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
- Amazon Elastic Compute Cloud (EC2) Instance deployment and configuration
- Storage solutions including Elastic Block Storage (EBS), and snapshot management
- The Simple Storage Service (S3)

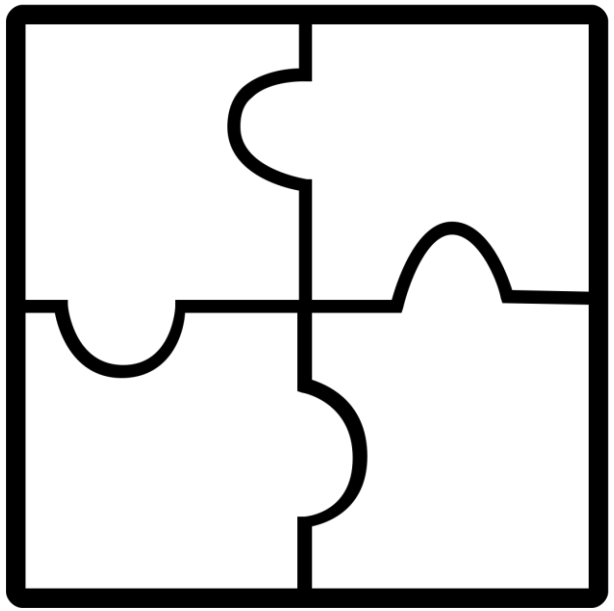
Communication

Q and A in class

Instructor Email:

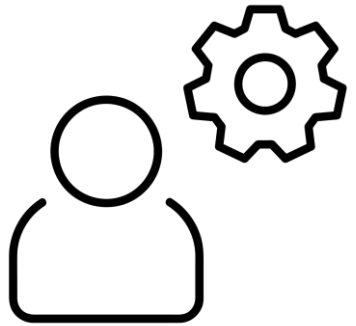
Mark@wilkinssolutions.ca

Core Architecture Concepts



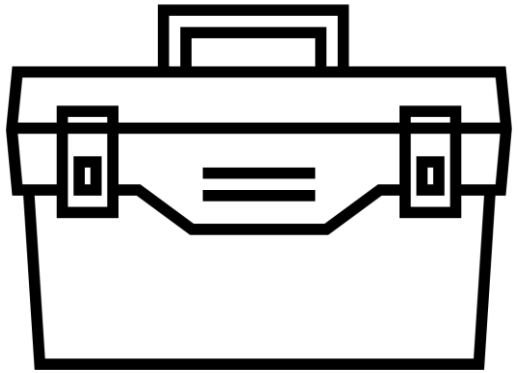
Managed Services

- Change management – Management Portal
- Incident management – Automated, self-healing
- Provisioned management – Predefined cloud stack installs
- Patch management – Automated patching
- Access management – Automated security best practices
- Security management – Security management per stack
- Continuity – Controlled backups and snapshots
- Reporting – Detailed logs and performance metrics

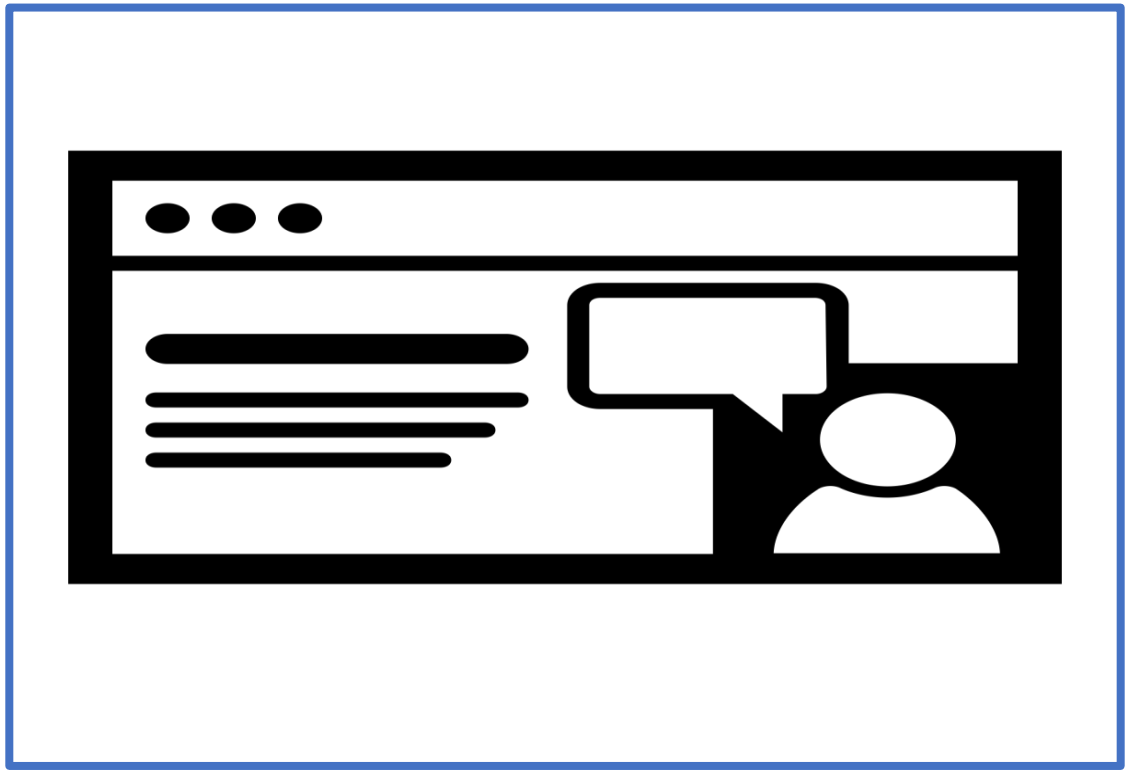


Unmanaged Cloud Services

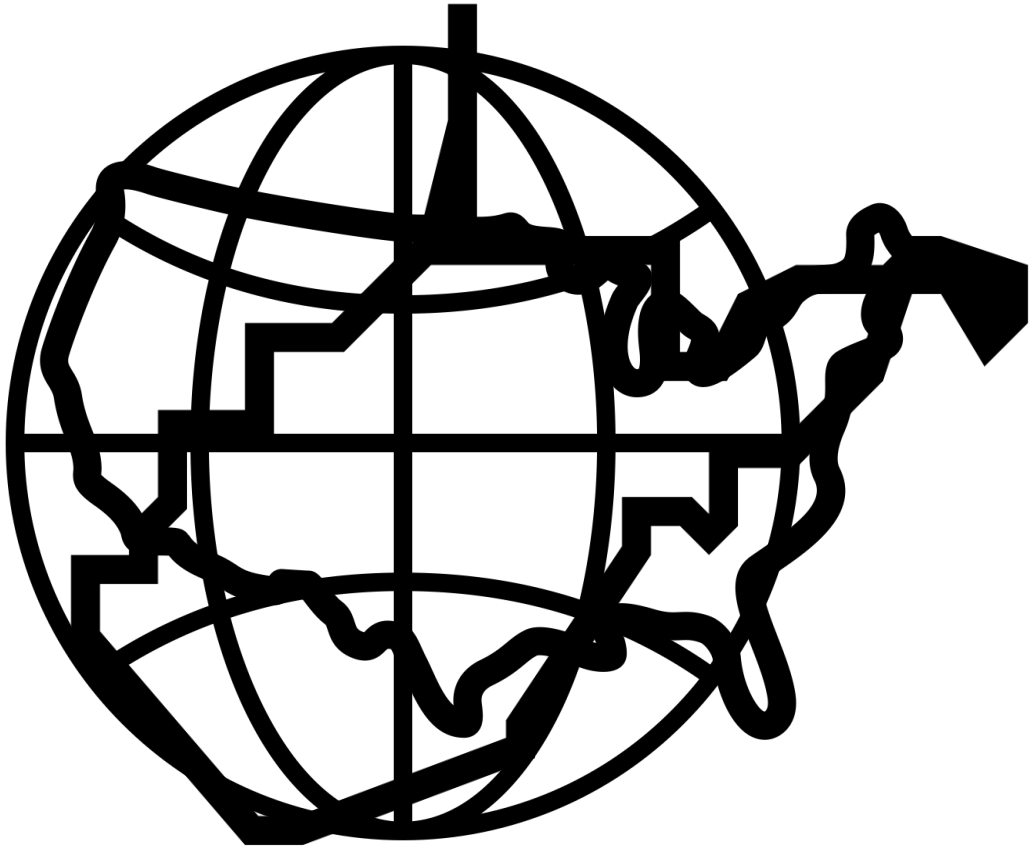
- The good news: You can do whatever you want
- The bad news: You have to do more of the setup and management, and monitoring
- The reality – there are no completely unmanaged services at AWS



Exercise: Essential AWS Managed Services

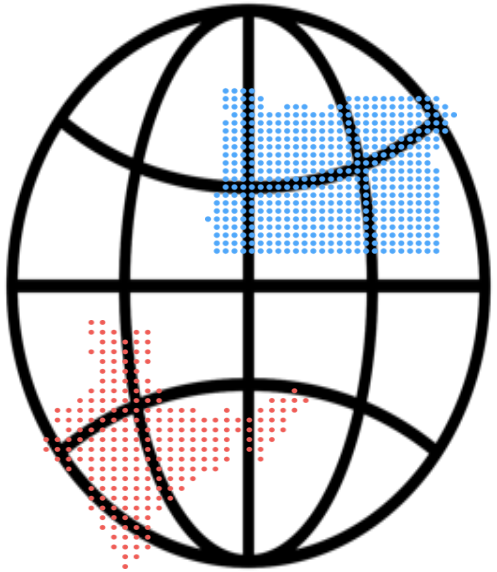


Regions

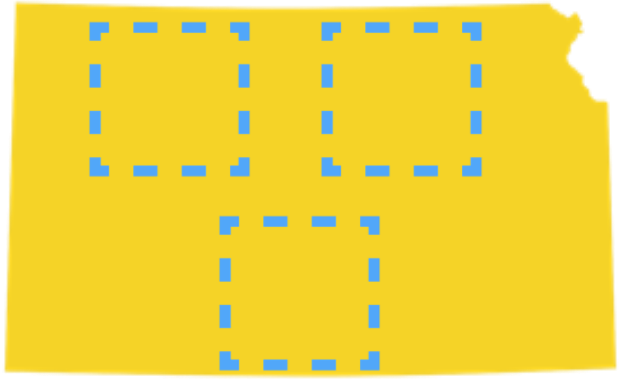


US East
N. Virginia

AWS Regions



Regions are Independent



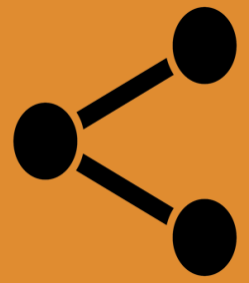
Regions have (multiple) Availability Zones

Data transfer charges between regions may apply

Resources are not automatically replicated between regions

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

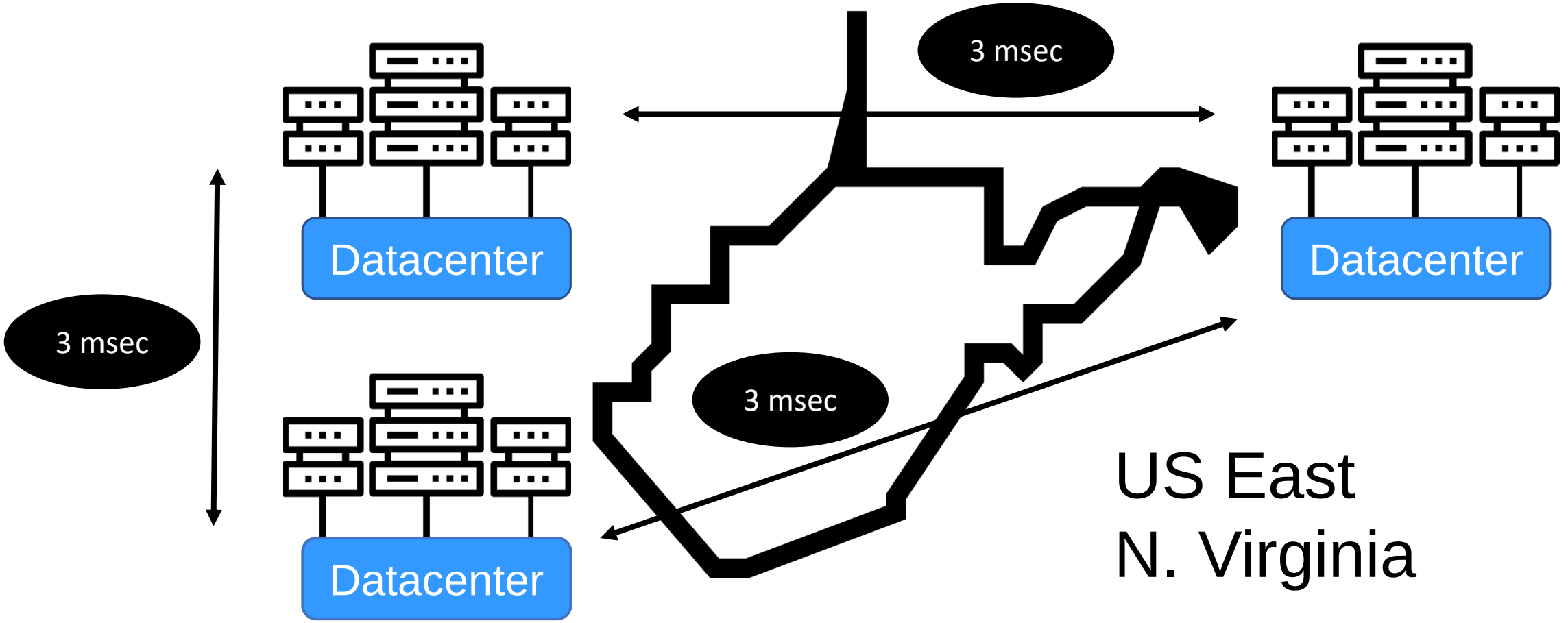

Latency ?
Cost ?
Where will you place your workloads ?
Features ?
Compliance ?

Workload Considerations

Select region matching compliance needs

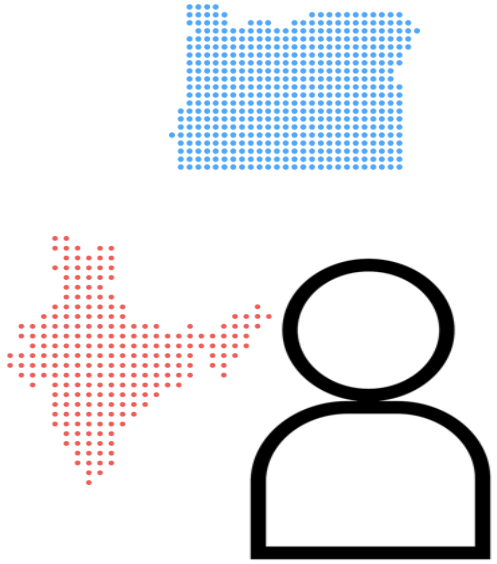
Choose availability zones for application failover

Availability Zones (AZ)



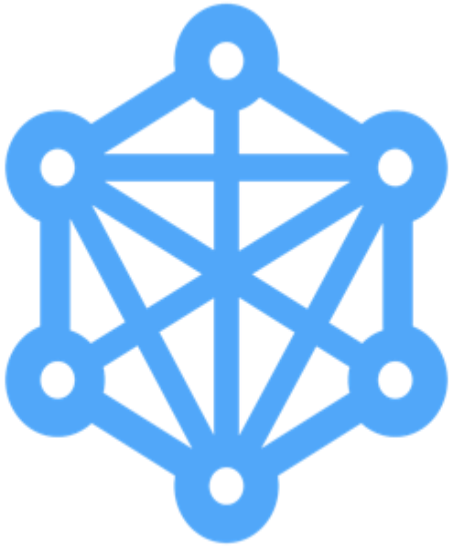
Availability Zones (AZ)

Isolated locations



AWS account has access to multiple regions

AWS GovCloud (US) Account only has access to the GovCloud region



Connected with multiple Tier-1 transit private connections

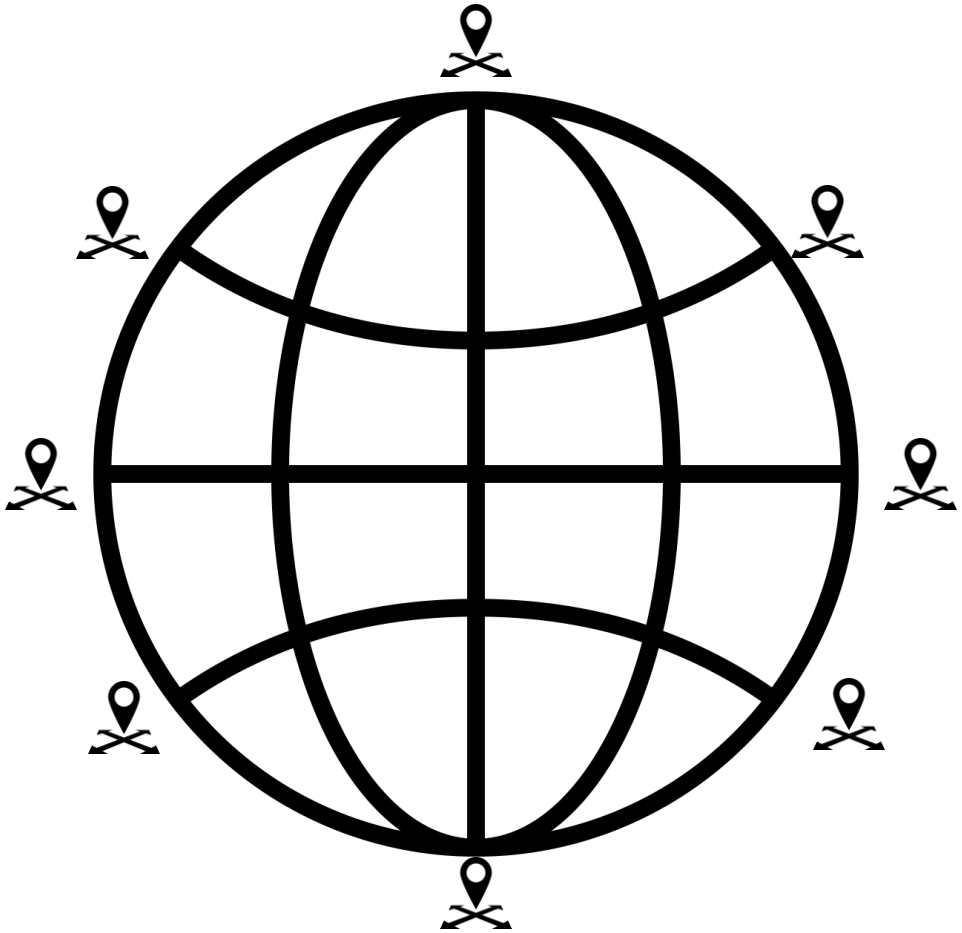
Availability Zones are represented by a region code followed by a letter identifier

Example: us-east-1a

Single or Multi-AZ Design ?

