AWS cheat code 2nd version

Date	@10 juin 2025

- Trade "capital expense (capex)" for "variable expense (opex)" (Pay-as-you-go) more expensive
- Increased speed and agility (react quickly as your needs evolve)
- Benefit from massive economies of scale
- Stop guessing capacity
- Stop spending money running and maintaining data centers
- "Go global" in minutes
- By using cloud computing,reduce their pricing due to AWS can achieve higher economies of scale, which translates into lower pay as-you-go prices.
- **Reduce the cost of maintaining idle resources (idle resources"** refer to **cloud services or infrastructure components that are running but not being used effectively or at all** — meaning you're paying for them **without getting value**.)

AWS Well-Architected Framework

- 🔷 6 Pillars of the AWS Well-Architected Framework
    - Security
    - Cost Optimization
    - Operational Excellence

  Perform operations as code

  Make frequent, small, reversible changes

  Refine operations procedures frequently

  Anticipate failure

  Learn from all operational failures

    - Reliability
    - Performance Efficiency (experiment more often align with)
    - Sustainability
- The AWS Well-Architected Framework is a set of best practices and guidelines for designing and operating workloads on AWS. It helps customers achieve operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability. (A company has migrated its workloads to AWS. The company wants to adopt AWS at scale and operate more efficiently and securely.)
- AWS Config can be used to track the configuration state of your resources and how the state has changed over time. With **CloudTrail** you can audit **who made what** API calls on what resources at what time. This can help with identifying changes that cause reliability issues.

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.

CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

Compute Services

- **AWS Lambda: Serverless Compute**
    - Build Event Driven Applications (React to notifications from S3, SQS, SNS or DynamoDB)
- **EC2 Options :**
    - On Demand. Flexible and Most Expensive, low fault tolerance Apps.
    - Spot Instances - Cheapest (upto 90% off).Fault tolerant, Non immediate workloads.
    - Reserved Instances. Upto 75% off. 1 or 3 years reservation. Scheduled (All Upfront option is the cheapest): **Reserve ** for specific time period in a day. (5% to 10% off)
    - Savings Plans - flexibility to switch from EC2 instances to AWS Lambda or AWS Fargate. Upto 66% off. 1 or 3 years reservation. (Amazon SageMaker: Amazon SageMaker is a service that helps you build and deploy machine learning models. You can use Amazon SageMaker to access Jupyter notebooks, use common machine learning algorithms, train and tune models, and deploy them to a hosted environment.Amazon SageMaker is eligible for SageMaker Savings Plans)
    - EC2 Dedicated Hosts

    An Amazon EC2 Dedicated Host is a physical server with EC2 instance capacity fully dedicated to your use. Dedicated Hosts allow you to use your existing per-socket, per-core, or per-VM software licenses, including Windows Server, Microsoft SQL Server, SUSE, Linux Enterprise Server, and so on.

        - Physical servers dedicated to one customer
        - You have visibility into the hardware of the underlying host (sockets and physical cores)
        - (Use cases) Regulatory needs or server-bound software licenses like Windows Server, SQL Server
    - An Amazon EC2 Dedicated Host is a physical server fully dedicated for your use, so you can help address corporate compliance requirements. Amazon EC2 Dedicated Hosts allow you to use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2, so that you get the flexibility and cost effectiveness of using your own licenses, but with the resiliency, simplicity and elasticity of AWS
    - A convertible reserved instance enables you to exchange one or more Convertible Reserved Instances for another Convertible Reserved Instance with a different configuration, including instance family, operating system, and tenancy.

- **AWS Fargate** is a serverless offering that lets us run containers on Amazon Elastic Container Service (Amazon ECS), without the need to manage the underlying EC2 instances
- **Amazon Lightsail** - Pre-configured development stacks in AWS - LAMP, MEAN. Run websites on WordPress.Low, predictable monthly price.
- **Lightsail**: simplified cloud compute offering with limited complexity, so they can get up and running quickly
- **AWS Amplify (mobile app)** is an AWS service that is a set of tools and services that enables developers to build secure, scalable, full-stack applications, powered by AWS, with a flexible, declarative programming model. AWS AppConfig is an AWS service that enables application owners to centrally manage feature configurations and settings for their applications, allowing you to deploy application configurations in a controlled and monitored way.
- **AWS AppConfig** is the correct answer because it allows users to deploy application configuration changes quickly and reliably without needing to write additional code or restart services. It supports validation checks to ensure configuration data is syntactically and semantically correct before deployment, avoiding potential outages.
- **AWS Batch** enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS.
- A company is planning to deploy an application with a relational database on AWS. The application layer requires access to the database instance's operating system in order to run scripts. EC2

Storage Services

- **EC2 Instance Store** (Ephemeral)
- **Elastic Block Store (EBS)**: Network Storage
  - More Durable. Very flexible Provisioned capacity
  - Increase size when you need it - when attached to EC2 instance
  - 99.999% Availability & replicated within the same AZ
  - can be attached with only one EC2 instance
  - Use case : Run your custom database
  - The fundamental charges for EBS volumes are the **volume type** (based on performance), the storage volume in GB per month provisioned, **the number of IOPS provisioned** per month, the storage consumed by snapshots, and outbound data transfer.
- **S3** - The key is the name assigned to the object and the access control information determines who can access the object.
  - Standard - Frequently accessed data. First Byte: ms
  - Standard-IA - Long-lived, infrequently accessed data (backups for disaster recovery). First Byte: ms
  - One Zone-IA - Long-lived, infrequently accessed, non-critical data (Easily re-creatable data - thumbnails for images). First Byte: ms
  - Intelligent-Tiering - Long-lived data with changing or unknown access patterns
  - Glacier - Archive data with retrieval times ranging from minutes to hours
  - Glacier Deep Archive - Archive data that rarely, if ever, needs to be accessed with retrieval times in few hours
  - Reduced Redundancy (Not recommended) - Frequently accessed, non-critical data
  - S3 and EFS are auto-scaling by default.
  - (S3) offers virtually unlimited storage. The total volume of data and number of objects you can store are unlimited. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 5 terabytes. The largest object that can be uploaded in a single PUT is 5 gigabytes.
  - ACLs are an AWS service or feature that the developer can use to restrict read and write access to the S3 bucket. ACLs are access control lists that grant basic permissions to other AWS accounts or predefined groups. They can be used to grant read or write access to an S3 bucket or an object3

Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets. Buckets that are configured for object replication can be owned by the same AWS account or by different accounts. You can copy objects between different AWS Regions or within the same Region.

Both source and destination buckets must have versioning enabled. The source bucket owner must have the source and destination AWS Regions enabled for their account. The destination bucket owner must have the destination Region-enabled for their account.

With the standard storage class you pay a per GB/month storage fee, and data transfer out of S3. Standard-IA and One Zone-IA have a minimum capacity charge per object. Standard-IA, One Zone-IA, and Glacier also have a retrieval fee. You don't pay for data into S3 under any storage class.

What charges are applicable to Amazon S3 Standard storage class

Data egress & Per GB/month storage fee

- **Amazon FSx for Lustre**
  - File system optimized for performance
  - High performance computing (HPC) and media processing use cases

  It's designed to support terabytes per second of throughput and millions of IOPS.

- **Aws storage gateway**
  - Hybrid : Cloud + On Premise
- **Storage Tape Gateway** - Virtual tape backups
  - Tapes stored in Amazon S3 & Glacier
  - Avoid complex physical tape backups (wear and tear)
  - No change needed for tape backup infrastructure
- **Exabytes, Petabyptes**

    - Use Snowmobile Trucks (100PB per truck) for dozen petabytes to exabytes
- **We can use Amazon S3 Object Lock** to protect an Amazon S3 object that we are required to retain.

