Applied Virtual Networks

COMP 4912

Instructor: **Dawood Sajjadi**

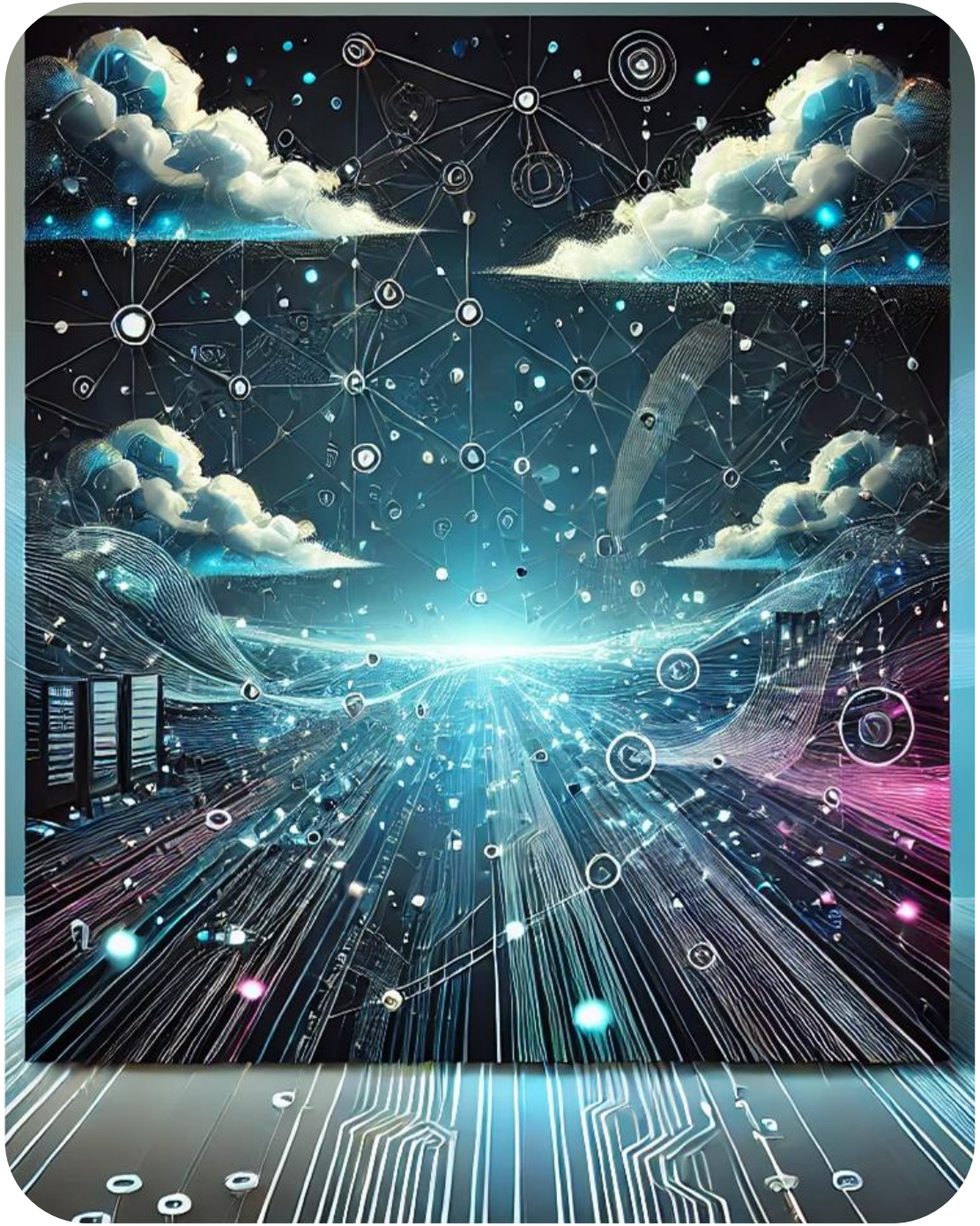
PhD, SMIEEE, CISSP

ssajjaditorshizi@bcit.ca

Winter-Spring 2025

Week #6

BCIT™



Selected Topics for the Course Projects

Cusson

Kubernetes Multi-Cluster Management: Challenges and Solutions

Investigate the latest tools and strategies for managing multiple Kubernetes clusters, including federation, hybrid cloud setups, and edge computing.

Jenny

Edge Computing with Kubernetes: KubeEdge and MicroK8s

Investigate how Kubernetes is being adapted for edge computing scenarios using projects like KubeEdge and MicroK8s.

Jimmy

Emerging Virtualization Technologies: Firecracker, gVisor, and Kata Containers

Investigate lightweight virtualization technologies like Firecracker (AWS Lambda), gVisor (Google), and Kata Containers for secure and efficient workloads.

Rahat

OpenStack as a Private Cloud Solution: Architecture, Use Cases, and Challenges

Explore the architecture of OpenStack, its components (Nova, Neutron, Cinder, etc.), and its role in building private clouds.

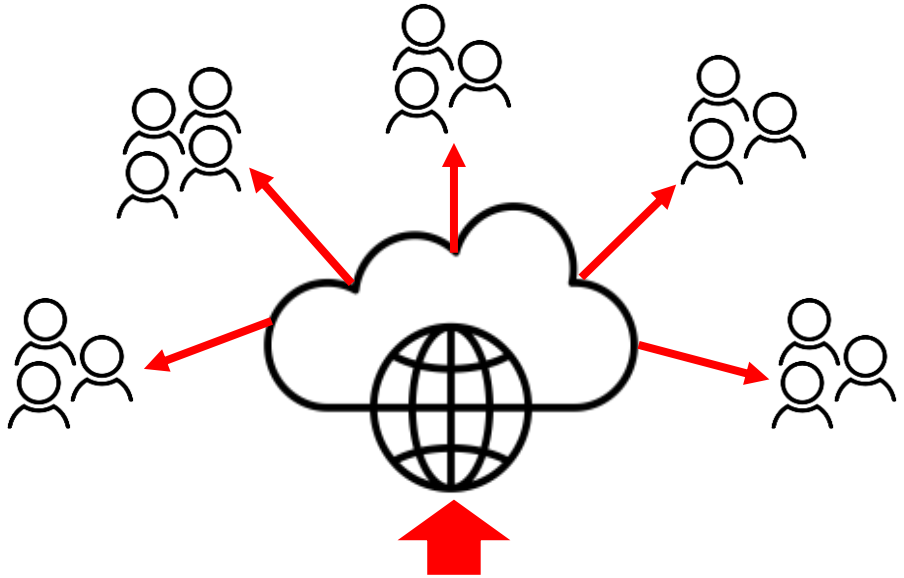
BCIT™

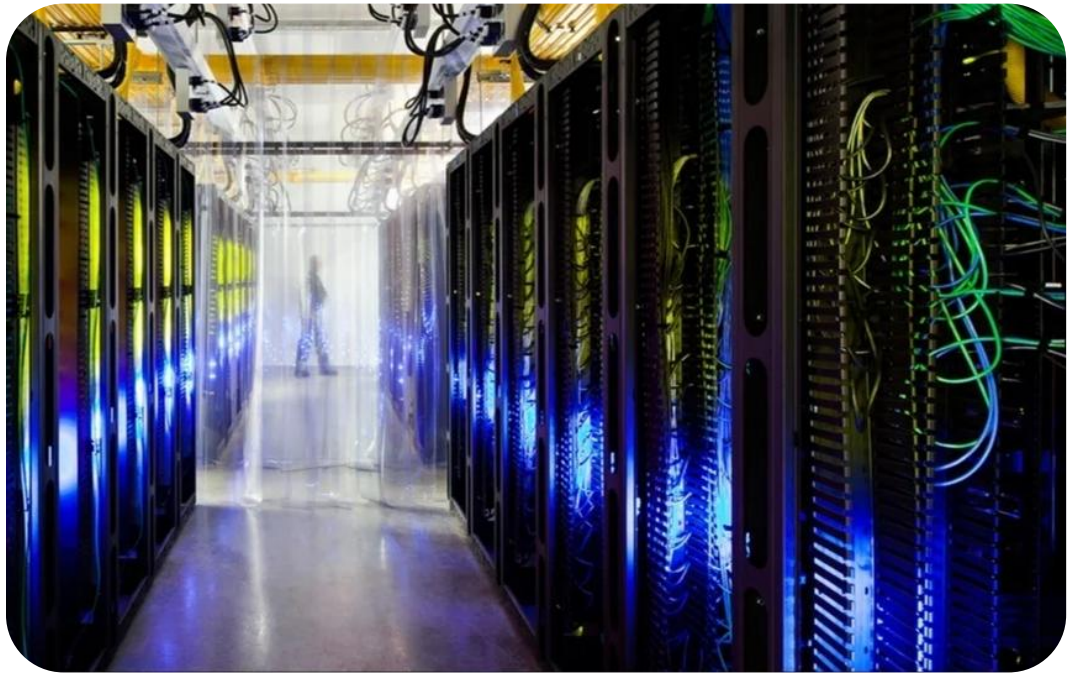
Learning Outcomes of Week #6

1. Explaining the necessity of using Public Cloud services such as Amazon Web Service (AWS).
1. Describing the key terminologies to deploy VMs (instances) in AWS.
1. Understanding security model and measures introduced by the AWS.
1. Explaining the storage options provided by the AWS to the users
1. Grasping Virtual Private Cloud (VPC) concept and its applications in public cloud.
1. Finding out how to define a Security Group to manage access to instances.