SINGLE - AZ	MULTI - AZ
▪No recovery when disaster happens ▪No potential high availability ▪Single AZ is not the test answer! ▪All regions have at least 2 availability zones	▪High availability designs ▪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 global entry point to AWS resources

client

dns

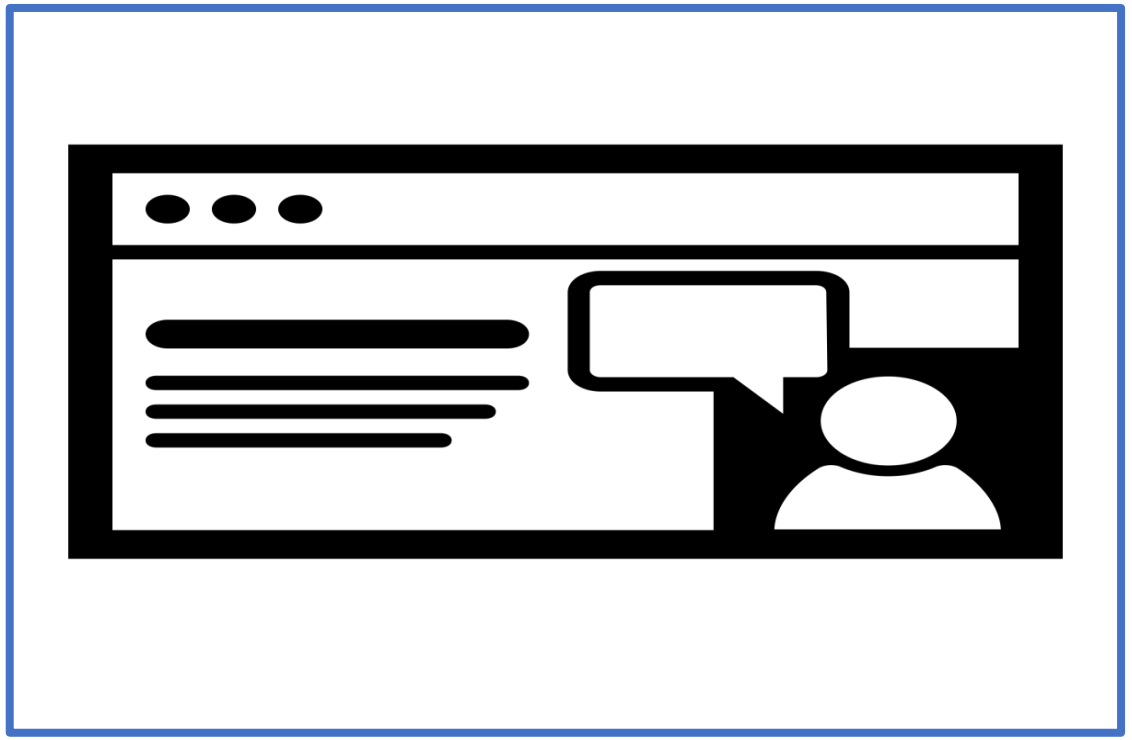
data

- 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)
  - 11 Regional Edge Cache locations

AWS Resource Locations

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

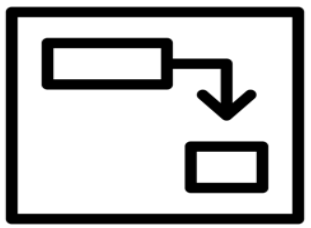
Exercise: Regions and Availability Zones

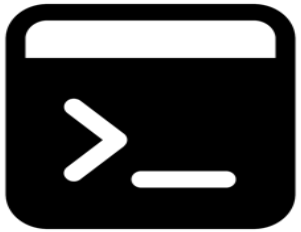


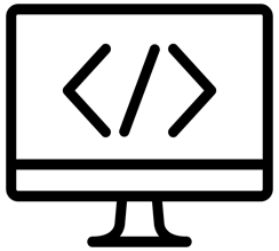
Discussion: Security and the Cloud

Accessing AWS Cloud Services

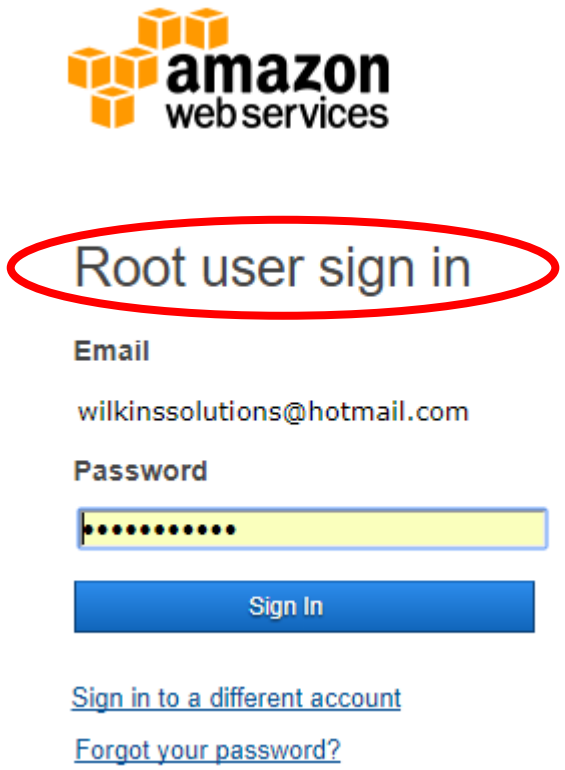
- Access to AWS services is accomplished by using API calls
- Application Programming Interface (API)
- Common Access Methods
  - The AWS Management Console – web-based application
  - AWS Command Line Interface (CLI) – Windows, Mac, and Linux
  - AWS Tools for Windows PowerShell
  - AWS Software Development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

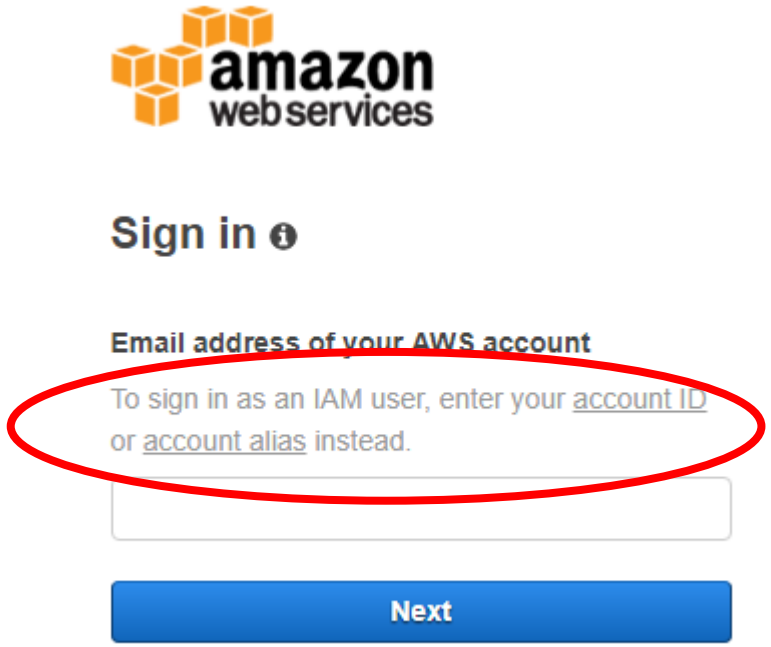




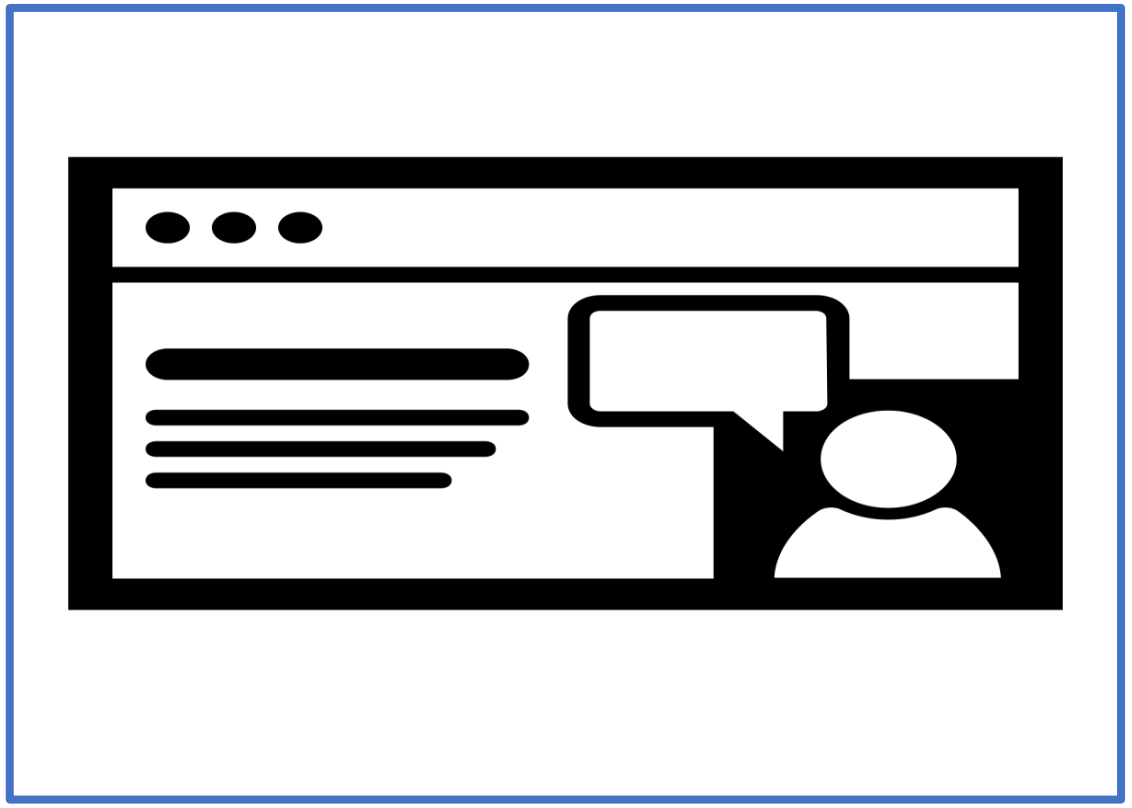


Signing in to the AWS Console





Exercise: Using the Management Console



Using the CLI

- Describe existing EC2 Instance in my account:

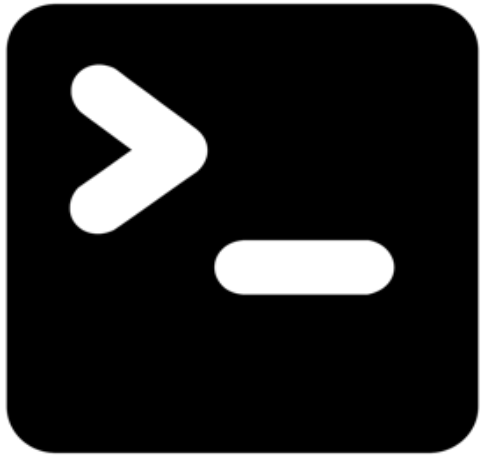
  $ aws ec2 describe-instances

- Start an EC2 Instance:

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

- Get help for a service:

  $ aws autoscaling help



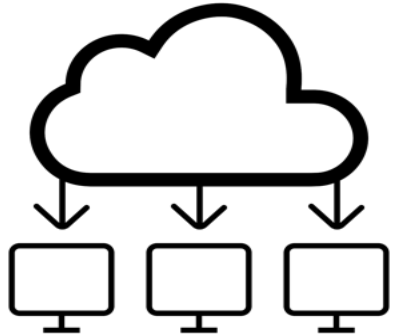
Using PowerShell

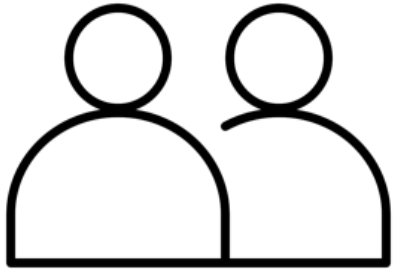
- **Launch an EC2 Instance:**

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

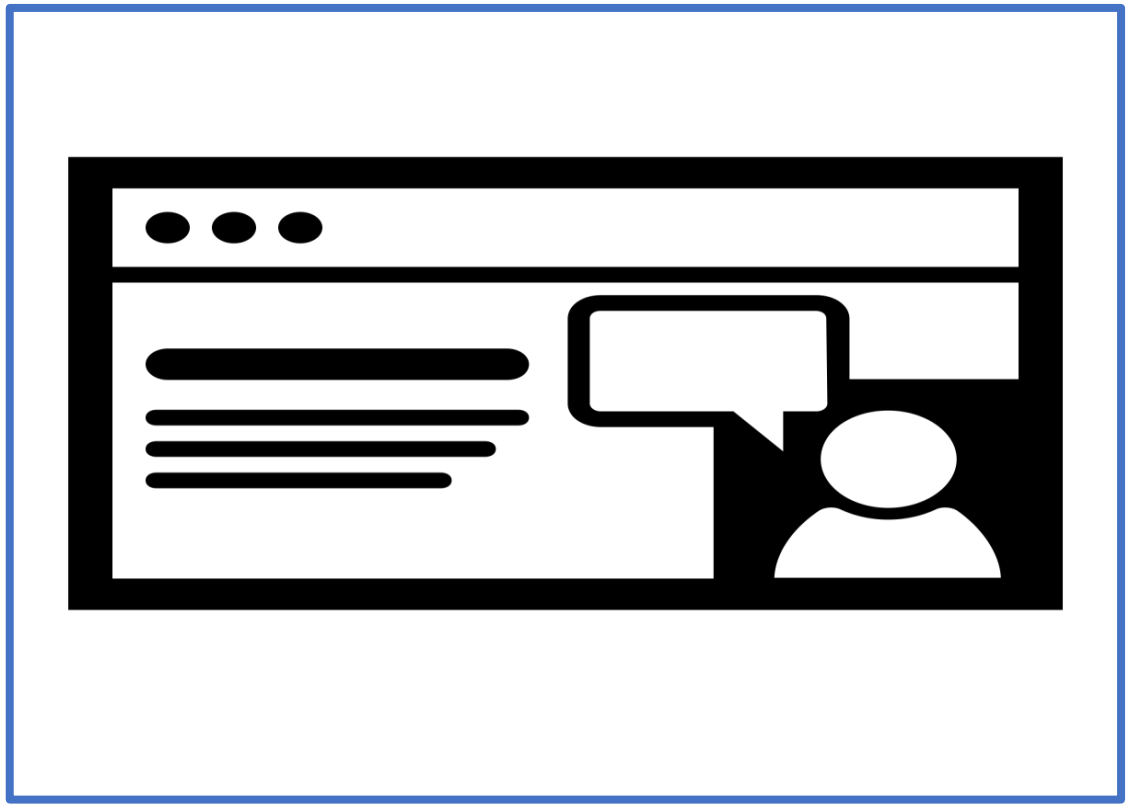
- **Create a Security Group:**

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





Exercise: Using the CLI



Virtual Private Cloud

What is a VPC?