Database Services

- 🔷 **ElastiCache**
    - Cache Query Results from databases. Can act as a session store as well.
- **EMR** - Managed Hadoop. Large scale data processing with high customization (machine learning, graph analytics)

Amazon Elastic Map Reduce (EMR) is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data. EMR utilizes a hosted Hadoop framework running on Amazon EC2 and Amazon S3.

- **Amazon RDS (OLTP)** - Transactional use cases needing predefined schema and very strong transactional capabilities
    - Amazon RDS is billed by the uptime of the instance.
- **Redshift (OLAP)** - Datewarehouse, reporting, analytics & intelligence apps - Analyse Petabytes of data.
    - **Redshift Spectrum** - Use when you already have Redshift and want to query S3 + warehouse data together (without loading data from S3 into data warehouse)
    - Amazon Redshift is a data warehouse, optimized for: Read-heavy, analytical workloads, Batch processing, Handling structured, historical data (for BI, reporting, etc.). It's not designed for frequent small updates or real-time write/read workloads. Redshift is append-optimized, meaning: Frequent updates or deletes are expensive and inefficient, Not suitable for data that changes regularly or needs frequent write access.
- **DynamoDB** - Apps needing quickly evolving semi structured data (schema-less). Terabytes of data with millisecond responses for millions of TPS. Content management, catalogs, user profiles, shopping carts, session stores and gaming applications
- **Neptune** is a graph database that helps us understand relationships between highly connected data.
- **Amazon QLDB** is a immutable database that cannot be overwritten or deleted, only added to.

Networking & Content Delivery

- **AWS VPN**: Tunnels from VPC to on premises
    - Traffic over internet
    - encrypted using IPsec protocol
    - VPN gateway(**A Virtual Private Gateway)** + customer gateway(the company's side)
- **NAT** allow EC2 in a private subnet to download while denying inbound traffic from internet
    - NAT Instance: Install a EC2 + NAT AMI and configure as a gateway
    - NAT Gateway: IPv4 ONLY (Egress Internet Gateways: For IPv6 subnets)
    - NAT gateway is to grant internet access to our private subnets?
- **Network Access Control List (NACL)** - stateless firewall at the subnet level. control traffic in and out of a subnet
    - Network ACLs: Stateless. Return traffic must be explicitly allowed. If you allow inbound traffic, you must also allow outbound traffic for replies. Unlike security groups (which are stateful and handle return traffic automatically). Rule Evaluation Order: Ascending (Lowest to Highest Rule Number)
- **Security Groups** - Virtual firewall to control incoming and outgoing traffic to/from AWS resources (EC2 instances, databases etc)
- **VPC Flow Logs**
    - Monitor network traffic; Troubleshoot connectivity issues (NACL and/or security groups misconfiguration); Capture traffic going in and out of your VPC (network interfaces)
- **Amazon CloudWatch Logs** lets you monitor and troubleshoot your systems and applications using your existing system, application and custom log files. CloudWatch Logs can be used for real time application and system monitoring as well as long term log retention.

Application performance

Resource utilization

- **AWS Direct Connect**: Private pipe from AWS to on-premises
- **AWS VPN**: Encrypted (IPsec) tunnel over the internet to on-premises
- **Internet Gateway**: Allows Public Subnets to connect/accept traffic to/from internet
- **Elastic Load Balancers** work by distributing requests to a resource pool.
- **AWS Transit Gateways** and VPC Peering can be used to connect multiple VPCs together

AWS Transit Gateway is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. (What is the most efficient way to establish network connectivity from on-premises to multiple VPCs in different AWS Regions)

- **Route 53** rules: (No rules provided)
- **AWS Local Zones** helps us put resources closer to the customers in large metro areas.(help us extend our VPCs into large population centers to help reduce latency)
- Launch the instances in multiple AWS Regions, and use Elastic IP addresses" is incorrect. You cannot use an ELB with instances in multiple Regions and using an EIP does not help.

Management & Governance

- **managing servers, Deployment, Monitoring and Support**
- **serverless, Iac, CICD**
- Which of the authentication options below can be used to authenticate using AWS APIs:

Access keys

Server certificates

- **Cloud Formation**: Use Infrastructure As Code
- **AWS CloudTrail** - Track events, API calls, changes made to your AWS resources. if EC2 is ended. Who (made the request), What (action, parameters, end result) and When?
  - audit and monitor changes made to your AWS resources, audit the usage of your IAM Users
- **AWS Config** - Auditing: Complete inventory of your AWS resources**. Resource history** and change tracking - Find how a resource was configured at any point in time Governance - Customize Config Rules for specific resources or for entire AWS account and Continuously evaluate compliance against desired configuration. provides predefined, customizable rules that are used to evaluate whether your AWS resources comply with common best practices
  - AWS Config is an AWS service that enables you to assess, audit, and evaluate the configurations of your AWS resources to help organizations simplify compliance auditing, security analysis, change management, and operational troubleshooting.
  - AWS Config monitors system configurations & logs when selected configurations are changed.
  - In order to comply with a government privacy policy, we need to actively monitor system configuration & log when specific configurations are changed to support audits.
- **Amazon CloudWatch** - Monitoring and observability service
  - Metrics for AWS services Example EC2: CPUUtilization, NetworkIn, NetworkOut
  - CloudWatch - Monitoring and observability service
  - Amazon CloudWatch is a performance monitoring service. AWS services send metrics about their utilization to CloudWatch which collects the metrics. You can then view the results in CloudWatch and configure alarms. "AWS Systems Manager" is incorrect. Systems Manager is used for managing EC2 instances such as installing patches and software. (monitor a new Amazon EC2 instances CPU and network utilization)
- **AWS Systems Manager** - Run commands(operational tasks) on Amazon EC2 instances. Manage your OS and Database patches.
- **AWS Professional Services** - Get help for cloud migration. Get advise from AWS Teams for APP Migration & Modernization, Advisory solutions for AWS adoption
  - AWS Professional Services can provide expert help for one time events such as migrations & AWS IQ allows us to post work and receive bids from interested AWS partners.
- **AWS Partner Network** - Consulting and technology firms. Get help with design, architecture, build, connectivity and migration to AWS
- **The AWS Knowledge Center** is a repository of expert-maintained articles, white papers, and technical documentation for troubleshooting and understanding AWS services.

Unlike AWS Prescriptive Guidance, which focuses on specific configurations, or AWS re:post, which is community-driven, the Knowledge Center provides curated solutions.

- **AWS Artifact** - Self-service portal for on-demand access to AWS compliance reports, certifications, accreditations, and other third-party attestations. (governance, risk, and compliance (GRC)) Review, accept, and manage your agreements with AWS.

What is the name of the online, self-service **portal** that AWS provides to enable customers to view reports and, such as PCI reports, and accept agreements

- **Personal Health Dashboard** - Personalized alerts when AWS is experiencing events that may impact you Provides troubleshooting guidance
- **AWS Trusted Advisor**: Provides Cost optimization, performance, security & fault tolerance recommendations, service limits (A dashboard-based tool, You can still use Cost Explorer and Budgets for free cost insights even if you don't have full Trusted Advisor access.

When you allow public access to Amazon S3 buckets

When you don't turn on user activity logging (AWS CloudTrail)

AWS Trusted Advisor checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data). The ports with highest risk are flagged red, and those with less risk are flagged yellow. Ports flagged green are typically used by applications that require unrestricted access, such as HTTP and SMTP.

AWS Trusted Advisor is an online tool that provides you real time guidance to help you provision your resources following AWS best practices. Trusted Advisor checks help optimize your AWS infrastructure, improve security and performance, reduce your overall costs, and monitor service limits.