BCIT™

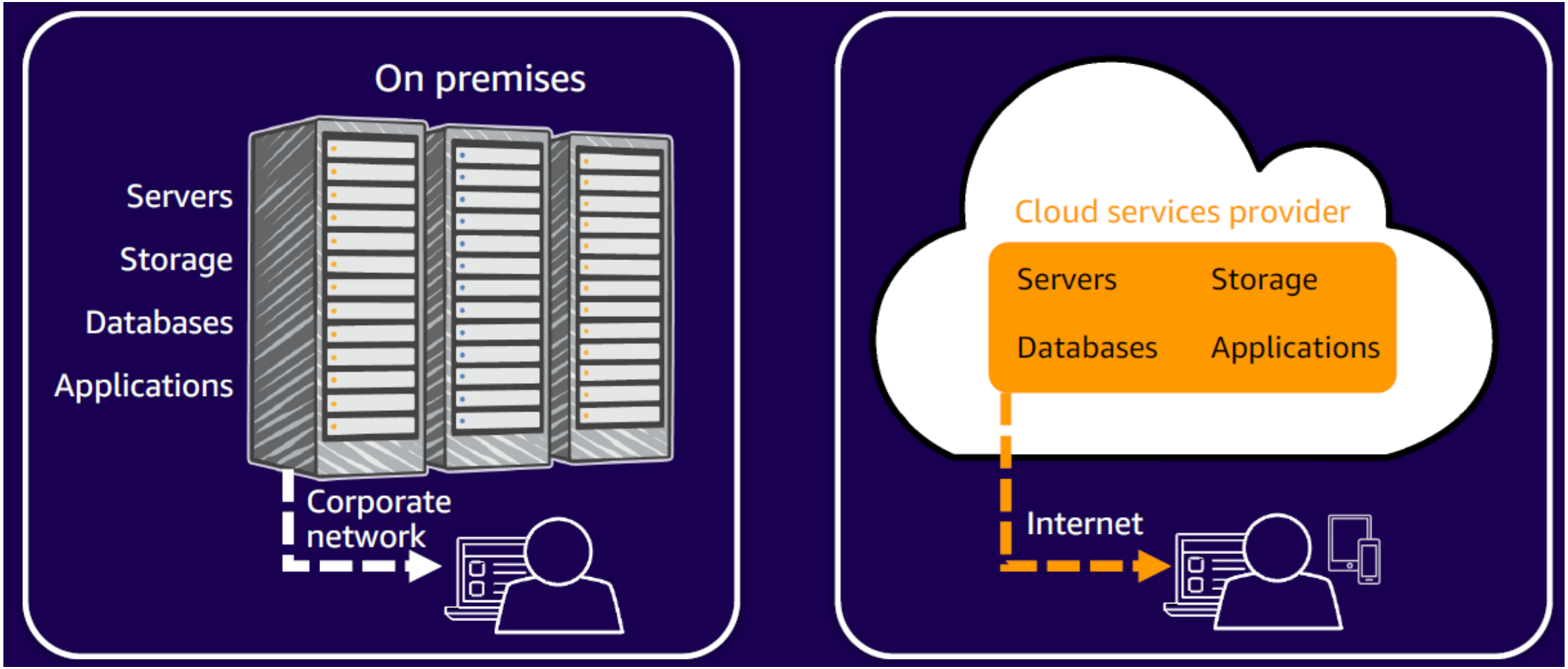
Internet & Servers





BCIT™

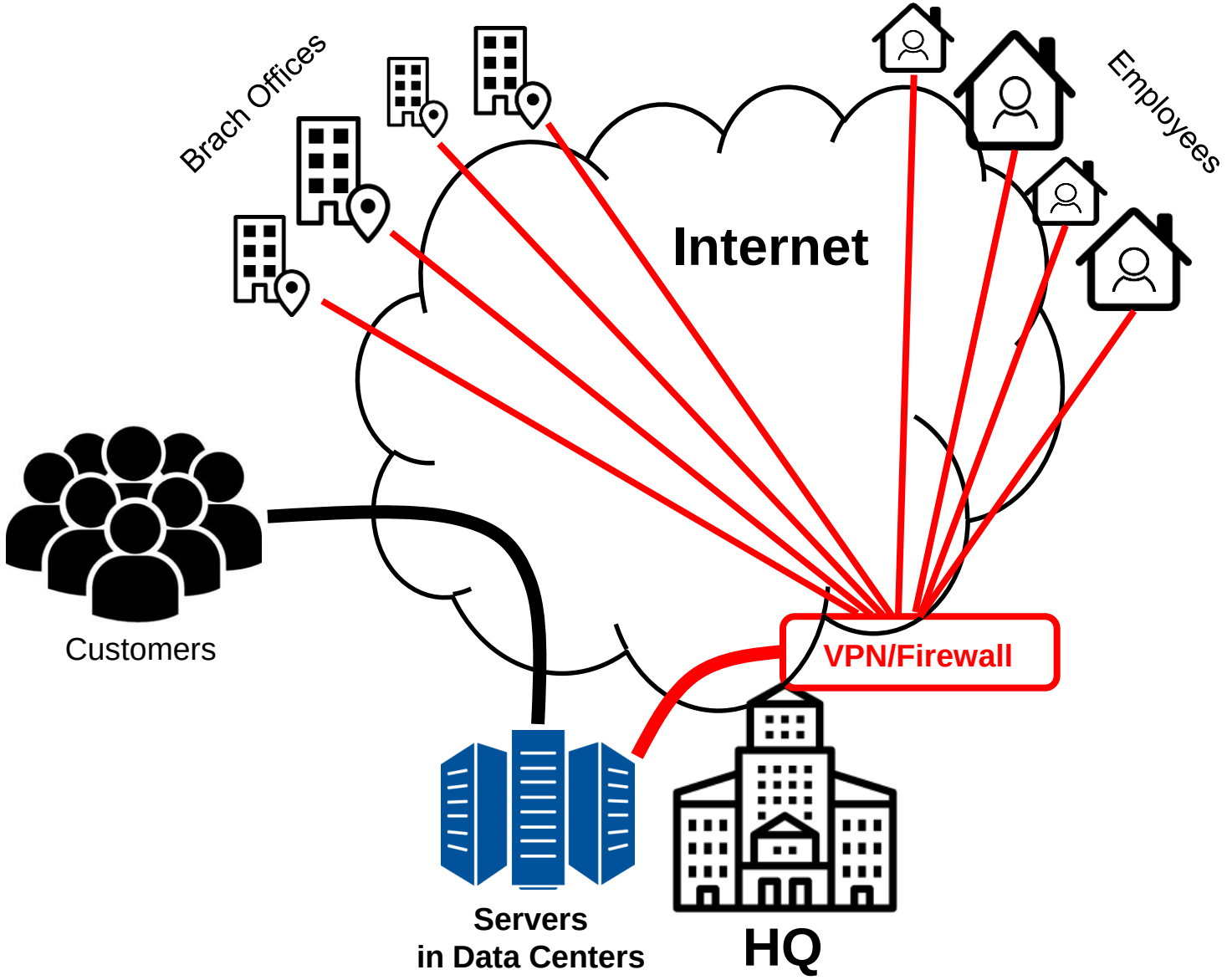
On-Premise vs. Cloud



BCIT™

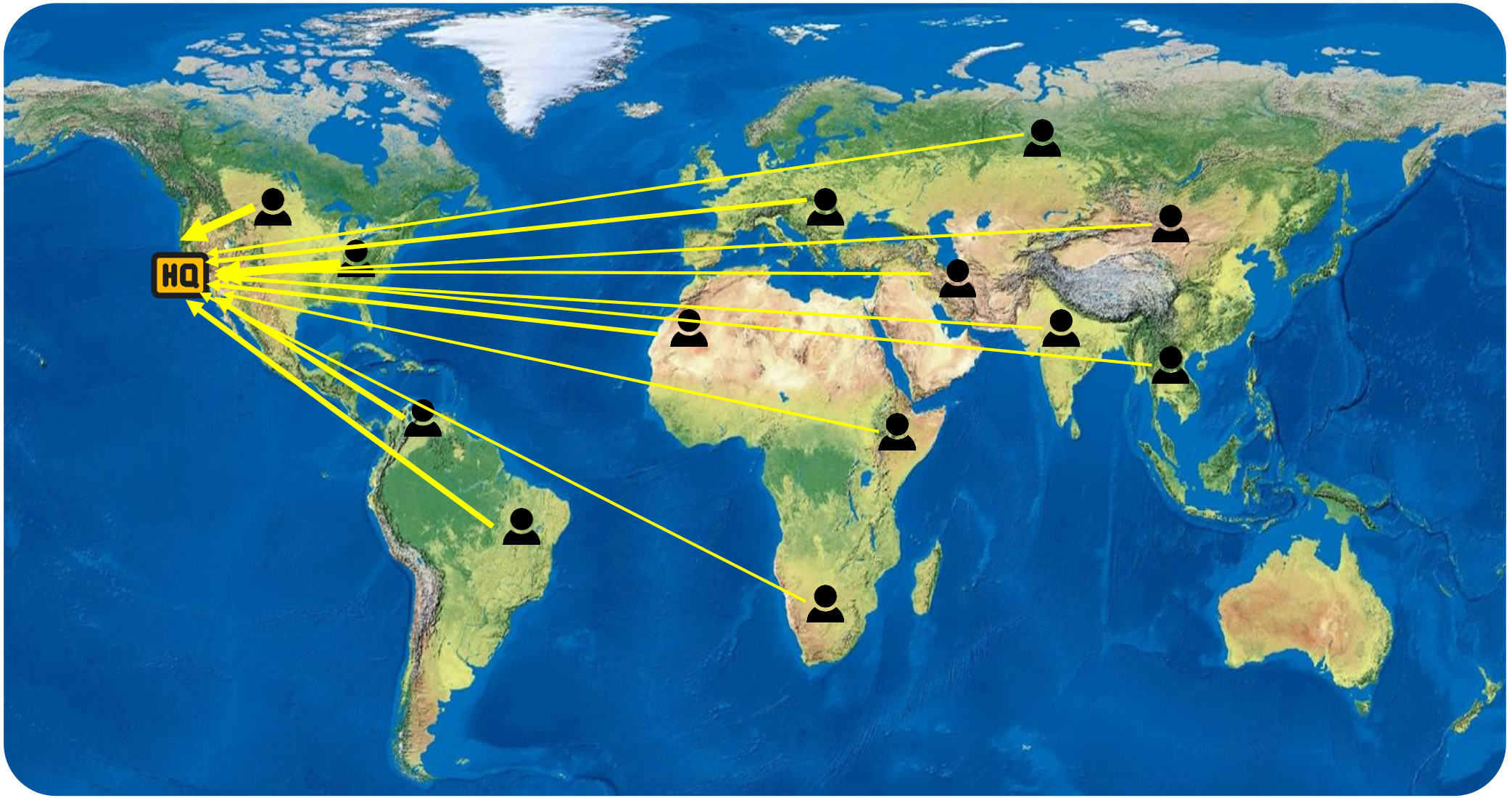
Reference: AWSome Day, Michalynn J. Koziol (2024)

Secure Access to Servers



BCIT™

Connected to the HQ



BCIT™

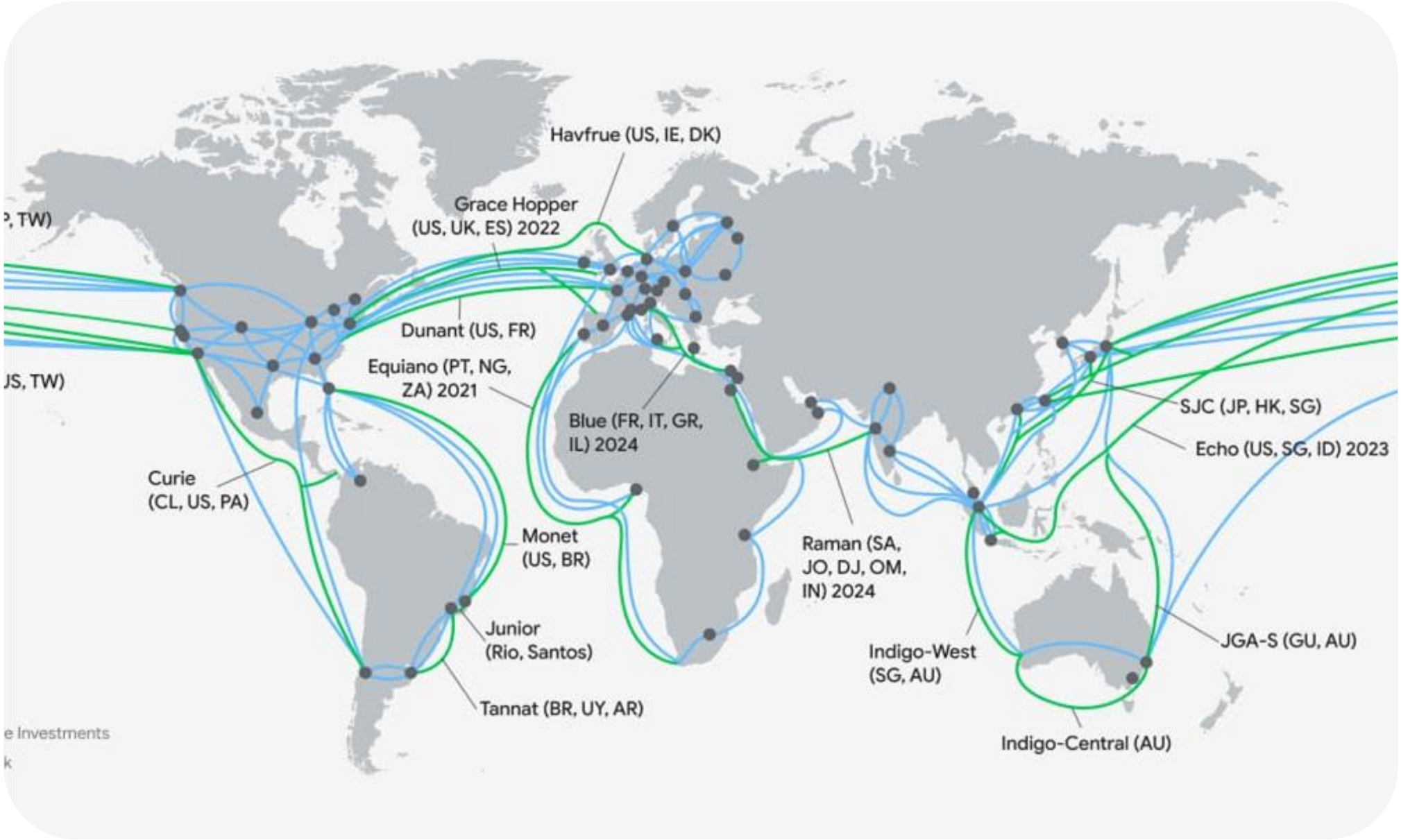
Emergence of Public Clouds

[Spacelift report (Mar 2024)]

