cloud is a combination of networks,hardware,services,storage,and interfaces that helps in delivering computing as a servicve

AWS CAF : AWS Cloud Adoption Framework

->The AWS Cloud Adoption Framework (AWS CAF) helps organizations develop efficient and effective plans for their cloud adoption journey. The guidance and best practices that the framework provides help you build a comprehensive approach to cloud computing across your organization, and throughout your IT lifecycle.

-> The AWS CAF breaks down the complex process of planning a move to the cloud into manageable pieces that are called perspectives. Perspectives represent essential areas of focus that span people, processes, and technology. Capabilities within each perspective identify which areas of your organization require attention. From that, actions are organized into prescriptive work streams that support a successful cloud journey

-> At the highest level, the AWS CAF organizes guidance into six areas of focus, called perspectives. Each perspective covers distinct responsibilities that functionally related stakeholders own or manage. In general, the Business, People, and Governance Perspectives focus on business capabilities. The Platform, Security, and Operations Perspectives focus on technical capabilities.

AWS WAF : AWS well Architected Framework

-> AWS WAF describes key concept , design principles , architectural best practices for designing and runing workload on AWS.

-> AWS WAF have 5 pillars:

-> AWS Well-Architected Framework helps you design of your architecture from five different perspectives, or pillars. The pillars are Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization, sustainiability.

Security needs to be applied at all network layers, like edge of network, VPC, all instances & application with the VPC. Applying Security controls at the edge of the network is not an efficient security control & against security design principles.

As per AWS Well-Architected Framework, the following are the design principles for security in the cloud:

- Implement a strong identity foundation.
- Enable traceability.
- Apply security at all layers.
- Automate security best practices.
- Protect data in transit and at rest.
- Keep people away from data.
- Prepare for security events.

IAM :- -> Identity and Access Management.

-> IAM allow you to manage users and their access to the AWS console.

-> it create the user , permissions , and roles.

-> Use IAM to configure AUTHENTICATION , which is the first step, because it controls who can access AWS resources.

-> IAM is used to configure authorization, which is based on knowing who the user is. Authoriza tion controls what resources users can access and what they can do to or with those resources.

-> IDENTITY: create to provide authentication to people and processes in your account.
-> 3 identities r there: Users, groups , roles.

AWS Systems Manager is a management service that helps a user: • Collect software inventory. • Apply operating system (OS) patches. • Create system images. • Configure Microsoft Windows and Linux operating systems.
Systems Manager is designed to be highly automation-focused, which enables the configuration and management of systems that run on-premises or in AWS. With Systems Manager, a user can select the instances that they want to manage, and define the management tasks that they want to perform.
Systems Manager offers many features and benefits that systems operations (SysOps) specialists should find useful.
Systems Manager enables you to safely automate common and repetitive IT operations and management tasks across AWS resources.
• Systems Manager provides a suite of features that help automate operational tasks across AWS and on-premises resources.

AWS CloudFormation enables you to create, update, and delete AWS infrastructure deployments predictably and repeatedly.

AWS Elastic Beanstalk:- -> its an easy to use service for deploying and scaling the web applications.
-> it reduce the management complexity without any restriction of choice or controls.
-> You simply have to upload your code and elastic beanstalk will handle it automatically.
-> It is an PAAS (Platform as a service)
-> It deploy , manage and scales the web application automatically.
-> Elastic Beanstalk provides all the applications services that you need for your application. You only need to create your code and deploy it. You can use the AWS Management Console, a Git repository, or an integrated development environment (IDE) (such as Apache Eclipse or Microsoft Visual Studio) to upload your application. Then, Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, automatic scaling, and application health monitoring. By using Elastic Beanstalk, you can focus on writing code instead of managing and configuring servers, databases, load balancers, firewalls, and networks. Elastic Beanstalk provisions and operates the infrastructure and manages
Elastic Load Balancing offers three different load balancers: • The Application Load Balancer is best suited for load balancing HTTP and HTTPS traffic. It provides advanced request routing that is targeted at the delivery of modern application architectures, including microservices and containers.
• The Network Load Balancer is best suited for load balancing TCP traffic where extreme performance is required.
• The Classic Load Balancer provides basic load balancing across multiple EC2 instances, and operates at both the request level and the connection level.
the application stack (platform) for you.

ROUTE 53: It is a highly scalable and avavilable DNS web service. It connects user request to internet applications on AWS .
-> its name came from the fact that DNS server respond to queries on port 53.

-> it resolve domain names to IP addresses.

Amazon Route 53 supports seven different routing policies.

1.Simple routing policy: Use for a single resource that performs a given function for your domain—for example, a web server that serves content for the example.com website.

2. Weighted routing policy: Use to route traffic to multiple resources in proportions that you specify.

3. Latency routing policy: Use when you have resources in multiple AWS Regions and you want to route traffic to the Region that provides the lowest latency.

4. Failover routing policy: Use when you want to configure active-passive failover.

5. Geolocation routing policy: Use when you want to route traffic based on the location of your users.

6. Geoproximity routing policy: Use to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another location.

7. Multivalue answer routing policy: Use when you want Route 53 to respond

ELASTIC LOAD BALANCING : It automatically distribute the incoming application traffic across multiple EC2 instance.