- **The AWS Trust and Safety team** is responsible for addressing and investigating reports of abuse associated with AWS resources.
- **AWS hosts events** that unite partners from diverse industries for learning, collaboration, and networking. These AWS Partner gatherings encompass webinars, online workshops, and face-to-face educational sessions.
- **X-Ray** - Trace request across microservices/AWS services - Analyze, Troubleshoot errors, Solve performance issues (for debug)
- **AWS SDKs** (Software Development Kits)
  - Write Code (Java, JavaScript, Python, Go etc) using AWS APIs
  - Integrate into Existing Applications
- **KMS & Cloud HSM** - Generate, store, use and replace your keys in AWS
  - CloudHSM: Dedicated single-tenant HSM for regulatory compliance
  - (Remember) AWS KMS is a multi-tenant service
  - Use Cases: Compliance to Regulations, Very high security
- **Availability Zones** - Each Regions has multiple AZs Discrete data centers, with redundant power, networking, and connectivity. Increase availability of applications in the same region.
- **Subnet**: Separate private resources from public resources
- **IAM Policies** are attached to an IAM entity to provide it with permissions to access AWS resources

Use customer managed policies instead of inline policies .

Create individual IAM users.

Use groups to assign permissions to IAM users.

- **Consolidated Billing** allows us to combine the usage of multiple accounts in order to reach volume discounts. It also allows us to view AWS Service usage across multiple accounts
- **AWS Migration Hub** is an interface where we can access multiple AWS migration tools, track our migration with a dashboard and utilize workflow templates to accelerate our migration.
- **AWS Wavelength** is an AWS service that extends AWS infrastructure to telecom networks, enabling ultra-low latency and high-bandwidth applications to deliver innovative, responsive, and real-time experiences.
- **AWS Outposts** is a hybrid cloud environment that will allow us to keep a portion of our infrastructure on premises. keep the customer data on premises. AWS Outposts is an AWS service that extends AWS infrastructure, services, APIs, and tools to virtually any datacenter, co-location space, or on-premises facility for a truly consistent hybrid experience.
- **AWS Session Manager** requires a role to be in place on the target instance in order to function.
- **AWS CodeArtifact** is used to manage approved software packages, and can be configured to auto update those packages from public repositories. AWS CodeArtifact is an AWS service that serves as a fully managed artifact repository compatible with language-native package managers and the build tools that help organizations store, publish, and share packages used in their software development process.
- **AWS License Manager** can help us manage our 3rd party licenses.
- **AWS Audit Manager** constantly checks for compliance and can help us determine if our environment meets compliance requirements. (We are getting ready to release a new product in the healthcare space and want to assess our environment internally before 3rd party auditors check our environment.) automates the process of assessing and managing the compliance of AWS resources with industry standards and regulatory requirements, facilitating audit preparation and tracking.
- **AWS Health Dashboards** can give us the status of all AWS services, including AWS services being used in our account. to see the status of all AWS Services in a region we are thinking about utilizing
- **AWS Prescriptive Guidance** is a set of strategies, guides and patterns that help us identify business outcomes and strategies to migrate, modernize and optimize in AWS.
- **AWS Partner Central** can help companies build and grow their AWS business.
- **AWS Activate** can help us with resources for our startups running on AWS.
- **AWS Launch Wizard** is used to provision resources for applications like SQL Server and SAP HANA without the need to provision individual resources.
- **Platform as a Service or PaaS** allows the customer deploy applications without the need to manage the virtual infrastructure.
- **AWS AppSync** is used to create and manage specialized APIs like GraphQL and pub/sub APIs.
- **AWS Billing Conductor** allows us to add rules & logic to our bill as well as add a margin, so we can pass along costs to our customers.

It is a customizable billing service that allows the organization to define billing groups, set pricing rules, create custom line items, and generate a unique Cost and Usage Report (CUR) for each billing group. This service would help the corporation to streamline and customize their billing data efficiently according to different business logics. (A corporation with multiple departments each having their own AWS accounts wants to implement a solution to customize billing data to match their specific showback or chargeback business logic. They wish to group accounts with similar financial owners and generate a distinct Cost and Usage Report (CUR) for each group)

The AWS Cost & Usage Report (AWS CUR) contains the most comprehensive set of cost and usage data available. You can use Cost and Usage Reports to publish your AWS billing reports to an Amazon Simple Storage Service (Amazon S3) bucket that you own. You can receive reports that break down your costs by the hour or month, by product or product resource, or by tags that you define yourself.

- **The AWS Enterprise Support Concierge team** is a group of billing and account experts who specialize in working with enterprise customers.
- A **Scheduled or Dynamic Scaling policy** would be appropriate for a workload that is predictable and cyclical in nature. With an application time that takes a long time to scale up,
- **AWS Service Catalog** can help us create, organize and share our IaC templates, and create self service deployments of approved infrastructure.
- **IAM Access Analyzer** is used to determine which AWS resources are being shared externally.
- **AWS Data Exports** can periodically send billing data to an S3 bucket or be exported to an Amazon QuickSight dashboard.
- **AWS Glue** is an extract, transform and load (ETL) service that can help us prepare data for analysis. AWS Glue is an AWS service that provides a fully managed, serverless data integration service that makes it easy to discover, prepare, and combine data for analytics, machine learning, and application development.(to enable reliable, secure data preparation and loading workflows)
- **AWS Directory Services** can be used to host Microsoft Active Directory in AWS.
- **The AWS Business Support Plan** is a good option for small businesses starting to go into production.
- **AWS IQ** allows us to post work and receive bids from interested AWS partners. AWS IQ is an AWS service that helps you find, collaborate, and pay AWS-Certified third-party experts for on-demand project work, facilitating a seamless connection to experienced professionals for project assistance.
- **AWS Cloud9** is a cloud based Integrated Development Environment (IDE) that runs on a managed EC2 instance.
- **AWS Application Discovery Service** will often be our first step to migrating into AWS. It can help us prepare to migrate by discovering our application servers, connections and dependencies.
- **AWS Compute Optimizer** can analyze our compute resources and help identify resources that are under or over provisioned.
    - AWS Compute Optimizer to provide sizing recommendations based on workload metrics? EC2
    - A company wants to identify the optimal AWS resource configuration for its workloads so that the company can reduce costs and increase workload performance
    - AWS Compute Optimizer recommends optimal AWS resources for your workloads to reduce costs and improve performance by using machine learning to analyze historical utilization metrics. Over-provisioning resources can lead to unnecessary infrastructure costs, and under-provisioning resources

can lead to poor application performance. Compute Optimizer helps you choose optimal configurations for three types of AWS resources: Amazon EC2 instances, Amazon EBS volumes, and AWS Lambda functions, based on your utilization data.

- **Amazon AppStream 2.0** is used to stream applications to users via web browsers or clients. It would not be used to replace VDI infrastructure.
- **AWS DataSync** can be used to discover our data and migrate it into AWS over AWS Direct Connect or the internet.
- **AWS Migration Evaluator** will collect data on our environment, provide insights and help us build out a business case
- **AWS CodeStar** can be used to create dashboards for development projects. AWS CodeStar is an into can be used to manage team members access to development projects in AWS. able to give them access to the project without having to go IAM.
- **AWS Step Functions** is the correct answer because it allows developers to coordinate multiple AWS services into serverless workflows. It provides a visual console to visualize the steps in the workflow, helping to build and update applications quickly and monitor the status of each step in the process.