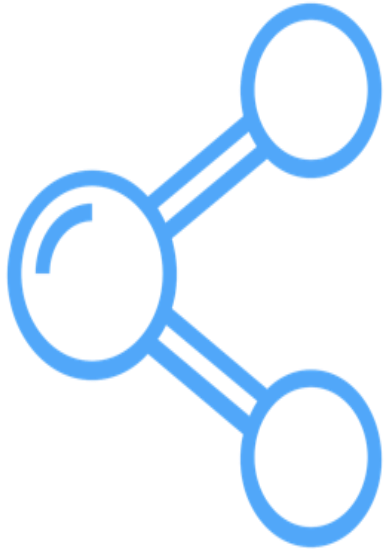
- Network layer at AWS
- Defined as a logical and isolated network (virtual private cloud)
- Launch EC2 Instances and various AWS resources into your own virtual network
- Logically isolated from other virtual networks hosted in the AWS cloud
- Two different networking platforms: EC2 - Classic and EC2 - VPC
- EC2 classic is not available for new customers

VPC Supported Platforms

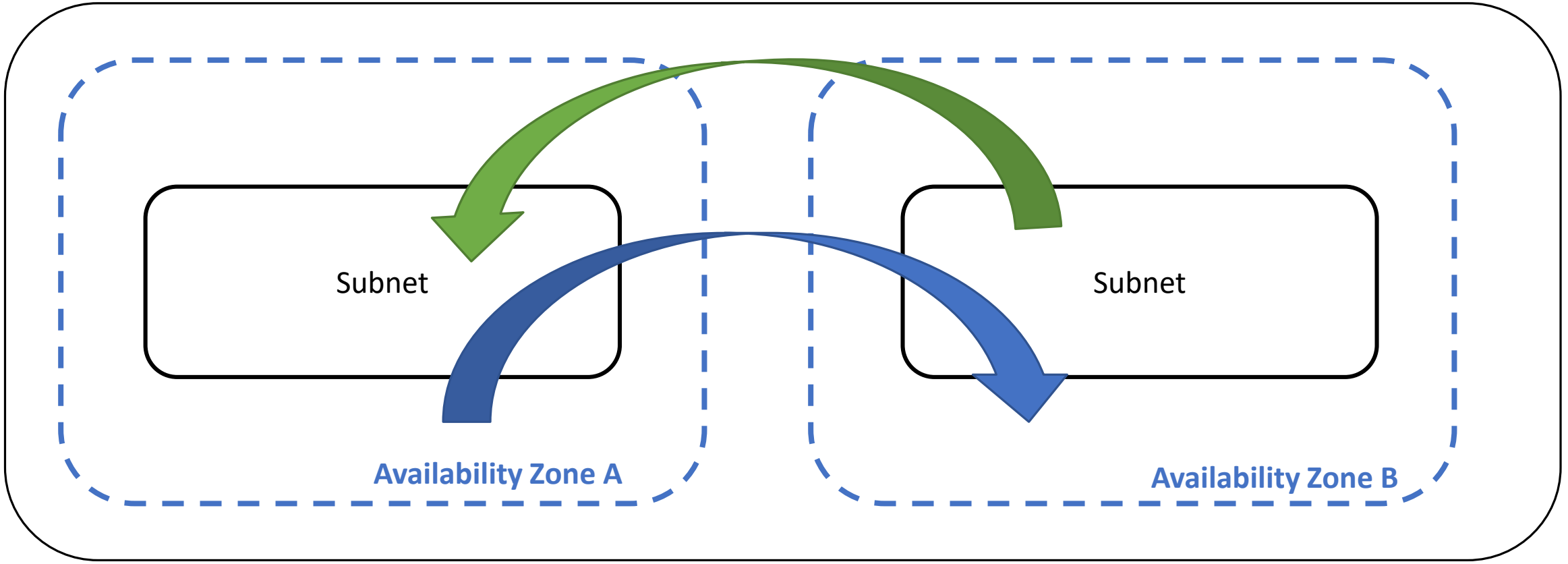
- EC2 – Classic
  - The original network infrastructure for EC2 instances
  - Instances run in a single flat network that you share with other customers
  - Doesn’t support enhanced networking, multiple IP addresses, changing security groups, etc.
- EC2 – VPC
  - Instances run in a virtual private cloud 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 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 VPC has a default route that enables local routing throughout the Subnets contained within each VPC

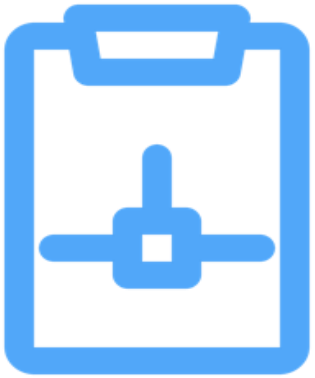


VPC Design: Best Practice



VPC Design Decisions

- EC2 Instance placement
- IP address range
- Subnets
- Route tables
- Network gateways
- Security settings – Instances
- Security settings – Subnet

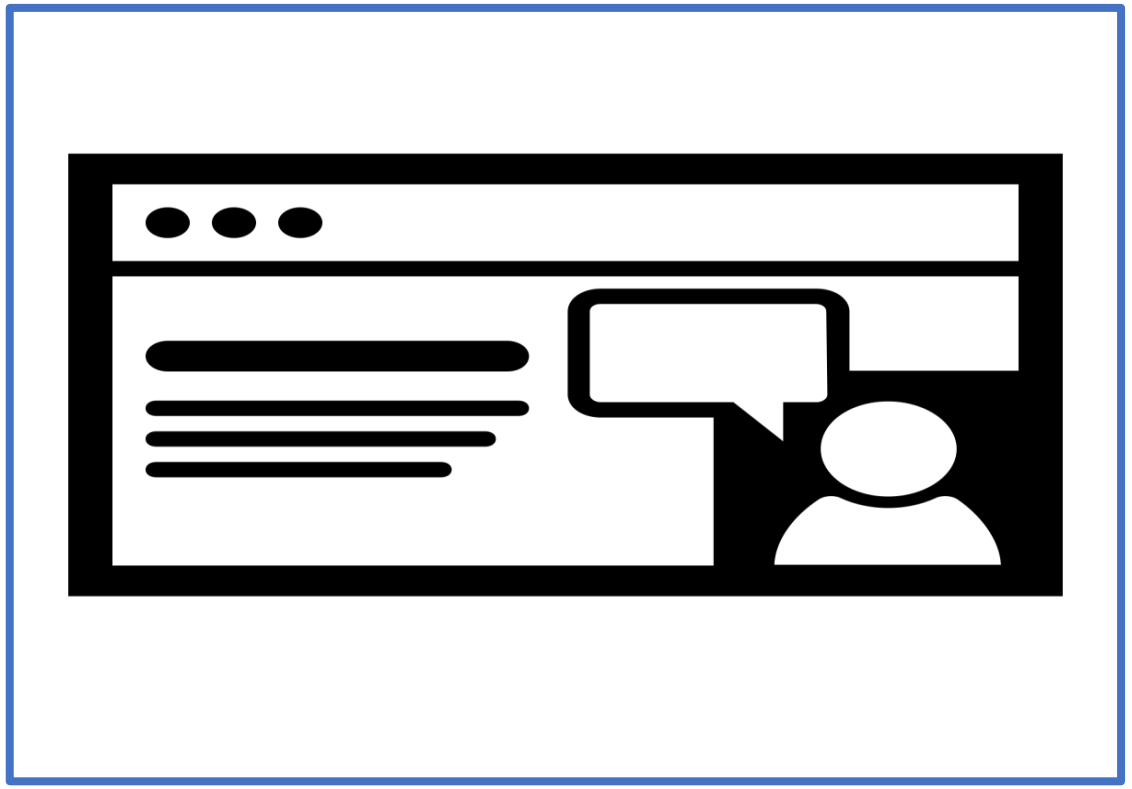


VPC Components

- 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, CCWs, VPNs)

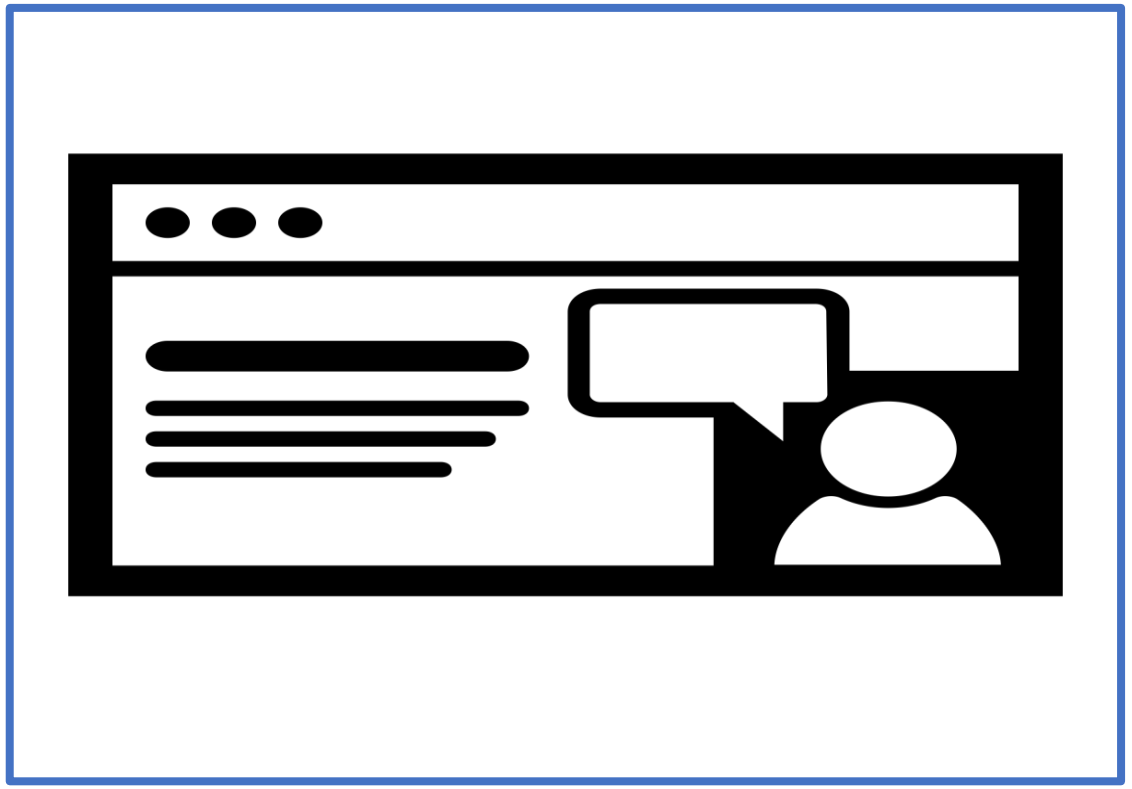
Exercise: Create a Custom VPC



The Default VPC

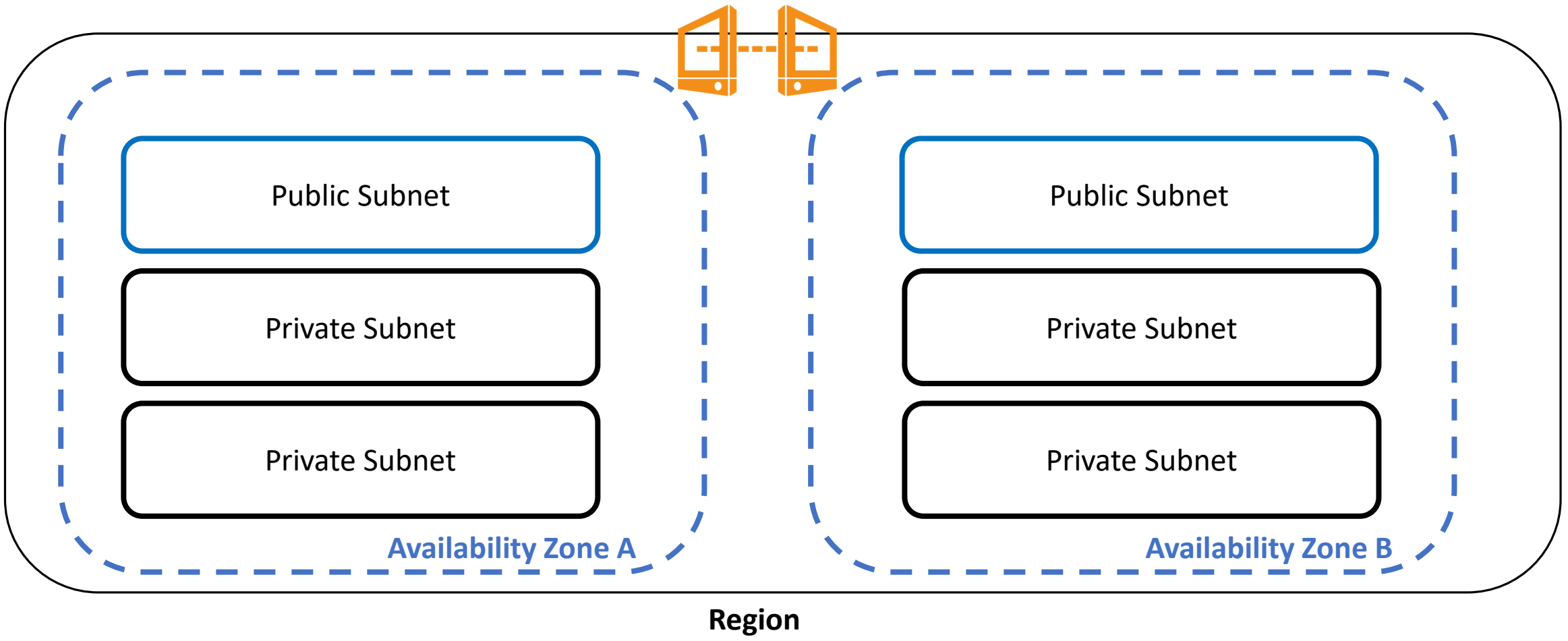
- /20 CIDR Block is assigned by default
- An Internet gateway is connected to the default VPC
- Main route table sends Internet traffic to the Internet gateway
- Default security group
- Default network access control list
- Default DHCP options
- Default subnets are public subnets
- Instances are assigned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