-> It detect unhealthy instance so it reroute the traffic to the healthy instance. until the instance restored.

1. Application Load Balancer: Application Load Balancer is best suited for load balancing of HTTP and HTTPS traffic and provides advanced request routing targeted at the delivery of modern application architectures, including microservices and containers. Application Load Balancer routes traffic to targets within Amazon VPC based on the content of the request.

2. Network Load Balancer: Network Load Balancer is best suited for load balancing of Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Transport Layer Security (TLS) traffic where extreme performance is required. Network Load Balancer routes traffic to targets within Amazon VPC and is capable of handling millions of requests per second while maintaining ultra-low latencies.

3. Classic Load balancer - Classic Load Balancer provides basic load balancing across multiple Amazon EC2 instances and operates at both the request level and the connection level. Classic Load Balancer is intended for applications that were built within the EC2-Classic network

ELASTIC LOAD BALANCER LISTENER:

-> Listener : A listener checks for connection requests from clients to an instance by using the protocol and port that you specify.

-> The listener rules that you define also determine how the load balancer routes traffic from connecting clients to one or more targets or target groups.

-> Some Command to use in ELB in AWS CLI:

1. Use the create-load-balancer command to create a load balancer. You must specify two subnets that are not from the same Availability Zone.

2. Use the create-target-group command to create a target group. You must specify the VPC where your EC2 instances are running

3. Use the register-targets command to register your instances with your target group.

4. Use the create-listener command to create a listener for your load balancer. The listener has a default rule that forwards requests to your target group

5. Optionally, verify the health of the registered targets for your target group by using the describe-target-health command.

CLOUDFRONT: Amazon CloudFront is a web service that speeds up the distribution of static and dynamic web content (such as .html, .css, .js, and image files) to users. CloudFront delivers content through a worldwide network of data centers that are called edge locations

-> To deliver content to your users, Amazon CloudFront uses the global network of edge locations for content delivery.

-> CloudFront costs are calculated based on geographic region, number and type of requests, and the amount of data that is transferred out.

AWS LAMBDA: -> AWS Lambda is an event-driven, serverless computing platform provided by Amazon as a part of Amazon Web Services. Therefore, you don’t need to worry about which AWS resources to launch, or how will you manage them. Instead, you need to put the code on Lambda, and it runs.

-> The running time of a Lambda function is limited to a maximum of 15 minutes. In addition, multiple languages are supported.

-> Pay only for the compute time that you consume – you pay nothing when your code is not running.

-> Other Lambda use cases include: •Automated backups,,, Processing objects that are uploaded to Amazon S3,,, Event-driven log analysis ,,,,Event-driven transformations,,,, Internet of Things (IoT)

-.>The diagram shows the process of developing and deploying an AWS Lambda function with dependencies:

1. Define a Lambda handler class in your code. The handler enables you to specify where AWS Lambda can begin running your code. You can learn more about Lambda handlers here: https://docs.aws.amazon.com/lambda/latest/dg/python-handler.html
2. Create your AWS Lambda function. You can think of the function as the code that you want to run. It includes your code, associated configuration information, and resource requirements.
3. Configure access to resources with AWS Identity and Access Management (IAM) and IAM roles. You can use security groups and network access control lists (network ACLs) to provide your functions with access to your resources.
4. Upload your code.
5. Test the function, verify results, and review your logs.
6. Monitor your Lambda functions and reports metrics through Amazon CloudWatch. Examples of what you can track include the number of requests, latency, and the number of requests that result in errors.

->The maximum memory allocation for a single Lambda function is 3 GB.

API: Application Programming Interface

-> Provide programmatic access to an application.

For example, they are often used for programs that communicate with each other.

-> APIs communicate over HTTP. Web-based APIs that adhere to the REST design principles are said to be RESTful. REST is a popular API design that has largely replaced Simple Object Access Protocol (SOAP) as the standard for web services. Next, you explore the REST design principles.

\

Here are some common HTTP status codes:

- 200 – Indicates success. The server received and accepted the request.
- 401 – Indicates a client error, Unauthorized. Authentication is required, but the provided credentials were not accepted, or perhaps no credentials were provided in the request.
- 403 – Indicates a client error, Forbidden. The request was properly made,but the server is not allowing the request.
- 404 – Indicates a client error, Not Found. The resource is unavailable or could not be accessed.

500 – Indicates an unspecific internal server error.

503 – Indicates that the service is temporarily unavailable.

Amazon API GATEWAY : Amazon API Gateway is an Amazon Web Services (AWS) service that enables developers to create, publish, maintain, monitor, and secure application programming interfaces (APIs) at any scale. You can create APIs that access AWS or other web services, and also data that is stored in the AWS Cloud.

CONTAINER in AWS: ->Containers provide a standard way to package your application’s code, configurations, and dependencies into a single object. Containers share an operating system installed on the server and run as resource-isolated processes, ensuring quick, reliable, and consistent deployments, regardless of environment.

->What is containers in cloud?

Containers are packages of software that contain all of the necessary elements to run in any environment. In this way, containers virtualize the operating system and run anywhere, from a private data center to the public cloud or even on a developer’s personal laptop.