AWS Step Functions is a **workflow orchestrator** for **running and managing *already deployed* applications and processes.**

- Amazon EventBridge is a serverless event bus that makes it easier to build event-driven applications at scale using events generated from your applications. You can set rules for actions to take place when certain events happen, like instance state changes, items are uploaded to an S3 bucket etc.
- **AWS Data Exchange is an AWS service that makes it easy to find, subscribe to, and use third-party data in the cloud, facilitating secure and streamlined data sharing and analysis. AWS Data Exchange** is the correct answer because this service allows customers to find, subscribe to, and use third-party data in the cloud. Companies can subscribe to a diverse selection of data products provided by various data providers. The media company in this scenario can enrich their existing datasets through AWS Data Exchange by easily finding and subscribing to third-party data sources.
- **IAM credential report** is a feature that allows you to generate and download a report that lists all IAM users in your AWS account and the status of their various credentials, including access keys and MFA devices.
- **AWS Security Token Service (AWS STS)** is a service that provides temporary security credentials to users or applications that need to access AWS resources.
- **Amazon Simple Workflow Service (SWF)** is a web service that makes it easy to coordinate work across distributed application components. SWF enables applications for a range of use cases, including media processing, web application back-ends, business process workflows, and analytics pipelines, to be designed as a coordination of tasks.(A Cloud Practitioner is creating the business process workflows associated with an order fulfilment system. Which AWS service can assist with coordinating tasks across distributed application components?)
- **A company wants to implement controls (guardrails) in a newly created AWS Control Tower landing zone. Which AWS services or features can the company use to create and define these controls**
    - Service control policies (SCPs)
    - AWS Config
    - AWS Config and service control policies (SCPs) are AWS services or features that the company can use to create and define controls (guardrails) in a newly created AWS Control Tower landing zone. AWS Config is a service that enables users to assess, audit, and evaluate the configurations of their AWS resources. It can be used to create rules that check for compliance with the desired configurations and report any deviations.
    - AWS Control Tower provides a set of predefined AWS Config rules that can be enabled as guardrails to enforce compliance across the landing zone1. **Service control policies (SCPs)** are a type of policy that can be used to manage permissions in **AWS Organizations**. They can be used to restrict the actions that the users and roles in the member accounts can perform on the AWS resources. AWS Control Tower provides a set of predefined SCPs that can be enabled as guardrails to prevent access to certain services or regions across the landing zone2.
    - Amazon GuardDuty is a service that provides intelligent threat detection and continuous monitoring for AWS accounts and resources. It is not a feature that can be used to create and define controls (guardrails) in a landing zone.
    - Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.
- **Amazon Personalize** is a fully managed service that enables developers to create personalized recommendations for customers using their own data. Amazon Personalize can automatically process and examine the data, identify what is meaningful, select the right algorithms, and train and optimize a personalized recommendation model

Security & Identity

- **Security : Settings to make your AWS solution more secure** (ex: security group)
- **GuardDuty** - Continuously monitor AWS environment for suspicious activity (Intelligent Threat Detection). Analyzes AWS CloudTrail events, VPC Flow Logs etc.
- **AWS Security Hub** - Consolidated view of your security status in AWS. Automate security checks, manage security findings, and identify the highest priority security issues across your AWS environment.
- **Amazon Detective** - Investigate and quickly identify the root cause of potential security issues. Automatically collect log data from your AWS resources and uses machine learning to help you visualize and conduct security investigations.
- **Amazon Inspector** is an automated vulnerability management service that will help identify & automate responses for vulnerabilities in AWS. It perform vulnerability scans on AWS EC2 instances for software vulnerabilities automatically in a periodic fashion.

Automate security assessments

Inspect running operating systems (OS) against known vulnerabilities

Analyze against unintended network accessibility

Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Inspector automatically assesses applications for vulnerabilities or deviations from best practices. Inspector uses an agent installed on EC2 instances.

- Amazon Inspector uses AWS Systems Manager (SSM) and the SSM Agent to collect information about the software application inventory of the EC2 instances. This data is then scanned by Amazon Inspector for software vulnerabilities
- Amazon Inspector also integrates with other AWS services, such as Amazon EventBridge and AWS Security Hub, to automate discovery, expedite vulnerability routing, and shorten mean time to remediate (MTTR) vulnerabilities

- **AWS WAF** - Web Application Firewall, OWASP (Open Web Application Security Project) Web traffic filtering : block attacks
    - Filter traffic based on IP addresses, geo locations, HTTP headers and body (block attacks from specific user-agents, bad bots, or content scrapers)
    - Is paired with CloudFront and API gateway

    - WAF can assist with protecting a website that is hosted outside of AWS?
- **IAM Roles**: Temporary identities
    - Does NOT have credentials attached
    - (Advantage) Expire after a set period of time
    - Used to give access to federated users or EC2 instances
- **Shared Responsibility (security pillar)**
    - Patch Management: AWS (Infrastructure Patches), Customer (Guest OS Patches and Software Patches)
    - Configuration Management: AWS (Infrastructure), Customer (Guest OS, databases, and applications)
    - Awareness & Training
    - Customer Responsiblity
    - Controls based on the applications deployed to AWS
    - Data Security Requirements
    - Inherited Controls (Customer fully inherits from AWS): Physical and Environmental controls

  both responsibilites: shared controls:

  Configuration management

  Operating system (OS) configuration

  Customer responsibility:

  As a customer on AWS you take responsibility for encrypting data. This includes encrypting data at rest and data in transit. It's also a customer's responsibility to properly train their staff in security best practices and procedures for the AWS services they use.

  As a customer on AWS you take responsibility for encrypting data. This includes encrypting data at rest and data in transit. (**Setting up server-side encryption on an Amazon S3 bucket)**

  Another security responsibility the customer owns is setting network and firewall configurations. For instance, you must configure Network ACLs and Security Groups and any operating system-level firewalls on your EC2 instances.

  Customers are responsible for networking traffic protection

- **Principal element** specifies the user, account, service, or other entity that is allowed or denied access to a resource. The bucket policy below has a Principal element set to * which is a wildcard meaning any user. To grant access to a specific IAM user the following format can be used:
    - "Principal":{"AWS":"arn:aws:iam::AWSACCOUNTNUMBER:user/username"}

Cost Management

- **Tools estimate the cost of your architecture solution :**
    - AWS Pricing Calculator (NEW)
    - AWS Simple Monthly Calculator (OLD) shows you how much you would pay in AWS if you move your resources.
    - TCO - Total Cost of Ownership Calculator (OLD) - Compare Cost of running applications in AWS vs On Premise

  The TCO calculator asks for the number of servers (Physical or VMs) you are running on-premises. You also need to supply the resource information (CPU, RAM) and specify whether the server is a DB or non-DB.

  Use this new calculator to compare the cost of your applications in an on-premises or traditional hosting environment to AWS. Describe your on-premises or hosting environment configuration to produce a detailed cost comparison with AWS.

    - AWS Pricing Calculator can provide cost estimations for AWS services based on the data that we input.
- **Cost allocation tags** can be used to tag and categorize your resources and then run view the billing in Cost Explorer and the cost allocation report. For example you can tag your resources by department or project and then view costs attributed to the resources used by those groups.
- You can use ***resource groups*** to organize your AWS resources. Resource groups make it easier to manage and automate tasks on large numbers of resources at one time.
- **Resource-level cost breakdown**: Cost allocation tags are key-value pairs that users can attach to AWS resources to organize and track their AWS costs. Users can use cost allocation tags to filter and group their AWS costs by categories such as project, department, environment, or application. Users can also use cost allocation tags to generate detailed billing reports that show the costs associated with each tag
- **Account-level cost separation**: A company wants to launch multiple workloads on AWS. Each workload is related to a different business unit. The company wants to separate and track costs for each business unit. Use AWS Organizations and create one account for each business unit.
- Create tags by department on the instances and then run a cost allocation report.A company uses Amazon EC2 instances to run applications that are dedicated to different departments. The company needs to break out the costs of these applications and allocate them to the relevant department. The EC2 instances run in a single VPC.