Exercise: The Default VPC

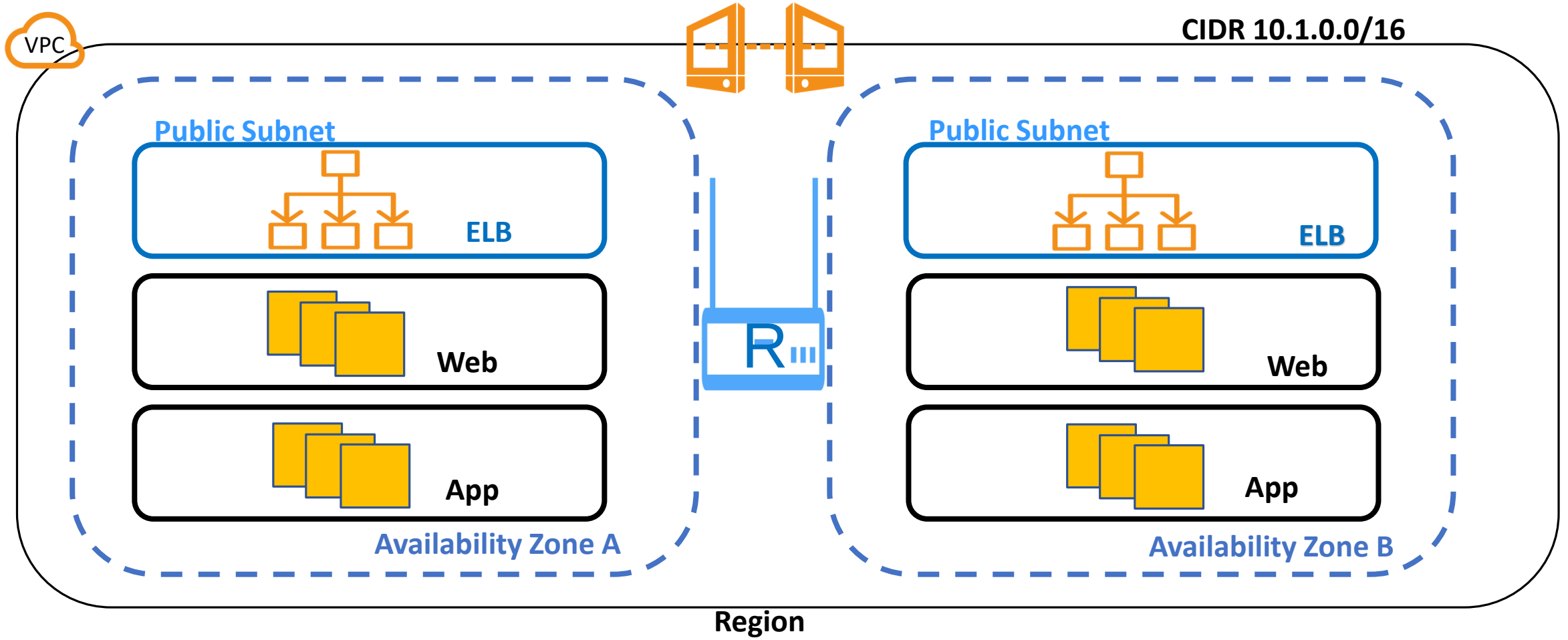


VPC Design

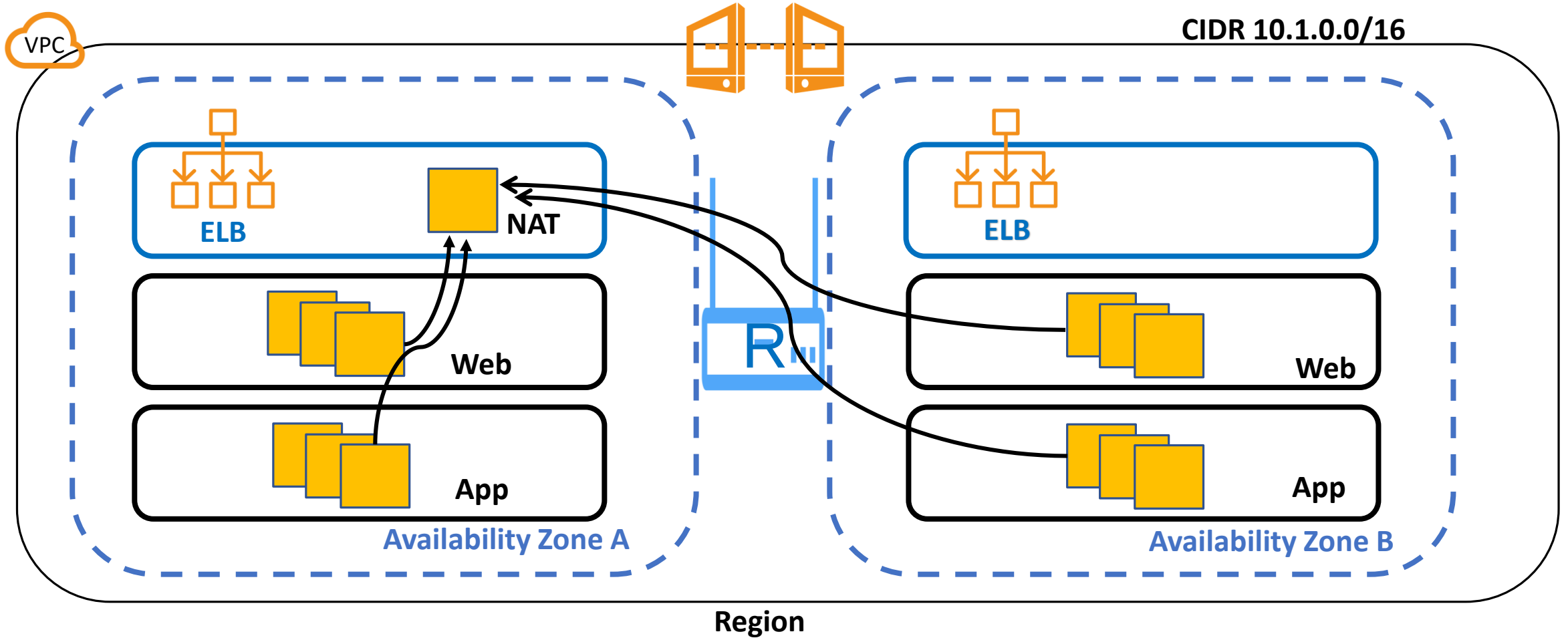
VPC: Public Web App



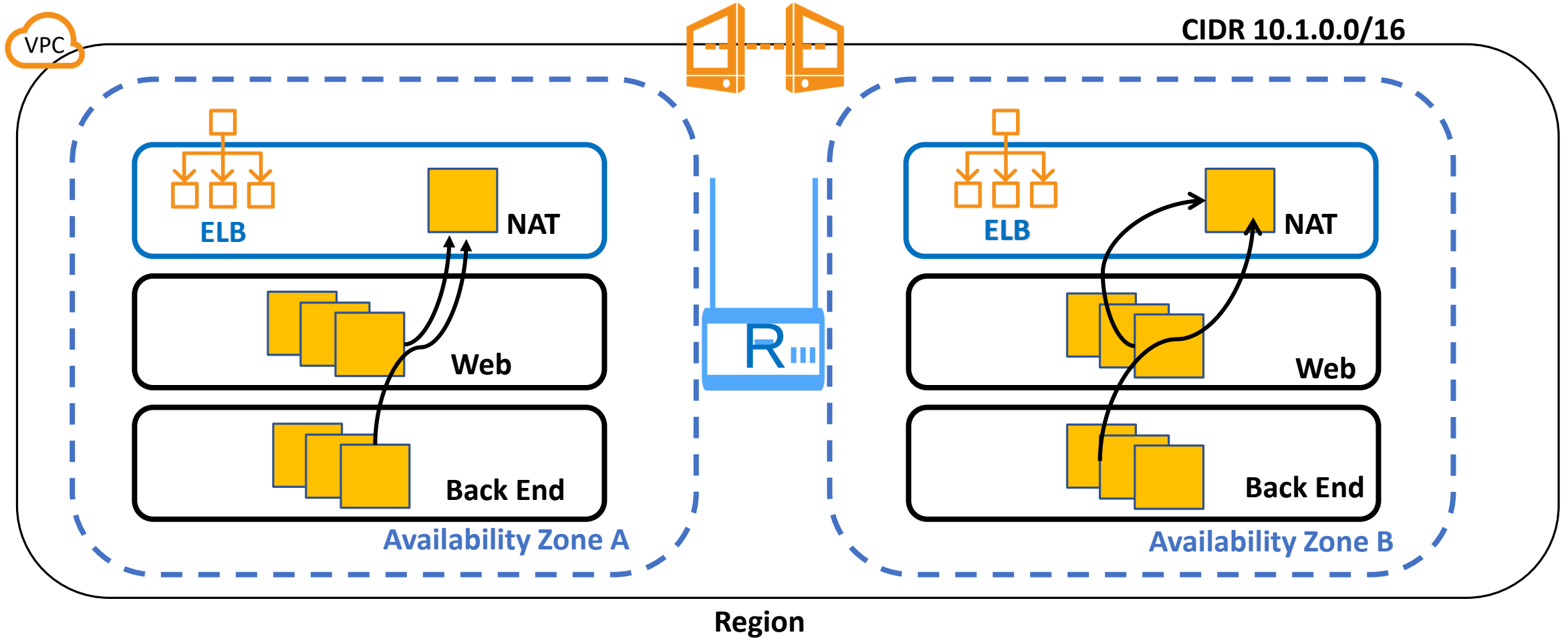
VPC: Public Web App



VPC: Public Web App



VPC: Public Web App



Subnets and Addressing

Subnets (Private / Public)

- Public or Private 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
- Subnets must reside within the selected Availability Zone
- Subnets cannot span Availability Zone, however VPC's do span AZs
- Subnets can be classified as public, private, or VPN only
  - Public subnet: the associated route table routes the subnets traffic to an Internet gateway
  - Private subnet: the associated route table does not route the subnets traffic to an Internet gateway
  - VPN only subnet: the associated route table routes to subnets traffic to a virtual private gateway and does not have a route to the Internet gateway

Subnets

- Subnets cannot span availability zones (Reminder)
- 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**
- A subnet that doesn't route to an Internet gateway but has traffic routed to a virtual private gateway, (VPN connection) is called a **VPN only subnet**

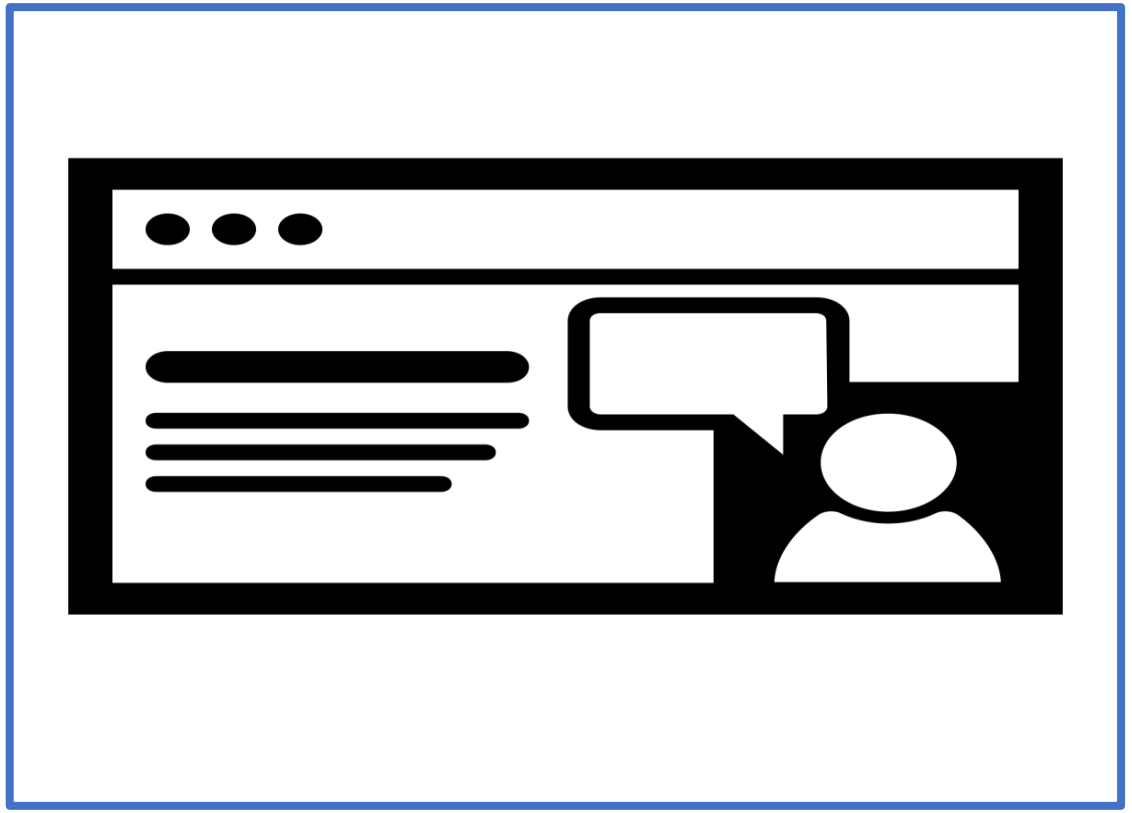
Reserved Addresses

- The first four IP addresses and the last IP address in each subnet CIDR block are not available for use.
- 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 a 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



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 route table assigned to the VPC
- Each subnet must be associated with a route table
- Outbound traffic patterns are defined with a route table
- The default route can be modified
- 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

Route Tables

- Each VPC has implicit routing services provided by default
- The main route table can be customized
- Custom route tables can also be created
- Each subnet must be associated with a route table
- If a subnet is not associated explicitly with a custom route table, the main route table will be associated by default

Security Groups

Security Groups (SG)

- 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
- 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 port range
- Any protocol that is defined with a standard protocol and number is supported

Default Security Group

- Each EC2 Instance launched in a VPC is automatically associated with the default security group
- You can't delete the default security group
- However you can change the association or the default security group
- No inbound traffic is allowed inbound rules are added

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.

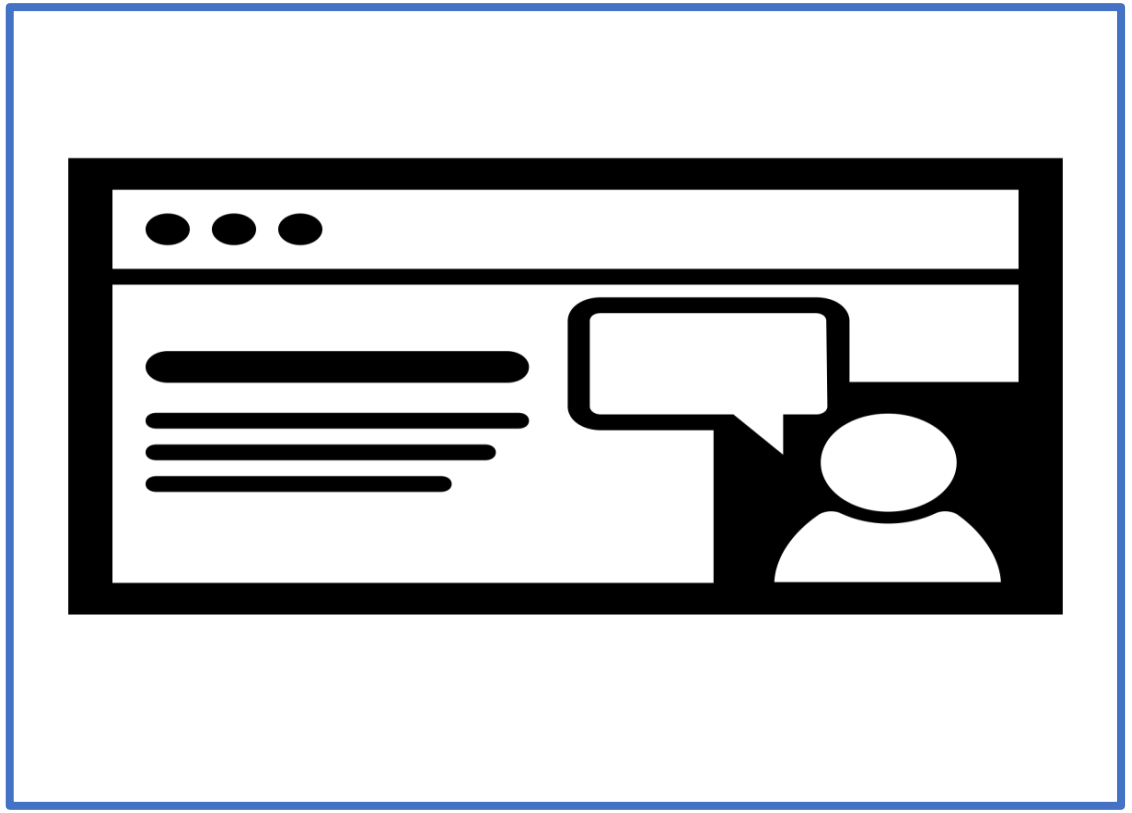
Security Groups

- Allow rules **can** be specified
- Deny rules **can't** be specified
- Separate rules can be defined for both inbound and outbound traffic
- A brand new security group has no inbound rules – these must be created
- By default security groups include an outbound rule that if not changed, allows all outbound traffic
  - The default outbound rule allowing all traffic can be removed
- Instances associated with the same security group still can't talk to each other until rules are allowed to allow communication
- Additional rules for specific outbound traffic can also be added

Security Groups

- Security groups are **stateful** – if a request is made from your instance's flowing outbound, the response traffic for that request is allowed to flow into regardless of inbound security group rules
- Responses to allowed inbound traffic are also allowed to flow out regardless of the outbound rules
- 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

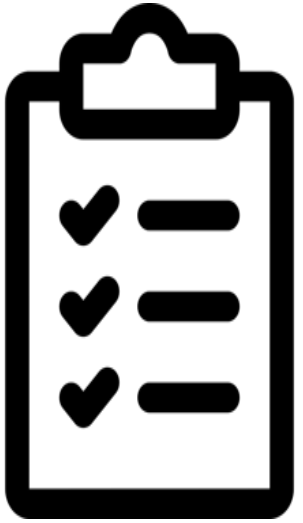
Exercise: Create Security Groups



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 one or more subnets
- The default Network ACL for a VPC allows all inbound and outbound IPv4 traffic
- When a custom Network ALC is created, all inbound and outbound traffic is denied until separate rules are added



Network ACL Rules

- Rule Numbering: Number rules spaced by 10 to allow space for changes
  - Rule evaluation starts at the lowest defined number
- Inbound Rule
  - Allow or deny for the specified traffic pattern
- Outbound Rule
  - Allow or deny for the specified traffic pattern
- Custom network ACLs deny all inbound and outbound traffic by default until rules are created
- Each subnet within a VPC must be associated with a network ACL (The default is the default ACL)

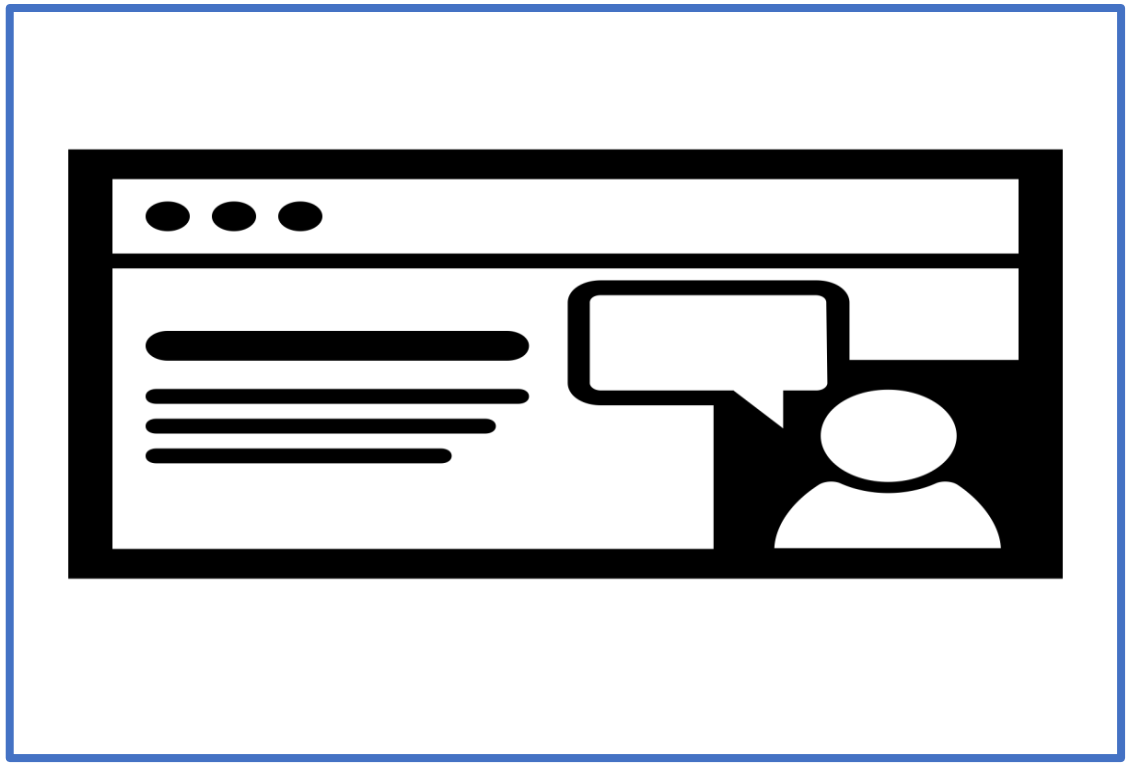
Network ACLs

- A subnet can be associated with only one network ACL at a time
- A network ACL can be associated with multiple subnets
- Rules are evaluated in order **starting 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
- A network ACL has separate inbound and outbound rules either allowing or denying traffic flow
- NACL rules are defined as **stateless**

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
▪Apply to selected instances	▪Applied to the subnet; which is at a lower level of protection than security groups

Exercise: Configure Network ACLs



VPC Options

Endpoints

- A private direct connection between a VPC and S3
- A private direct connection between a VPC and DynamoDB
- PrivateLink for AWS services

