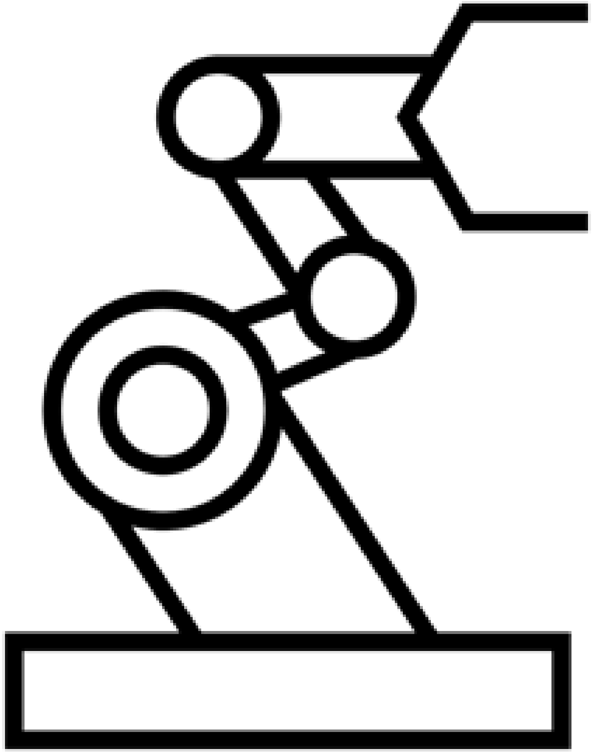
1. Customize an EC2 instance and save configuration as an AMI

   Launch (many) instances from customized AMI

2. Update Golden Image

   Launch (many) instances from modified AMI

3. Manual snapshots of individual EBS volumes

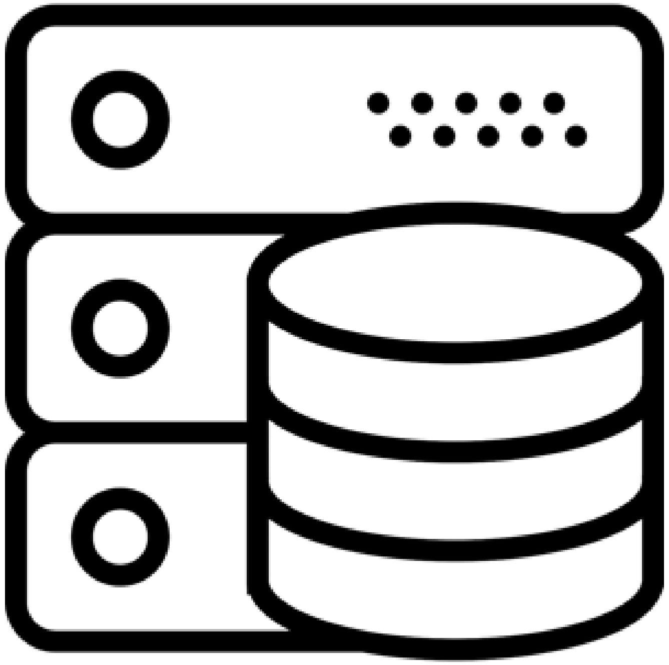


Instantiating Computer Resources

- No more manual processes is the goal
- Bootstrapping – install software, updates, copy data records
  - Cloud-init, User data
  - Scripts (Bash, PowerShell)
- CloudFormation – JSON template

EC2 Instances Stores

- Local disks attached to the bare metal server that hosts your instance(s)
- Called “Ephemeral storage”
- Temporary storage – buffers , cache, etc.
- Up to 24 TB depending on instance type
- Deleted when instance is stopped, or fails