Scalability & Resilience

- **Maintain Redundancy**
    - If you need 10 instances to handle the load, typically you will have a few more instances running. These instances are called Redundant instances. Even if one or two instances fail, the performance of the application will not get affected.
- **With Vertical Scaling** we add resources to our instance as the workload grows." This is vertical scaling — you're adding resources to a single instance, not adding more instances

- **Loose coupling** is when you break systems down into smaller components that are loosely coupled together. This reduces interdependencies between systems components. This is achieved in the cloud using messages buses, notification and messaging services.
- **Removing single points of failure** ensures fault tolerance and high availability. This is easily achieved in the cloud as the architecture and features of the cloud support the implementation of highly available and fault tolerant systems.

Messaging & Integration

- **Amazon SNS** is well suited to send data to multiple recipients and can send App to App and App to People messages.(We have a diagnostic application that sends application data to a machine learning tool, a parts ordering department and diagnostic information to the customer via e-mail. Which AWS Service can help us manage these integrations)
- **Amazon MSK (Managed Streaming for Kafka)** is the correct choice as it is a fully managed service that facilitates building and running applications built on Apache Kafka without having to manage the underlying infrastructure. It would allow the financial services firm to focus on building their analytics platform without being concerned about Kafka's infrastructure management, hence reducing the operational overhead.

Customer Engagement

- **Amazon Connect** is a customer experience solution which allows us to manage things like chat bots, Interactive Voice Response (IVR), customer service workflows and incoming customer calls.

AWS Cloud Adoption Framework (CAF)

- Think of AWS CAF as: A cloud strategy playbook for new clouders
- Business risk reduction is an essential aspect of the AWS Cloud Adoption Framework, focusing on minimizing potential threats and vulnerabilities during the cloud migration process, and safeguarding organizational assets.
- The AWS CAF helps us :
  - prepare for a migration into AWS.
  - gauge & improve cloud readiness in preparation to migrate into AWS
  - Organizational alignment
  - Organization design
  - CAF framework
- AWS CAF does not focus on operational support for existing workloads on AWS.

Chief Information Officers (CIOs) and **IT Architects** are primary stakeholders involved in the process

- **The Operations perspective** (foundational capabilities) helps you monitor and manage your cloud workloads to ensure that they are delivered at a level that meets your business needs.Common stakeholders include chief operations officer (COO), cloud director, cloud operations manager, and cloud operations engineers1.The Operations perspective covers capabilities such as workload health monitoring, incident management, change management, release management, configuration management, and disaster recovery2.
- **The Business perspective** helps ensure that your cloud investments accelerate your digital transformation ambitions and business outcomes. Common stakeholders include chief executive officer (CEO), chief financial officer (CFO), chief information officer (CIO), and chief technology officer (CTO).The Business perspective covers capabilities such as business case development, value realization, portfolio management, and stakeholder management
- **The Governance perspective:**
  - governance framework, budget and cost management(Benefits management)
  - compliance management
  - data governance
- **The Platform perspective** (**Chief Technology Officer (CTO) , data engineers)**helps you build an enterprise-grade, scalable, hybrid cloud platform, modernize existing workloads, and implement new cloud-native solutions.
  - It covers capabilities such as platform design and implementation, workload migration and modernization, cloud-native development, and DevOps, data engineering
  - includes a capability for well-designed data and analytics architecture. This capability helps you design, implement, and optimize your data and analytics solutions on AWS, using services such as Amazon S3, Amazon Redshift, Amazon EMR, Amazon Kinesis, Amazon Athena, and Amazon QuickSight.
- **(AWS CAF) cloud transformation journey** is a four-phase process that helps customers plan and execute their cloud migration and digital transformation.
  - **Envision phase**: This phase focuses on demonstrating how cloud will help accelerate the business outcomes of the customer. It involves identifying and prioritizing transformation opportunities across four domains: business, people, governance, and platform. It also involves associating the transformation initiatives with key stakeholders and measurable business outcomes
  - **Align phase**: This phase focuses on identifying capability gaps across six perspectives: business, people, governance, platform, security, and operations. It also involves identifying crossorganizational dependencies and surfacing stakeholder concerns and challenges. The goal of this phase is to create strategies for improving the cloud readiness, ensure stakeholder alignment, and facilitate relevant organizational change management activities
  - **Launch phase**: This phase focuses on delivering pilot initiatives in production and demonstrating incremental business value. Pilots should be highly impactful and influence future direction. The customer should learn from the pilots and adjust their approach before scaling to full production
  - **Scale phase**: This phase focuses on expanding production pilots and business value to the desired scale and ensuring that the business benefits associated with the cloud investments are realized and sustained1.

Glaciers options:

Service	Expedited	Standard	Bulk
Amazon S3 Glacier	1–5 minutes	3–5 hours	5–12 hours

User data:

When you launch an instance in Amazon EC2, you have the option of passing user data to the instance that can be used to perform common automated configuration tasks and even run scripts after the instance starts.

You can pass two types of user data to Amazon EC2: shell scripts and cloud-init directives. User data is data that is supplied by the user at instance launch in the form of a script. User data is limited to 16KB. User data and meta data are not encrypted.

Amazon Elasticsearch Service is involved with operational analytics such as application monitoring, log analytics and clickstream analytics. Amazon Elasticsearch Service allows you to search, explore, filter, aggregate, and visualize your data in near real-time.

RDS scaling:

To handle a higher load in your database, you can vertically scale up your master database with a simple push of a button. There are currently over 18 instance sizes that you can choose from when resizing your RDS MySQL, PostgreSQL, MariaDB, Oracle, or Microsoft SQL Server instance.

For Amazon Aurora, you have 5 memory-optimized instance sizes to choose from. The wide selection of instance types allows you to choose the best resource and cost for your database server.

In addition to scaling your master database vertically, you can also improve the performance of a read-heavy database by using read replicas to horizontally scale your database. RDS MySQL, PostgreSQL, and MariaDB can have up to 5 read replicas, and Amazon Aurora can have up to 15 read replicas.

CORRECT: "You can scale up by moving to a larger instance size" is a correct answer.

CORRECT: "You can scale up by increasing storage capacity" is also a correct answer.

Which type of Amazon RDS automated backup allows you to restore the database with a granularity of as little as 5 minutes?

Point-in-time recovery

Where are Amazon EBS snapshots stored on S3

When you restore a DB instance to a point in time, you can choose the default virtual private cloud (VPC) security group. Or you can apply a custom VPC security group to your DB instance.

Restored DB instances are automatically associated with the default DB parameter and option groups. However, you can apply a custom parameter group and option group by specifying them during a restore.

If the source DB instance has resource tags, RDS adds the latest tags to the restored DB instance.

RDS uploads transaction logs for DB instances to Amazon S3 every five minutes. To see the latest restorable time for a DB instance, use the AWS CLI describe-db-instances command and look at the value returned in the `LatestRestorableTime` field for the DB instance. To see the latest restorable time for each DB instance in the Amazon RDS console, choose **Automated backups**.

Elastic IP addresses are for use in a specific region only and can therefore only be remapped between instances within that region. You can use Elastic IP addresses to mask the failure of an instance in one **Availability Zon**e by rapidly remapping the address to an instance in another Availability Zone.

Each subnet in a VPC is mapped to all AZs in the region

Which AWS program can help an organization to design, build, and manage their workloads on AWS? **APN Consulting Partners**

APN Consulting Partners are professional services firms that help customers of all sizes design, architect, build, migrate, and manage their workloads and applications on AWS. Consulting Partners include System Integrators (SIs), Strategic Consultancies, Agencies, Managed Service Providers (MSPs), and Value-Added Resellers (VARs).

Which AWS service provides fully managed third-party file systems, with native compatibility and a rich feature set, to be used with a broad range of AWS services?

Amazon FSx is the correct answer because it offers fully managed third-party file systems, including Windows File Server and Lustre, giving users native compatibility and a feature-rich experience, thereby facilitating the use of these file systems with a wide variety of AWS services.

