AWS Cloud Practitioner Essentials

MODULE 1

Cloud Computing Models:

- Cloud-Based
- On-Premises (private)
- Hybrid

Cloud Computing Implementations:

- IaaS
- PaaS
- SaaS

Benefits of Cloud Computing:

- Trade upfront expense: you only pay for computing resources you consume.
- Stop spending money to run and maintain data centers
- Stop guessing capacity
- Massive economies of scale
- Increase speed and agility
- Go global

MODULE 2

Amazon Elastic Compute Cloud (Amazon EC2):

- Instance in which you can use a virtual server to run applications in the AWS Cloud. If you have applications that you want to run in Amazon EC2, you must do the following:
  - Provision instances (virtual servers).
  - Upload your code.
  - Continue to manage the instances while your application is running.

EC2 Instance Types

General Purpose

Balance of compute, memory and networking resources (application, gaming, backend servers for enterprise applications or small and medium db)

Compute Optimized

Ideal for high-performance. For example, batch processing workload.

Memory Optimized

Ideal for high-performance database or workload that involves performing real-time processing of a large amount of unstructured data. For example, you have a workload that requires large amounts of data to be preloaded before running an application.

Accelerated Computing

Use hardware accelerators or coprocessors to perform function more efficiently than is possible in software running of CPUs (floating-point number calculations, graphics processing and data pattern matching).

Storage Optimized

Ideal for delivering tens of thousands of low-latency, random IOPS to applications (input/output operations per second).

EC2 Pricing

On-Demand

Ideal for short-term, irregular workloads that cannot be interrupted (developing and testing applications and running applications that have unpredictable usage patterns). On-Demand instances are not recommended for workloads that last a year or longer (only pay for the duration that your instance runs for per hour or per second - it usually when you get started).

Savings Plans

Enable you to reduce your compute costs by committing you to a consistent amount of compute usage for a 1-year or 3-year term. This term commitment results in savings of up to 72% over On-Demand costs.

Reserved Instances

You can purchase Standard Reserved and Convertible Reserved Instances for a 1-year or 3-year term and Scheduled Reserved Instances for a 1-year term (predictable usage).
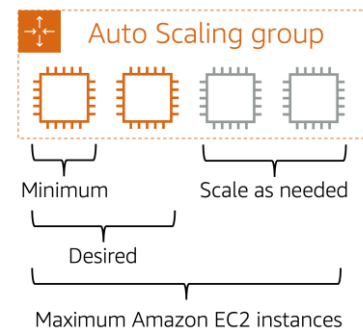
Spot Instances

Ideal for workloads with flexible start and end times or that can withstand interruptions. Spot Instances use unused Amazon EC2 computing capacity and offer you cost saving at up to 90% off of On-Demand prices. Unlike Savings Plans, Spot Instances do not require contracts or a commitment to a consistent amount of compute usage (Amazon can need your instance and give you two minutes for closing your instance).

Dedicated Hosts

DHs are physical servers with Amazon EC2 instance capacity that is fully dedicated to your use (On-Demand Dedicated Hosts and Dedicated Hosts Reservations).

Scaling Amazon EC2

- Involves beginning with ony the resources you need and designing your architecture to automatically respond to changing demand by scaling out or in. As a result, you pay for only the resources you use. You don't have to worry about a lack of computing capacity to meet your customers' needs.
- <u>Amazon EC2 Auto Scaling:</u>
  - Auto Scaling enables you to automatically add or remove Amazon EC2 instances in response to changing application demand.
    - <u>Dynamic</u>: responds to changing demand.
    - <u>Predictive</u>: automatically schedules the right number of Amazon EC2 instances based on predicted demand.

Elastic Load Balancing

- Elastic Load Balancing is the AWS service that automatically distributes incoming application traffic across multiple resources such as Amazon EC2 instances (traffic routes to the load balancer first and then the requests spread across multiple resources that will handle them).
- A load balancer acts as a single point of contact for all incoming web traffic to your Auto Scaling group.
- Although Elastic Load Balancing and Auto Scaling are separate services, they work together to help ensure that applications running in Amazon EC2 can provide high performance and availability.

Messaging and Queuing

Monolithic Application: the components (servers, db, user interface and business logic) communicate with each other to transmit data, fulfill requests and keep the application running.
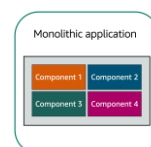
Microservices: you can take a microservices approach with services and components that fulfill different functions. Two services facilitate application integrations: Amazon Simple Notification Service (Amazon SNS) and Amazon Simple Queue Service (Amazon SQS).
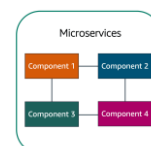
Simple Notification Service

SNS is a publish/subscribe service (publisher messages to subscribers). In Amazon SNS, subscribers can be web servers, email addresses, AWS Lambda functions or several other options.

Simple Queue Service

SQS you can send, store and receive messages between software components, without losing messages or requiring other services to be available.

Serverless Computing

You cannot see or access the underlying infrastructure or instances that are hosting your application. Your code runs on servers but you don't need to provision or manage these servers. Another benefit of serverless computing is the flexibility to scale serverless applications automatically (throughput and memory).

AWS Lambda

AWS Lambda is a service that lets you run code without needing to provision or manage servers. For example, a simple Lambda function might involve automatically resizing uploaded images to the AWS Cloud. In this case, the function triggers when uploading a new image.
- Host short running functions.
- Service-oriented applications.
- Event driven applications.
- No provisioning or managing servers.

Containers

Containers provide you with a standard way to package your application's code and dependencies into a single object (a package for your code).

Amazon Elastic Container Service (Amazon ECS)

ECS is a highly scalable, high-performance container management system that enables you to run and scale containerized applications on AWS.

Docker

Docker is a software platform that enables you to build, test and deploy applications quickly. With Amazon ECS you can use API calls to launch and stop Docker-enabled applications.

Amazon Elastic Kubernetes Service (Amazon EKS)

EKS is a fully managed service that you can use to run Kubernetes on AWS.

Kubernetes

Kubernetes is open-source software that enables you to deploy and manage containerized applications at scale.

AWS Fargate

Serverless environment managed for you (without Amazon EC2 instance). AWS Fargate manages your server infrastructure for you. It works with both Amazon ECS and Amazon EKS.

MODULE 3

AWS Global Infrastructure

Regions

A geographical area that contains AWS resources. A region consists of two or more AZ.

Factors

When determining the right Region four your services, data and applications, consider the following four business factor:
- Compliance: data governance and legal requirements. You might need to run your data out of specific areas.
- Proximity: selecting a region is close to your customers will help you to get content to them faster.
  - Latency: the time it takes for data to be sent and received.
- Availability: making new services available around the world sometimes requires AWS to build out physical hardware one Region at a time (Amazon Braket - Quantum Computing Platform).
- Pricing: cost of services vary from Region to Region.

Availability Zones

AZ is one or more discrete data centers with redundant power, networking and connectivity. AZ is a single data center or a group of data centers within a Region. You should run across at least two AZ in a Region.
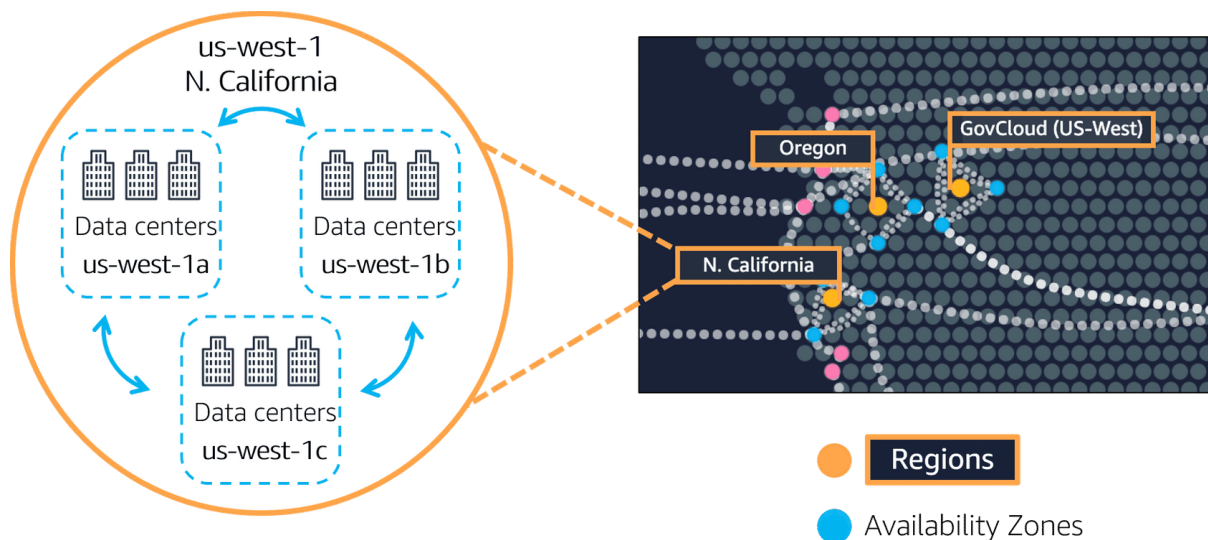
Edge locations