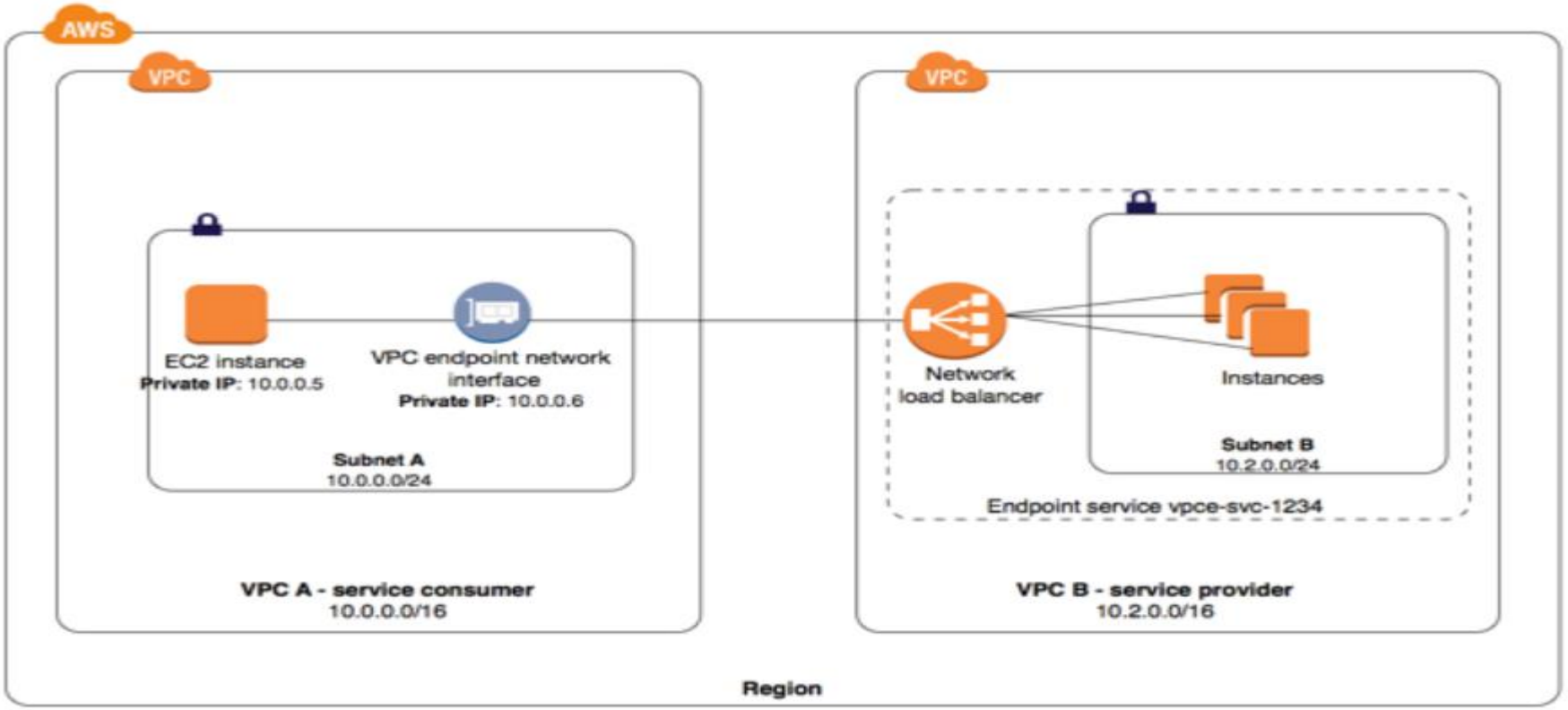
Endpoint Creation Steps:

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

PrivateLink for AWS Services

- Access AWS services from a VPC without using Public IP's
- Endpoints for AWS services powered by PrivateLink use Elastic Network Interfaces with private IP's within your VPC. Supported services include:
  - Amazon EC2
  - ELB
  - EC2 Systems Manager
- On Premise resources accessed through AWS Direct Connect

PrivateLink Options

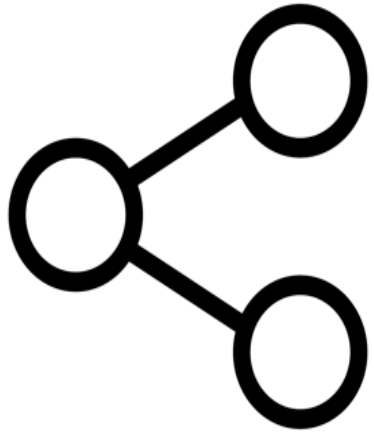


DHCP Option Sets

- Default options provided by AWS when a VPC is created
- DHCP option sets allow you to pass configuration information to EC2 instances
- DHCP option sets can be used across your VPCs
  - Domain Name Servers
  - Domain Name
  - NTP Servers
  - NetBIOS Name Servers

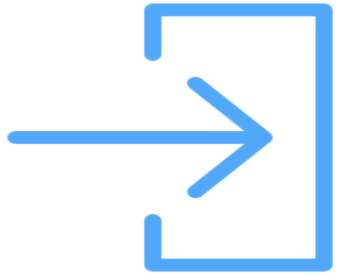
Peering VPC's

- Networking connection between two VPC's
- Your VPC's or: Your VPC's and 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

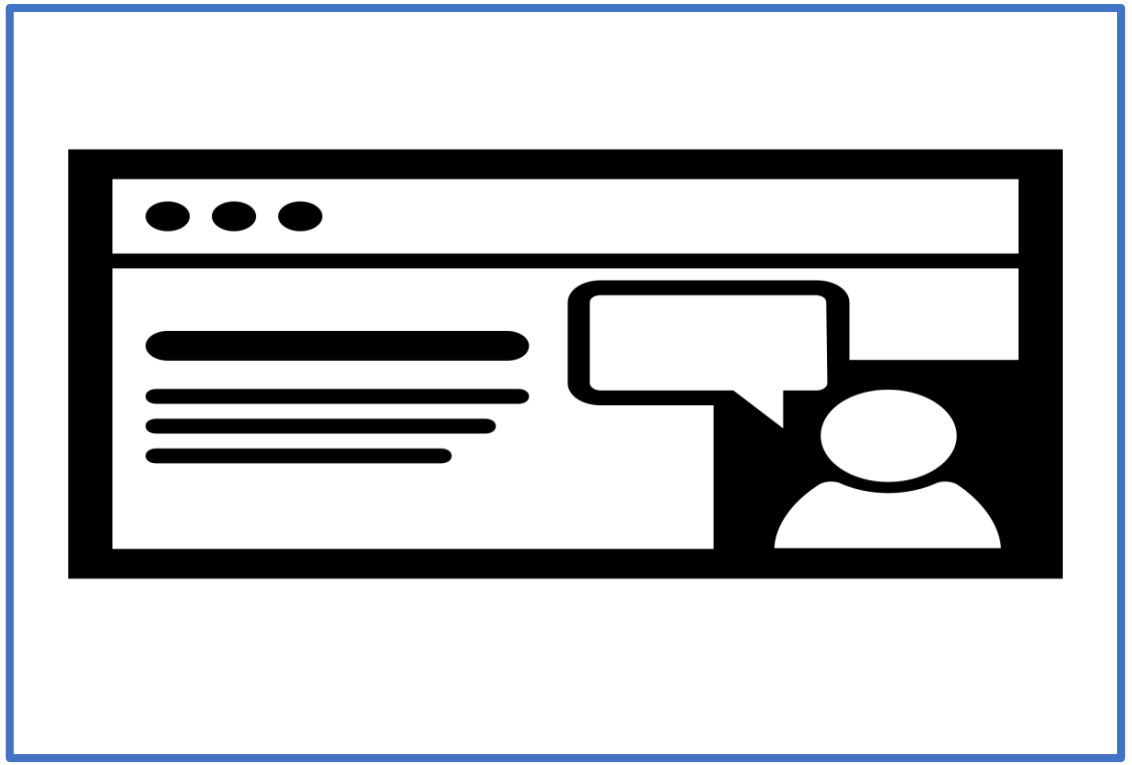


VPC Flow Logs

- 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 Logs
- Does not capture DNS, license, metadata, or default VPC router traffic



Exercise: Enable Flow Logs



NAT Instances

- A NAT Instance accepts traffic from Instances hosted on a private subnet
  - Translate the source IP address to the public IP address of the Nat instance
  - Forward the traffic request to the IGW
  - Return traffic to the private instance that made the request
- NAT Instance creation steps:

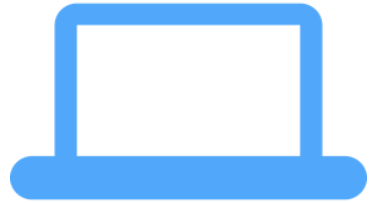
1. Create a security group for the Nat instance
2. Disable the Source / Destination Check attribute of the instance
3. Configure the route table
4. Associate an EIP with the NAT instance

NAT Gateway Service

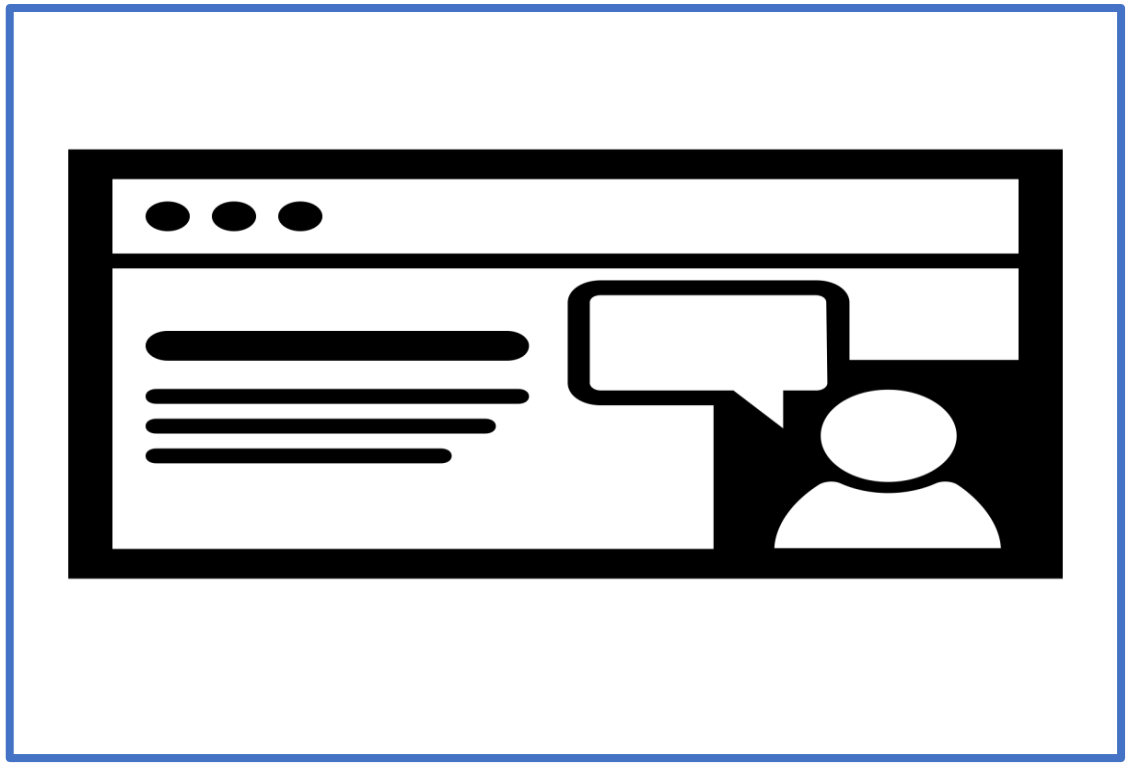
- The AWS NAT gateway service is designed with High Availability per Region

NAT Creation Steps:

1. Configure the route table
2. Associate an EIP with the NAT gateway



Exercise: Create NAT Gateway



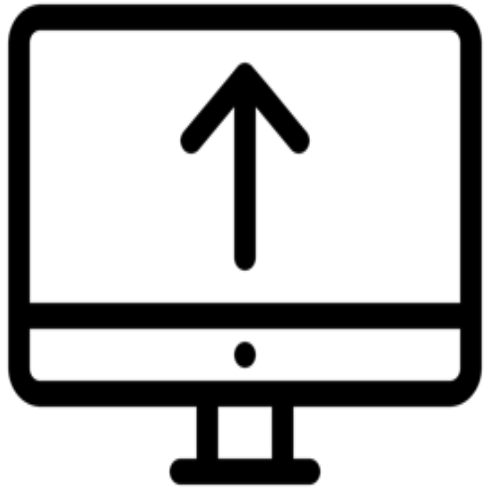
EC2 Instances

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



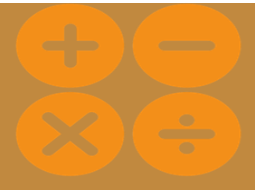
Amazon Machine Images

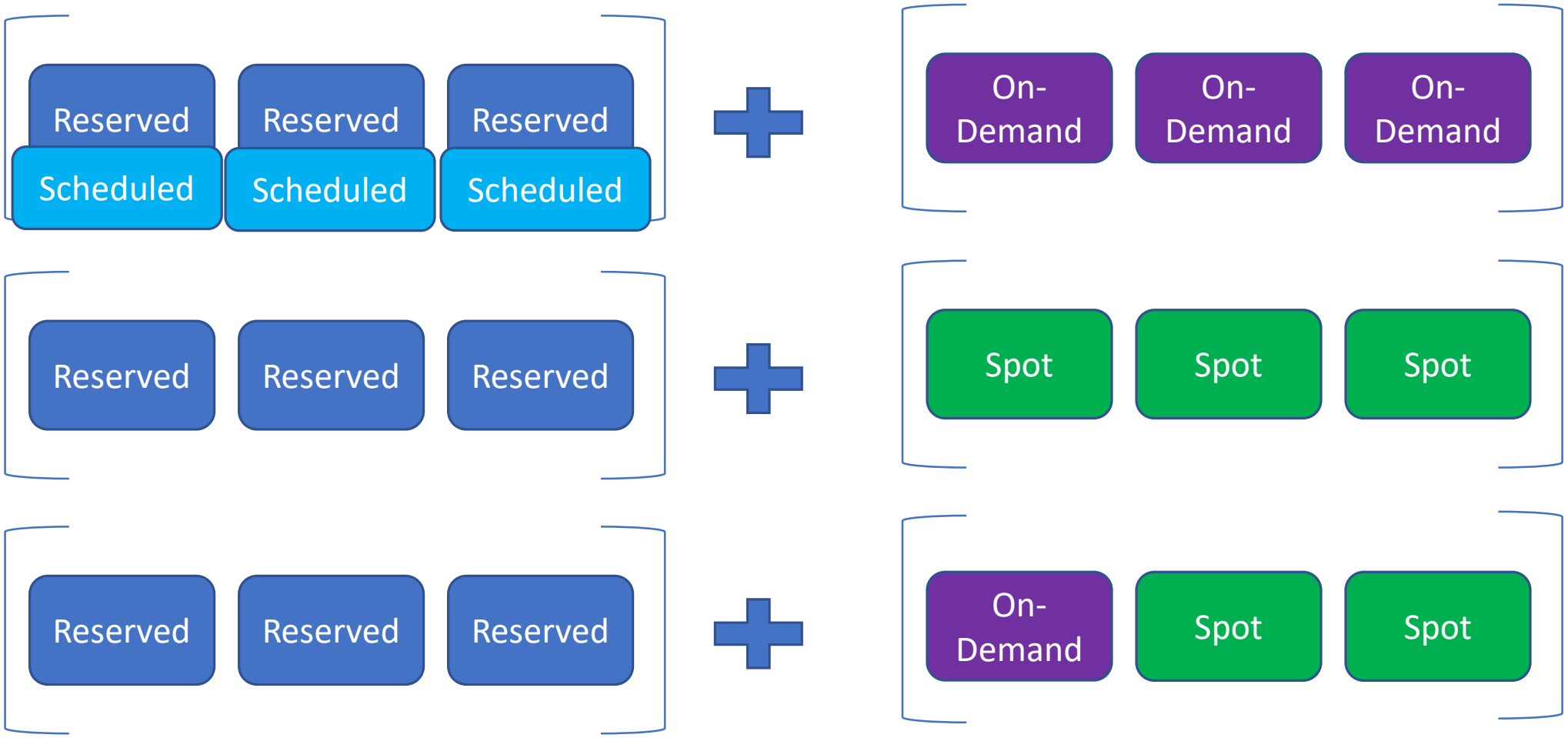
- AMI - Amazon Machine Images
- Defines initial s/w installed on Instance when launched
  - O/S, state, system software
- AMI Types
  - Published – Marketplace
  - Published by AWS – Linux and Window versions / variants
  - VM Import / Export Service
  - Generated from existing Instances – Create image
- Access after launch
  - Across the Internet – Public IP Address, or Elastic IP
  - Private IP address
  - Behind an ELB

EC2 Pricing Options

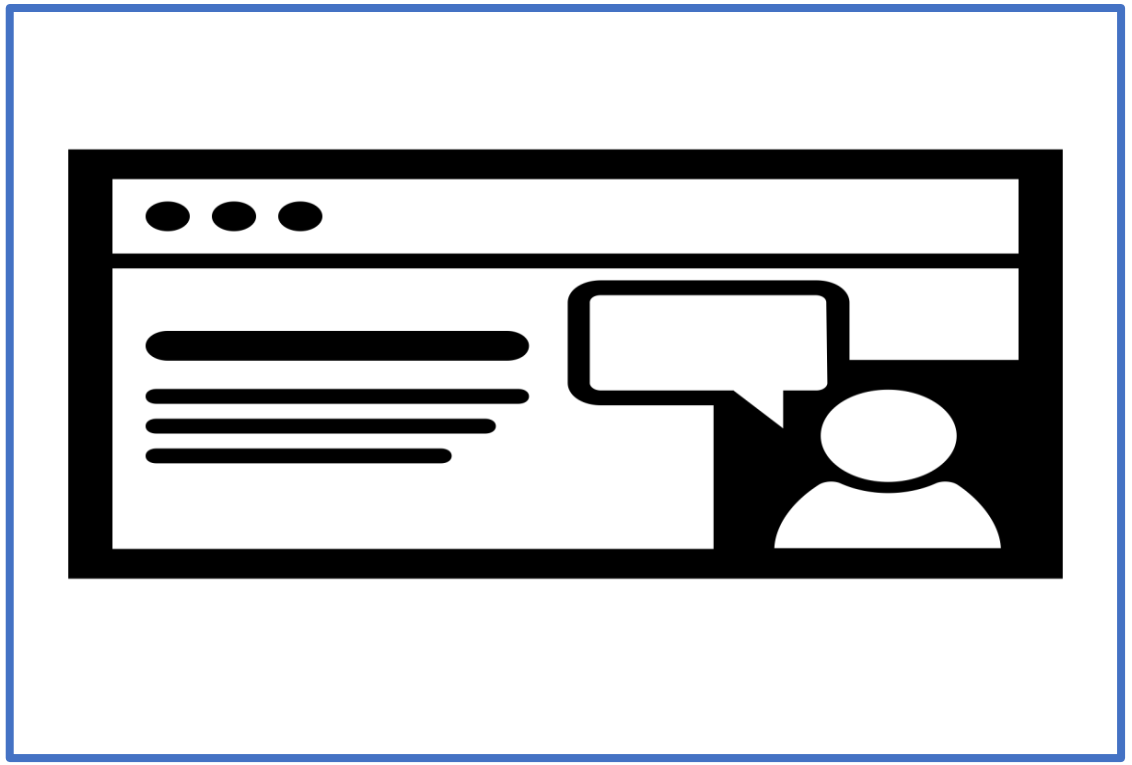
- On-Demand – Billed by the second
- Reserved – All upfront, No upfront, Partial upfront (1, and 3 year)
- Scheduled – Example: Monday, Wednesday, Friday 1-7PM
  - Capacity reservations – 1 or 3 year, Fixed schedule
- Spot Instances – Bid on spot price; 2 minute warning