AWS Firewall Manager allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organization, helping to set up AWS WAF, AWS Shield Advanced, and **AWS Network Firewall** rules. AWS Network Firewall is a managed service that makes it easy to deploy essential network protections for all your Amazon VPCs.

A cloud practitioner needs to decrease application latency and increase performance for globally distributed users: S3 and CloudFront

Which type of EBS volumes can be encrypted? **Both non-root and root volumes**

Amazon EBS encryption offers a straight-forward encryption solution for your EBS resources that doesn't require you to build, maintain, and secure your own key management infrastructure. It uses AWS Key Management Service (AWS KMS) customer master keys (CMK) when creating encrypted volumes and snapshots.

Encryption operations occur on the servers that host EC2 instances, ensuring the security of both data-at-rest and data-in-transit between an instance and its attached EBS storage.

All volumes can now be encrypted at launch time and it’s possible to set this as the default setting.

ELB adventages :

High availability – ELB automatically distributes traffic across multiple EC2 instances in different AZs within a region.

Elasticity – ELB is capable of handling rapid changes in network traffic patterns.

What are the benefits of using IAM roles for applications that run on EC2 instances

It is easier to manage IAM roles

More secure than storing access keys within applications

AWS Resource Access Manager (AWS RAM) is designed to enable you to securely share your AWS resources with any AWS account or, if you are part of AWS Organizations, with Organizational Units (OUs) or within your organization, reducing overheads and centralizing access management to shared resources.

Internet gateway & VPC :

An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic.

An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

You cannot use the Internet Gateway for making VPN connections to a VPC, you need a Virtual Private Gateway for this purpose.

CAPEX = Big upfront investment to own something long-term.

A company wants to utilize a pay as you go cloud model for all of their applications without CAPEX costs and which is highly elastic. Which cloud delivery model will suit them best?

The public cloud is offered under a purely pay as you go model (unless you choose to reserve), and allows companies to completely avoid CAPEX costs. The public cloud is also highly elastic so companies can grow and shrink the applications as demand changes.

Private and on-premise clouds are essentially the same, though both could be managed by a third party and even could be delivered under an OPEX model by some vendors. However, they are typically more CAPEX heavy and the elasticity is limited.

A hybrid model combines public and private and this company wants to go all in on a single model.

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 is aggregated in the cloud, providers such as AWS can achieve higher economies of scale, which translates into lower pay as-you-go prices

Quick Starts are built by AWS solutions architects and partners to help you deploy popular technologies on AWS

AWS Elastic Disaster Recovery is the correct choice because it enables businesses to recover applications, whether they are based on premises or on the cloud, quickly and reliably while utilizing economical storage and minimum compute resources. It is designed to minimize downtime and data loss, thus aiding in disaster recovery strategies.

Which of the following are advantages of using the AWS cloud computing over legacy IT?

You can bring new applications to market faster

You don't need to worry about over provisioning as you can elastically scale

Amazon Route 53 health checks monitor the health and performance of your web applications, web servers, and other resources.

To make the deployment highly available the user should launch the instances across multiple Availability Zones in a single AWS Region. Elastic Load Balancers can only serve targets in a single Region so it is not possible to deploy across Regions.

AWS WAF can be used to protect on-premises resources if they are deployed behind an Application Load Balancer (ALB). In this scenario the on-premises website servers are added to a target group by IP address. The ALB has a WAF WebACL attached to it and distributes connections to the on-premises website.

With AWS managed services you can reduce your time spent performing common IT tasks. With services such as Amazon RDS, AWS will patch the database host operating system and database software and perform patch management activities.(**Taking a backup of a database , Patching database software)**

You can run **Amazon EC2** compute instances hosted on a Snowball Edge with the sbe1, sbe-c, and sbe-g instance types. The sbe1 instance type works on devices with the Snowball Edge Storage Optimized option. The sbe-c instance type works on devices with the Snowball Edge Compute Optimized option. Both the sbe-c and sbe-g instance types work on devices with the Snowball Edge Compute Optimized with GPU option.

What can be used to allow an application running on an Amazon EC2 instance to securely store data in an Amazon S3 bucket without using long-term credentials? IAM roles (temporate)

AWS are able to continue to reduce their pricing due to: **Economies of scale**

Cost optimization can include using Auto Scaling groups to scale the number of EC2 instances according to actual demand. Also, using Amazon EC2 reserved instances for suitable workloads is a good way of optimizing costs over the longer term.

AWS **OpsWorks** is a configuration management service that provides managed instances of **Chef and Puppet.** Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers.

AWS Activate for Startups is specially designed to provide startups with the low-cost, easy-to-use infrastructure needed to scale and grow. It offers a host of benefits including AWS credits, training, technical support, and other resources which can aid startups in building their business successfully.

AWS IQ help customers find AWS certified third-party experts for on-demand help. Through AWS IQ, business owners can find, communicate with, and hire AWS experts quickly and securely to help them implement AWS solutions and projects, making it the best fit for the scenario described.

How can an organization track resource inventory and configuration history for the purpose of security and regulatory compliance?

Configure AWS Config with the resource types

Amazon EC2 Auto Scaling launches and terminates instances as demand changes. This helps with resiliency and high availability as it can also be set to ensure a minimum number of instances are always available.

AWS AppSync and AWS Amplify both services facilitate the building of secure and scalable mobile and web applications. AWS AppSync enables the creation of flexible APIs, including options for real-time updates and offline functionalities. AWS Amplify is a set of tools and services that can be used to build scalable full-stack apps powered by AWS, also supporting real-time functionalities and offline operations.

Are there any AWS services or features that will identify and search for externally shared AWS resources? **AWS IAM Access Analyzer.**

Access Analyzer helps you identify the resources in your organization and accounts, such as Amazon S3 buckets or IAM roles, shared with an external entity. This lets you identify unintended access to your resources and data, which is a security risk.

Which AWS tools can be used for automation

AWS CloudFormation

AWS Elastic Beanstalk

Reservations provide you with greater discounts, up to 75%, by paying for capacity ahead of time. Some of the services you can reserve include: EC2, DynamoDB, ElastiCache, RDS, and RedShift.

NOOOOO S3, not ok to be reserved

Edge Locations are parts of the Amazon CloudFront content delivery network (CDN) that are all around the world and are used to get content closer to end-users for better performance.

AWS Shield which protects against Distributed Denial of Service (DDoS) attacks is available globally on Amazon CloudFront Edge Locations.

With AWS Snowmobile you can move 100PB per snowmobile. AWS call this an **"Exabyte-scale d**ata transfer service".

Access to the ports on an Amazon EC2 instance is controlled through security groups. AWS Trusted Advisor scans the security groups in your account to see if any security groups allow unrestricted access to any ports. This information is then presented to you in the console and you can then act on this information to secure the ports through editing the rules in the security group.

Amazon **MemoryDB** for Redis is the correct answer because it is a Redis-compatible, in-memory database service built on Redis architecture, which offers sub-millisecond latency, fulfilling the requirements mentioned in the question.

With IAM Roles you can delegate permissions to resources for users and services without using permanent credentials (e.g. username and password). To do so you can create a role and assign an IAM policy to the role that has the permissions required.

You don't apply the policy to the service, you apply it to the role. The role is then used to assign permissions to the AWS service.

Only the Enterprise Support plan gets a Technical Account Manager (TAM).

You do not get an AWS Solutions Architect with any plan.

Cloud Support Associates are provided in the Developer plan.

An organization moves a workload to Amazon EC2 instances on AWS. Cost-effectiveness is the key to running the workload properly in the Cloud.

Rightsize all the EC2 instances that are used in the deployment

✅ IAM Groups:

- An **IAM Group** is a collection of **IAM users**.
- You **attach policies (permissions)** to the group.
- All users in that group **inherit those permissions** automatically.
- Makes it easy to **manage permissions for multiple users** together.