An edge location is a site that **Amazon CloudFront** uses to store cached copies of your content closer to your customers for faster delivery.
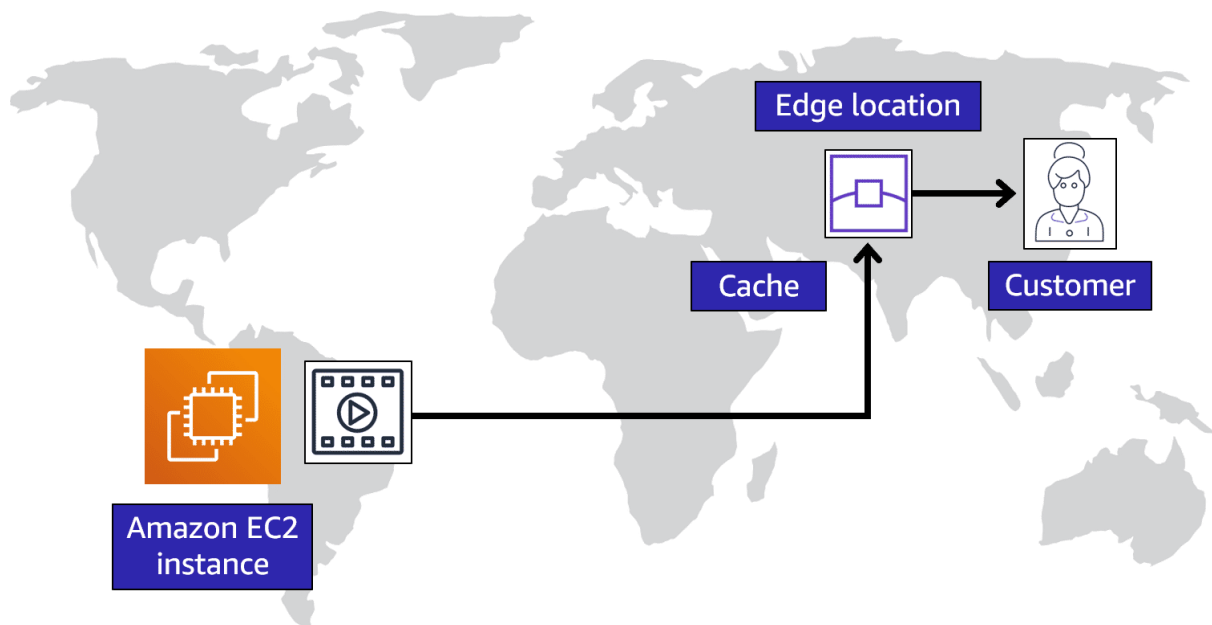
AWS CloudFront

Amazon CloudFront is a content delivery service (CDN). It uses a network of edge locations to cache content and deliver content to customers all over the world.

AWS Outposts

AWS Outposts is a fully managed service that offers the same AWS Infrastructure, AWS Services, APIs and tools to virtually any datacenter, co-location space or on-premises facility for a truly consistent hybrid experience. It is ideal for workloads that require low latency access to on-premises systems, local data processing, data residency and migration of applications with local system interdependencies.

AWS Resources

AWS Management Console

AWS Management Console is a web-based interface for accessing and managing AWS services. The console includes wizards and automated workflows that can simplify the process of completing tasks. You can also use the AWS Console mobile application to perform tasks such as monitoring resources, viewing alarms and accessing billing information.

- Test environments
- View AWS bills
- View monitoring
- Work with non-technical resources

AWS Command Line Interface (CLI)

- Make API calls using the terminal on your machine.
- By using AWS CLI, you can automate the actions that your services and applications perform through scripts. For example, you can use commands to launch an Amazon

EC2 instance, connect an Amazon EC2 instance to a specific Auto Scaling group and more.

AWS Software Development Kits (SDKs)

- Interact with AWS resources through various programming languages.
- Supported programming languages include C++, Java, .NET and more.

AWS Elastic Beanstalk

AWS Elastic Beanstalk provides code and configuration settings and it deploys the resources necessary to perform the following tasks:
- Adjust capacity
- Load balancing
- Automatic scaling
- Application health monitoring

AWS CloudFormation

You can build an environment by writing lines of code instead of using the AWS Management Console to individually provision resources. It enables you to build infrastructure and applications without having to perform manual actions or write custom scripts.
- Storage
- Database
- Analytics
- Machine Learning

MODULE 4

Amazon Virtual Private Cloud (Amazon VPC)

VPC is a networking service that you can use to establish boundaries around your AWS resources.
Amazon VPC enables you to provision an isolated section of the AWS Cloud.

Subnet

Subnet is a section of a VPC that can contain resources such as Amazon EC2 instances. Subnets can be public or private.
- Public subnets: online store's website.
- Private subnets: in a VPC, subnets can communicate with each other. For example, you might have an application that involves Amazon EC2 instances in a public subnet communicating with databases that are located in a private subnet.
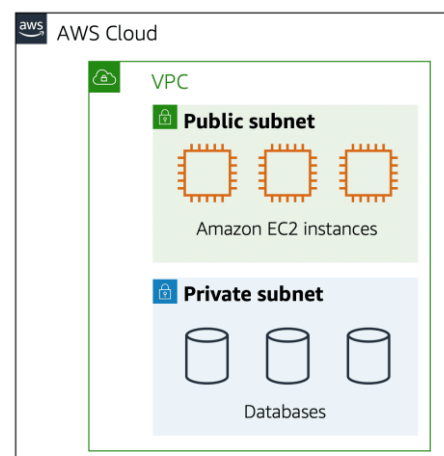
Internal Gateway

To allow public traffic from the internet to access your VPC, you attach an internet gateway to the VPC (connections between a VPC and the internet).
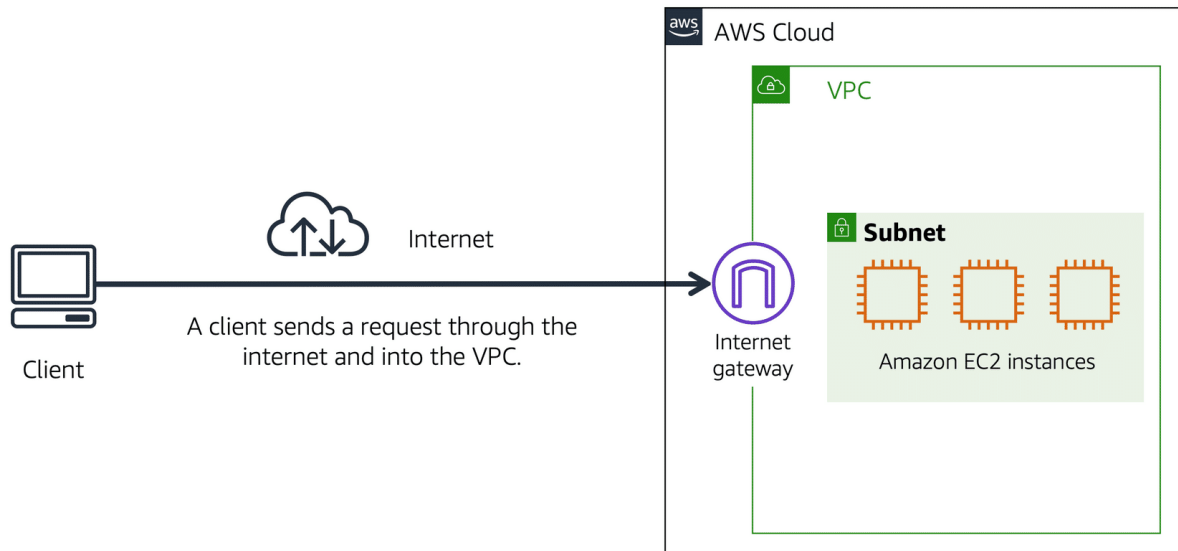