Pricing Scenarios



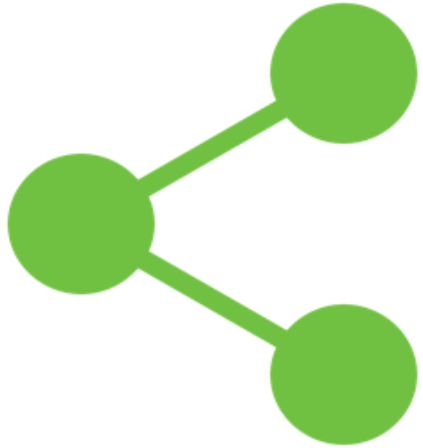


Exercise: Review EC2 Pricing



EC2 Tenancy Options

- Shared tenancy (Default)
- Dedicated instance
- Dedicated host
- Bare metal
- Placement Groups – Instances within a single AZ

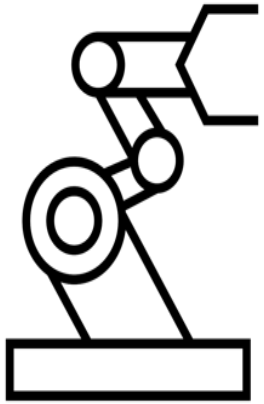


Golden Image Maintenance

- EC2 Instances
- Customize an EC2 Instance and save configuration using an AMI
  - Launch (many) Instances from AMI
- Update Golden Image
  - Launch (many) Instances from AMI
- EBS Volumes – Manual snapshots of System drives or RDS snapshots

Instantiating Computer Resources

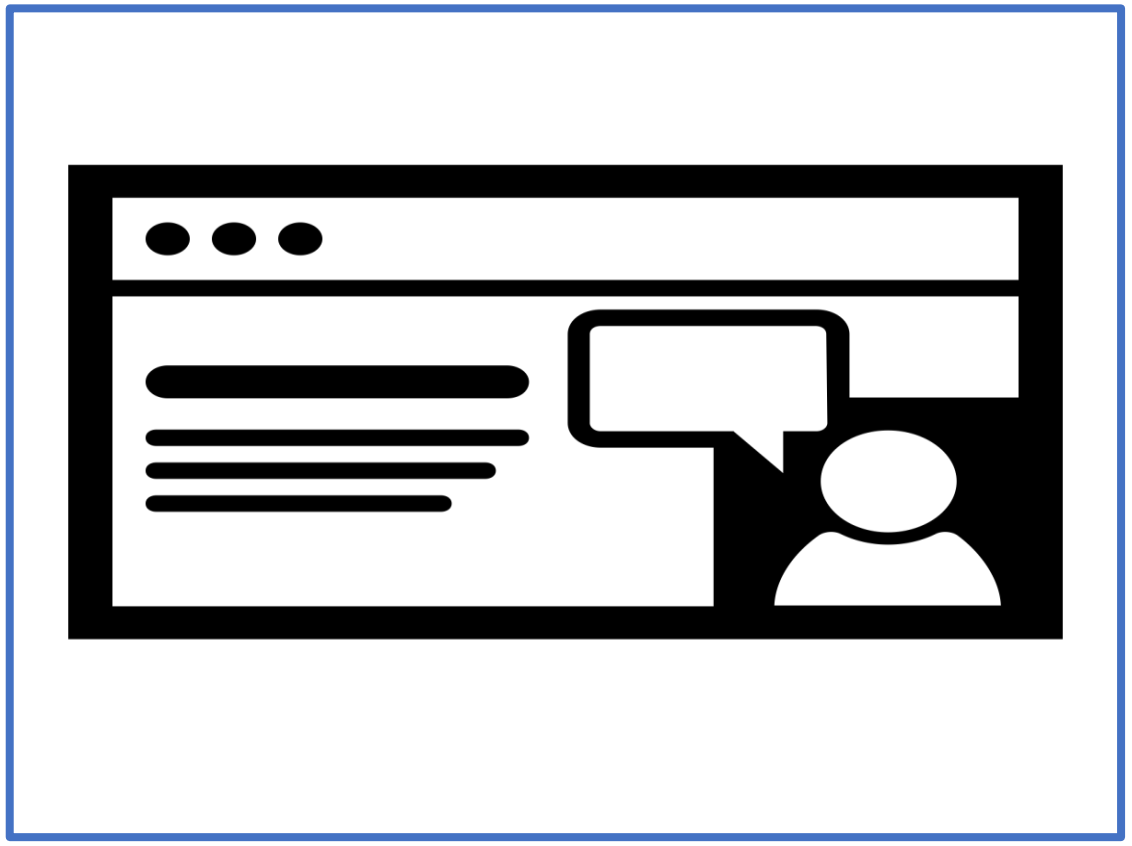
- No more manual processes is the goal
- Bootstrapping – install software, updates, copy data records
- Cloud-init, User data
- Scripts (Bash, PowerShell)
- CloudFormation – JSON template



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 within the same VPC, or a different VPC within the same region

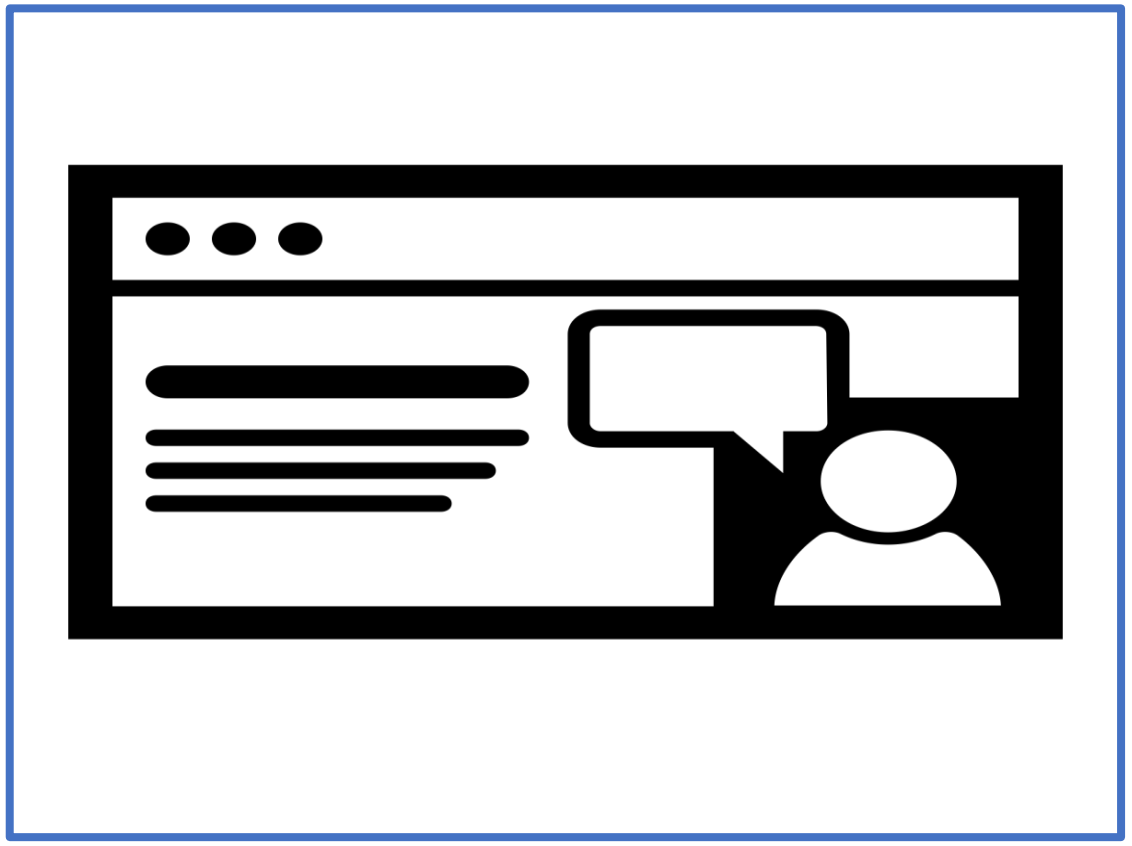
Exercise: Create Elastic IP



Elastic Network Interfaces (ENIs)

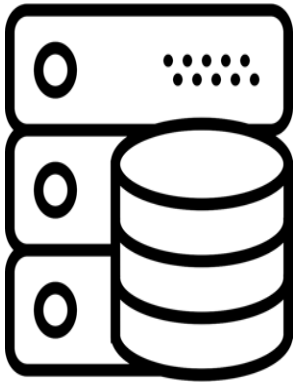
- Virtual network interface that can be attached to an instance within a VPC
- Each ENI can have one public IP address and multiple private IP addresses
- ENI's once created are associated with a subnet
- Use case: Management networks, Dual-homed instances, or Virtual appliances

Exercise: Add Network Interface Card

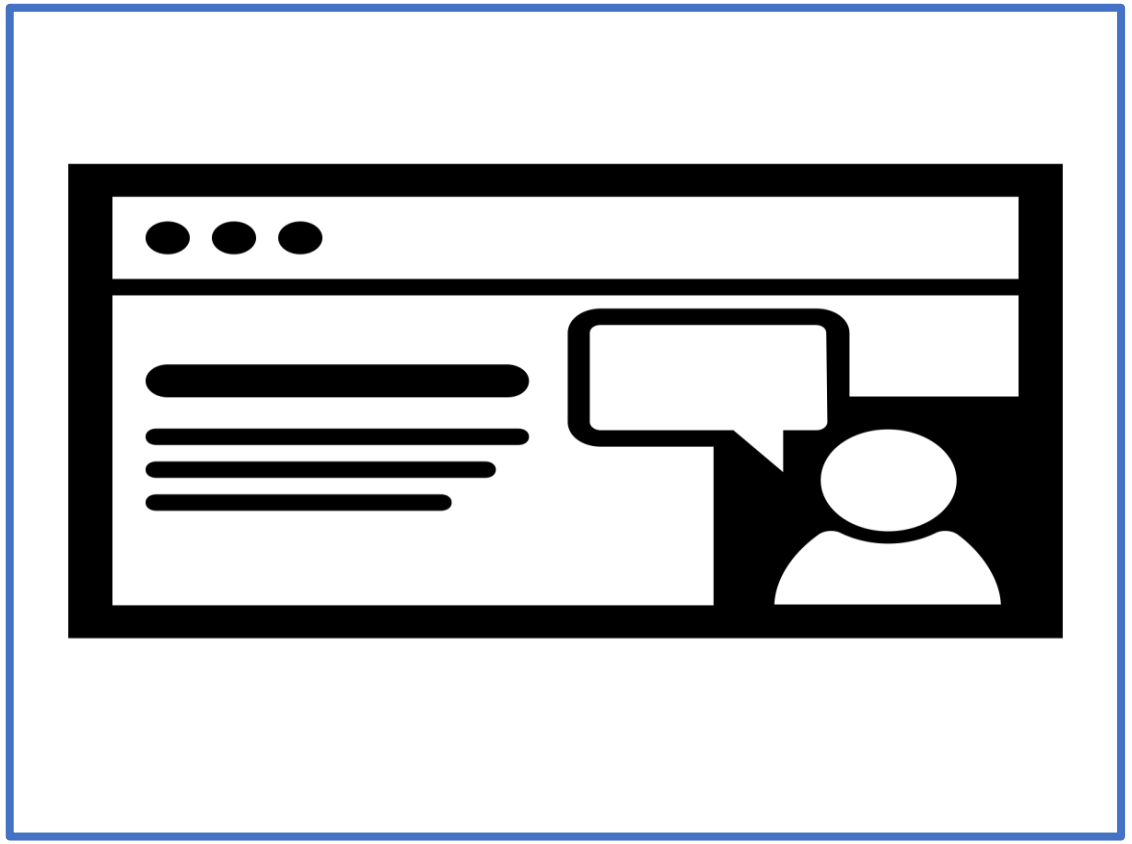


EC2 Instances Stores

- Local disks attached to the bare metal server which hosts your instance(s)
- Called “ephemeral storage”
- Temporary storage – buffers , cache, etc.
- From none at all to 24 TB
- Deleted when Instance is stopped, or fails



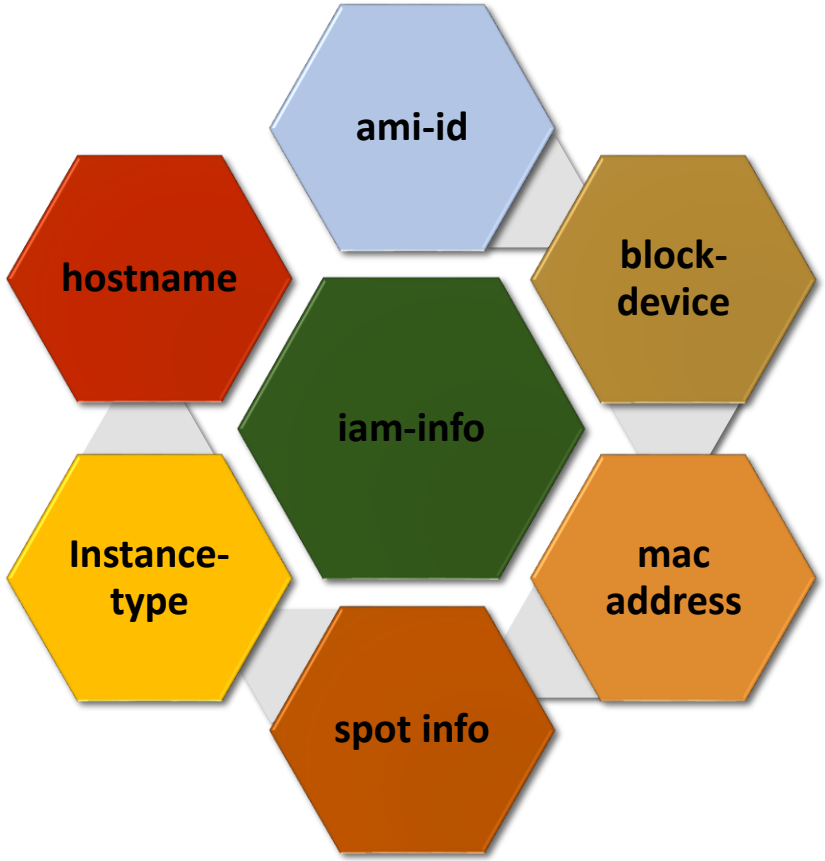
Exercise: Order an EC2 Instance



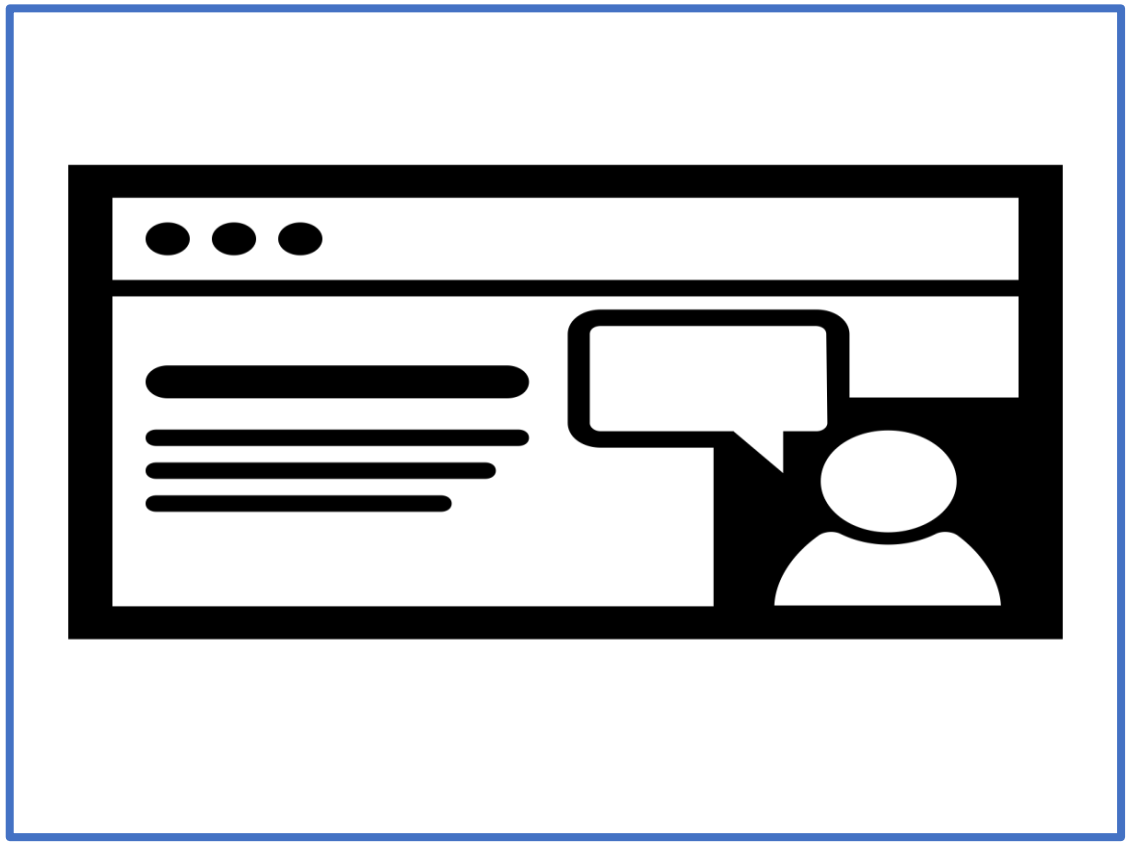
EC2 Instance Metadata

- Wget, cURL, or GET makes a HTTP web request to 169.254.169.254 on the running instance
- EC2 returns the meta-data that is requested including the instance id
- Amazon guarantees it will return the correct data for the requesting instance with no chance of anybody else interfering
- You can only access instance metadata and user data within the Instance itself