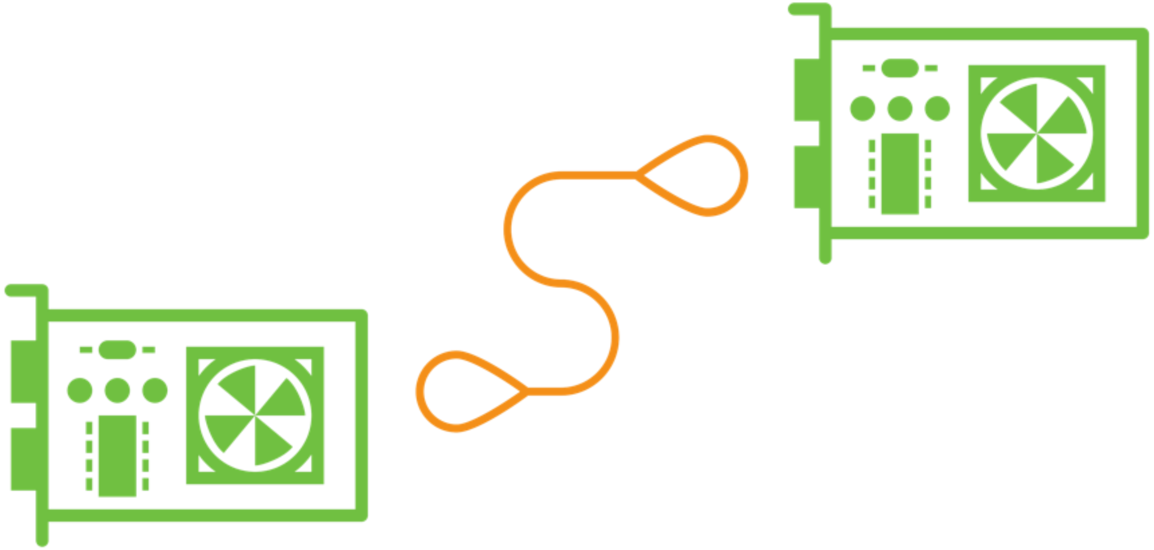
Exercise: Order an EC2 Instance

EC2 Admin Tasks

- Initial Logon
  - Public / Private key pair
  - Windows instances – decrypt p/w with private key
  - Linux instances – Private key is used to login via SSH
- Instance Lifecycle
  - Bootstrapping initial launch – User Data
  - Running – instance metadata (169.254.169.254)
  - Managing instances – Tagging
  - Monitoring instances – CloudWatch
- Modifying an Instance
  - Change instance type – Turn Off / Change instance type / Turn on (New billing cycle)

Exercise: EC2 Administration

Elastic Network Interfaces (ENIs)



- Virtual network interface that can be attached to an instance within a VPC
- Each ENI can have one public IP address and multiple private IP addresses
- ENI’s once created are associated with a subnet, then instance
- Use case: Management networks, Multi-homed instances, or Virtual appliances

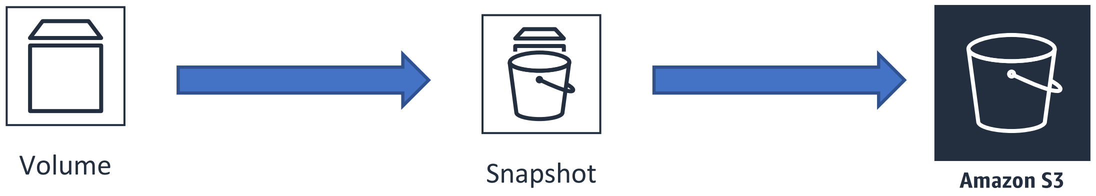
Exercise: Add Network Interface Card

Elastic Block Storage (EBS)

Elastic Block Storage (EBS)

- Persistent Block Storage
  - Each EBS volume replicated within it’s AZ location
  - Single EBS volume attached to one instance
  - Multiple EBS volumes can be attached to one instances
- Magnetic Volume – 1 GB to 16 TB
  - Min: 100 Max: 2000 IOPS
  - Throughput Optimized (500) / Cold storage (Min:100, Max: 20000)
- General Purpose SSD – 1 GB to 16 TB
  - (3 IOPS per GB) burstable to 10,000 IOPS
- Provisioned IOPS SSD   4GB – to 16 TB
  - Minimum 100 IOPS, Max: 32000 IOPS