Example:

Create a group called `Developers` and attach a policy that allows S3 and EC2 access. Every user added to the group will now have S3 and EC2 permissions—no need to assign policies individually.

🚫 IAM Roles:

- IAM Roles are **not intended for groups of users**.
- A **role is assumed temporarily** by an entity (user, service, application).
- Used for:
  - **Cross-account access**
  - **EC2 or Lambda assuming roles**
  - **Temporary access for federated users (e.g., SSO)**

Roles are
not "assigned" to multiple users for daily permissions the way groups are.

AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources.

Which service allows an organization to view operational data from multiple AWS services through a unified user interface and automate operational tasks?

AWS Systems Manager

An organization is considering implementing a new workload in the AWS Cloud. However, the company first wants to forecast costs.

Which tool should the company use to estimate the cost of the workload?

AWS Pricing Calculator.

AWS Pricing Calculator is a web-based planning tool that you can use to create estimates for your AWS use cases. You can use it to model your solutions before building them, explore the AWS service price points, and review the calculations behind your estimates. You can use it to help you plan how you spend, find cost saving opportunities, and make informed decisions when using Amazon Web Services.

Amazon S3 is the only service out of the answers which can be used for backup and restore, data lakes and archival solutions. Because S3 is an object storage service, there are lots of different use cases.

Direct connect

AWS Transit Gateway connects your Amazon Virtual Private Clouds (VPCs) and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once.

As you expand globally, inter-Region peering connects AWS Transit Gateways together using the AWS global network. Your data is automatically encrypted and never travels over the public internet.

AWS Organizations offers Service control policies (SCPs) which are a type of organization policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions (API actions) for all accounts in your organization. SCPs help you to ensure your accounts stay within your organization's access control guidelines. SCPs are available only in an organization that has all features enabled.

Volume discounts for Amazon EC2 and Amazon S3 aggregated across the member AWS accounts

Share the reserved Amazon EC2 instances amongst the member AWS accounts

CloudWatch Logs Insights enables you to interactively search and analyze your log data in Amazon CloudWatch Logs. You can perform queries to help you more efficiently and effectively respond to operational issues. If an issue occurs, you can use CloudWatch Logs Insights to identify potential causes and validate deployed fixes.

Amazon FSx for Windows File Server provides fully managed Microsoft Windows file servers, backed by a fully native Windows file system. Amazon FSx supports a broad set of enterprise Windows workloads with fully managed file storage built on Microsoft Windows Server. Amazon FSx has native support for Windows file system features and for the industry-standard Server Message Block (SMB) protocol to access file storage over a network.

AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for the following eight services:

- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers.
- Amazon RDS.
- Amazon CloudFront.
- Amazon Aurora.
- Amazon API Gateways.
- AWS Lambda and Lambda Edge functions.
- Amazon LightSail resources.
- Amazon Elastic Beanstalk environments.

You can monitor your estimated AWS charges by using Amazon CloudWatch. When you enable the monitoring of estimated charges for your AWS account, the estimated charges are calculated and sent several times daily to CloudWatch as metric data.

Included as part of the Enterprise Support plan, the Support Concierge Team are AWS billing and account experts that specialize in working with enterprise accounts. The Technical Account Manager provides expert monitoring and optimization for your environment and coordinates access to other programs and experts.

Amazon SageMaker is a managed Machine Learning service. With Amazon SageMaker, you can package your own algorithms that can then be trained and deployed in the SageMaker environment.

AWS Data Pipeline is a web service that helps you reliably process and move data between different AWS compute and storage services, as well as on-premises data sources, at specified intervals. It does not use Machine Learning.

AWS Audit Manage assists organizations in continuously auditing their AWS usage, facilitating risk assessment and compliance with various regulations and industry standards. It automates evidence collection to make the audit process more efficient and effective. "AWS Artifact" is incorrect as it is more about providing on-demand access to AWS' security and compliance reports and select online agreements, rather than helping in the continuous auditing of AWS usage considering risk and compliance assessments.

AWS PrivateLink provides private connectivity between VPCs, AWS services, and your on-premises networks, without exposing your traffic to the public internet.

The AWS Health API is available to all Business, Enterprise On-Ramp, or Enterprise Support customers. You can use the API operations to get information about events that might affect your AWS services and resources.

AWS technical account manager (TAM)” and AWS Support concierge are in entreprise plan.

You rent the hardware: Amazon EC2 Dedicated Hosts allow you to use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2, so that you get the flexibility and cost effectiveness of using your own licenses, but with the resiliency, simplicity and elasticity of AWS. An Amazon EC2 Dedicated Host is a physical server fully dedicated for your use, so you can help address corporate compliance requirements.

AWS Application Discovery Service helps you plan your migration to the AWS cloud by collecting usage and configuration data about your on-premises servers.

(for migration from on premises) AWS Managed Services (AMS) helps you adopt AWS at scale and operate more efficiently and securely. We leverage standard AWS services and offer guidance and execution of operational best practices with specialized automations, skills, and experience that are contextual to your environment and applications. You can easily leave a lot of the heavy lifting to AWS when you are using managed services.

AWS Enterprise Support is a support plan which provides a less than 15 minutes response time for business-critical system failure, and AWS Enterprise On-Ramp provides a less than 30 minutes response time for business-critical system failure.

AWS Launch Wizard offers a guided way of sizing, configuring, and deploying AWS resources for third-party applications, such as SQL Server Always On and SAP, without needing to manually identify and provision individual AWS resources.

AWS Compute Optimizer (AI) leverages machine learning to analyze the historical usage patterns of your workloads, helping you to identify the most optimal AWS resources, reducing costs, and enhancing performance.

The Business support plan provides a service level agreement (SLA) of < 1 hour for production system down support cases.

AWS Direct Connect is a low-latency, high-bandwidth, private connection to AWS. This can be used to create a private hybrid cloud connection between on-premises and the AWS Cloud.(An organization has an on-premises cloud and accesses their AWS Cloud over the Internet. How can they create a private hybrid cloud connection that avoids the internet)

AWS organizations allow you to consolidate multiple AWS accounts into an organization that you create and centrally manage. Unused reserved instances (RIs) for EC2 are applied across the group so the organization can utilize their unused reserved instance instead of consuming on-demand instances which will lower their costs.

In IAM, a user can be a member of multiple groups. One IAM user can be a part of a maximum of 5 groups. Also Groups are a flat hierarchy of users with similar permissions, and you cannot place a group within another group.

is that possible to have conflits ?

AWS Service Catalog is a service that allows you to create and manage catalogs of IT services that are approved for use on AWS. You can use AWS Service Catalog to centrally manage commonly deployed IT services and help your organization achieve consistent governance and meet your compliance requirements, while enabling users to quickly deploy only the approved IT services they need1. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS software development kits (SDKs) are tools that enable you to easily integrate your applications with AWS services using your preferred programming language. AWS AppSync is a service that simplifies application development by letting you create a flexible

API to securely access, manipulate, and combine data from one or more data sources. None of these services can help you limit your employees' AWS access to a portfolio of predefined AWS resources.

AWS Identity and Access Management (IAM) access advisor

IAM Access advisor shows the service permissions granted to a user and when those services were last accessed. You can use this information to revise your policies. To summarize, you can identify unnecessary permissions so that you can revise your IAM policies accordingly.

Which AWS tool/service will help you define your cloud infrastructure using popular programming languages such as Python and JavaScript? **AWS Cloud Development Kit (AWS CDK)**

Amazon CodeGuru is a developer tool that provides intelligent recommendations to improve code quality and identify an application's most expensive lines of code. Integrate Amazon CodeGuru into your existing software development workflow to automate code reviews during application development, continuously monitor application performance in production, provide recommendations and visual clues for improving code quality and application performance, and reduce overall cost.