EC2 Instance Metadata



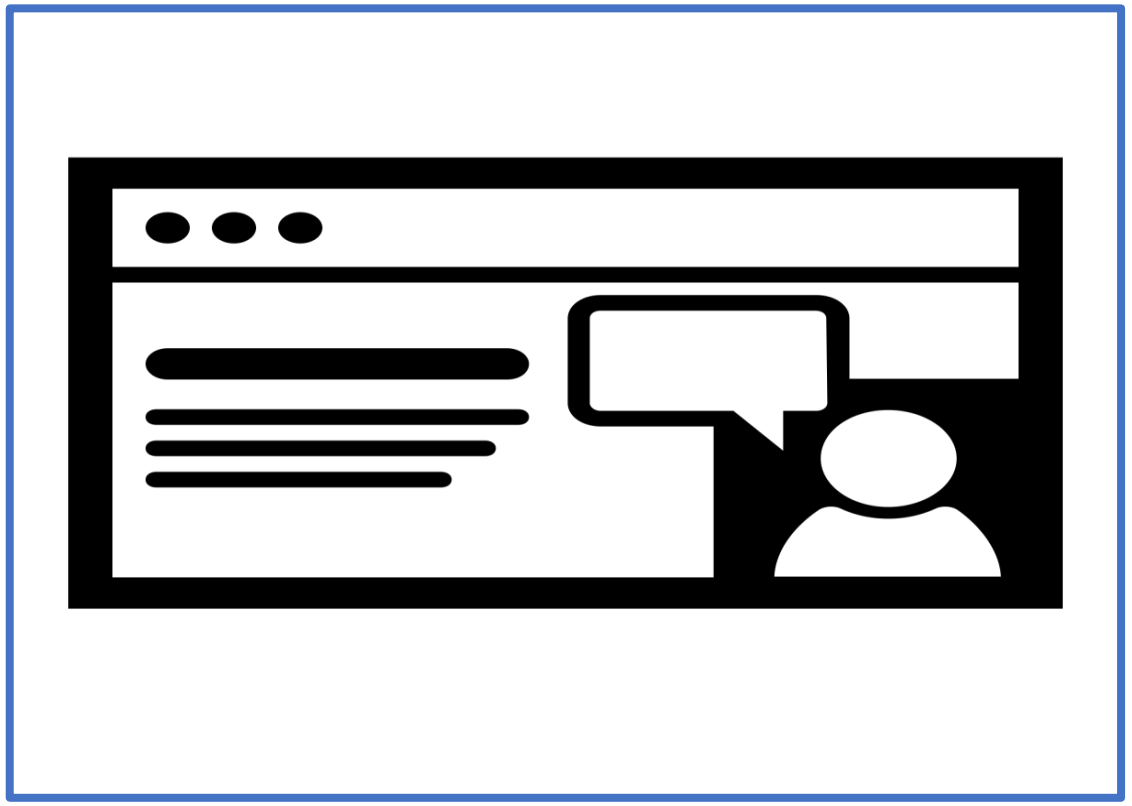
Exercise: Access Metadata



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



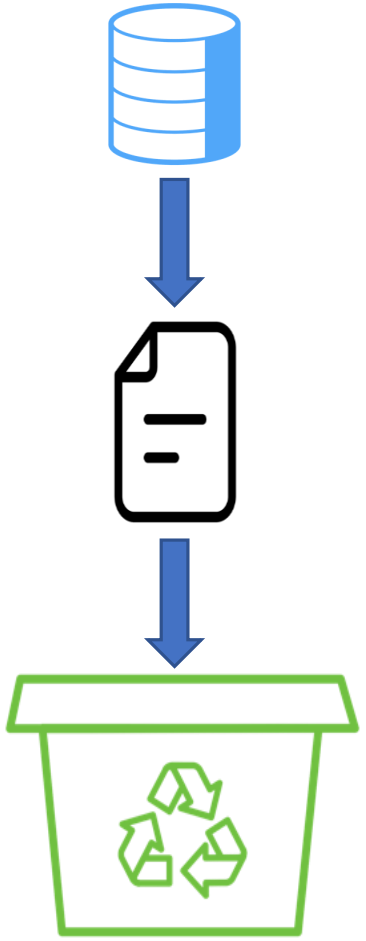
Elastic Block Storage (EBS)

Elastic Block Storage (EBS)

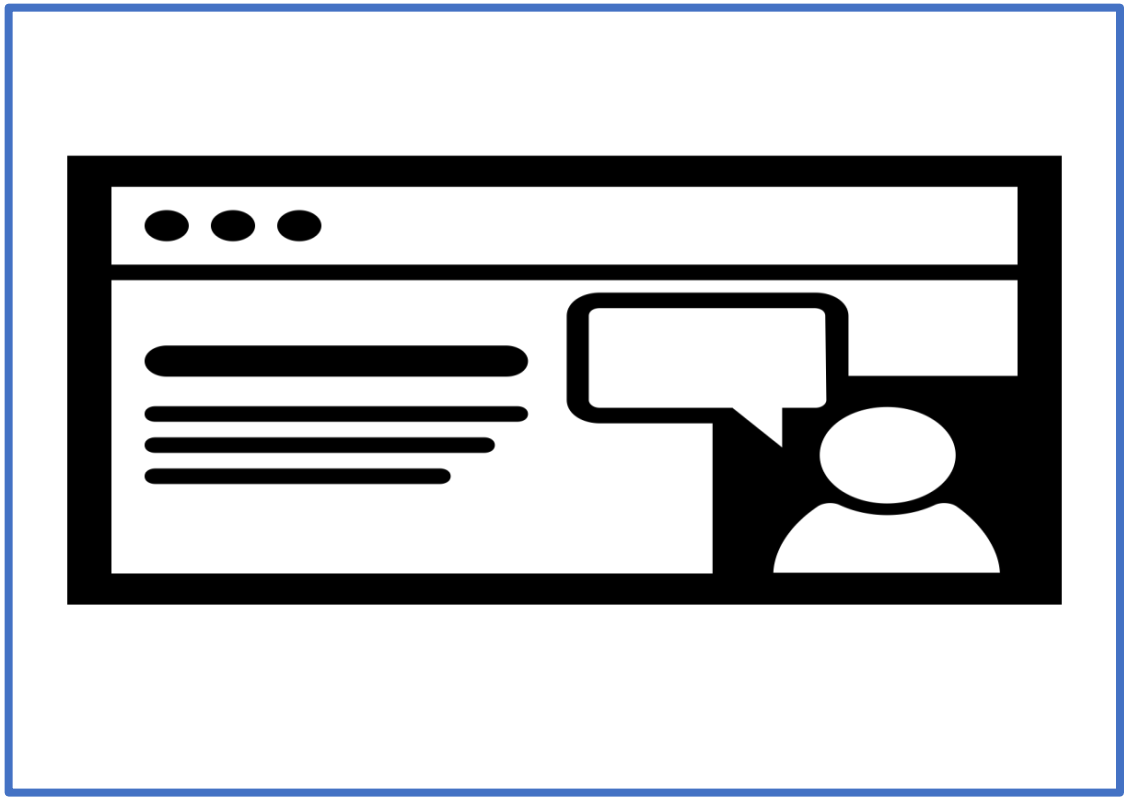
- Persistent Block Storage
  - Each EBS volume replicated within it's AZ location
  - Single EBS Volume attached to one instance
  - Multiple EBS volumes can be attached to one instances
- Magnetic Volume – 1 GB to 16 TB
  - Average 100 IOPS – can burst to 250 -500 IOPS
  - Throughput Optimized (500) / Cold Storage (250)
- General Purpose SSD – 1 GB to 16 TB
  - (3 IOPS per GB) 10,000 IOPS
- Provisioned IOPS SSD 4GB – to 16 TB
  - Up to the lower of the maximum of 30 times the # of GB or 20,000 IOPS

Protecting EBS Volumes

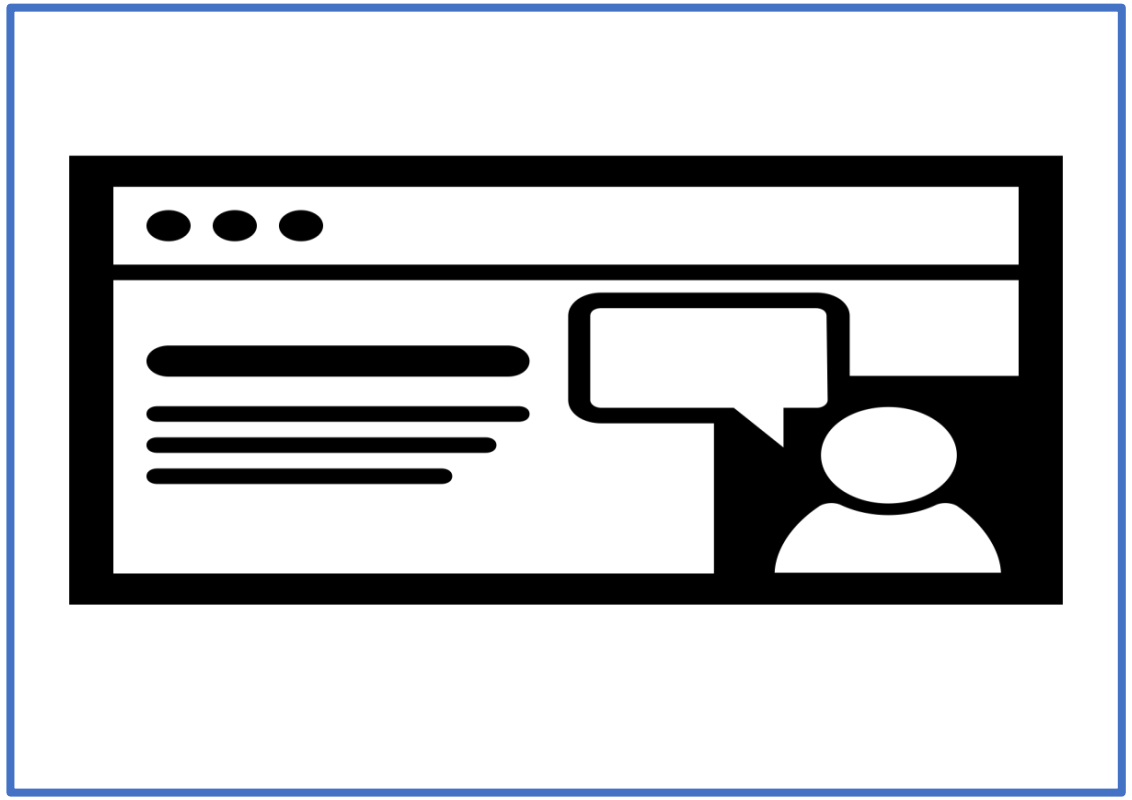
- Backup / Recovery Snapshots
  - Snapshot
  - Point in time
  - S3 in AWS controlled storage
- Create a Volume from a Snapshot
- Increase the size of an EBS volume
  - Re-attach existing volumes
- EBS volumes can be encrypted – KMS service handles key management



Exercise: Create EBS Volumes



Exercise: Create Snapshots



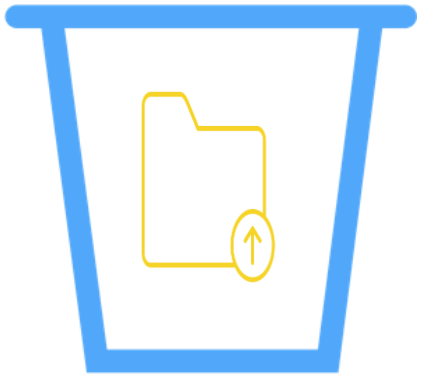
Amazon S3

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

- 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

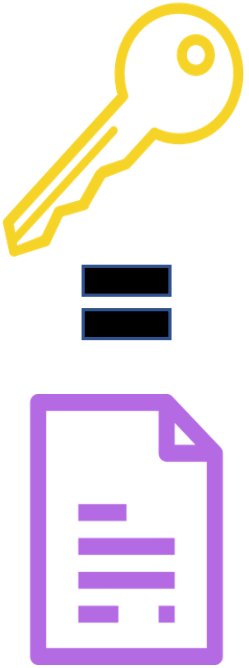


S3 is Object Storage

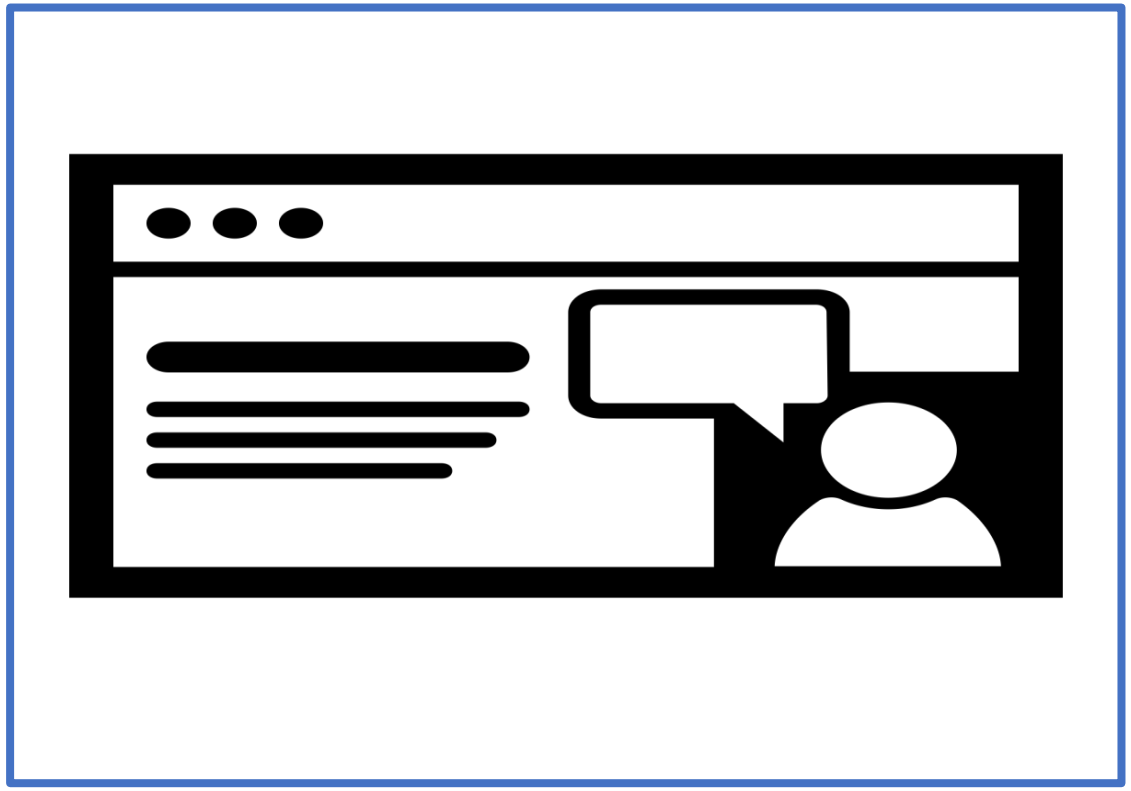
- S3 can store any type of data
  - Up to 5 TB
  - Multi-Part Upload for objects greater than 5 GB
  - Bucket contents can be manually copied to buckets in other regions (Additional costs)
- Metadata describes the data
  - System metadata – AWS date, size, content-type
  - User Metadata – tags specified only at the time the object is created

S3 Object Naming

- Each object has a unique key
  - Key = filename
  - Must be unique within each bucket
- 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

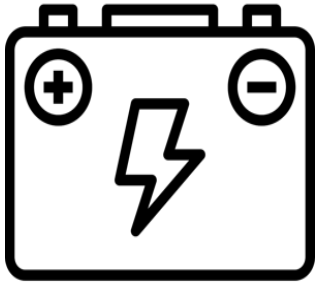


Exercise: Create S3 Bucket



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



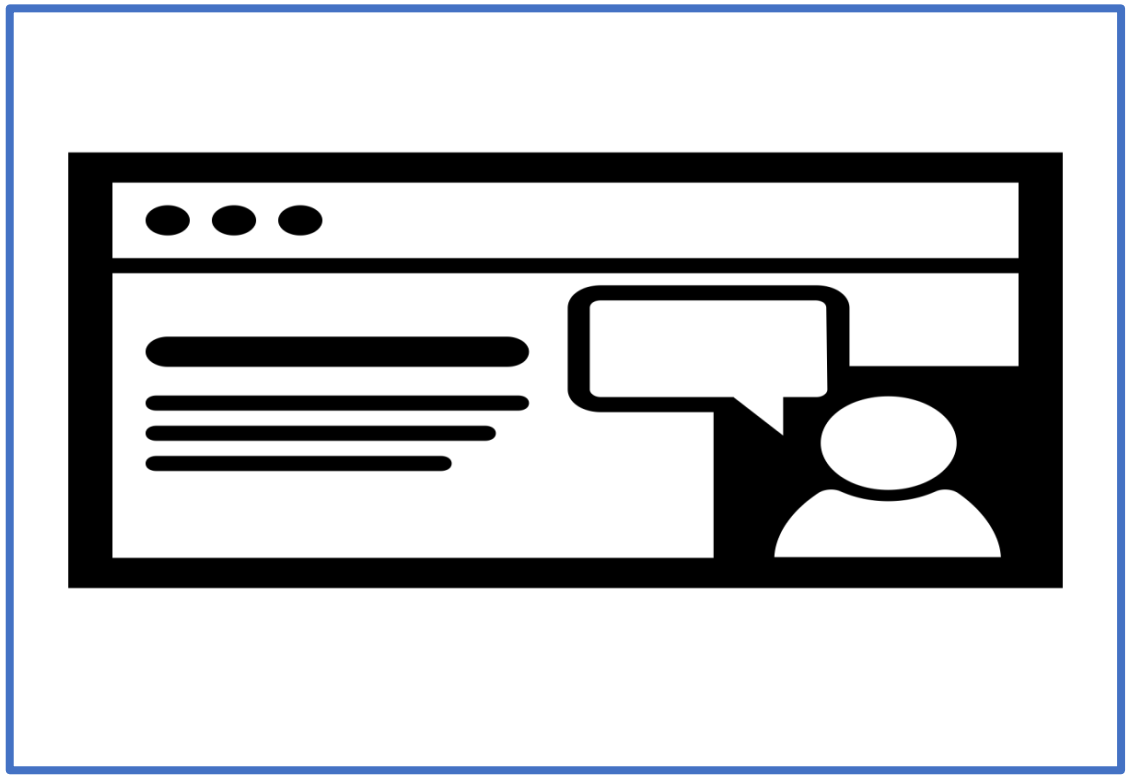
S3 Consistency

- 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

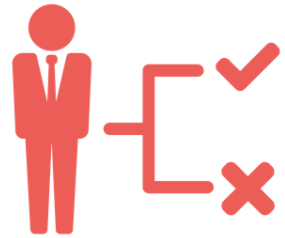
- Only owner has access by default
  - Private by default
- Coarse grained – S3 ACLs
  - Read Write Full Control at object level
- Fine-grained – bucket policies
  - Associated with the bucket / not an IAM security principal
  - Can specify access from where, who can access, and what time of day
- IAM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