Protecting EBS Volumes

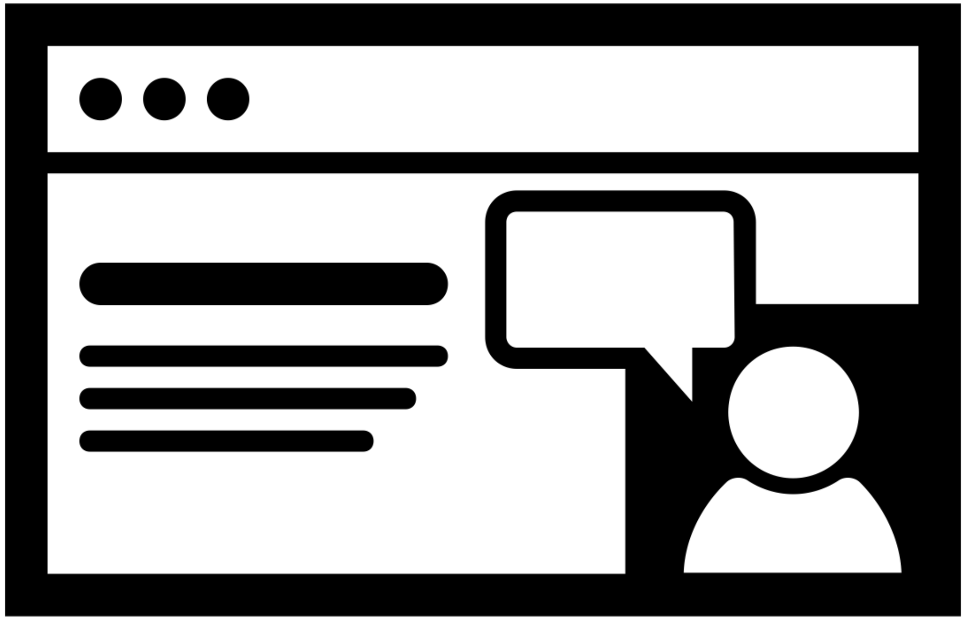


- Backup / Recovery snapshots
    - Snapshot
        - Point in time
        - Stores in S3 in AWS “Controlled storage”
- Create a Volume from a snapshot
- Increase the size of an existing EBS volume
- Detach, and re-attach existing volumes
- EBS volumes can be encrypted – KMS service handles key management

Exercise: Create EBS Volumes

Do you think it’s a good idea for the database server’s master and slave instances to be hosted in separate availability zones?

Do you think the replication between the master and the slave replicas is worth the additional replication costs?



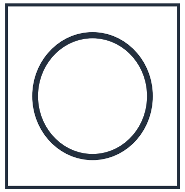
Exercise: Create Snapshots

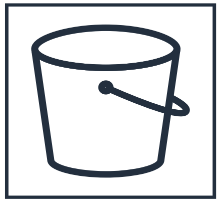
Amazon S3

What is S3 Storage ?

- Simple Storage Service
  - Secure, durable and scalable
- Object Storage – Cloud object storage
  - Pay only for the storage you use
  - Each object contains data and metadata
- Accessed over the Internet: Private endpoint from a subnet hosted in a VPC
  - Data is managed as an object using API calls and HTTP verbs (PUT,GET)
  - Native interface to S3 using a Restful API (HTTP or HTTPS methods)
  - Using through an S3 client (CloudBerry)
  - Apps developed using the SDK