Virtual Private Gateway

The virtual private gateway is the component that allows protected internet traffic to enter into the VPC. A virtual private gateway enables you to establish a VPN connection between your VPC and private network, such as an on-premises data center or internal corporate network. A virtual private gateway allows traffic into the VPC only if it is coming from an approved network.
This connection is private and encrypted, it travels through the public internet, not through a dedicated connection.
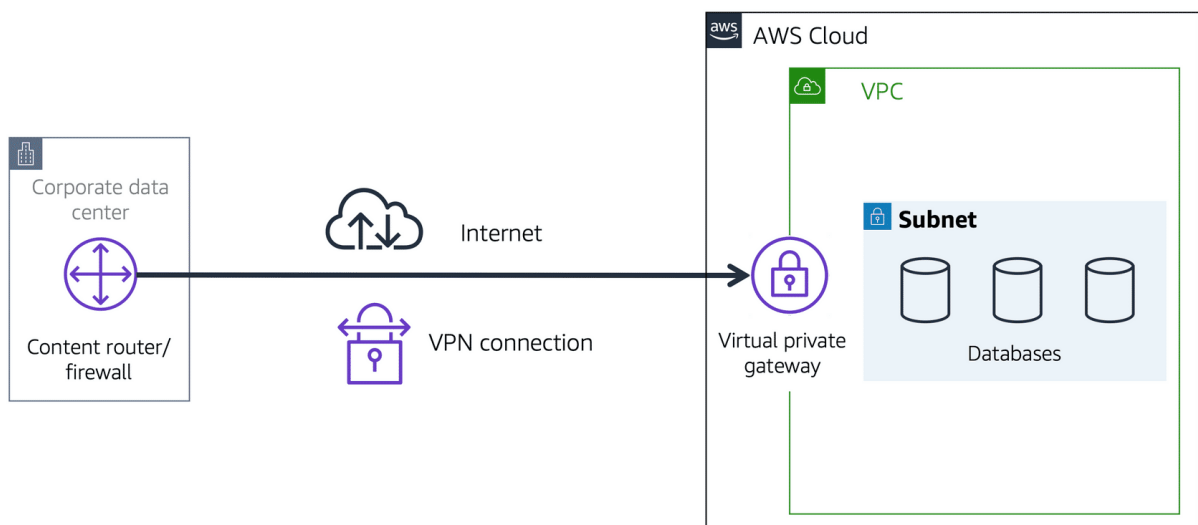
AWS Direct Connect

AWS Direct Connect is a service that enables you to establish a dedicated private connection between your data center and a VPC. The private connection that AWS Direct Connect provides helps you to reduce network costs and increase the amount of bandwidth that can travel through your network.
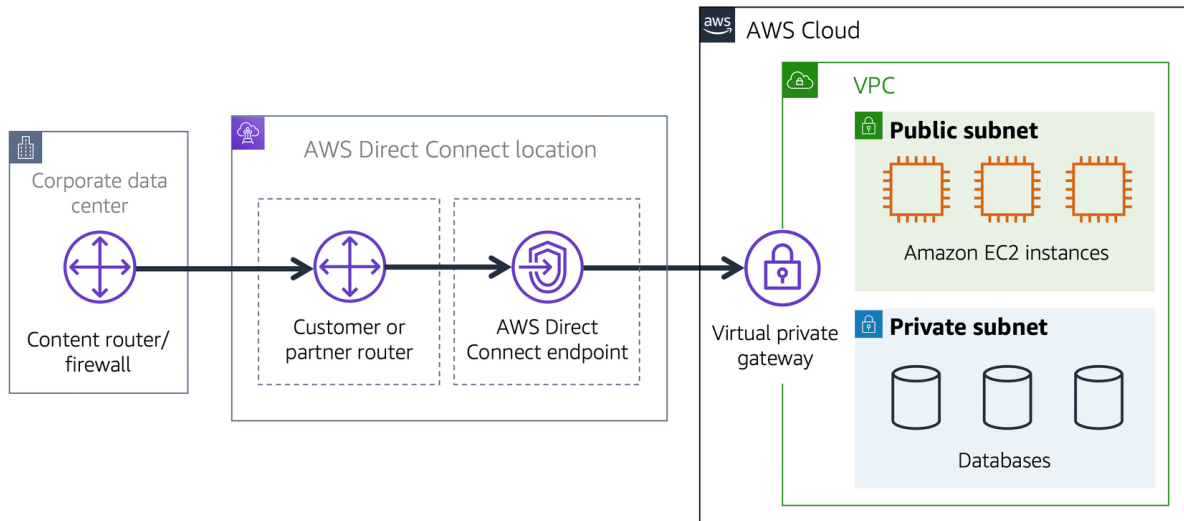
## Network traffic in a VPC

The VPC component that checks packet permissions for subnets is a network access control list (ACL).

Network access control lists (ACLs)

A network access control list (ACL) is a virtual firewall that controls inbound and outbound traffic at the subnet level.
By default, your account's default network ACL allows all inbound and outbound traffic, but you can modify it by adding your own rules. **For custom network ACLs, all inbound and outbound traffic is denied** until you add rules to specify which traffic to allow. Additionally, all network ACLs have an explicit deny rule.
Network ACLs perform stateless packet filtering.
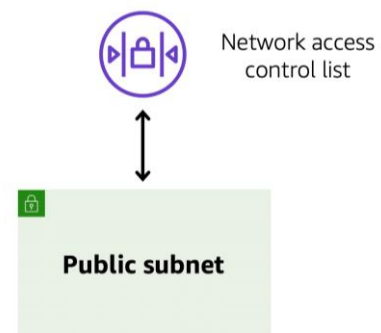
Security Group

A Security Group is a virtual firewall that controls inbound and outbound traffic for an Amazon EC2 instance. **By default, a security group denies all inbound traffic and allows all outbound traffic.** You can add custom rules to configure which traffic to allow or deny. If you have multiple Amazon EC2 instances within a subnet, **you can associate them with the same security group or use different security groups for each instance.**

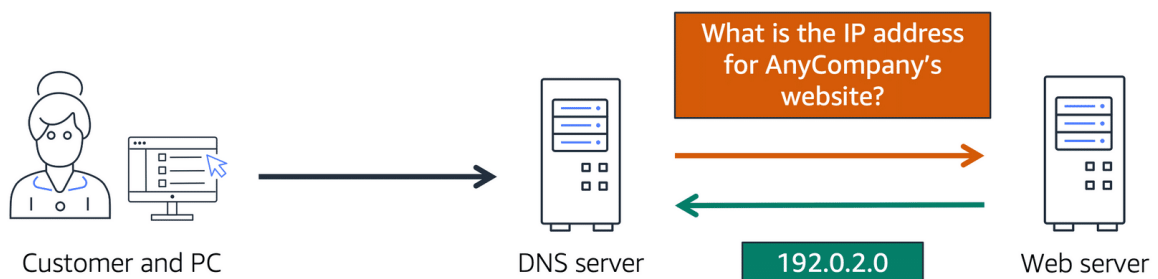**Security groups perform stateful packet filtering. They remember previous decisions made for incoming packets.**
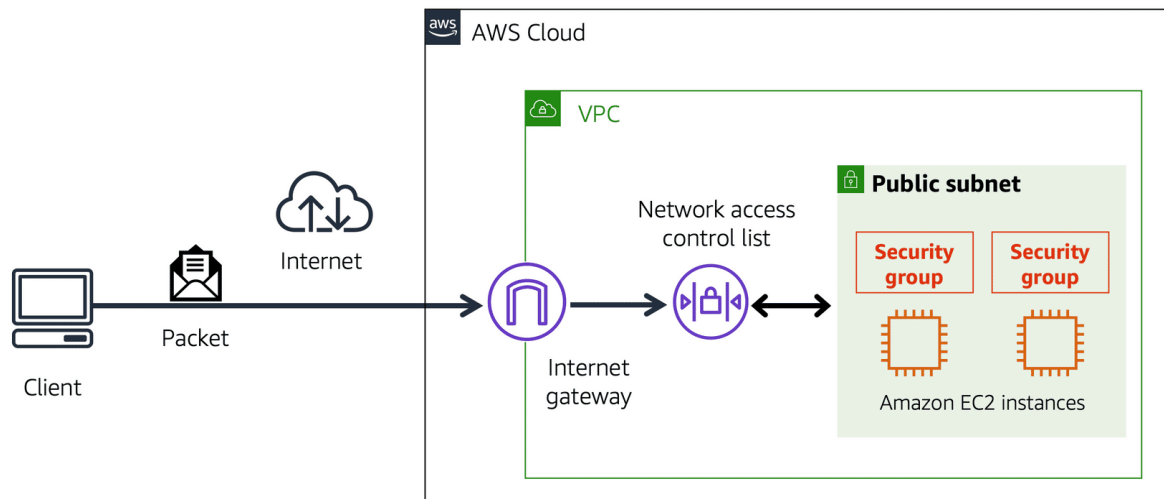
Global networking

Domain Name System (DNS)

DNS resolution involves a DNS server communicating with a web server.