DOCKER:- Docker is an operating system for containers. Similar to how a virtual machine virtualizes (removes the need to directly manage) server hardware, containers virtualize the operating system of a server. Docker is installed on each server and provides simple commands you can use to build, start, or stop containers.

-> Docker is an open source containerization platform. It enables developers to package applications into containers

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

-> Kubernetes manages clusters of Amazon Elastic Compute Cloud (EC2) compute instances and runs containers on those instances with processes for deployment, maintenance, and scaling. Using Kubernetes, you can run any type of containerized applications using the same toolset on-premises and in the cloud.

ECR : Amazon Elastic Container Registry (Amazon ECR) is an AWS managed container image registry service that is secure, scalable, and reliable. Amazon ECR supports private repositories with resource-based permissions using AWS IAM.

-> This is so that specified users or Amazon EC2 instances can access your container repositories and images.

ECS :- Amazon Elastic Container Service (ECS) is a cloud-based and fully-managed container orchestration service or container management service . It lets you run your applications in the cloud without having to configure and maintain the infrastructure.

> You can use it to run, stop, and manage containers on a cluster. With Amazon ECS, your containers are defined in a task definition that you use to run an individual task or task within a service.

EKS: Amazon Elastic Kubernetes Service (Amazon EKS) is a managed Kubernetes service that makes it easy for you to run Kubernetes on AWS and on-premises. Kubernetes is an open-source system for automating deployment, scaling, and management of containerized applications.

-> Amazon EKS lets you run your Kubernetes applications on both Amazon Elastic Compute Cloud (Amazon EC2) and AWS Fargate.

AWS FARGATE: - AWS Fargate is a serverless, pay-as-you-go compute engine that lets you focus on building applications without managing servers. AWS Fargate is compatible with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS).

AWS STEP FUNCTION : AWS Step Functions enables you to coordinate AWS services into serverless workflows

- With AWS Step Functions, you define your workflow as a series of steps and transitions between each step, which is known as a state machine.

AMAZON REDSHIFT: Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud.

-> Petabyte: It is a 10^15 bytes of information.

-> Data Warehouse : it is a centralized repository from where we can easily get data at faster pace and organised.

-> Amazon Redshift is a fast and powerful, fully managed data warehouse that is simple and cost effective to set up, use, and scale. It enables you to run complex analytic queries against petabytes of structured data. It uses sophisticated query optimization, columnar storage on high-performance local disks, and massively parallel query execution. Most results come back in seconds.

-> AWS Redshift is a data warehouse product built by Amazon Web Services. \

->It's used for large scale data storage and analysis, and is frequently used to perform large database migration

-> Amazon redshift uses database type: RDBMS (Relational database management service)

AMAZON AURORA: Amazon Aurora is a relational database service provided by Amazon RDS (Relational Database Service).

-> Amazon Aurora is an affordable cloud based relational database compatible with MySQL and PostgreSQL

-> As a part of Amazon RDS, management of an Aurora database is automated. Data is automatically backed up to Amazon S3 (Simple Storage Service). Multiple instances of the data is maintained for availability and failovers.

-> Aurora is made up of clusters

AWS DMS: AWS Database Migration Service (AWS DMS) helps you migrate databases to AWS quickly and securely.

-> The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database.

-> DMS Types:

1. Homogeneous database migration: both source and target are of same or compatible type. Because the schema structure, data types, and database code are compatible between the source and target databases, migration is a one-step process.
2. Heterogeneous database migration: -n heterogeneous database migrations, the source and target databases engines are different. Examples include migrations from Oracle to Amazon Aurora or from Microsoft SQL Server to MySQL.

-> The steps in the process are:

• The first step uses AWS SCT to convert the source schema and code to match the schema and code of the target database.

• The second step uses AWS DMS to migrate data from the source database to the target database.

->The AWS DMS architecture consists of four components.

• Replication instance: An EC2 instance that runs the tasks that the migration process needs.

• Task: The process that performs the work of data migration.

• Source: The endpoint of the source database, which can be running on premises, on Amazon RDS, or on Amazon EC2.

• Target: The endpoint of the target database on AWS.

• AWS DMS and AWS SCT help migrate homogenous and heterogeneous databases from on-premises data centers and cloud instances to AWS.

• Most database migrations involve two steps: converting the schema by using AWS SCT, and migrating the data by using AWS DMS

VPC : Amazon Virtual Private Cloud (Amazon VPC) provides a logically isolated area of the AWS cloud where you can launch AWS resources in a virtual network that you define.

-> A VPC can span multiple Availability Zones, and its key component types include::-

1.• Subnet – Subnets are logical network segments within your VPC. They enable you to subdivide your VPC network into smaller networks inside a single Availability Zone. A subnet is public if it is attached to an internet gateway, or private if it is not. A subnet is required to deploy an instance into a VPC.

2.Security group – A security group is a set of firewall rules that secure instances. They allow or block inbound and outbound traffic into an instance (stateful). If you do not specify a particular group at launch time, an instance is automatically assigned to the default security group for the VPC. A security group is associated with an instance.

3.• Primary network interface (elastic network interface) – An elastic network interface is a virtual network interface (NIC) that connects an instance to a network. Each instance in a VPC has a default network interface, the primary network interface, which cannot be detached from the instance.