[Gartner report (Nov 2023)]

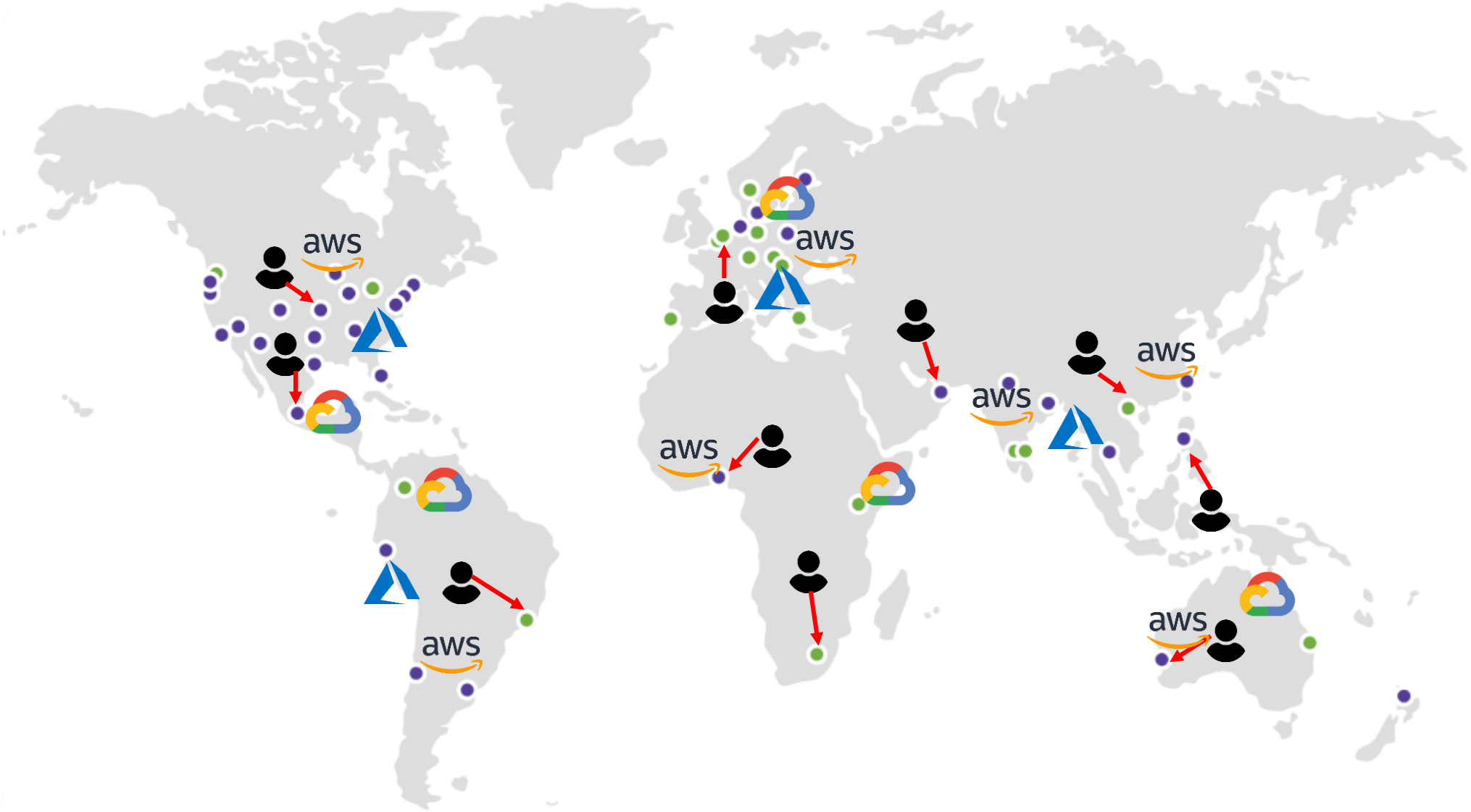
BCIT™

Emergence of Public Clouds



BCIT™

Connecting to the closest site



BCIT™

by: Dawood Sajjadi

Key advantages of Public Cloud (Cloud Computing)

BCIT™

Reference: AWSome Day, Michalynn J. Koziol (2024)

AWS Certifications

https://aws.amazon.com/certification/

BCIT™

List of All Services

BCIT™

Services by category

Compute
- EC2
- Lightsail
- Lambda
- Batch
- Elastic Beanstalk
- Serverless Application Repository
- AWS Outposts
- EC2 Image Builder
- AWS App Runner
- AWS SimSpace Weaver
- EC2 Global View
- Parallel Computing Service

Containers
- Elastic Container Service
- Elastic Kubernetes Service
- Red Hat OpenShift Service on AWS
- Elastic Container Registry

Storage
- S3
- EFS
- FSx
- S3 Glacier
- Storage Gateway
- AWS Backup
- AWS Elastic Disaster Recovery

Developer Tools
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- Cloud9
- CloudShell
- X-Ray
- AWS FIS
- CodeArtifact
- Amazon CodeCatalyst
- AWS AppConfig
- Amazon Q Developer (Including Amazon CodeWhisperer)
- Infrastructure Composer
- AWS App Studio

Customer Enablement
- AWS IQ
- Managed Services
- Activate for Startups
- Support
- AWS re:Post Private

Robotics
- AWS RoboMaker

Blockchain
- Amazon Managed Blockchain

Machine Learning
- Amazon SageMaker AI
- Amazon Augmented AI
- Amazon CodeGuru
- Amazon DevOps Guru
- Amazon Comprehend
- Amazon Forecast
- Amazon Fraud Detector
- Amazon Kendra
- Amazon Personalize
- Amazon Polly
- Amazon Rekognition
- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- AWS DeepComposer
- AWS DeepRacer
- AWS Panorama
- Amazon Monitron
- AWS HealthLake
- Amazon Lookout for Vision
- Amazon Lookout for Equipment
- Amazon Lookout for Metrics
- Amazon Lex
- Amazon Comprehend Medical
- AWS HealthOmics
- Amazon Bedrock
- AWS HealthImaging
- Amazon Q
- Amazon Q Business

Cloud Financial Management
- AWS Marketplace
- AWS Billing Conductor
- Billing and Cost Management

Front-end Web & Mobile
- AWS Amplify
- AWS AppSync
- Device Farm
- Amazon Location Service

Application Integration
- Step Functions
- Amazon AppFlow
- Amazon MQ
- Simple Notification Service
- Simple Queue Service
- SWF
- Managed Apache Airflow
- Amazon EventBridge
- AWS B2B Data Interchange

Business Applications
- Amazon Connect
- Amazon Chime
- Amazon Simple Email Service
- Amazon WorkDocs
- Amazon WorkMail

List of All Services

BCIT™

Database

RDS
ElastiCache
Neptune
Amazon QLDB
Amazon DocumentDB
Amazon Keyspaces
Amazon Timestream
DynamoDB
Amazon MemoryDB
Amazon Aurora DSQL
Oracle Database@AWS

Migration & Transfer

AWS Migration Hub
AWS Application Migration Service
Application Discovery Service
Database Migration Service
AWS Transfer Family
AWS Snow Family
DataSync
AWS Mainframe Modernization
Amazon Elastic VMware Service (Preview)

Networking & Content Delivery

VPC
CloudFront
API Gateway
Direct Connect
AWS App Mesh
Global Accelerator
AWS Cloud Map
Amazon Application Recovery Controller
AWS Private 5G
Route 53

Satellite

Ground Station

Quantum Technologies

Amazon Braket

Management & Governance

AWS Organizations
CloudWatch
AWS Auto Scaling
CloudFormation
AWS Config
OpsWorks
Service Catalog
Systems Manager
Trusted Advisor
Control Tower
AWS Well-Architected Tool
AWS Chatbot
Launch Wizard
AWS Compute Optimizer
Resource Groups & Tag Editor
Amazon Grafana
Amazon Prometheus
AWS Resilience Hub
Incident Manager
AWS License Manager
Service Quotas
AWS Proton
CloudTrail
AWS Resource Explorer
AWS User Notifications
AWS Health Dashboard
AWS Telco Network Builder

Media Services

Kinesis Video Streams

Analytics

Athena
Amazon Redshift
CloudSearch
Amazon OpenSearch Service
Kinesis
QuickSight
AWS Data Exchange
AWS Lake Formation
MSK
AWS Glue DataBrew
Amazon FinSpace
AWS Glue
Amazon Data Firehose
EMR
AWS Clean Rooms
Amazon SageMaker
AWS Entity Resolution
Managed Apache Flink
Amazon DataZone

Security, Identity, & Compliance

Resource Access Manager
Cognito
Secrets Manager
GuardDuty
Amazon Inspector
Amazon Macie
IAM Identity Center
Certificate Manager
Key Management Service
CloudHSM
Directory Service
AWS Firewall Manager
AWS Artifact
Detective
AWS Signer
AWS Private Certificate Authority
Security Hub

Amazon WorkMail
AWS Supply Chain
AWS AppFabric
AWS Wickr
Amazon Chime SDK
Amazon One Enterprise
Amazon Pinpoint
AWS End User Messaging

End User Computing

WorkSpaces
AppStream 2.0
WorkSpaces Secure Browser
WorkSpaces Thin Client

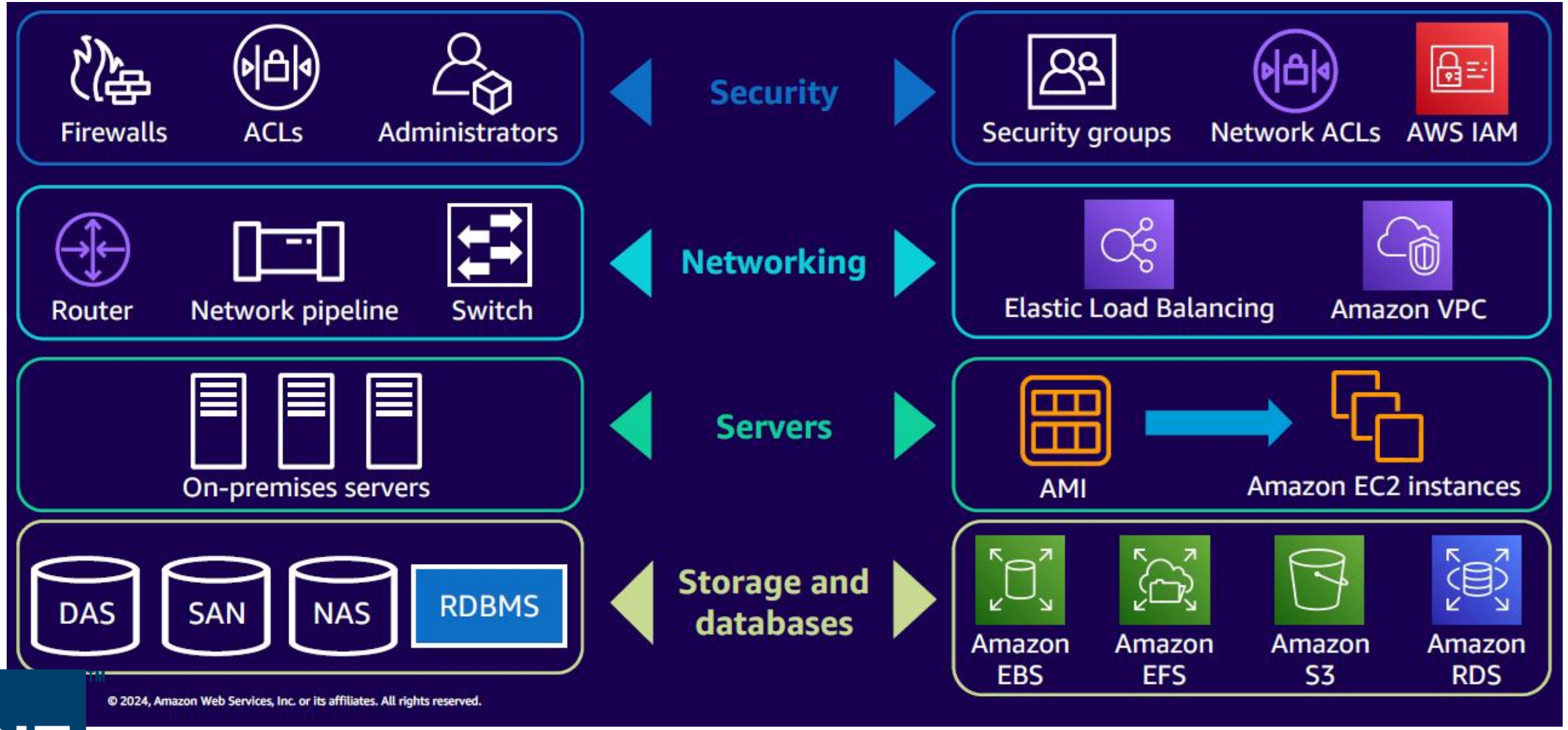
Internet of Things

IoT Analytics
IoT Device Defender
IoT Device Management
IoT Greengrass
IoT SiteWise
IoT Core
IoT Events
AWS IoT FleetWise
IoT TwinMaker