Amazon Route 53

Amazon Route 53 is a DNS web service. It gives developers and businesses a reliable way to route end users to internet applications hosted in AWS. It can route users to infrastructure outside of AWS.
Another feature of Route 53 is the ability to manage the DNS records for domain names. You can register new domain names directly in Route 53. You can also transfer DNS records for existing domain names managed by other domain registrars.
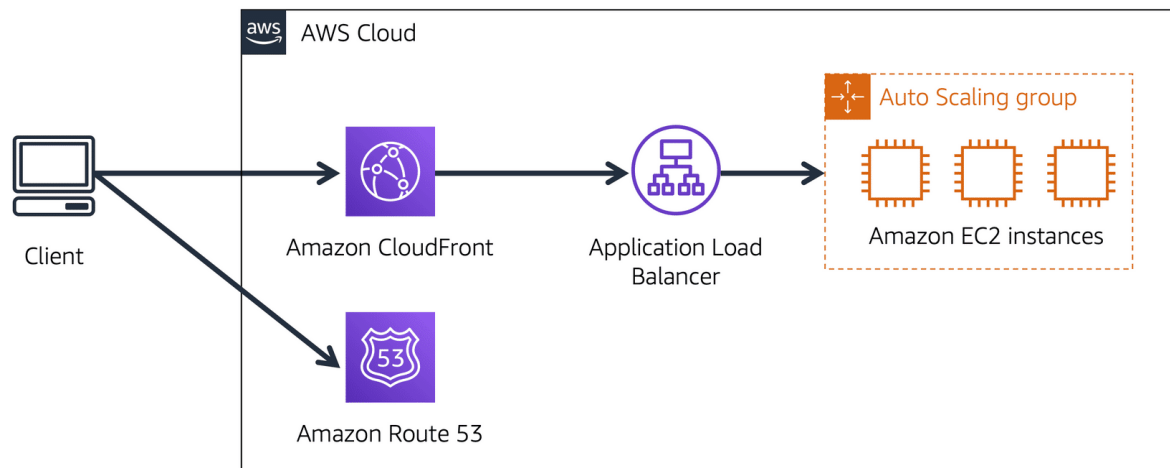
1. A customer requests data from the application by going to example.com
2. Amazon Route 53 uses DNS resolution to identify example.com corresponding IP address 192.0.2.0. This information is sent back to the customer.
3. The customer's request is sent to the nearest edge location through Amazon CloudFront.
4. Amazon CloudFront connects to the Application Load Balancer which sends the incoming packet to an Amazon EC2 instance.

MODULE 5

Instance Stores

Block-level storage volumes behave like physical hard drives. An instance store provides temporary block-level storage for an Amazon EC2 instance. When the instance is terminated, you lose any data in the instance store.
All data on the attached instance store is deleted when the Amazon EC2 instance is stopped.
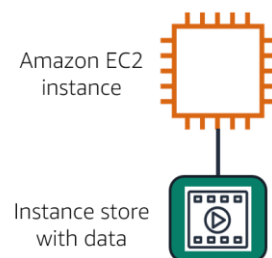
Amazon Elastic Block Store (Amazon EBS)

Amazon EBS is a service that provides block-level storage volumes that you can use with Amazon EC2 instances. **If you stop or terminate an Amazon EC2 instance, all the data on the attached EBS volume remains available.**
To create an EBS volume, you define the configuration (such as volume size and type) and provision it. After you create an EBS volume, it can attach to an Amazon EC2 instance.
Because EBS volumes are for data that needs to persist, it's important to back up the data. You can take incremental backups of EBS volumes by creating Amazon EBS snapshots.
EBS volumes store data within a single Availability Zone. Amazon EFS file systems store data across multiple Availability Zones.

An EBS snapshot is an incremental backup. This means that the first backup taken of a volume copies all the data. For subsequent backups, only the blocks of data that have changed since the most recent snapshot are saved.

EBS snapshots

EBS volume (Source data)

Day 1 — All data is backed up.

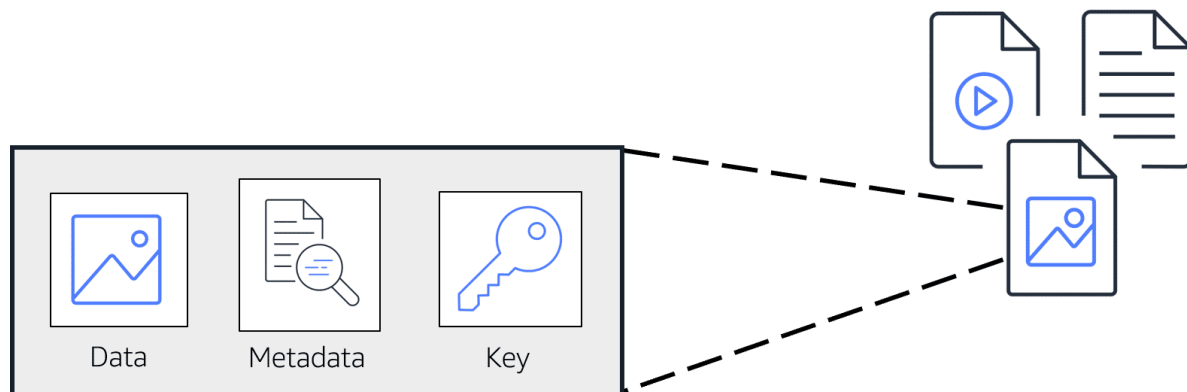**Day 2** — Only data that has changed since the most recent snapshot is backed up.

Day 3

In object storage, each object consists of data (image, video, text or any type of file), metadata (size, information and so on) and a key (unique identifier).

Data   Metadata   Key
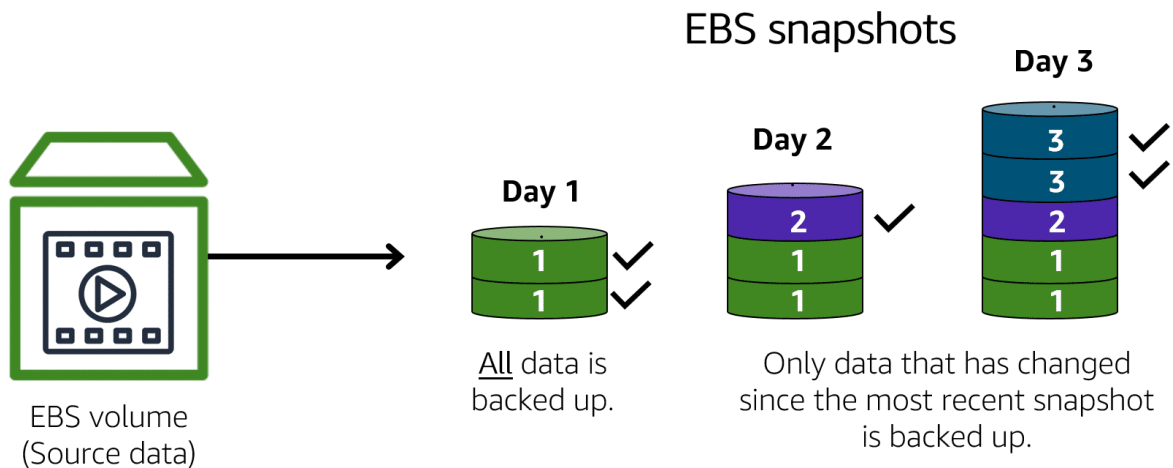
Amazon Simple Storage Service (Amazon S3) is a service that provides object-level storage. Amazon S3 stores data as objects in buckets. The maximum file size for an object in Amazon S3 is 5 TB.

When you upload a file to Amazon S3, you can set permissions to control visibility and access to it. You can also use the Amazon S3 versioning feature to track changes to your objects over time.

When selecting an Amazon S3 storage class consider these two factors:
- How often you plan to retrieve your data
- How available you need your data to be

- Designed for frequently accessed data

- Stores data in a minimum of three Availability Zones
- S3 Standard has a higher cost than other storage classes intended for infrequently accessed data and archival storage.
- It stores data in an object storage service.
- Examples: websites, content distribution and data analytics.

S3 Standard-Infrequent Access (S3 Standard-IA)

- Ideal for infrequently accessed data
- Similar to S3 Standard but has a lower storage price and higher retrieval price.
- It stores data in a minimum of three Availability Zones (idem S3 Standard) and same level of availability as S3 Standard but with a lover storage price and a higher retrieval price.
- Examples: data infrequently accessed but requires high availability when needed.

S3 One Zone-Infrequent Access (S3 One Zone-IA)

- Stores data in a single Availability Zone
- Has a lower storage price than S3 Standard-IA
- Save costs on storage
- You can easily reproduce your data in the event of an Availability Zone failure.

S3 Intelligent-Tiering

- Ideal for data with unknown or changing access patterns.
- Requires a small monthly monitoring and automation fee per object.
- Amazon S3 monitors objects' access patterns. If you haven't accessed an object for 30 consecutive days, Amazon S3 automatically moves it to the infrequent access tier, S3 Standard-IA. If you access an object automatically, move it to the frequent access tier, S3 Standard.