S3 Buckets

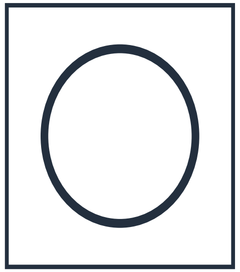

Object


Bucket

- Objects are stored in containers called buckets
  - Buckets are top-level management components
- Bucket names are global, must be unique across all AWS accounts
- Each object is identified, and accessed using a specified unique key
- Each bucket can be divided into folders (delimiters) \
  - Each bucket can hold an unlimited number of objects
  - You can’t mount a bucket, install software, open files, host a database
- Highly durable, scalable object store optimized for Reads

S3 is Object Storage

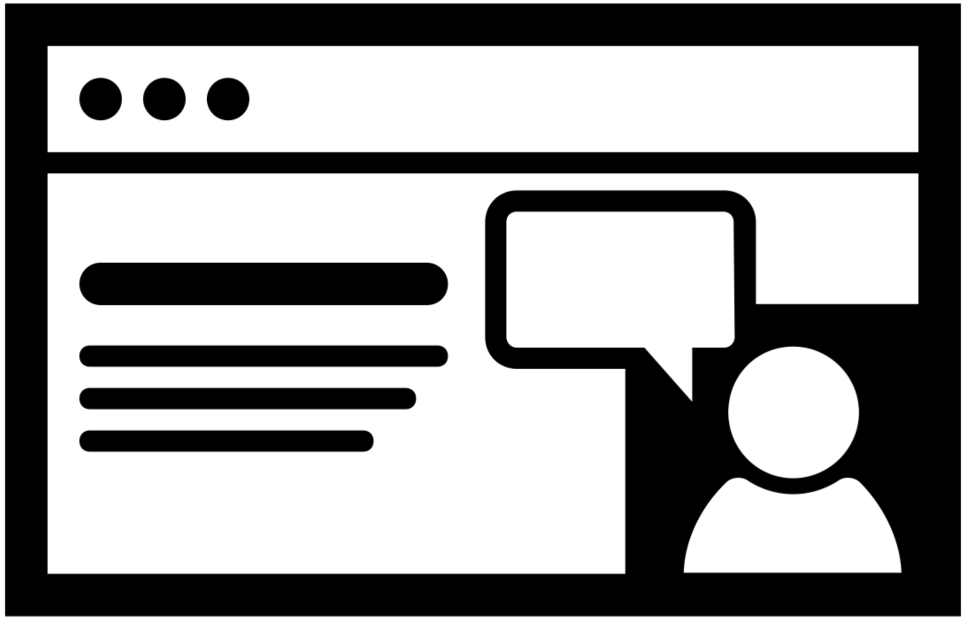
- S3 can store any type of data
  - Up to 5 TB max of single object
- Each object has a unique key
  - Key = filename
  - Must be unique within each bucket
  - Multi-Part upload for objects greater than 5 GB
  - Bucket contents can be copied to buckets in other regions (Additional costs)
- Metadata describes the data
  - System metadata – AWS   date, size, content-type
  - User metadata – tags specified only at the time the object is created



Object

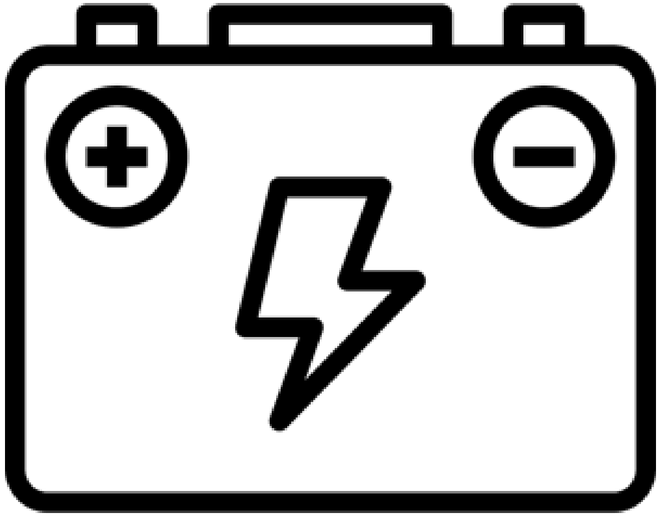
S3 Object Replication

- Cross-Region Replication
  - Asynchronous replication from source bucket in one region to bucket in another region.
  - Helps move data closer to end-users
  - Compliance / additional durability