4. • Router – A router is a component that routes traffic within the VPC.

5.• Internet gateway – An internet gateway is a VPC component that enables communication between instances in a VPC and the internet.

6.• Virtual private gateway – A virtual private gateway is the component that is defined on the AWS side of a virtual private network (VPN) connection. A VPN connection provides a secure and encrypted tunnel between two network endpoints.

7.• Customer gateway – A customer gateway is a physical device or software application that is defined on the client side of a VPN connection.

CIDR block : The Classless Inter-Domain Routing (CIDR) format is used to specify IP address ranges when you create a VPC or a subnet. It specifies a block (known as a CIDR block) of IP addresses that use the format x.x.x.x/n.

• x.x.x.x is an IP address. An IPv4 IP address is a 32-bit number that is represented as four numbers, which are separated by periods. Therefore, each x is an 8-bit number (a byte) that can have a value in the range 0 – 255. The IP address is logically divided into a network prefix and a host identifier, which identify the network and the host within the network, respectively.

• /n specifies the length in bits of the network prefix portion of the IP address (starting from the leftmost bit). For an IPv4 IP address, the value of n can be in the range 0 – 32. In a VPC, the value of n is restricted to 16 – 28. In general, the larger the value of n, the smaller the range size becomes, which results in a smaller number of usable IP addresses

STORAGE:

->The main AWS Cloud storage services are grouped into four categories:

1. Block storage – Amazon Elastic Block Store (Amazon EBS) provides highly available and low-latency block storage capabilities to workloads that require persistent storage that is accessible from an Amazon Elastic Compute Cloud (Amazon EC2) instance.

2. Object storage – Two services fall in this category.

• Amazon Simple Storage Service (Amazon S3) is designed to store objects of any type in a secure, durable, and scalable way, and make them accessible over the internet.

• Amazon Simple Storage Service Glacier provides low-cost and highly durable object storage for long-term backup and archive of any type of data.

3. File storage – Two services support storing data at the file level.

• Amazon Elastic File System (Amazon EFS) provides a simple, scalable, elastic file system for Linux-based workloads.

• Amazon FSx for Windows File Server provides a fully managed native Microsoft Windows file system to support Windows applications that run on AWS.

4. Hybrid cloud storage – AWS Storage Gateway provides a link that connects your on-premises environment to AWS Cloud storage services in a resilient and efficient manner

AWS EBS:-Elastic block store. Amazon EBS is a block storage system offered by AWS. It is best used for storing persistent data. Amazon EBS provides highly available block-level storage volumes for use with EC2 instances.

-> EBS is a virtual disk in cloud.

-> AWS EBS allow you to create storage volume and then attach it to EC2 instance.

-> EBS volume are of 2 types: SSD , HDD

->Volumes

Volume storage for all EBS volume types is charged by the amount that you provision in GB per month, until you release the storage.

->IOPS

Input/output operations per second (IOPS) is a way to measure the performance of storage devices. A higher IOPS means that a storage device can handle more input and output (that is, write and read) operations.

0

1. SSD- > Solid state drives. also known as General purpose storgae. , support upto 4000 IOPS.

-> High performance , and quite expensive than HDD.

-> SSD are of 2 types: General purpose SSD ,   Provisioned IOPS SSD

a-> General Purpose SSD : also known as GP2.

b-> Provisioned IOPS SSD : also knows as IO1. , used for high performance.

2 HDD->Hard disk drive , size can be 1 GB 1TB, suppport 100 IOPS which is very low.

-> HDD are of 3 types: Throughput Optimized HDD , cold HDD , Mangnetic HDD

a-> Throughput Optimized HDD : also known as st1. , low cost HDD designed for application that require higher throughput up to 500 MP/s , used for data warehouse , log processing , Big data.

b-> Cold HDD : known as sc1. , lowest cost storage designed for those application where workloads are infrequently accessed or rarely accessed.

c-> Magnetic Volume: - Lowest cost in all. , used for those where data is infrewuntly used. used when lowest cost is important for storage.

INSTANCE STORE : An AWS instance store is a temporary storage type located on disks that are physically attached to a host machine. Instance stores are made up of single or multiple instance store volumes exposed as block devices. Block storage on AWS is available with AWS EBS.

->Some Amazon Elastic Compute Cloud (Amazon EC2) instance types come with a form of directly attached, block-device storage known as the instance store

-> Use an instance store for storage of information that does not need to be kept beyond the life of the instance

EFS :->Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed, elastic (Network File System) NFS storage. A network file system (NFS) enables you to store and retrieve data in a network.

->Amazon EFS is a file storage service for use with Amazon compute (EC2, containers, serverless) and on-premises servers. EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently accessible storage for up to thousands of EC2 instances.

AMAZON GLACIER:-

->Amazon Glacier, also known as Amazon Simple Storage Service (S3) Glacier, is a low-cost cloud stora ge service for data with longer retrieval times offered by Amazon Web Services (AWS).

-> Data model concepts are there:-

1. The first data model concept is the : archive.

Archive: Any object, such as a photo, video, file, or document that you store in Amazon S3 Glacier. It is the base unit of storage in Amazon S3 Glacier. Each archive has its own unique ID and it can also have a description.