AWS Fault Injection Simulator (AWS FIS)

AWS Fault Injection Simulator (AWS FIS) is a fully managed service for running fault injection experiments on AWS that makes it easier to improve an application's performance, observability, and resiliency. Fault injection experiments are used in chaos engineering, which is the practice of stressing an application in testing or production environments by creating disruptive events, such as a sudden increase in CPU or memory consumption, observing how the system responds, and implementing improvements. Fault injection experiment helps teams create the real-world conditions needed to uncover the hidden bugs, and monitor blind spots, and performance bottlenecks that are difficult to find in distributed systems.

AWS Fault Injection Simulator (AWS FIS) simplifies the process of setting up and running controlled fault injection experiments across a range of AWS services so teams can build confidence in their application behavior. With AWS Fault Injection Simulator (AWS FIS), teams can quickly set up experiments using pre-built templates that generate the desired disruptions. AWS Fault Injection Simulator (AWS FIS) provides the controls and guardrails that teams need to run experiments in production, such as automatically rolling back or stopping the experiment if specific conditions are met. With a few clicks in the console, teams can run complex scenarios with common distributed system failures happening in parallel or building sequentially over time, enabling them to create the real-world conditions necessary to find hidden weaknesses.

Route 53

Health checks and monitoring

Domain registration

Which AWS service can be used to subscribe to an RSS feed to be notified of the status of all AWS service interruptions?

AWS Health Dashboard - Service Health

Total Cost of Ownership (TCO) estimate?

Server administration

Power/Cooling

VPC's in a same region , can not cross region

Amazon EBS Elastic Volumes are bound to a specific Availability Zone (AZ)

Amazon EBS Elastic Volumes can be mounted to one instance at a time

Amazon EBS Elastic Volumes can persist data after their termination

AWS IAM Identity Center is the successor to AWS Single Sign-On (AWS SSO). It is built on top of AWS Identity and Access Management (IAM) to simplify access management to multiple AWS accounts, AWS applications, and other SAML-enabled cloud applications. In IAM Identity Center, you create or connect, your workforce users for use across AWS. You can choose to manage access just to your AWS accounts, just to your cloud applications, or to both.

A Cloud Practitioner would like to get operational insights of its resources to quickly identify any issues that might impact applications using those resources. Which AWS service can help with this task?

AWS Systems Manager allows you to centralize operational data from multiple AWS services and automate tasks across your AWS resources. You can create logical groups of resources such as applications, different layers of an application stack, or production versus development environments.

With AWS Systems Manager, you can select a resource group and view its recent API activity, resource configuration changes, related notifications, operational alerts, software inventory, and patch compliance status. You can also take action on each resource group depending on your operational needs. AWS Systems Manager provides a central place to view and manage your AWS resources, so you can have complete visibility and control over your operations.

Purchase convertible reserved instance (RI) if you need additional flexibility, such as the ability to use different instance families, operating systems, or tenancies over the reserved instance (RI) term. Convertible reserved instance (RI) provides you with a significant discount (up to 54%) compared to an on-demand instance and can be purchased for a 1-year or 3-year term.

Convertible reserved instance (RI) can be useful when workloads are likely to change. In this case, a convertible reserved instance (RI) enables you to adapt as needs evolve while still obtaining discounts and capacity reservation.

(estimation no recommendations) AWS Pricing Calculator - AWS Pricing Calculator lets you explore AWS services, and create an estimate for the cost of your use cases on AWS. It does not provide Savings Plan recommendations. (A startup wants to set up its IT infrastructure on AWS Cloud. The CTO would like to get an estimate of the monthly AWS bill based on the AWS services that the startup wants to use. As a Cloud Practitioner, which AWS service would you suggest for this use-case?)

AWS Cost Explorer(forcast) lets you explore your AWS costs and usage at both a high level and at a detailed level of analysis and empowers you to dive deeper using several filtering dimensions (e.g., AWS Service, AWS Region, Linked Account, etc.). AWS Cost Explorer also gives you access to a set of default reports to help you get started, while also allowing you to create custom reports from scratch.

(free) AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your website or applications. While AWS Shield Standard helps protect all AWS customers, you get better protection if you are using Amazon CloudFront and Amazon Route 53. All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge.

run above:

EC2

Amazon CloudFront

protecting:

Amazon Route 53

AWS Global Accelerator

A financial services company wants to ensure that its AWS account activity meets the governance, compliance and auditing norms. As a Cloud Practitioner, which AWS service would you recommend for this use-case? cloudtrail

Partial upfront payment option with standard 3-years term is cheapest

Amazon S3 and Amazon DynamoDB support **VPC gateway endpoint.** All other services that support VPC Endpoints use a VPC interface endpoint (note that Amazon S3 supports the VPC interface endpoint as well).

There are three fundamental drivers of cost with AWS: compute, storage, and outbound data transfer. In most cases, there is no charge for inbound data transfer or data transfer between other AWS services within the same region.

Outbound data transfer is aggregated across services and then charged at the outbound data transfer rate.

Per AWS pricing, data transfer between S3 and EC2 instances within the same region is not charged

A company runs an application on a fleet of EC2 instances. The company wants to automate the traditional maintenance job of running timely assessments and checking for OS vulnerabilities? **Amazon Inspector**

can be reserved:

Amazon Elastic Compute Cloud (Amazon EC2)

Amazon DynamoDB

Amazon Relational Database Service (Amazon RDS)

Fault tolerance is achieved by a scale up operation : Wrong !

Which of the following AWS services should be used to automatically **distribute** incoming traffic **across multiple targets**? ELB

DynamoDB global tables replicate data automatically across your choice of AWS Regions and automatically scale capacity to accommodate your workloads. With global tables, your globally distributed applications can access data locally in the selected regions to get single-digit millisecond read and write performance. DynamoDB offers active-active cross-region support that is needed for the company.

You can use Amazon Transcribe to add speech-to-text capability

, Amazon S3 Object Lambda Access Point

- **AWS Single Sign-On (SSO) / AWS IAM Identity Center:** Centralized access management to AWS accounts and cloud applications.

4. Specific Management & Governance Tools (Beyond CloudWatch, CloudTrail, Config):

- **AWS Systems Manager:** Collection of capabilities to help manage and automate operational tasks across your AWS resources (e.g., patching, run commands, inventory).
- **AWS Organizations:** Centralized management for multiple AWS accounts, including consolidated billing and policy application.
- **AWS Control Tower:** Sets up and governs a secure, multi-account AWS environment.
- **AWS Service Catalog:** Create and manage catalogs of IT services that are approved for use on AWS.

- **AWS Compute Optimizer:** Recommends optimal AWS resources for your workloads to reduce costs and improve performance.

Each AWS Region consists of a minimum of three Availability Zones (AZ)

Each Availability Zone (AZ) consists of one or more discrete data centers

There is a one-minute minimum charge for Linux based EC2 instances

The AWS account must be able to operate as a standalone account. Only then it can be removed from AWS organizations

Service and Communications Protection or Zone Security - Customers are responsible for Service and Communications Protection or Zone Security which may require the customers to route or zone data within specific security environments.

Which AWS Support plan provides architectural guidance contextual to your specific use-cases?

AWS Business Support

Which of the following AWS authentication mechanisms supports an AWS Multi-Factor Authentication (AWS MFA) device that you can plug into a USB port on your computer?

U2F security key

AWS CodeDeploy is a service that automates application deployments to a variety of compute services including Amazon EC2, AWS Fargate, AWS Lambda, and on-premises instances. CodeDeploy fully automates your application deployments eliminating the need for manual operations. CodeDeploy protects your application from downtime during deployments through rolling updates and deployment health tracking.