Exercise: Create 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)



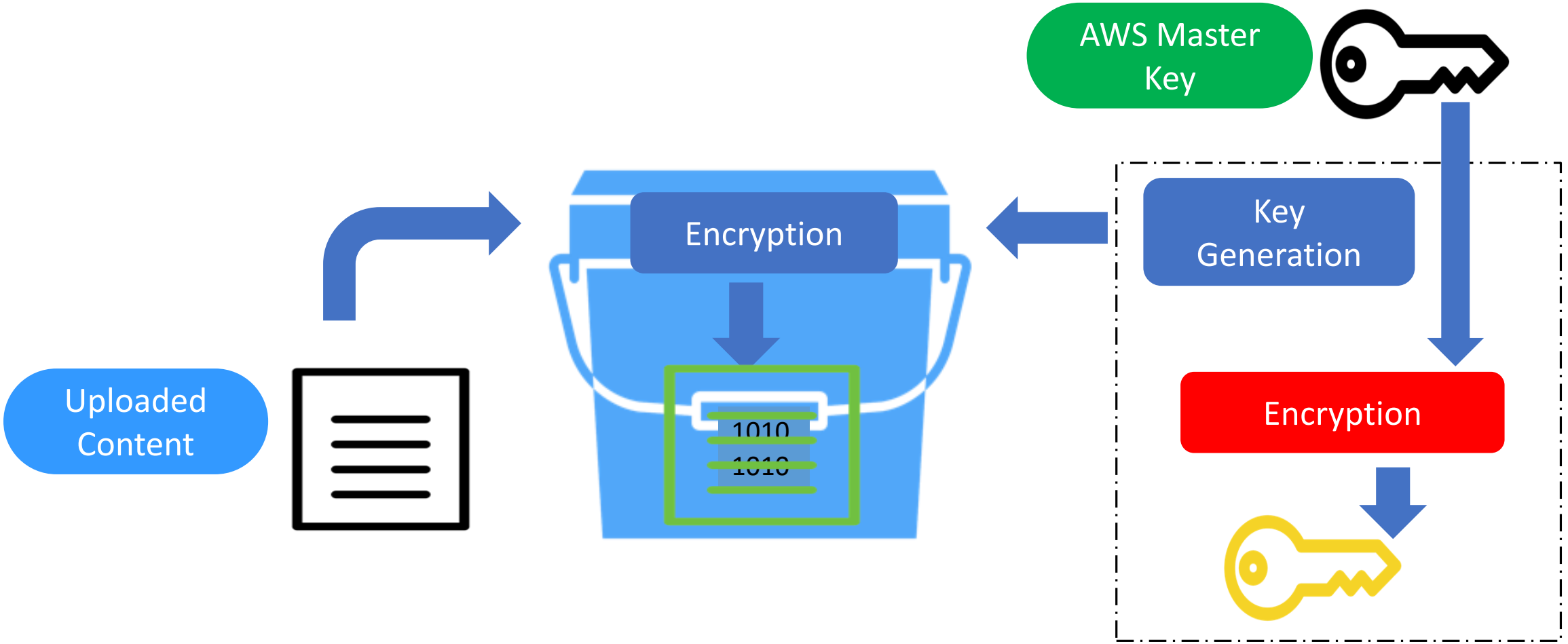
S3 Static Web Site Hosting

1. Create a bucket with the same name as the desired website hostname
2. Upload the static files to the bucket
3. Make all files Public
4. Enable static web site hosting for the bucket
5. Create a CNAME in Route 53

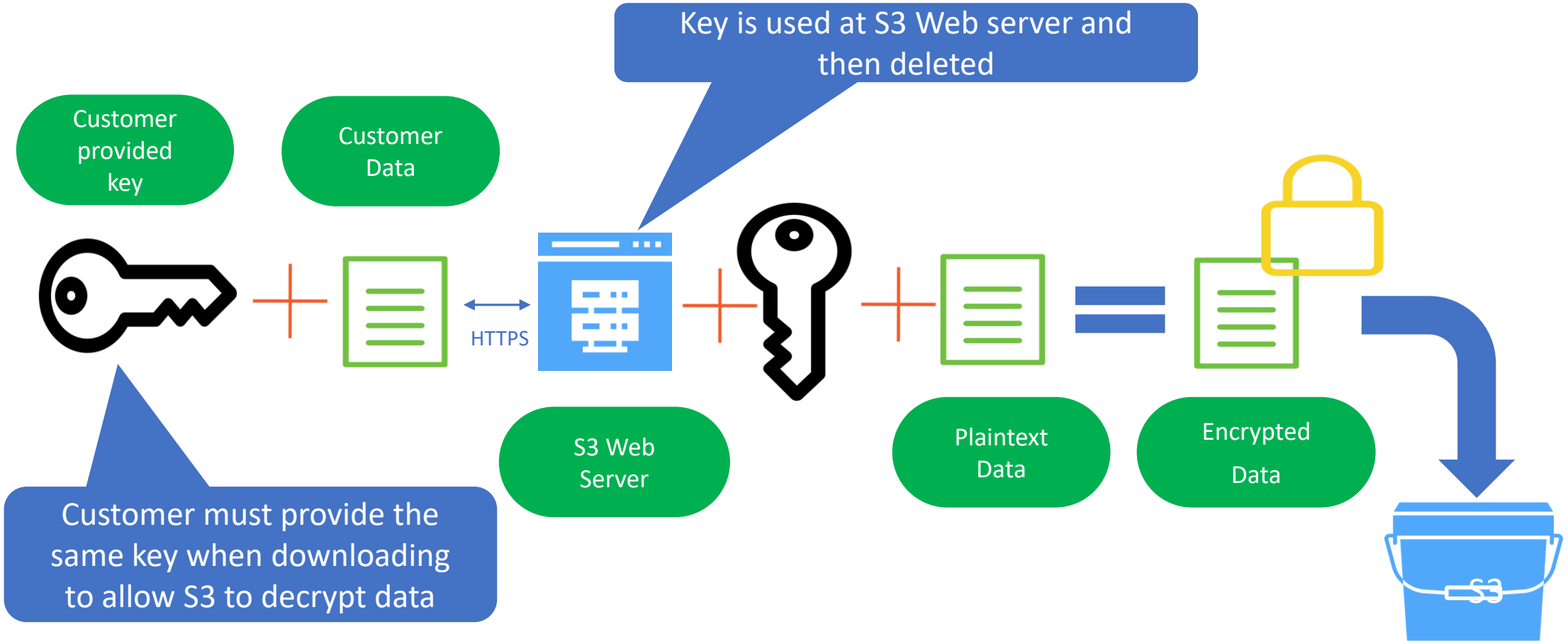
S3 Encryption

- 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

S3 Server-side Encryption



Customer Provided Encryption Key (SSE-C)



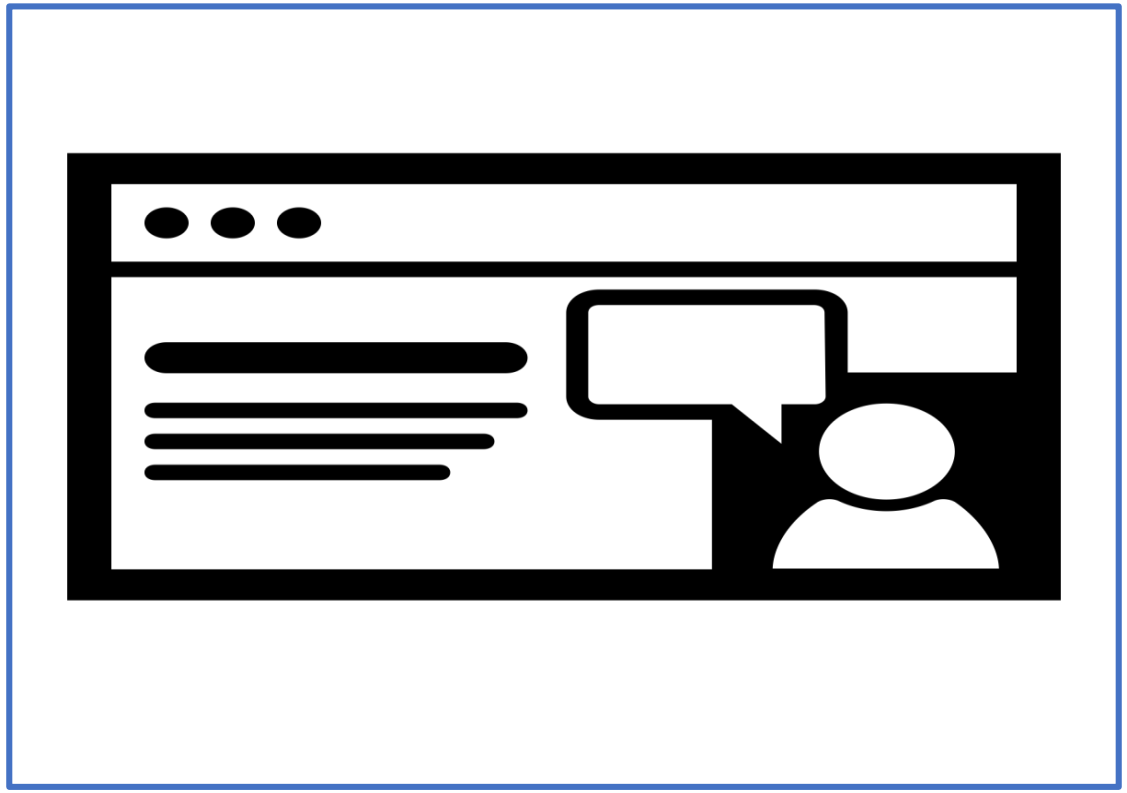
Key Management Service

- 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

Exercise: Enable Versioning



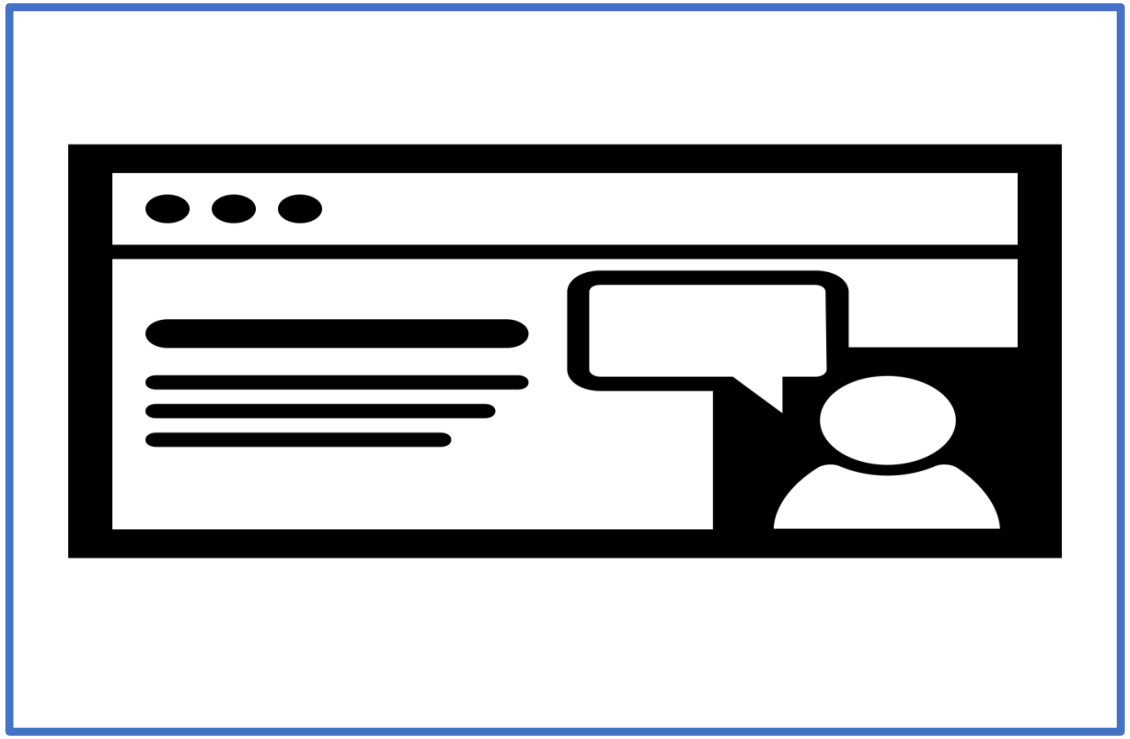
S3 Administration

- 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

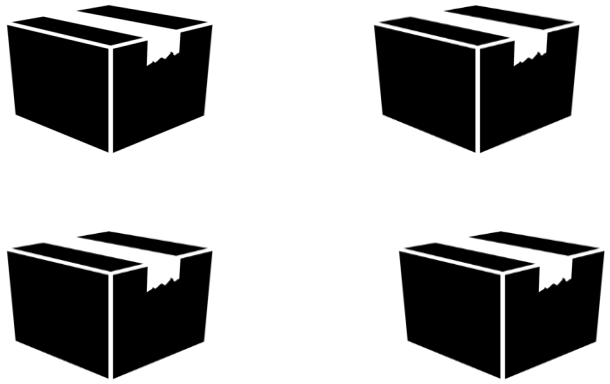


Glacier Storage

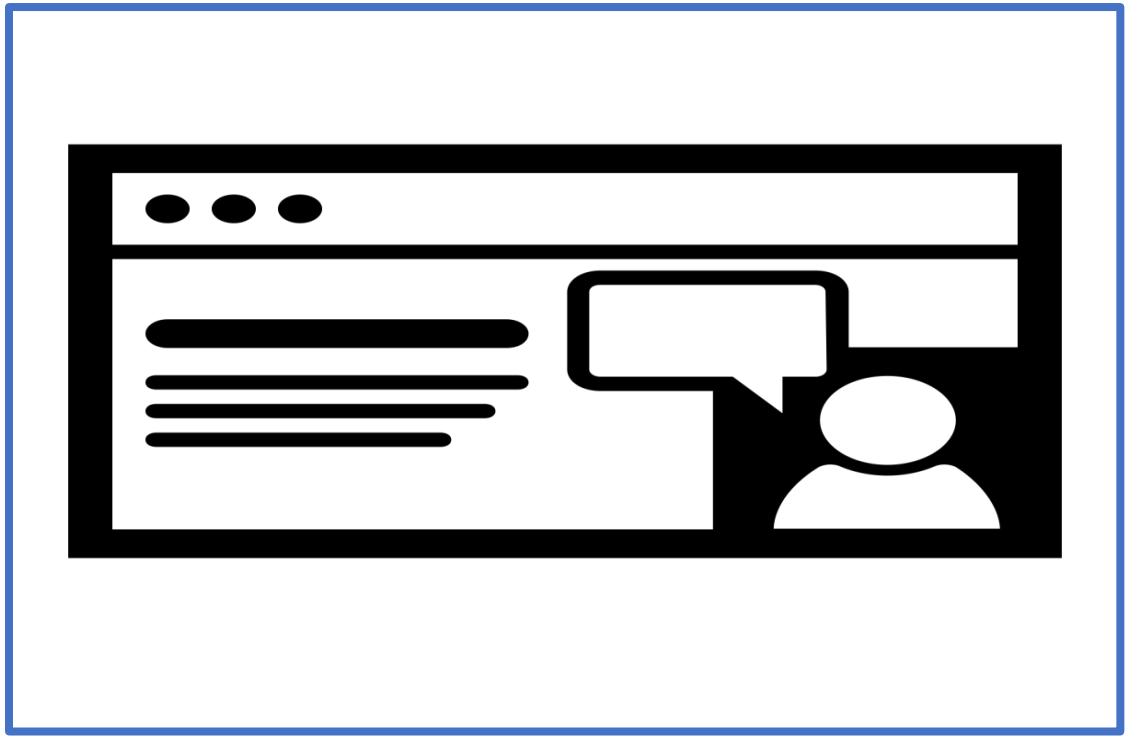
- Low cost archival storage
  - Data is stored in Archives (Up to 40 TB)
  - Unlimited # of archives
  - Automatically encrypted
  - After creation it can’t be modified
- S3 – 5 TB Limit
- Glacier – 40 TB Archives
- Glacier – Encrypted by default
- Glacier – Archive IDs
- S3 – Friendly names

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: Lifecycle Options



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)

Q and A / Wrap-up