Exercise: Create S3 Bucket

S3 Durability



- Stored in multiple devices in multiple facilities, within a region
  - Designed to sustain concurrent loss of two facilities without loss of data
- Standard
  - 11 9’s durability
  - 4 9’s availability
  - Over a given year
- RRS Reduced Redundancy Storage
  - 4 9’s durability

S3 Consistency

- Objects are eventually consistent
- Multiple copies means replicated storage
- PUT’s to new objects – read after write consistency
- PUT’s to existing object – eventual consistency

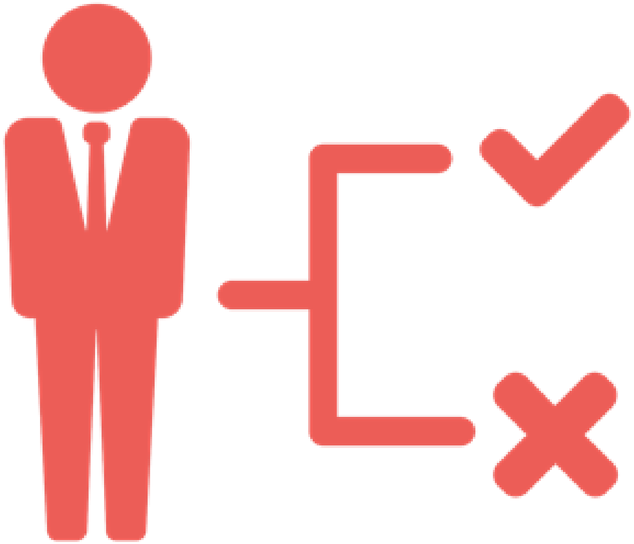
Access Control

- Only owner has access by default
  - Private by default
- Coarse grained – S3 ACLs
  - Read Write Full Control at object level
- Fine-grained – bucket policies
  - Associated with the bucket / not an IAM security principal
  - Can specify access from where, who can access, and what time of day
- IAM polices can also be created for control
- Can be associated with different AWS accounts

Exercise: S3 Bucket Policy

S3 Storage Classes

- Standard
  - High durability and availability, low latency, high performance
- Standard 1-A
  - Infrequent Accessed lower cost but minimum object size (128KB) and minimum duration (30 days) and per GB retrieval costs
- Reduced Redundancy Storage (RRS)
  - 4 - 9’s durability
  - Lower cost per month
  - Example : Data that can be easily re-produced (Thumbnails)



S3 Encryption

- SSE – S3 (AWS Managed Keys)
  - AWS rotates the keys
  - New master key every month
  - Data, Encryption, and Master keys are stored on separate hosts
- SSE - S3 (AWS KMS Keys) Customer Managed
  - Separate permissions for the master key
  - AWS provided auditing; view failed attempts
- SSE - C (Customer Provided Keys)
  - Maintain your own encryption keys
  - Amazon does the work (encryption / decryption) using your keys

Key Management Service

- AWS offers services to manage symmetric or asymmetric keys
- **AWS KMS** – Managed service allow you to generate, store, enable / disable and delete symmetric keys
- Customer managed keys – Each CMS is per customer and is used to encrypt and decrypt data
- Data keys – Used to encrypt data objects within your own applications
- **AWS Cloud HSM** – Secure your cryptographic key storage using Hardware Security Modules
- Recommendation is to use two HSM’s configured in a highly available configuration

Versioning / Lifecycle Management

- Multiple copies of each object in the bucket
  - Preserve, retrieve, and restore every version of every object
  - Enabled at the bucket level
  - Can be suspended but not disabled
- Lifecycle Management
  - Example: S3 to Glacier then Delete

Exercise:
Lifecycle Management

How would a lifecycle rule help manage office records moved to S3 cloud storage?