S3 Glacier

- Low-cost storage designed for data archiving.
- Able to retrieve objects within a few minutes to hours.

S3 Glacier Deep Archive

- Lowest-cost object storage class ideal for archiving
- Able to retrieve objects within 12 hours.

Amazon Elastic File System (EFS)

EFS is a scalable file system used with AWS Cloud services and on-premises resources. As you add and remove files, Amazon EFS grows and shrinks automatically. It can scale on demand to petabytes without disrupting applications.

EBS	EFS
It is a volume stores data in a single Availability Zone	It is a regional service. It stores data in and across multiple Availability Zones
To attach an Amazon EC2 instance to an	The duplicate storage enables you to

EBS volume, both the Amazon EC2 instance and the EBS volume reside within the same Availability Zone.	access data concurrently from all the Availability Zones in the Region where a file system is located. Additionally, on-premises servers can access Amazon EFS using AWS Direct Connect.

Amazon Relational Database Service (Amazon RDS)

RDS is a service that enables you to run relational databases in the AWS Cloud.

RDS is a managed service that automates tasks such as hardware provisioning, database, setup, patching and backups. Many RDS database engines offer encryption at rest (protecting data while it is stored) and encryption in transit (protecting data while it is being sent and received).

Database Engines

- Amazon Aurora
- PostgreSQL
- MySQL
- MariaDB
- Oracle Database
- Microsoft SQL Server

Amazon Aurora

Amazon Aurora is an enterprise-class relational database. It is compatible with MySQL and PostgreSQL relational databases. It is up to five times faster than standard MySQL databases and up to three times faster than standard PostgreSQL databases.
Consider Amazon Aurora if your workloads require high availability. It replicates six copies of your data across three Availability Zones and continuously backs up your data to Amazon S3.

Non Relational databases

NoSQL databases use structures other than rows and columns to organize data. One type of structural approach for nonrelational databases is key-value pairs. With key-value pairs. data is organized into items (keys), and items have attributes (values).

Amazon DynamoDB

Amazon DynamoDB is a key-value database service. It delivers single-digit millisecond performance at any scale.
- Serverless: it means that you don't have to provision, path, or manage servers, you also don't have to install, maintain or operate software.
- Automatic scaling: as the size of your db shrinks or grows, DynamoDB automatically scales you adjust for changes in capacity while maintaining consistent performance (high performance while scaling).

Amazon Redshift

Amazon Redshift is a data warehousing service that you can use for big data analytics. It offers the ability to collect data from many sources and helps you to understand relationships and trends across your data.

AWS Database Migration Service (Amazon DMS)

AWS Database Migration Service (AWS DMS) enables you to migrate relational databases, non relational databases and other types of data stores.

Types
- Homogeneous databases (same tech)
- Heterogeneous databases (2-step process, AWS Schema Conversion Tool, Migrate)

Use Cases
- Enabling developers to test applications against production data without affecting production users.
- Combining several databases into a single db.
- Sending ongoing copies of your data to other target sources instead of doing a one-time migration.

Additional Database Services

Amazon DocumentDB

Amazon DocumentDB is a document database service that supports MongoDB workloads.

Amazon Neptune

Amazon Neptune is a graph database service. You can use Amazon Neptune to build and run applications that work with highly connected datasets, such as recommendations engines, fraud detection and knowledge graphs.

Amazon Quantum Ledger Database (Amazon QLDB)

Amazon QLDB is a ledger database service. You can use Amazon QLDB to review a complete history of all the changes that have been made to your application data.

Amazon Managed Blockchain

Amazon Managed Blockchain is a service that you can use to create and manage blockchain networks with open-source frameworks.
Blockchain is a distributed ledger system that lets multiple parties run transactions and share data without a central authority.

Amazon ElastiCache

Amazon ElastiCache is a service that adds caching layers on top of your db to help improve the read times of common requests.

Amazon DynamoDB Accelerator

Amazon DAX is an in-memory cache for DynamoDB.

It helps improve response times from single-digit milliseconds to microseconds.

MODULE 6

AWS Shared responsibility model

AWS Responsibilities

- Physical security of data centers
- Hardware and software infrastructure
- Network infrastructure
- Virtualization infrastructure

Customer Responsibilities

- Selecting on Amazon EC2
- Configuring on Amazon EC2
- Patching OS
- Security Groups on Amazon EC2
- Accounts on Amazon EC2

CUSTOMERS	CUSTOMER DATA		
	PLATFORM, APPLICATIONS, IDENTITY AND ACCESS MANAGEMENT		
	OPERATING SYSTEMS, NETWORK AND FIREWALL CONFIGURATION		
	CLIENT-SIDE DATA ENCRYPTION	SERVER-SIDE ENCRYPTION	NETWORKING TRAFFIC PROTECTION

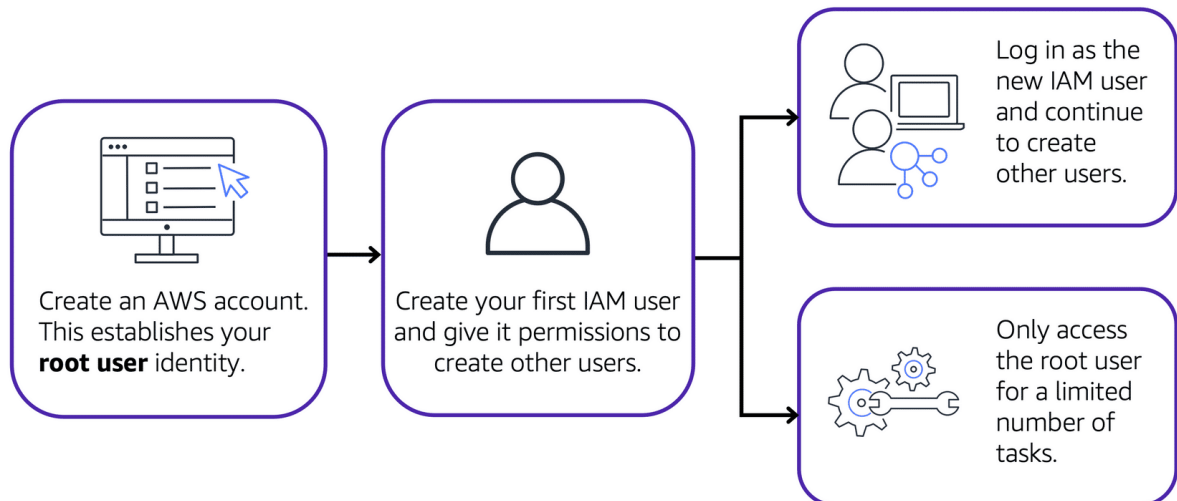| AWS	SOFTWARE			
	COMPUTE	STORAGE	DATABASE	NETWORKING
	HARDWARE/AWS GLOBAL INFRASTRUCTURE			
	REGIONS	AVAILABILITY ZONES		EDGE LOCATIONS

AWS Identity and Access Management (IAM)

AWS IAM enables you to manage access to AWS services and resources securely. IAM gives you the flexibility to configure access based on your company's specific operational and security needs.
- IAM users, groups and roles
- IAM policies
- Multi-Factor authentication

AWS Root User

The root user is accessed by signing in with the email address and password that you used to create your AWS account.

Create an AWS account. This establishes your **root user** identity.

Create your first IAM user and give it permissions to create other users.

Log in as the new IAM user and continue to create other users.

Only access the root user for a limited number of tasks.

IAM Users

An IAM User is an identity that you create in AWS. It represents the person or application that interacts with AWS services and resources. It consists of a name and credentials.
By default, when you create a new IAM user in AWS, it has no permissions associated with it. To allow the IAM user to perform specific actions in AWS, such as launching an Amazon EC2 instance or creating an Amazon S3 bucket, you must grant the IAM user the necessary permissions.

IAM Policies

IAM Policy is a document that allows or denies permissions to AWS services and resources. IAM policies enable you to customize users' levels of access to resources (follow the security principle of least privilege when granting permissions).