2. The next data model concept is a vault.

Vault: A container for storing archives. When you create a vault, you specify the vault name and the Region where you want the vault to be located

3.The third data model concept is the vault access policy.

Vault access policy: Determines who can and cannot access the data that is stored in the vault. Also determines what operations users can and cannot perform.

4.The next data model concept is a job.

Job: Amazon S3 Glacier jobs can perform a select query on an archive, retrieve an archive, or get an inventory of a vault.

S3 VS S3 GLACIER : Amazon S3 is a durable, secure, simple, and fast storage service, while Amazon S3 Glacier is used for archiving solutions. Use S3 if you need low latency or frequent access to your data. Use S3 Glacier for low storage cost, and you do not require millisecond access to your data.

AMAZON S3 SERVICE: Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere.

Amazon S3 offers a range of storage classes that are designed for different use cases and access performance requirements.

These storage classes include:

- Amazon S3 Standard for general-purpose storage of frequently accessed data
- Amazon S3 Intelligent-Tiering for data with unknown or changing access patterns
- Amazon S3 Standard-Infrequent Access (S3 Standard-IA) and Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) for long-lived, but less-frequently accessed data
- Amazon S3 Glacier (S3 Glacier) for long-term archive and digital preservation

-> Some key concepts of S3 :

1. Buckets : A bucket is a container for objects that are stored in Amazon S3. Every object is contained in a bucket.
2. Objects : Objects are the fundamental entities that are stored in Amazon S3. Objects consist of object data and metadata. The data portion is opaque to Amazon S3. The metadata is a set of name-value pairs that describe the object. An object is uniquely identified within a bucket by a key (name) and a version ID.
3. Keys A key is the unique identifier for an object in a bucket. Each object in a bucket has exactly one key. The combination of a bucket, key, and version ID uniquely identifies each object. S
4. Regions A Region is the geographical AWS Region where Amazon S3 will store the buckets that you create. Objects that are stored in a Region do not leave the Region, unless you explicitly transfer them to another Region

S3 VERSIONING :- Amazon S3 provides a versioning feature to protect objects from accidental overwrites and deletes. Versioning enables you to recover from both unintended user actions and application failures.

-> Enable versioning at the bucket level. Each object in a bucket has a version ID, and when versioning is disabled, its value is set to null. When versioning is enabled, Amazon S3 creates a new object and assigns a unique value to its version ID (increments it) each time it is uploaded.

Amazon S3 OBJECT LOCK:- Amazon S3 object lock enables you to store objects by using the write once , read many (WORM) model. With Amazon S3 object lock, you can prevent an object from being deleted or overwritten, either for a fixed amount of time or indefinitely. Amazon S3 object lock enables you to meet regulatory requirements that require WORM storage. You can also use it to add an additional layer of protection against object changes and deletion.

AWS STORAGE GATEWAY : Storage Gateway is a service in AWS that connects an on-premises software appliance with the cloud-based storage to provide secure integration between an organization’s on-premises IT environment and AWS storage infrastructure.
-> AWS Storage Gateway is a hybrid storage service that enables your on-premises applications to use AWS Cloud storage. You can use Storage Gateway for backup and archiving, disaster recovery (DR), cloud data processing, storage tiering, and migration. Storage Gateway provides a standard set of storage protocols such as Internet Small Computer Systems Interface (iSCSI), Server Message Block (SMB), and Network File System (NFS). These protocols enable you to use AWS storage without rewriting your existing applications.

Storage gateway are of 3 types: File gateway , Volume gateway , Tape gateway
1. File gateway: -It is using the technique NFS.
It is used to store the flat files in S3 such as word files, pdf files, pictures, videos, etc.
It is used to store the files to S3 directly.
Files are stored as objects in S3 buckets, and they are accessed through a Network File System (NFS) mount point.

2. Volume Gateway : - If on-premises systems use iSCSI (Internet Small Computer Systems Interface) then volume gateways offer a way mechanism to Amazon S3 for storage.
The iSCSI block protocol is block-based storage that can store an operating system, applications and also can run the SQL Server, database.

3. Tape Gateway:- Tape Gateway is mainly used for taking backups.
It uses a Tape Gateway Library interface.
Tape Gateway offers a durable, cost-effective solution to archive your data in AWS cloud.

AWS TRANSFER FAMILY : AWS Transfer Family is the aggregated name of AWS Transfer for SFTP, AWS Transfer for FTPS, and AWS Transfer for FTP.

1. AWS SFTP : AWS Transfer for SFTP is a member of the AWS Transfer Family. It is a secure transfer service that you can use to transfer files into and out of AWS storage services over SFTP. You can use AWS Transfer for SFTP with Amazon Simple Storage Service (Amazon S3) or Amazon Elastic File System (Amazon EFS).

2. FTP stands for File Transfer Protocol. It is a network protocol that is used to transfer data.
• FTP uses a separate channel for control and data transfers. The control channel is open until it is terminated or there is an inactivity timeout. The data channel is active for the duration of the transfer.

3. FTPS stands for File Transfer Protocol over SSL. It is an extension to FTP. It uses Transport Layer Security (TLS) and Secure Sockets Layer (SSL) cryptographic protocols to encrypt traffic. • FTPS allows the encryption of both the control and data channel connections, either concurrently or independently.