S3 Administration

- Regions
  - The S3 namespace is global, however buckets are stored in a specific region that you choose
- Object URL
  - Must be unique
  - Web service endpoint, bucket name, object key
- MFA Delete
  - One-time code required for deletion
  - Only enabled by the root account
- Pre-signed URLs
  - Sharing
  - Time sensitive
  - Owner of bucket creates a pre-signed URL with credentials

S3 Notifications

- S3 server-access logs track requests to S3 bucket
  - Account name and IP Address
  - Bucket name
  - Request time
  - Action (GET PUT LIST)
  - Response or error code
- Event Notifications
  - Response to objects uploaded to S3
  - Monitored at the bucket level
- Object creation, removal triggers response
  - Simple notification service, Simple queue service, transcoding, Lambda

Exercise: S3 Administration

Glacier Storage

- Low cost archival storage
  - Data is stored in archives (Up to 40 TB)
  - Unlimited # of archives
  - Automatically encrypted

- S3 – 5 TB Object size limit
- Glacier – 40 TB archives
- Glacier – Encrypted by default
- Glacier – Archive IDs
- S3 – Friendly names

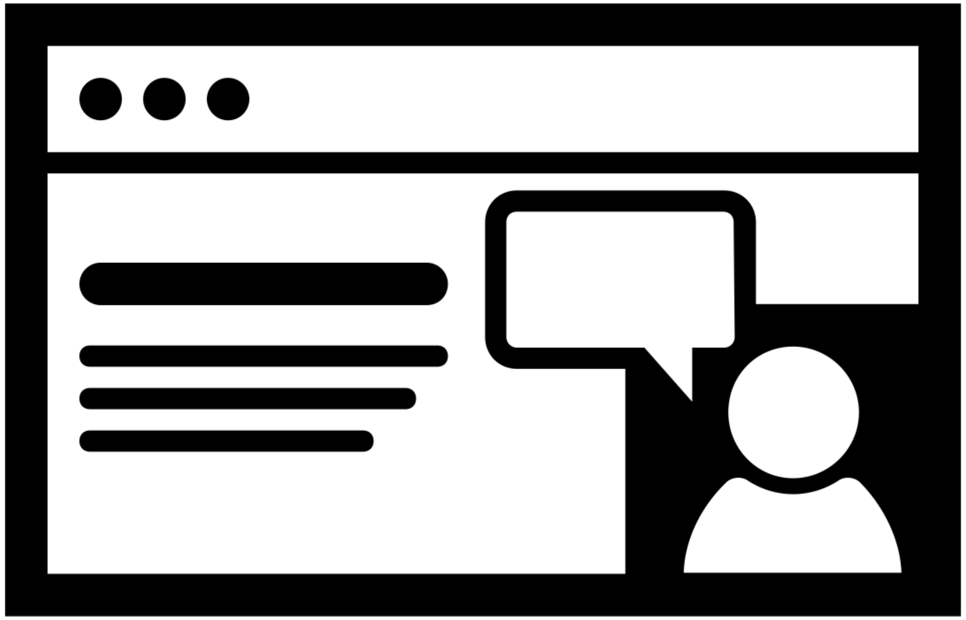
Amazon Glacier

What cloud storage option would you choose for archived records? S3 storage or Glacier?

Archive
Archive
Archive
Vault

Glacier Vaults

- Archives are held in containers called vaults
- Each account can have up to 1,000 vaults
- Compliance controls per vault with a vault lock policy (WORM)
- Retrieval policy to control data access



Exercise:
Glacier Vaults

Core: What We Covered

- Fundamentals of AWS architecture, terminology and concepts
- Virtual Private Cloud (VPC) networking
- Amazon Elastic Compute Cloud (EC2) Instance deployment and configuration
- Storage solutions including Elastic Block Storage (EBS), and snapshot management
- The Simple Storage Service (S3)
- Glacier storage

Q and A / Wrap-up