Game Development

Amazon GameLift

AWS Core Infrastructure-as-a-Service (IaaS)



BCIT

Reference: AWSome Day, Michalynn J. Koziol (2024)

Compute

BCIT™

Virtual machines vs. physical servers

Amazon EC2 can solve some problems that are more difficult with an on-premises server

When using disposable resources

Data-driven decisions

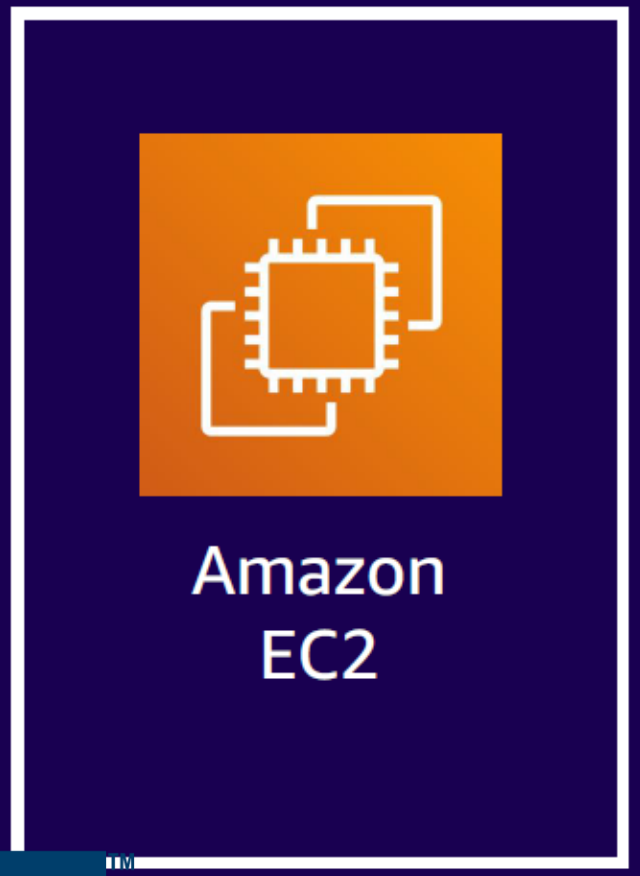
Quick iterations

Free to make mistakes

BCIT

Reference: AWSome Day, Michalynn J. Koziol (2024)

Amazon Elastic Compute Cloud (Amazon EC2)

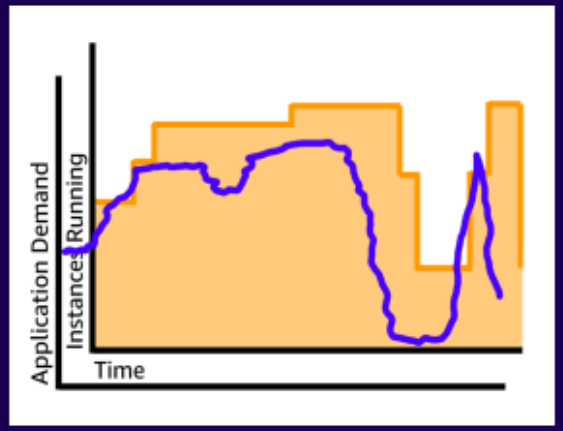


- Resizable compute capacity
- Complete control of your computing resources
- Reduced time required to obtain and boot new server instances

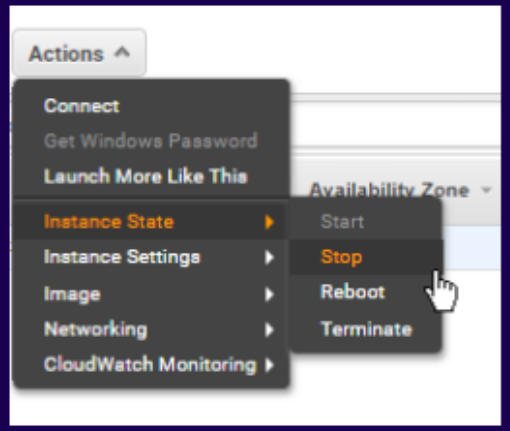
BCIT

Reference: AWSome Day, Michalynn J. Koziol (2024)

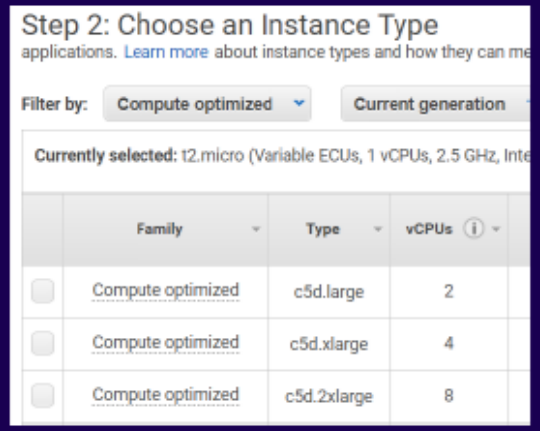
Benefits of Amazon EC2



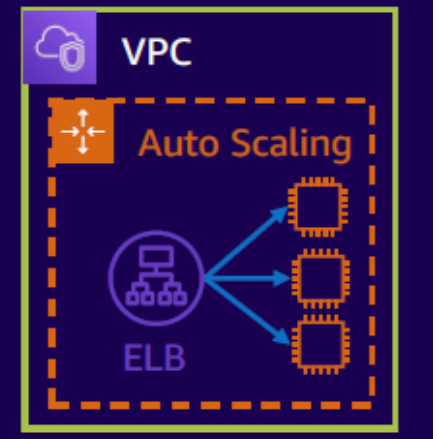
Elasticity



Control

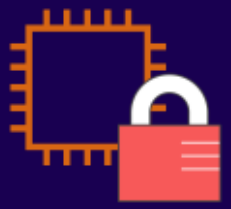


Flexibility



Integrated

Reliable



Secure

Inexpensive

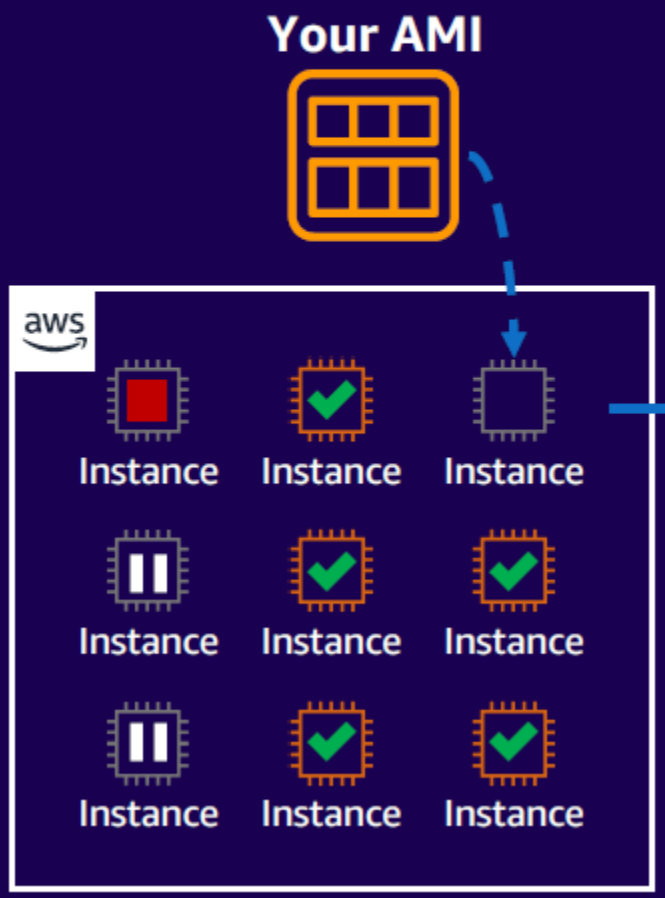
Simple

BCIT

Reference: AWSome Day, Michalynn J. Koziol (2024)

Amazon EC2

Amazon EC2 provides pay-as-you-go pricing and a broad selection of hardware and software that's available via the AWS Marketplace by using Amazon Machine Images (AMIs)



Template for
- Storage volumes
- Launch permissions
- A block device mapping

Examples
- ✓ Application server
- ✓ Web server
- ✓ Database server
- ✓ Game server
- ✓ Mail server
- ✓ Media server
- ✓ Catalog server
- ✓ File server

BCIT

Reference: AWSome Day, Michalynn J. Koziol (2024)

AWS Pricing Models

Free Tier

- Free
- Opportunity to try new services
- Suitable for trials and testing
- Easy to Set Up
- Impractical for production grade use

On-Demand

- No Commitment
- No Upfront Costs
- Highly Flexible
- Easy to Set Up
- Suitable for Short Term Projects
- Most Expensive Option

Spot Instance

- No Commitment
- No Upfront Costs
- Limited Flexibility
- Can be Terminated with little notice
- Suitable for Fault Tolerant Apps
- Cheapest Option

Reserved Instance

- 1 or 3 year Commitment
- Upfront Cost Option
- Limited Flexibility
- Suitable for Predictable apps
- Cheaper than On-Demand

Savings Plan

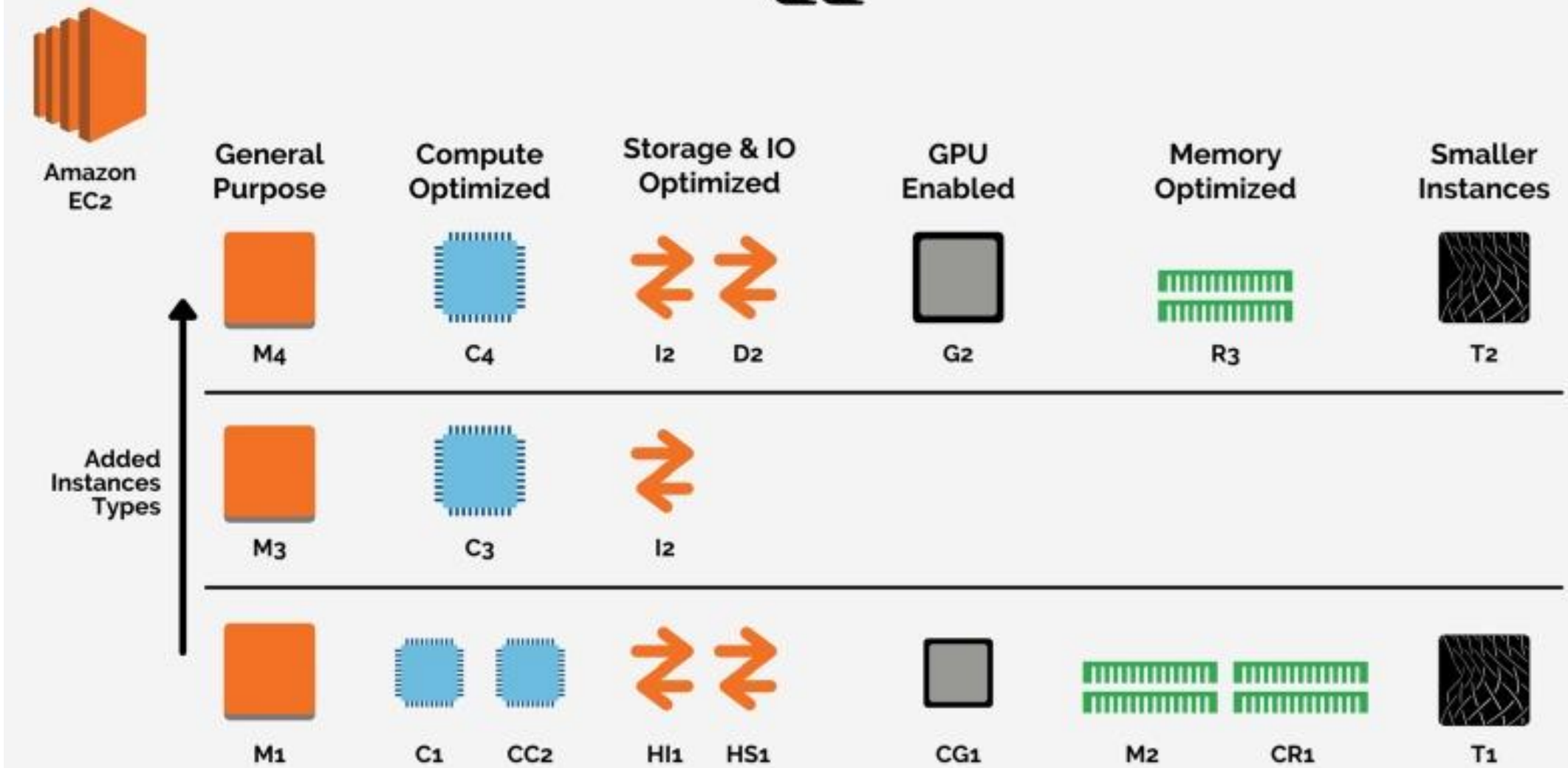
- 1 or 3 year Commitment
- Upfront Cost Option
- Flexible
- Predictable Costs
- Easy to work with
- Cheaper than On-Demand