AWS DATASYNC : AWS DataSync is a data transfer service that simplifies, automates, and accelerates moving and replicating data between on-premises storage systems and AWS storage services over the internet or through AWS Direct Connect

AWS SNOWBALL : AWS Snowball is a service that provides secure, rugged devices. You can bring AWS computing and storage capabilities to your edge environments, and transfer data in to and out of AWS.
-> The AWS Snowball service operates with AWS Snowball Edge devices, which include onboard computing capabilities in addition to storage.
-> What is Snowball Edge?   Snowball Edge is an edge computing and data transfer device that is provided by the AWS Snowball service.

CLOUDWATCH CloudWatch enables you to monitor your complete stack (applications, infrastructure, and services) and use alarms, logs, and events data to take automated actions and reduce mean time to resolution (MTTR). This frees up important resources and allows you to focus on building applications and business value.
-> The primary function of Amazon CloudWatch to monitor the performance and health of your AWS resources and applications. You can also use CloudWatch to collect and monitor log files from EC2 instances, AWS CloudTrail, Amazon Route 53, and other sources.
-> Amazon CloudWatch is a distributed statistics-gathering system. It collects and tracks your metrics from your applications. You can also create and use your own custom metrics and receive notifications when an alarm goes off.
->It enables you to:
• Track resource and application performance
• Collect and monitor log files
• Get notified when an alarm goes off

CLOUDTRAIL: AWS CloudTrail is an AWS service that generates logs of calls to the AWS application programming interface (API). The AWS API underlies both the AWS Command Line Interface (AWS CLI) and the AWS Management Console. Thus, CloudTrail can record all activity against the services that it monitors. It enables governance, compliance, operational auditing, and risk auditing of AWS accounts.
-> CloudTrail is enabled on your AWS account when you create it. When activity occurs in your AWS account, that activity is recorded in a CloudTrail event. You can easily view recent events in the CloudTrail console by going to Event history.
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. This event history simplifies security analysis, resource change tracking, and troubleshooting.

AMAZON ATHENA :Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL.
Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run.
-> Athena makes it easy for anyone with SQL skills to quickly analyze large-scale datasets.
-> Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run. You can quickly query your data without needing to set up and manage any servers or data warehouses. Athena enables you to query all your data in Amazon S3 without needing to set up complex processes to extract, transform, and load ETL) the data.

AWS ORGANISATION : AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage
-> AWS Organizations include consolidated billing and account management capabilities that help you to better meet the budgetary, security, and compliance needs of your business.

TAGGING: A tag is a label that you assign to an AWS resource. It enables you to identify it or categorize i t in a meaningful way. A tag consists of a key and a value, both of which you define.

AWS Support : AWS Support provides a unique combination of tools and expertise to customers, whether they are new or continue to adopt AWS services and applications as business solutions.
->AWS Support offers four different support plans to meet different user needs:

- Basic Support – Resource center access, Service Health dashboard, product FAQs, discussion forums, and support for health checks
- Developer Support – Support for early development on AWS
- Business Support – Support for customers that run production workloads
- Enterprise Support – Support for customers that run business and mission-critical workloads

AWS TRUSTED ADVISOR: It helps users follow best practices that increase the performance and fault tolerance of their AWS solutions. Trusted Advisor provides real-time guidance to help you reduce costs, increase performance, and improve security by optimizing your AWS environment. Trusted Advisor

AWS WHITEPAPERS : AWS whitepapers are a collection of technical documents that outline many topics that are relevant to AWS, like architecting best practices, security best practices, cloud computing economics, and serverless architecture. These technical documents cover a range of ideas, thoughts, and concepts that apply to cloud computing and AWS services.

AMI : An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an AMI when you launch an instance. If you need multiple instances with the same configuration, you can launch multiple instances from a single AMI. If you need instances with different configurations , you can use different AMIs to launch instances.

- Full AMI – The applications and all dependencies are pre-installed, which shortens boot times but increases build times. Full AMIs typically have a shorter lifespan. Consider your rollback strategy.
- Partially configured AMIs – Only prerequisite software and utilities are pre-installed, which leads to a longer shelf life for the AMI. This approach provides a balance between boot speed and build time. Rollbacks become easier.
- OS-only AMI – This approach is fully configurable and upgradeable over time and shortens build times. However, it makes your EC2 instances slow to boot because all required installations and configurations must be run at boot time.

- JSON
- Syntax for storing and transporting data.
- Text-based format, so it is human-readable.
- Documents are easily written.
- Stores key-value pairs and arrays of data.

- YAML
- Syntax for storing data.
- Text-based format, so it is human-readable.
- Documents are easily written.
- Store key-value pairs, lists, and associative arrays of data.
- Store complex data structures in a single YAML document.

Amazon CloudFront is a web service that gives businesses and web application developers an easy and

cost-effective way to distribute content with low latency and high data transfer speeds. Like other AWS services, Amazon CloudFront is a self-service, pay-per-use offering, requiring no long term commitments or minimum fees. With CloudFront, your files are delivered to end-users using a global network of edge locations.
• CloudTrail captures and records activities in an AWS account across Regions. • The information logged by CloudTrail gives visibility into user and resource activity. By using this information, you can identify who did what and when in your account.
• Because everything in AWS is an event, CloudTrail simplifies governance, compliance, and risk auditing.