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "s3:ListObject",
    "Resource": "arn:aws:s3:::
AWSDOC-EXAMPLE-BUCKET"
  }
}
```

IAM Groups

An IAM Group is a collection of IAM users. When you assign an IAM policy to a group, all users in the group are granted permissions specified by the policy.
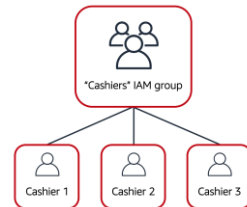
IAM Roles

IAM Role is an identity that you can assume to gain temporary access to permissions. Before an IAM user, application or service can assume an IAM role, they must be granted permissions to switch to the role. When someone assumes an IAM role, they abandon all previous permissions that they had under a previous role and assume the permissions of the new role (IAM roles are ideal for situations in which access to services or resources needs to be granted temporarily, instead of long-term).

Multi-Factor Authentication

In IAM, multi-factor authentication (MFA) proves an extra layer of security for your AWS account.

AWS Organizations

AWS Organizations to consolidate and manage multiple AWS accounts within a central location.
When you create an organization, AWS Organizations automatically creates a root, which is the parent container for all the accounts in your organization.
In AWS Organizations, you can centrally control permissions for the accounts in your organization by using service control policies (SCP). SCPs enable you to place restrictions on the AWS services, resources and individual API actions that users and roles in each account can access.
You are configuring service control policies (SCPs) in AWS Organizations. Which identities and resources can SCPs be applied to?
- An individual member account
- An organizational unit (OU)

Organizational units

In AWS Organizations, you can group accounts into organizational units (OU) to make it easier to manage accounts with similar business or security requirements. When you apply a policy to an OU, all the accounts in the OUT automatically inherit the permissions specified in the policy.
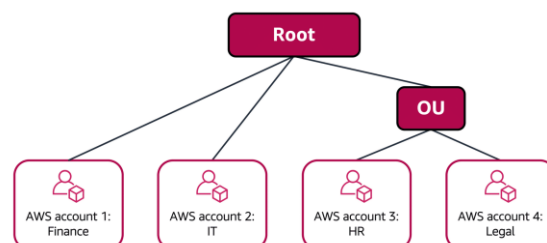
Compliance

AWS Artifact

AWS Artifact is a service that provides on-demand access to AWS security and compliance reports and select online agreements.

AWS Artifact Agreements

In AWS Artifact Agreements, you can review, accept and manage agreements for an individual account and for all your accounts in AWS Organizations.
- Access AWS compliance reports on-demand.
- Review, accept, and manage agreements with AWS.

AWS Artifact Reports

AWS Artifact Reports provide compliance reports from third-party auditors. These auditors have tested and verified that AWS is compliant with a variety of global, regional and industry specific security standards and regulations.

Customer Compliance Center

The Customer Compliance Center contains resources to help you learn more about AWS compliance.
You can also access compliance whitepapers and documentation on topics such as:
- AWS answers to key compliance questions
- An overview of AWS risk and compliance
- An auditing security checklist

Denial-of-Service

DoS

A denial-of-service (DoS) attack is a deliberate attempt to make a website or application unavailable to users.

DDoS

In a distributed denial-of-service (DDos) attack, multiple sources are used to start an attack that aims to make a website or application unavailable. This can come from a group of attackers, or even a single attacker.

AWS Shield

AWS Shield is a service that protects applications against DDoS attacks. AWS Shield provides two levels of protection: Standard and Advanced.
- Standard:
  - It automatically protects all AWS customers at no cost. It protects your AWS resources from the most common, frequently occurring types of DDos attacks.
- Advanced:
  - It is a paid service that provides detailed attack diagnostics and the ability to detect and mitigate sophisticated DDoS attacks.
  - It also integrates with other services such as Amazon CloudFront, Amazon Route 53 and Elastic Load Balancing. Additionally, you can integrate AWS Shield with AWS WAF by writing custom rules to mitigate complex DDoS attacks.

Additional Security Services

AWS Key Management Service (AWS KMS)

AWS KMS enables you to perform encryption operations through the use of cryptographic keys. You can use AWS KMS to create, manage and use cryptographic keys. You can also control the use of keys across a wide range of services and in your applications.

AWS WAF

AWS WAF is a web application firewall that lets you monitor network requests that come into your web applications.
AWS WAF works together with Amazon CloudFront and an Application Load Balancer. AWS WAF works in a similar way to block or allow traffic.
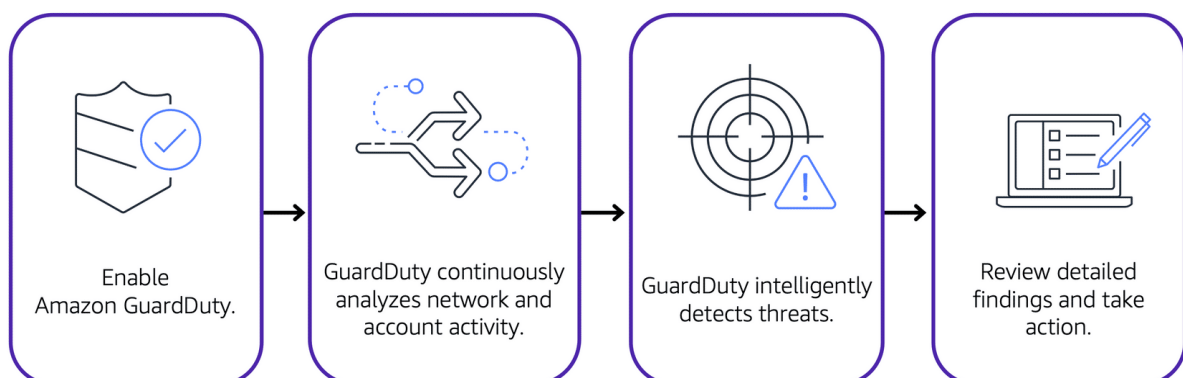
Amazon Inspector

Amazon Inspector helps to improve the security and compliance of applications by running automated security assessments. It checks applications for security vulnerabilities and deviations from security best practices, such as open access to Amazon EC2 instances and installations of vulnerable versions.

Amazon GuardDuty

Amazon GuardDuty is a service that provides intelligent threat detection for your AWS infrastructure and resources. It identifies threats by continuously monitoring the network activity and account behavior within your AWS environment.
GuardDuty analyzes data from multiple AWS sources, including VPC Flow Logs and DNS logs.
You can also configure AWS Lambda functions to take remediation steps automatically in response to GuardDuty's security findings.

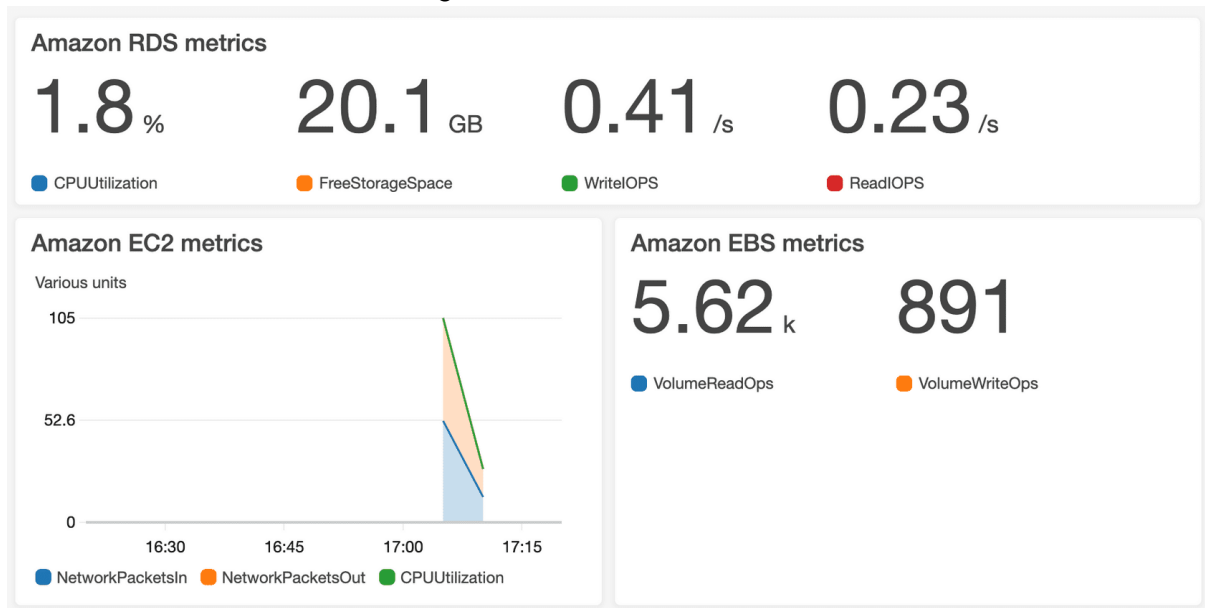| Enable Amazon GuardDuty. | GuardDuty continuously analyzes network and account activity. | GuardDuty intelligently detects threats. | Review detailed findings and take action. |

MODULE 7

Monitoring and Analytics

Amazon CloudWatch

Amazon CloudWatch is a web service that enables you to monitor and manage various metrics and configure alarm actions based on data from those metrics.

CloudWatch uses metrics to represent the data points for your resources. AWS services send metrics to CloudWatch. CloudWatch then uses these metrics to create graphs automatically that show how performance has changed over time.

- Monitor your resources' utilization and performance
- Access metrics from a single dashboard

Amazon RDS metrics

1.8 %	20.1 GB	0.41 /s	0.23 /s
● CPUUtilization	● FreeStorageSpace	● WriteIOPS	● ReadIOPS

Amazon EC2 metrics

Various units

(chart showing values 105, 52.6, 0 over time 16:30, 16:45, 17:00, 17:15)

● NetworkPacketsIn ● NetworkPacketsOut ● CPUUtilization

Amazon EBS metrics

5.62 k	891
● VolumeReadOps	● VolumeWriteOps

AWS CloudTrail

AWS CloudTrail records API calls for your account. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, and more. Recall that you can use API calls to provision, manage and configure your AWS resources. With CloudTrail, you can view a complete history of user activity and API calls for your applications and resources (events are typically updated in CloudTrail within 15 minutes after an API call).