https://zesty.co/blog/what-are-the-aws-pricing-models/

BCIT

Nand Kishore Ola

Amazon EC2: Instances Types



BCIT™

Amazon EC2 instance families and names

Choosing the correct type is very important for
efficient use of your instances and cost reduction

Instance family	Use cases
General purpose *e.g., A1, T3, T3a, T2, M6g, M5*	• Low-traffic websites and web applications • Small databases and midsize databases
Compute optimized *e.g., C5, C5n, C4, C7g*	• High-performance web servers • Video encoding
Memory optimized *e.g., R5, R5n, X1e, X1, z1d*	• High-performance databases • Distributed memory caches
Storage optimized *e.g., I3, I3en, D2, H1*	• Data warehousing • Log or data processing applications
Accelerated computing *e.g., P3, P2, Inf1, G4, G3, F1*	• 3D visualizations • Machine learning

BCIT

Reference: AWSome Day, Michalynn J. Koziol (2024)

Unmanaged services compared to managed services

Unmanaged

You manage scaling, fault tolerance, and availability

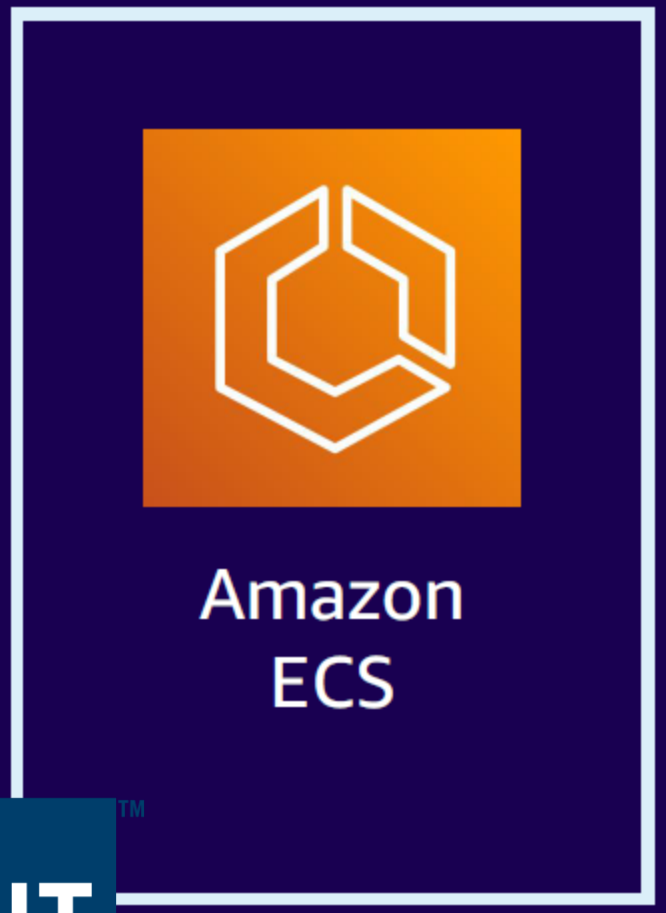
Managed

Scaling, fault tolerance, and availability are typically built in to the service

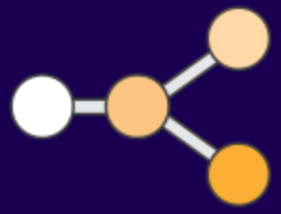
BCIT

Reference: AWSome Day, Michalynn J. Koziol (2024)

Amazon Elastic Container Service (Amazon ECS)



Orchestrates the execution of containers



Maintains and scales the fleet of nodes running your containers

Removes the complexity of standing up the infrastructure

BCIT

Reference: AWSome Day, Michalynn J. Koziol (2024)

What is Amazon EKS?

Amazon EKS

- Amazon EKS runs vanilla Kubernetes; EKS is an upstream and certified conformant version of Kubernetes (with backported security fixes)
- Amazon EKS supports 4 versions of Kubernetes, giving customers time to test and roll out upgrades
- Amazon EKS provides a managed Kubernetes experience for performant, reliable, and secure Kubernetes
- Amazon EKS makes Kubernetes operations, administration, and management simple

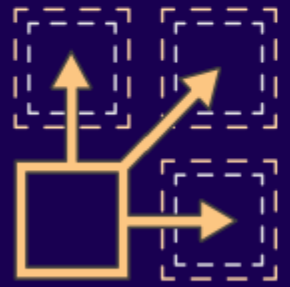
With Amazon EKS, you can build reliable, stable, and secure applications in any environment

BCIT

https://pages.awscloud.com/rs/112-TZM-766/images/SCMWQ1D1S2T2_Getting%20Started%20with%20Amazon%20EKS.pdf

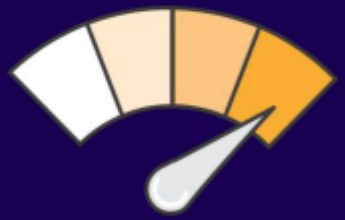
What is serverless computing?

Building and running applications and services without managing servers



No servers to provision or manage

Scales with usage



Never pay for idle

Availability and fault tolerance built in

BCIT

Reference: AWSome Day, Michalynn J. Koziol (2024)

Key Takeaways

- EC2 instances – Servers in the cloud!
  - Pay as you go pricing
  - Scale in/out as needed automatically
  - Different instance types (hardware) for your workloads
- Amazon ECS
  - Orchestration for your container deployments
- Serverless
  - You create the code, AWS manages the underlying compute
  - Lambda – On demand, per-request pricing to run code

BCIT™

Reference: AWSome Day, Michalynn J. Koziol (2024)

Spin Up Your (First) Amazon EC2 Instance in 10 Minutes

For this exercise, log into the AWS Management Console, navigate to the EC2 service & launch a new Ubuntu instance (e.g., Ubuntu Server AMI) with a t2.micro instance type.

Create a key pair for secure access and configure your security group to allow inbound traffic on port 22 for SSH.

Once the instance is running, use PuTTY (with the .ppk file associated with your key pair) to connect to the instance's public IP address as the "ubuntu" user. After successfully logging in, run **$ sudo apt-get update** to refresh package listings, and then install NGINX and cURL by running **$ sudo apt-get install -y nginx curl.**

BCIT™

Storage

BCIT™

AWS storage options

Amazon S3
Scalable, highly durable object storage in the cloud

AWS Storage Gateway
Hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage.

Amazon S3 Glacier
Low-cost, highly durable archive storage in the cloud

Amazon EBS
Network-attached volumes that provide durable block-level storage for Amazon EC2 instances

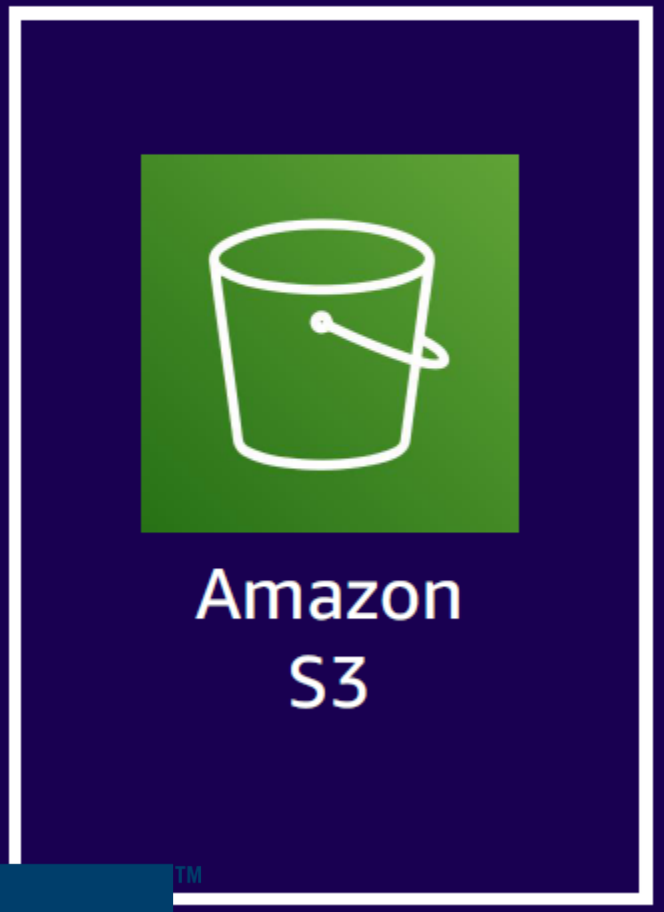
Amazon EFS
Scalable network file storage for Amazon EC2 instances

Amazon FSx
Fully managed, cost-effective file storage offering the capabilities and performance of popular commercial and open-source file systems

BCIT

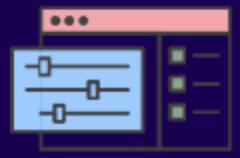
Reference: AWSome Day, Michalynn J. Koziol (2024)

Amazon S3



Object-level storage

Designed for 99.999999999% durability



Event triggers

Use cases

- Content storage and distribution
- Backup and archiving
- Big data analytics
- Disaster recovery
- Static website hosting

BCIT

Reference: AWSome Day, Michalynn J. Koziol (2024)

Simple Storage Service (S3)

- ✓ A bucket is a container for objects and describes location, logging, accounting, and access control. A bucket can hold any number of objects, which are files of up to 5TB. A bucket has a name that must be globally unique.

- ✓ Fundamental operations corresponding to HTTP actions:
  - http://bucket.s3.amazonaws.com/object
  - POST a new object or update an existing object.
  - GET an existing object from a bucket.
  - DELETE an object from the bucket
  - LIST keys present in a bucket, with a filter.

- ✓ A bucket has a flat directory structure.