AWS Config is a service used for assessing, auditing, and evaluating the configuration of your AWS resources. It continuously monitors and records your AWS resource configurations, and you can use it to automate the evaluation of recorded configurations against desired configurations.
With AWS Config, you can discover existing AWS resources and determine how a resource was configured at any point. It also provides configuration change notifications to facilitate security and governance.
You can use AWS Config together with AWS CloudTrail to gain complete visibility into the details of a configuration change. AWS Config notifies you when the configuration of a resource has changed, and CloudTrail provides you with additional details, such as who made the change.

AWS Shield - All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications

AWS Shield Advanced - For higher levels of protection against attacks targeting your web applications running on Amazon EC2, Elastic Load Balancing (ELB), CloudFront, and Route 53 resources, you can subscribe to AWS Shield Advanced. AWS Shield Advanced provides expanded DDoS attack protection for these resources.

Amazon Macie is a managed security service which can be used to detect personally identifiable information (PII) such as names, password, Credit card numbers from large amounts of data stored in Amazon S3 bucket.
Amazon Macie is a fully managed service from AWS that provides data security and privacy by utilizing Amazon’s machine learning and pattern matching capabilities.
AWS Macie primarily matches and discovers sensitive data such as personally identifiable information (PII) but does not have the capability to keep track of data behaviors between AWS services to detect anomalies. Therefore the service does not meet the requirement.

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS.
AWS Shield is a Distributed Denial of Service (DDoS) protection service that applies to applications running in the AWS environment. The service does not have machine learning capability to keep track of data behaviors between AWS services.

Amazon CloudWatch Anomaly Detection is a machine learning feature limited to Amazon CloudWatch metrics. It does not extend to all the AWS services, so it does not meet the requirement.

AWS Firewall Manager is a security management service that allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organization.

Amazon GuardDuty is a threat detection service that continuously monitors malicious activities and unauthorized behaviors to protect your AWS accounts, workloads, and data stored in Amazon S3.
AWS Artifact is a central resource for all the information about compliance. AWS artifact provides on-demand access to compliance reports at no additional cost.

Amazon CodeGuru is a developer tool powered by machine learning that provides intelligent recommendations for improving code quality and identifying an application’s most expensive lines of code.

AWS CodeStar enables you to develop, build, and deploy applications on AWS quickly. AWS CodeStar provides a unified user interface, enabling you to manage your software development activities in one place easily.

Amazon Athena a serverless query service that does not need to build databases on dedicated Elastic Block Store (EBS) volumes. Instead, it builds tables from data read directly from Amazon S3 buckets. Amazon Athena does not store any of the data. The service is compatible with the regular data formats that include CSV, JSON, ORC, AVRO and Parquet.

AWS Config will meet the scenario requirements. The service allowsS3 standard is ideal for general-purpose storage of frequently accessed data. the administrator to monitor and record configuration changes on AWS resources in their account. The service also allows the administrator to create a resource configuration inventory.

Running servers will incur costs. The number of running servers is one factor of Server Costs- a key component of AWS’s Total Cost of Ownership (TCO).

CodePipeline is typically utilized when orchestrating and automating the various phases involved in the release of application updates in-line with a release model that the developer defines.

AWS Data Sync is a simple and fast way to move huge amounts of data (hundreds of terabytes) between on-prem storage to S3, EFS, FSx.

AWS Data Pipeline is a web service that facilitates data processing and movement between various AWS services (like compute and storage). Data pipeline also works well with data sources that are on-premise. In the given data migration scenario, data sync is a more apt choice.

AWS Migration Hub is a service that facilitates discovery of the existing applications and IT assets and provides a view to better plan and track application migrations.

Global accelerator is a networking service that utilizes AWS global network to optimize the “user to application” path. The performance benefits realized by the use of the Global accelerator can be tested using a speed comparison tool provided by AWS.
Global accelerator differs from S3 transfer acceleration and DynamoDB accelerator.
S3 transfer acceleration accelerates the transfers of files to the S3 bucket by utilizing edge locations.
A fully managed DynamoDB Accelerator (DAX) is a highly available in-memory cache for Dynamodb.

AWS Artifact is a central resource for all the information about compliance. AWS artifact provides on-demand access to compliance reports at no additional cost.

Amazon S3 Intelligent-Tiering is best suited for data with “unknown/changing access pattern”.
S3 standard is ideal for general-purpose storage of frequently accessed data.
Amazon S3 Glacier is preferable for archival of data for a long term.
Amazon S3 Standard-Infrequent Access is better suited for less frequently accessed, long-lived data.

Weighted routing policy is suitable to route traffic to multiple resources based upon weights defined. This is useful when multiple resources are associated with a single domain name , & traffic needs to route based upon weighted proportions to each of the resources. For example , if there are 2 resources A & B for a single domain, using Weighted routing policy in Route 53 , traffic can be routed in any proportions like 90% to resource A & 10% to resource B.

Latency based routing is suitable for routing based upon lowest latency to the resources from user location.

Latency based routing is suitable for routing based upon lowest latency to the resources from user location.