- Filter logs to assist with operational analysis and troubleshooting
- Track user activities and API requests throughout your AWS infrastructure

What happened?	A new IAM user (Mary) was created.
Who made the request?	IAM user John
When did this occur?	January 1, 2020 at 9:00 AM
How was the request made?	Through the AWS Management Console

CloudTrail Insights

CloudTrail Insights is an optional feature allowing CloudTrail to automatically detect unusual API activities in your AWS account.

AWS Trusted Advisor

AWS Trusted is a web service that inspects your AWS environment and provides real-time recommendations in accordance with AWS best practices.
Pillars:
- Cost Optimization
- Performance
- Security
- Fault Tolerance
- Service Limits

Categories:
- Green: no problems
- Orange: investigations
- Red: actions

It enables you to review the security of your Amazon S3 buckets by checking for open access permissions

Cost Optimization	Performance	Security	Fault Tolerance	Service Limits
0 ✅ 9 ⚠️ 0 ⓘ	3 ✅ 7 ⚠️ 0 ⓘ	2 ✅ 4 ⚠️ 11 ❗	0 ✅ 15 ⚠️ 5 ❗	37 ✅ 0 ⚠️ 1 ❗
$7,516.85 Potential monthly savings				

MODULE 8

AWS Free Tier

The AWS Free Tier enables you to begin using certain services without having to worry about incurring costs for the specified period.
- Always free
  - These offers don't expire and are available to all AWS customers.
- 12 months free
  - These offers are free for 12 months following your initial sign-up date to AWS.
- Trials
  - Short-term free trial offers start from the date you activate a particular service. The length of each trial might vary by number of days or the amount of usage in the service.

AWS Pricing

- Pay for what you use

- For each service you pay for exactly the amount of resources that you actually use, without requiring long-term contracts or complex licensing.
- Pay less when you reserve
  - Some services offer reservation options that provide a significant discount compared to On-Demand Instance pricing.
- Pay less with volume-based discounts when you use more
  - Some services offer tiered pricing, so the per-unit cost is incrementally lower with increased usage.

AWS Pricing Calculator

The AWS Pricing Calculator lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can organize your AWS estimates by groups that you define. A group can reflect how your company is organized, such as providing estimates by cost center.

Consolidated billing

The consolidated billing feature of AWS Organizations enables you to receive a single bill for all AWS accounts in your organization. By consolidating, you can easily track the combined costs of all the linked accounts in your organization. The default maximum number of accounts allowed for an organization is 4, buy you can contact AWS Support to increase your quota, if needed.

AWS Budget

In AWS Budgets you can create budgets to plan your service usage, service costs and instance reservations.
In AWS Budgets you can also set custom alerts when you usage exceeds.

AWS Cost Explorer

AWS Cost Explorer is a tool that enables you to visualize, understand and manage your AWS costs and usage over time.
It includes a default report of the costs and usage for your top five cost-accruing AWS services. You can apply custom filters and groups to analyze your data.
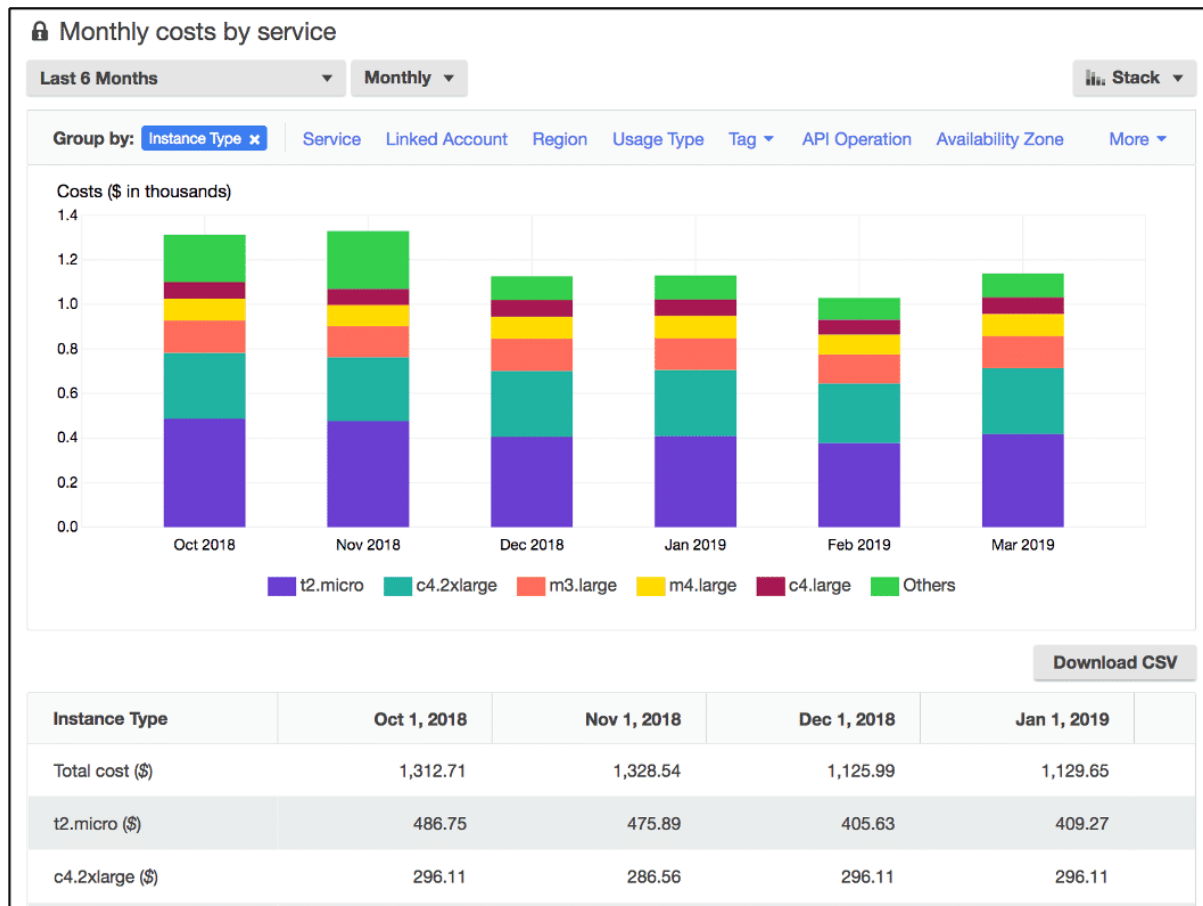
(12 months of history data)

AWS Support Plans

AWS offers four different Support Plans to help you troubleshoot issues, lower costs and efficiently use AWS service.

Basic

Basic Support is free for all AWS customers.
- Whitepapers
- Documentation
- Support Communities

With Basic Support, you have access to a limited selection of AWS Trusted Advisor checks. Additionally, you can use the AWS Personal Health Dashboard, a tool that provides alerts and remediation guidance when AWS is experiencing events that may affect you.

Developer

- Best practice guidance
- Client-side diagnostic tools
- Building-block architecture support, which consists of guidance for how to use AWS offerings, features, and services together.

Business

- Use-case guidance to identify AWS offerings, features and services that can best support your specific needs.
- All AWS Trusted Advisor checks
- Limited support for third-party software, such as common operating systems and application stack components

Enterprise

- Application architecture guidance, which is a consultative relationship to support your company's specific use cases and applications.
- Infrastructure event management: A short-term engagement with AWS Support that helps your company gain a better understanding of your use cases. This also provides your company with architectural and scaling guidance.
- A Technical Account Manager (TAM)

Technical Account Manager (TAM)

TAM provides guidance, architectura reviews, and ongoing communication with your company as you plan, deploy and optimize your applications. TAM helps you design solutions that efficiently use multiple services together through an integrated approach.

AWS Marketplace

AWS Marketplace is a digital catalog that includes thousands of software listings from independent software vendors. You can use AWS Marketplace to find, test and buy software that runs on AWS.

Business Applications

Data & Analytics

DevOps

Infrastructure Software

Internet of Things (IoT)

Machine Learning

Migration

Security

MODULE 9

AWS Cloud Adoption Framework (AWS CAF)

AWS CAF organizes guidance into six areas of focus, called **Perspectives**. Each **Perspective** addresses distinct responsibilities.

Business

The Business Perspective ensures that IT aligns with business needs and that IT investments link to key business results.
Common roles in the Business Perspective include:
- Business managers
- Finance managers
- Budget owners
- Strategy stakeholders

People

The People Perspective supports development of an organization-wide change management strategy for successful cloud adoption.
Common roles in the People Perspective include:
- Human resources
- Staffing
- People managers

Governance

The Governance Perspective focuses on the skills and processes to align IT strategy with business strategy. This ensures that you maximize the business value and minimize risks.
Common Roles in Governance Perspective include:
- CIO
- Program managers
- Enterprise architects
- Business analysts
- Portfolio managers

Platform

The Platform Perspective includes principles and patterns for implementing new solutions on the cloud, and migrating on-premises workloads to the cloud.
Common roles in the Platform Perspective include:
- CTO
- IT managers
- Solutions architects

Security

The Security Perspective ensures that the organization meets security objectives for visibility, auditability, control and agility.
Common roles in the Security Perspective include:
- CISO

- IT security managers
- IT security analysts

Operations