BCIT™

File services use cases

Amazon EFS

- Simplify Development Operations (DevOps)
- Modernize application development
- Enhance content management systems
- Accelerate data science

Amazon FSx for Lustre

- Accelerate machine learning
- Enable high performance computing
- Unlock big data analytics
- Increase media workload agility

Amazon FSx for Windows

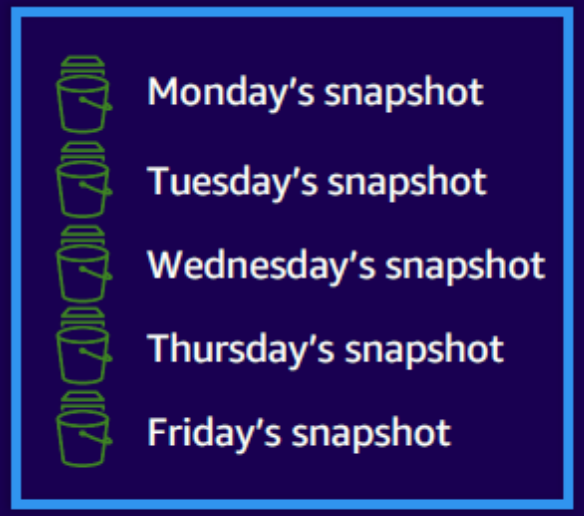
- Migrate Windows file servers to AWS
- Accelerate hybrid workloads
- Reduce Microsoft SQL Server deployment cost
- Simplify virtual desktops and streaming

BCIT

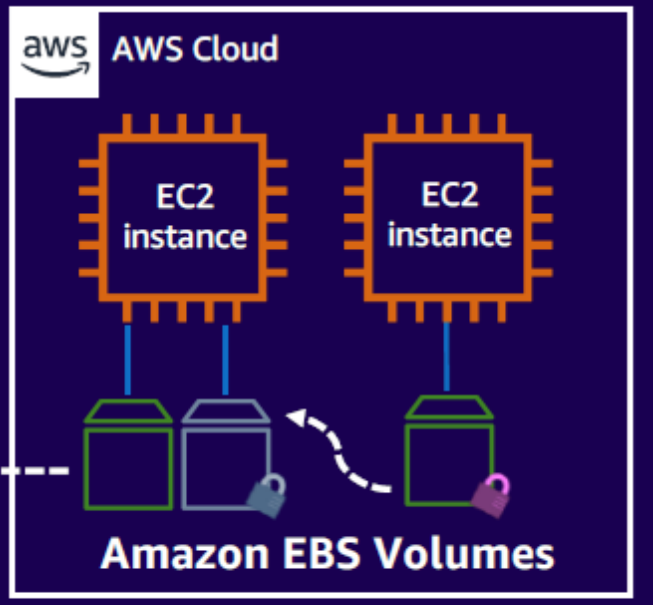
Reference: AWSome Day, Michalynn J. Koziol (2024)

Amazon Elastic Block Store (Amazon EBS)

- Persistent block storage for instances
- Protected through replication
- Different drive types
- Scale up or down in minutes
- Pay for only what you provision
- Snapshot functionality
- Encryption available



Create volume snapshots for backup and recovery



Detach and reattach volumes to other EC2 instances

Reference: AWSome Day, Michalynn J. Koziol (2024)

Elastic Block Store (EBS)

✓ An EBS volume is a virtual disk of a fixed size with a block read/write interface. It can be mounted as a file-system on a running EC2 instance where it can be updated incrementally. Unlike an instance store, an EBS volume is persistent.

✓ Compare to an S3 object, which is essentially a file that must be accessed in its entirety.

✓ **Fundamental operations:**

- CREATE a new volume (1GB-1TB)
- COPY a volume from an existing EBS volume or S3 object.
- MOUNT on one instance at a time.
- SNAPSHOT current state to an S3 object.

BCIT™

Key takeaways

AWS provides a variety of storage options

- Object (Amazon S3)
- File (Amazon EFS and Amazon FSx)
- Block storage (Amazon EBS)

- **Customers are using our storage services to build:**
  - Home directories
  - Data lakes
  - Modern and business-critical applications

BCIT™

Reference: AWSome Day, Michalynn J. Koziol (2024)

In this lab, you will use your Ubuntu EC2 instance (created previously) to interact with Amazon S3 by creating or identifying a new S3 bucket, configuring your instance to access S3, and uploading a file to confirm successful connectivity.

First, log in to the AWS Management Console, navigate to S3, click Create bucket, specify a unique name (e.g., my-lab-bucket-123), select a region, and complete setup. Next, on your EC2 instance, install the AWS CLI if not already installed (using sudo apt-get update && sudo apt-get install -y awscli), then either attach an IAM role via the EC2 console or run "**aws configure**" to enter your credentials.

Create a simple file on your instance (e.g., echo "Hello, S3 World!" > s3test.txt), then run aws s3 cp s3test.txt s3://my-lab-bucket-123/ to upload it & verify with aws s3 ls s3://my-lab-bucket-123/.

BCIT™

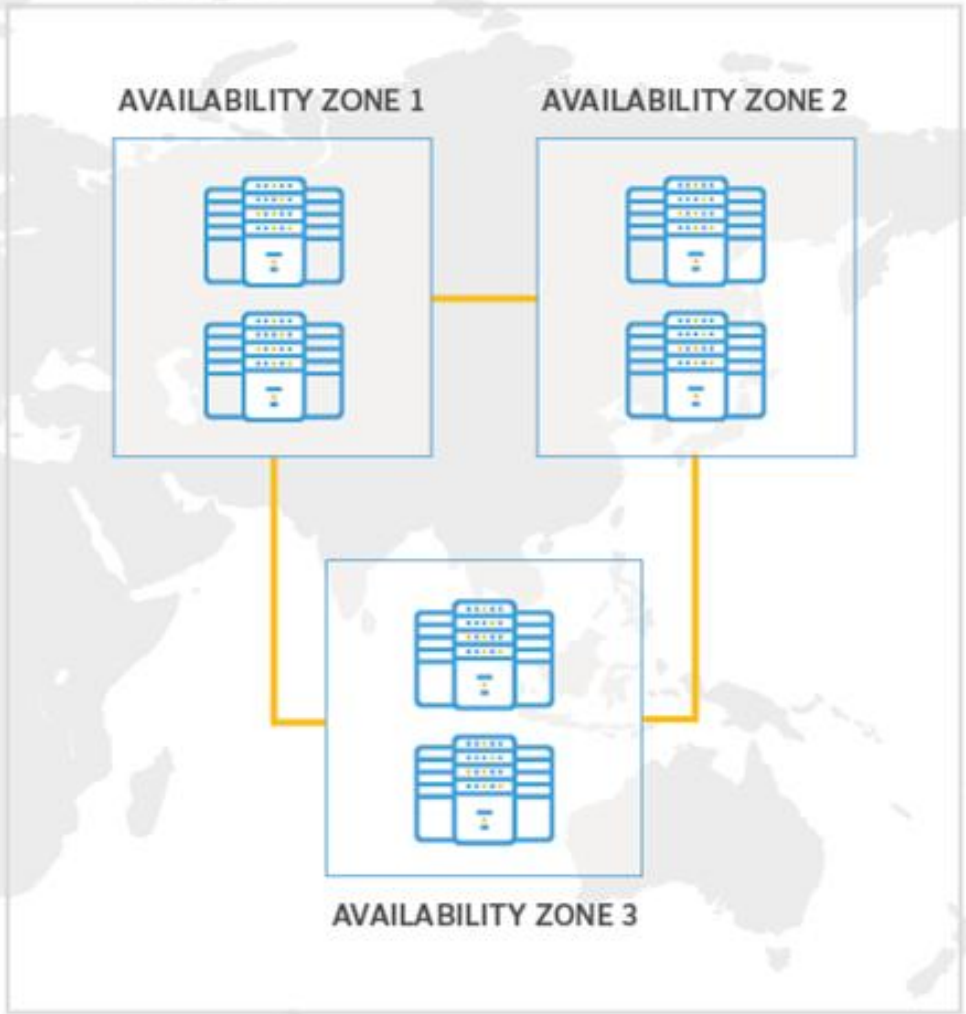
For extra confirmation, remove the local file (rm s3test.txt), download it back using aws s3 cp s3://my-lab-bucket-123/s3test.txt and view its contents (cat s3test.txt). Finally, to clean up, remove the file from the bucket (aws s3 rm s3://my-lab-bucket-123/s3test.txt) and optionally delete the entire bucket.

Networking

BCIT™

Availability zones vs. regions

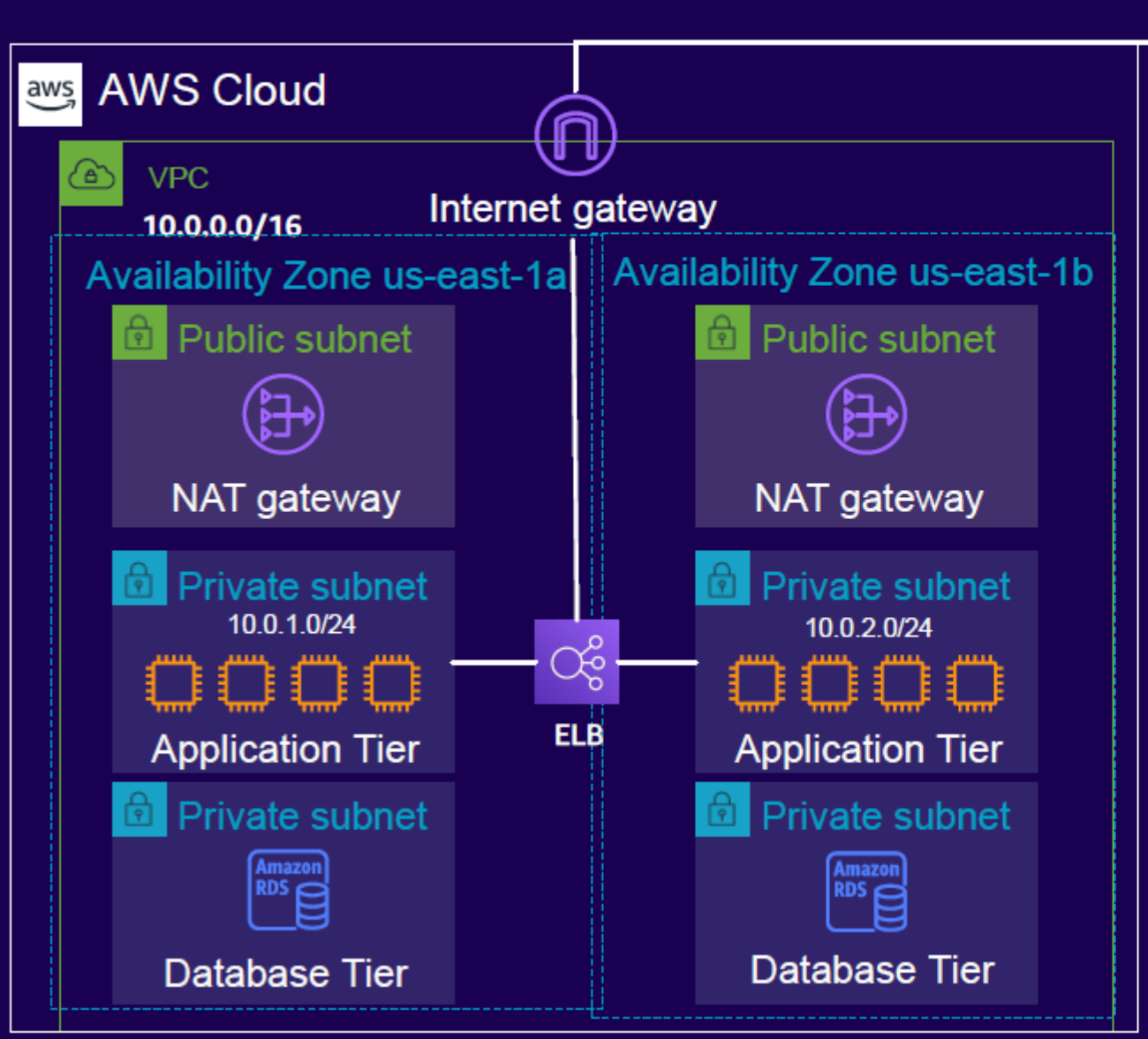
Region A



Region B

BCIT™

Amazon Virtual Private Cloud (Amazon VPC)



VPC: Your private network space in the AWS Cloud

Subnets: Provide network isolation for your workloads

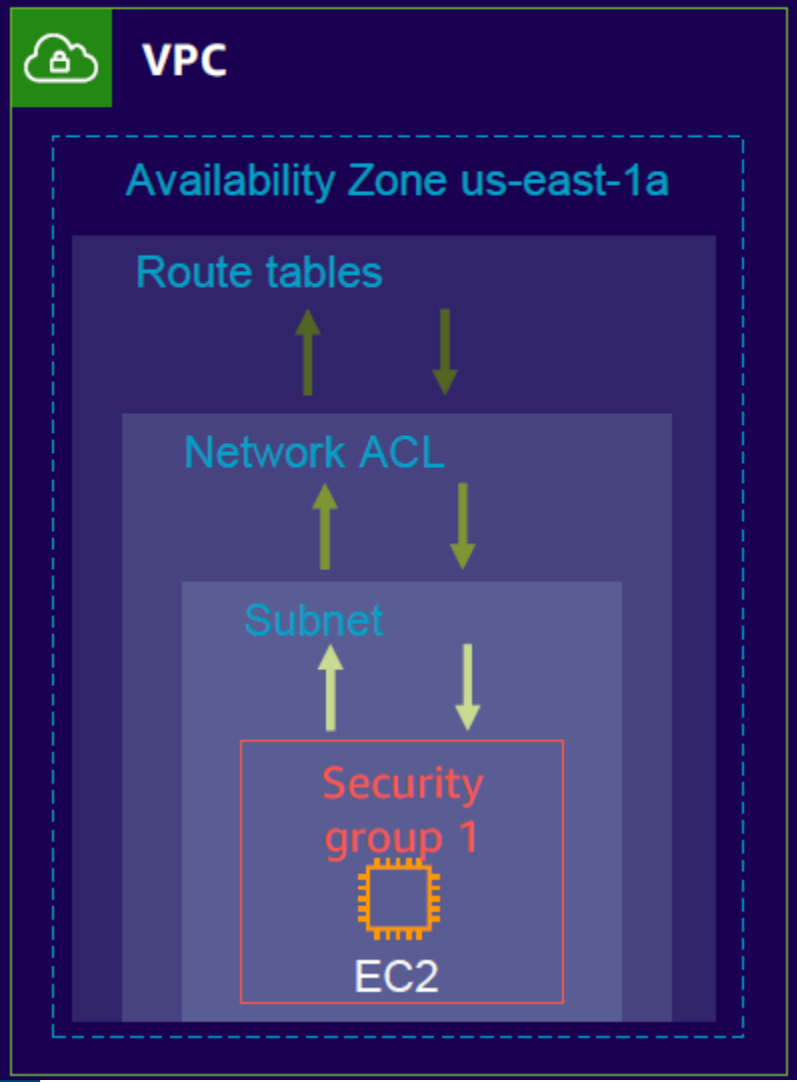
Public subnet: Directly accessible from the public internet

Private subnet: Not directly accessible from the public internet

ELB: Load balancer distributes incoming application network traffic

Reference: AWSome Day, Michalynn J. Koziol (2024)

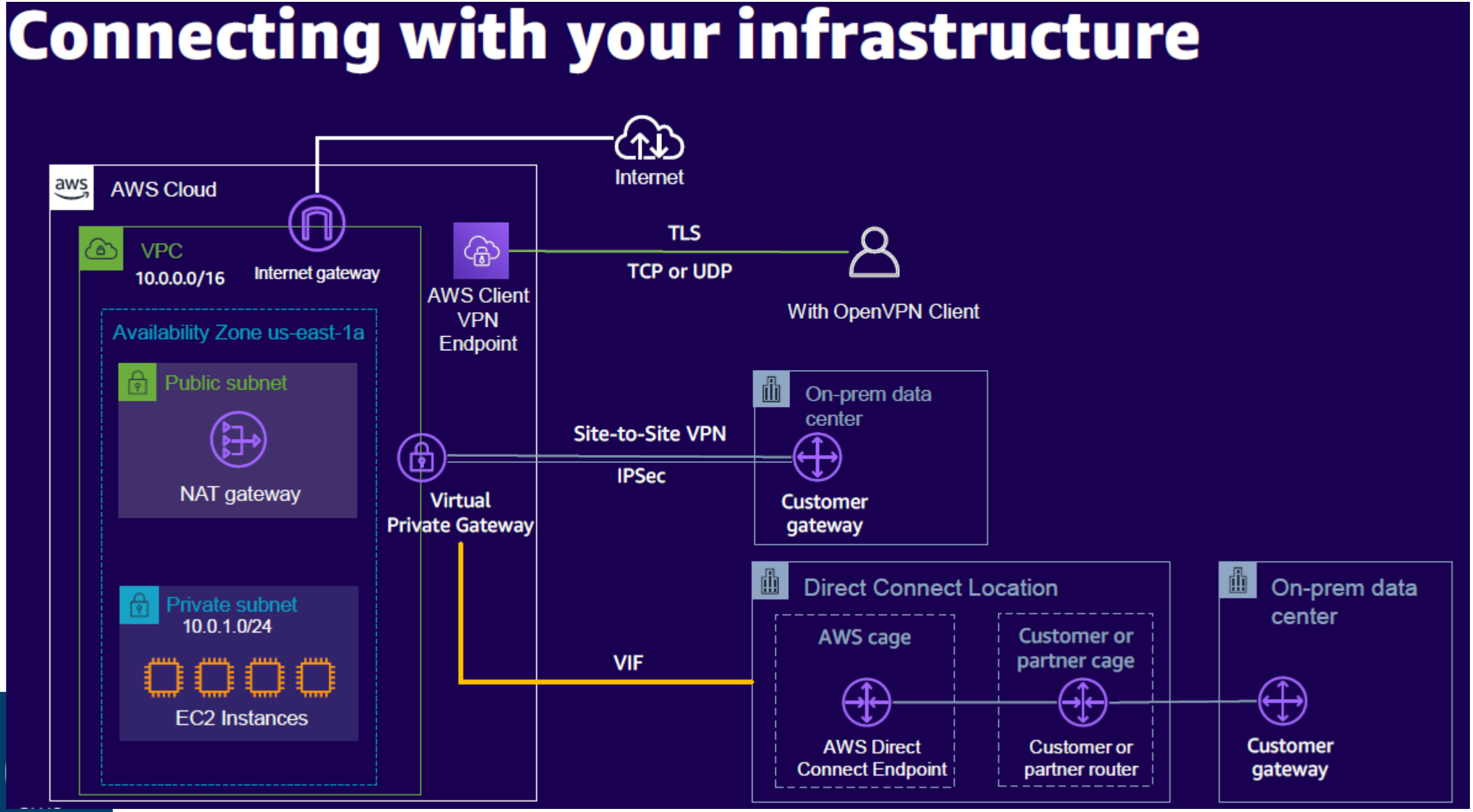
Securing your infrastructure



- **Route tables**
  - Contains a set of rules, called routes, that are used to determine where network traffic is directed
  - Routes tables can have association with VPC, gateways, and subnets
- **Network access control lists (network ACLs)**
  - Allow or deny traffic in and out of subnets
  - Hardens security as a secondary level of defense at the subnet level
- **Security groups**
  - Used to allow traffic to and from at the network interface (instance) level
  - Usually administered by application developers

Reference: AWSome Day, Michalynn J. Koziol (2024)

Connecting with your infrastructure



Reference: AWSome Day, Michalynn J. Koziol (2024)

Key Takeaways

Amazon VPC provides:

- Logically isolated network to launch applications
- Security Groups, network ACLs and route tables to secure your deployments

There are three main ways customers connect to AWS:

- Client VPN
- Site-to-site VPN
- Direct Connect

Reference: AWSome Day, Michalynn J. Koziol (2024)

Security

BCIT™

AWS security, identity, and compliance solutions

Identity & access management

AWS Identity & Access Management (IAM)

AWS Single Sign-On

AWS Organizations

AWS Directory Service

Amazon Cognito

AWS Resource Access Manager

Detection

AWS Security Hub

Amazon GuardDuty

Amazon Inspector

Amazon CloudWatch

AWS Config

AWS CloudTrail

VPC Flow Logs

Infrastructure protection

AWS Firewall Manager

AWS Shield

AWS WAF – Web application firewall

Amazon Virtual Private Cloud (VPC)

AWS PrivateLink

AWS Systems Manager

Data protection

Amazon Macie

AWS Key Management Service (KMS)