The Operations Perspective helps you to enable, run, use, operate and recover IT workloads to the level agreed upon with your business stakeholders.
Common roles in the Operations Perspective include:
- IT operations managers
- IT support managers

Migration Strategies

When migrating applications to the cloud, six of the most common migration strategies that you can implement are:

Rehosting

Rehosting also known as "lift-and-shift" involves moving applications without changes (large legacy migration)

Replatforming

Replatforming also known as "lift, thinker and shift" involves making a few cloud optimizations to realize a tangible benefit (changing the core architecture of the application)

Refactoring (re-architecting)

Refactoring involves reimagining how an application is architected and developed by using cloud-native features. Refactoring is driven by a strong business need to add features, scale or performance that would otherside be difficult to achieve in the application's existing environment.

Repurchasing

Repurchasing involves moving from a traditional license to a software-as-a-service model.

Retaining

Retaining consists of keeping applications that are critical for the business in the source environment.

Retiring

Retiring is the process of removing applications that are no longer needed.

AWS Snow Family

The AWS Snow Family is a collection of physical devices that help to physically transport up to exabytes of data into and out of AWS.

AWS Snowcone

AWS Snowcone is a small, rugged and secure edge computing and data transfer device. It features 2 CPUs, 4 GB of memory and 8 TB of usable storage.

AWS Snowball

- Snowball Edge Storage Optimized (large-scale data migrations)
  - Storage: 80 TB (HDD) and 1 TB (SSD)
  - Compute: 40 vCPUs and 80 GiB (equivalent to C5)
- Snowball Edge Compute Optimized (powerful computing such as machine learning, full motion video analysis, analytics and local computing snacks)
  - Storage: 42 TB (HDD) and 7.69 (SSD)
  - Compute: 52 vCPUs and 208 GiB (equivalent to C5, M5a, G3 and P3)

AWS Snowmobile

AWS Snowmobile is an exabyte-scale data transfer service used to move large amounts of data to AWS.
You can transfer up to 100 petabytes of data per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi trailer truck.

Innovation with AWS

Serverless applications

AWS serverless refers to applications that don't require you to provision, maintain or administer servers. AWS Lambda is an example of a service that you can use to run serverless applications. If you design your architecture to trigger Lambda functions to run your code, you can bypass the need to manage a fleet of servers.

Artificial Intelligence

- Convert speech to text with Amazon Transcribe
- Discover patterns in text with Amazon Comprehend
- Identify potentially fraudulent online activities with Amazon Fraud Detector

- Build voice and text chatbots with **Amazon Lex (A service that enables you to build conversational interfaces using voice and text)**

Machine learning

Traditional machine learning (ML) development is complex, expensive, time consuming and error prone. AWS offers Amazon SageMaker to remove the difficult work from the process and empower you to build, train and deploy ML models quickly.

MODULE 10

AWS Well-Architected Framework

The AWS Well-Architected Framework helps you understand how to design and operate reliable, secure, efficient and cost-effective systems in the AWS Cloud. It provides a way for you to consistently measure your architecture against best practices and design principles and identify areas for improvement.

Operational excellence

Security

Reliability

Performance efficiency

Cost optimization
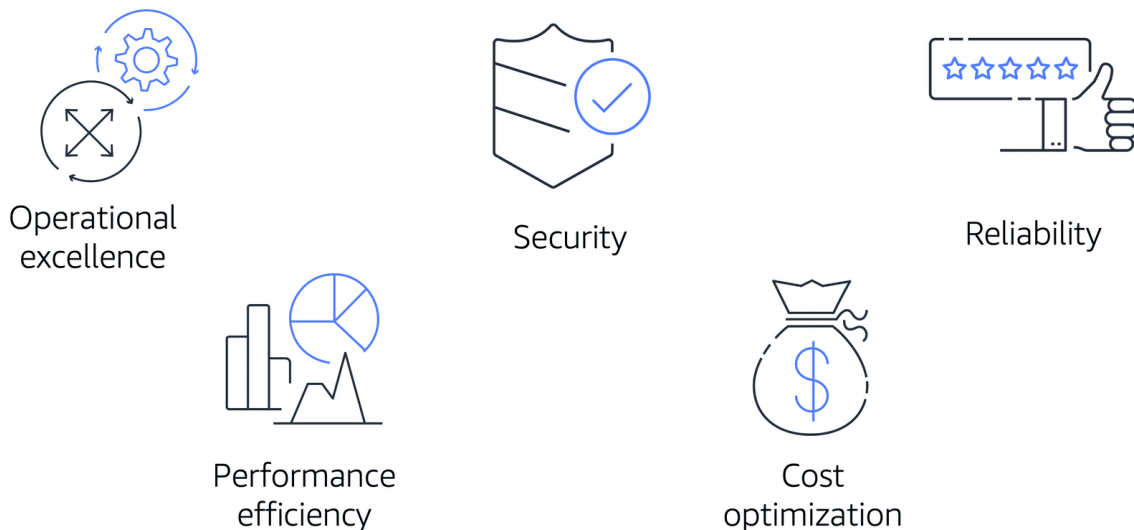
Operational excellence

Operational excellence is the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures.
- Operations as a code
- Annotating document
- Anticipating failure
- Making small, reversible changes

Security

The Security pillar is the ability to protect information, systems and assets while delivering business value through risk assessments and mitigation strategies.
Best practices:
- Automate security best practices when possible
- Apply security at all layers
- Protect data in transit and at rest

Reliability

Reliability is the ability of a system to do the following:
- Recover from infrastructure or service disruptions
- Dynamically acquire computing resources to meet demand
- Mitigate disruptions such as misconfigurations or transient network issues

Reliability includes testing recovery procedures, scaling horizontally to increase aggregate system availability and automatically recovering from failure.

Reliability is the pillar of the AWS Well-Architected Framework focuses on the ability of a workload to consistently and correctly perform its intended functions.

Performance efficiency

Performance efficiency is the ability to use computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve. Evaluating the performance efficiency of your architecture includes experimenting more often, using serverless architecture and designing systems to be able to go global in minutes.

The Performance Efficiency pillar focuses on using computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve.

Cost optimization

Cost optimization is the ability to run systems to deliver business value at the lowest price point.

Cost optimization includes adopting a consumption model, analyzing and attributing expenditure and using managed services to reduce the cost of ownership.

The Cost Optimization pillar focuses on the ability to run systems to deliver business value at the lowest price point.

Advantages of Cloud Computing

Operating in the AWS Cloud offers many benefits over computing in on-premises or hybrid environments.

Trade upfront expense for variable expense

Upfront expenses include data centers, physical servers and other resources that you would need to invest in before using computing resources.

Benefit from massive economies of scale

By using cloud computing, you can achieve a lower variable cost than you can get on your own. Because usage from hundreds of thousands of customers aggregates in the cloud, providers such as AWS can achieve higher economies of scale. Economies of scale translate into lower pay-as-you-go prices.

Stop guessing capacity

With cloud computing, you don't have to predict how much infrastructure capacity you will need before deploying an application.

Increase speed and agility

The flexibility of cloud computing makes it easier for you to develop and deploy applications.

Stop spending money running and maintaining data centers

Cloud computing in data centers often requires you to spend more money and time managing infrastructure and servers.

Go global in minutes

The AWS Cloud global footprint enables you to quickly deploy applications to customers around the world, while providing them with low latency.