AWS CloudHSM

AWS Certificate Manager

AWS Secrets Manager

AWS VPN

Server-Side Encryption

Incident response

Amazon Detective

CloudEndure DR

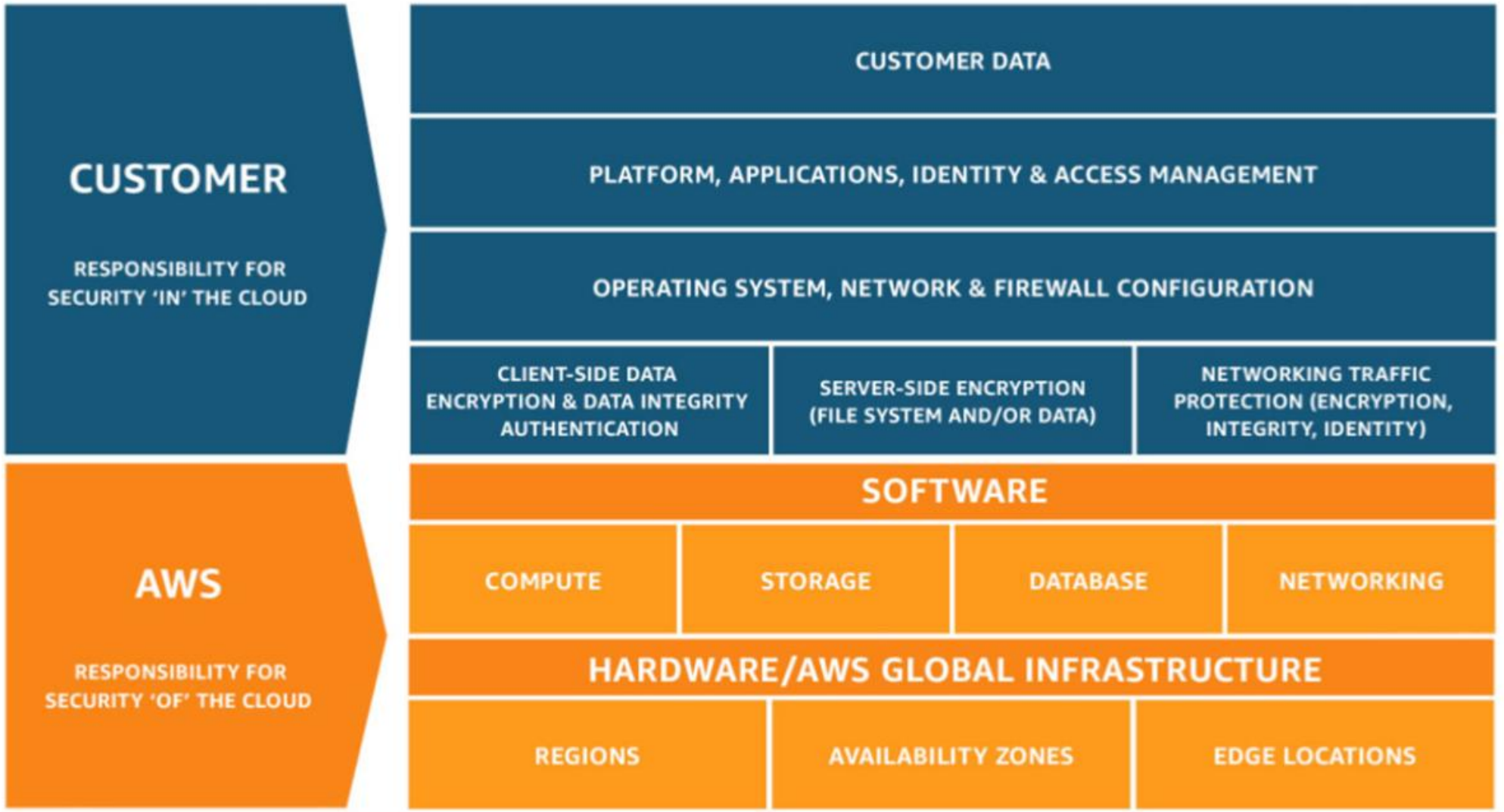
AWS Config Rules

AWS Lambda

BCIT

https://allcloud.io/blog/aws-security-panel-summary/

UNDERSTANDING AWS SHARED RESPONSIBILITY MODEL



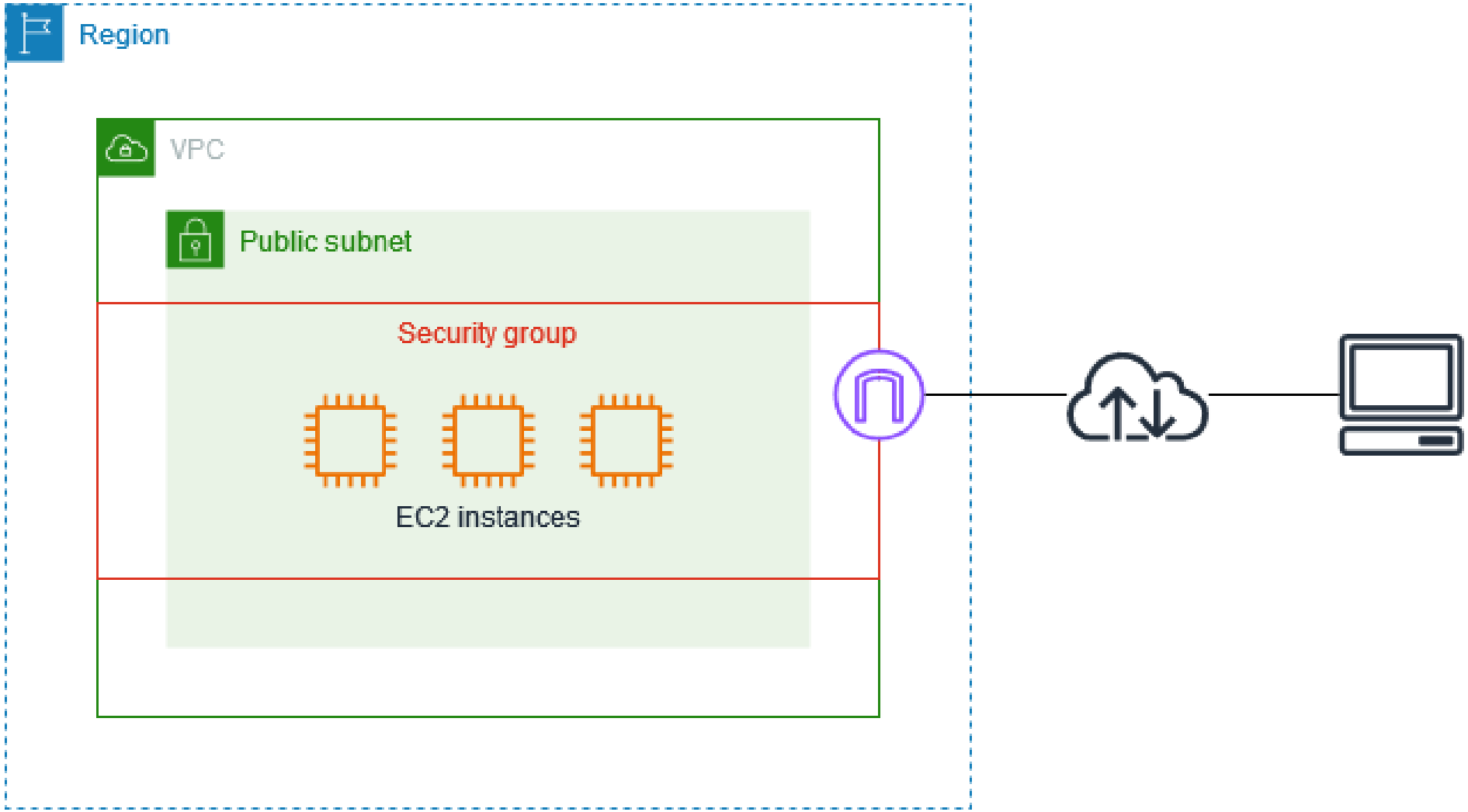
BCIT™

https://allcloud.io/blog/aws-security-panel-summary/


Nand Kishore Ola
AWS EC2 Instance
AWS SECURITY GROUPS
ALLOWED PORTS & IP ADDRESSES
DENIED PORTS & IP ADDRESSES

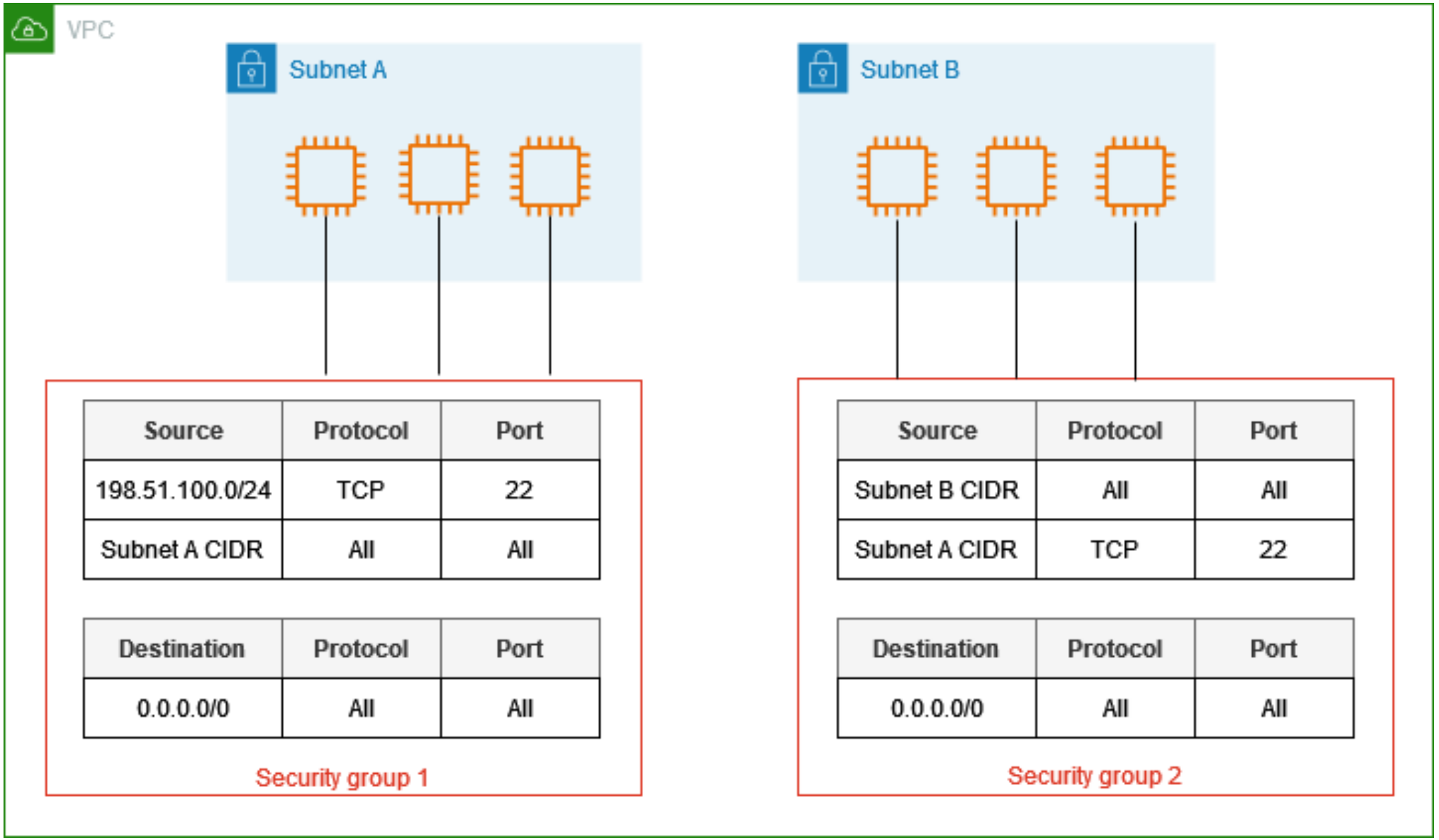
BCIT™

AWS Security Groups



BCIT™

AWS Security Groups



BCIT™

AWS Identity and Access Management (IAM)

Securely control access to your AWS resources

- Assign granular permissions to users, groups, or roles
- Share temporary access to your AWS account
- Federate users in your corporate network or with an internet identity provider

BCIT

IAM components

Create

Users
A person or application that interacts with AWS

Groups
Collection of users with identical permissions

Roles
Temporary privileges that an entity can assume

Permissions

Policies

IAM

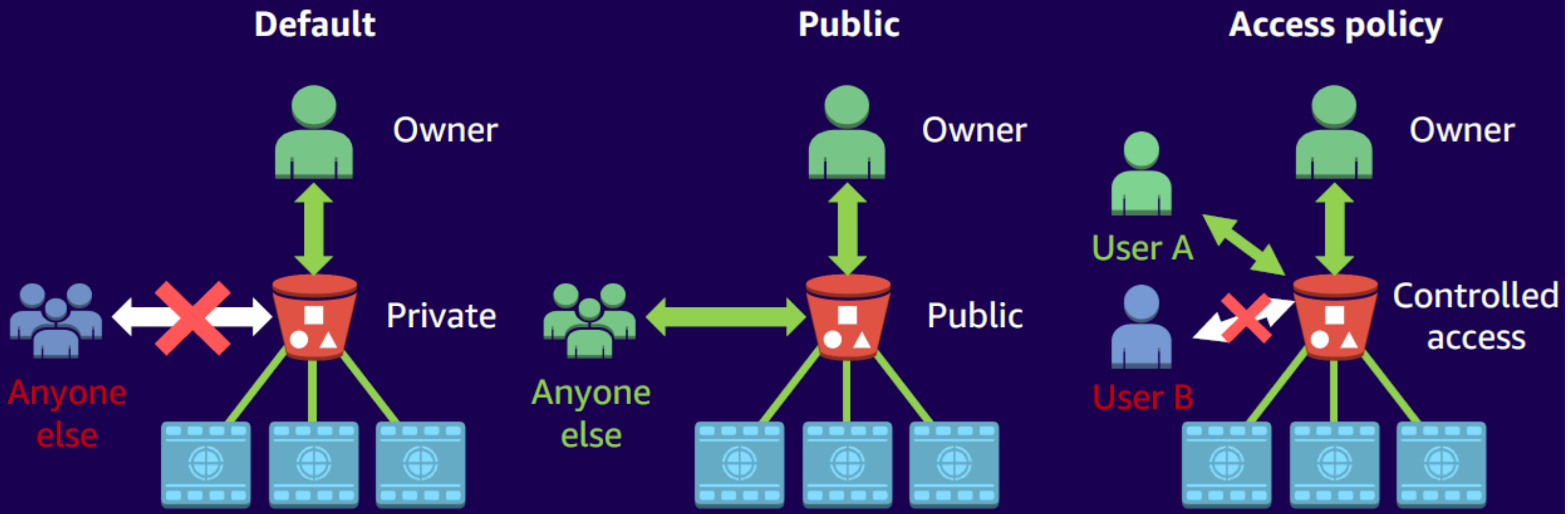
Defines permissions to control which AWS resources users can access

Helps you to meet identity and access control standards

- Authentication
- Authorization

Amazon S3 access control: General

Some services support resource-based policies, such as S3 bucket policies



For this lab, first log in to AWS, open the VPC console, and note how the default VPC is configured with one or more subnets; confirm that your instance is in one of these subnets.

Next, go to the EC2 console, select your instance, and under Security, locate and edit the inbound rules of its Security Group: remove “0.0.0.0/0” if present for HTTP, and replace it with your public IP address in CIDR notation (e.g., 203.0.113.4/32). To get your public IP address visit https://ifconfig.me/ or https://ipinfo.io

Then, via SSH or EC2 Instance Connect, modify the default NGINX page (usually at /var/www/html/index.nginx-debian.html) by inserting a unique message (e.g., “Welcome to My Custom NGINX!”) to differentiate from the default. Finally, test connectivity by opening your instance’s public IP in your browser from your own machine; you should see your custom message, but anyone else not using your IP address will be blocked, demonstrating the restricted access.

BCIT™

Lecture #6 Summary

1. Explaining the necessity of using Public Cloud services such as Amazon Web Service (AWS).
1. Describing the key terminologies to deploy VMs (instances) in AWS.
1. Understanding security model and measures introduced by the AWS.
1. Explaining the storage options provided by the AWS to the users
1. Grasping Virtual Private Cloud (VPC) concept and its applications in public cloud.
1. Finding out how to define a Security Group to manage access to instances.

BCIT™

End of Lecture #6

THANK

Y☺U

- Dawood Sajjadi

BCIT™