Multivalue answer routing policy will be suitable to respond with multiple (up to eight) records for any query made to Route 53.

Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. You can start with just a few hundred gigabytes of data and scale to a petabyte or more. This enables you to use your data to acquire new insights for your business and customers.

Users can use AWS Artifact to download AWS security & Compliance documents. AWS Artifacts consists of reports such as AWS ISO certifications, Payment Card Industry (PCI), and System and Organization Control (SOC).

AWS CloudHSM is a managed hardware security model for generating and managing encryption keys on the AWS cloud. AWS CloudHSM can be used for offloading SSL processing for web servers. In this case , SSL processing is done on AWS CloudHSM instead of web servers which reduces load on web servers.

AWS Certificate Manager can be used to store & provision SSL/TLS certificates.

AWS KMS is a managed service for encrypting data. It cannot be used for offloading SSL processing for web servers.

AWS Secrets Manager can be used to implement password rotation policy for secrets stored.It can also be used to manage & retrieve credentials/ secrets which an application can use during its lifecycle. AWS Secrets Manager is not suitable for offloading SSL processing.

Amazon Cognito User Pools is a managed service which can be used to manage user authentication to mobile applications. It can scale up to millions of users. It supports direct user sign-in as well as federated users using social and enterprise identity providers.

Amazon Cognito Identity Pools are used to provide privilege credentials for accessing AWS services. Amazon Cognito User pools are used for authenticating users while identity pools will provide authorization for accessing AWS resources.

AWS Single Sign-On is best suited for authenticating employees for accessing AWS services & is not useful for authenticating users to access mobile applications.

AWS IAM is used to control access to AWS services or resources. It is not suited for authenticating large numbers of users to mobile applications.

AWS Detective is a persistent machine learning-driven service that automatically collates log data from all AWS resources. This log data is then applied into machine learning algorithms to derive data patterns between AWS services and resources, graph theory and statistical analysis. This information allows the user to proactively visualize their AWS environment from a security standpoint, thereby allowing them to quickly and efficiently conduct security investigations when they occur.

AWS CodeCommit is a managed source control service. It can be used as a data store to store source code, binaries, scripts, HTML pages and images which are accessible over the internet. CodeCommit encrypts files in transit and at rest, which fulfills the additional client requirement (high confidentiality & security) mentioned in the question. Also, CodeCommit works well with Git tools and other existing CI/CD tools.

AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, serverless Lambda functions, or Amazon ECS services.

AWS Lambda will allow the developers in the scenario to run code without provisioning or managing servers. The company would pay only for the compute time consumed. There would be no charge when your code is not running.

AWS CodeStar provides a unified user interface, enabling you to manage your software development activities in one place easily. With AWS CodeStar, you can set up your entire continuous delivery toolchain in minutes, allowing you to start releasing code faster. AWS CodeStar makes it easy for your whole team to work together securely, allowing you to manage access and add owners, contributors, and viewers to your projects easily. However, this question asks for the service to store the source code. AWS CodeStar is improper because it is a software development management tool rather than a source control service.

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from the organization's premises to AWS. The service provides a dedicated network connection with one of the AWS Direct Connect locations. It makes it possible to guaranteed high bandwidth and very low latency connectivity.

Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. It does not guarantee the quality of connectivity between the organizations on-premise infrastructure and the AWS cloud build. The data KDS collects is available in milliseconds to enable real-time analytics use cases such as real-time dashboards, real-time anomaly detection, dynamic pricing, and more.

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data to get timely insights and react quickly to new information.

Amazon Kinesis Data Firehose is used to load streaming data into various destinations like data lakes, data stores and analytics tools. However, the service does not guarantee link quality between the organization's on-premise infrastructure and the AWS cloud.

what services the Trusted Advisor Dashboard offers.

Cost optimization

It helps to save cost, such as recommending you to delete unused resources or use reserved capacity.

Performance

It can improve the performance of the services by ensuring to take advantage of provisioned throughput, and monitoring for overutilized Amazon EC2 instances.

Security

It can improve the security of the application by recommending you to enable AWS security features, and review your permissions.

Fault tolerance

It can increase the availability of the AWS application by recommending to take advantage of auto-scaling , health checks, multi-AZ Regions, and backup capabilities.

Service quotas

Service quotas also referred to as Service limits, are the maximum number of service resources or operations that apply to an account or a Region. Trusted Advisor can notify you if you use more than 80% of a service quota.

Enterprise Plan is the recommended support plan for customers having a business-critical application hosted on AWS cloud. With this support plan, a Technical Account Manager is assigned to work with the customer, who proactively monitors business-critical applications as well as assists in optimisation of application. Technical Account Manager is also responsible for coordinating access to AWS programs & getting technical assistance from AWS experts.

Business Plan is a suggested plan for customers having a production application hosted on AWS Cloud. In this support plan ,no Technical Account Manager is assigned.

Developer Plan is a basic plan if the customer is using AWS Cloud resources for test purposes. In this support plan ,no Technical Account Manager is assigned.

Enterprise On-Ramp Plan supports business critical applications hosted on AWS cloud, but in this plan the assigned Technical Account manager does not proactively monitor resources hosted on AWS cloud. Technical Account Manager is only responsible for coordinating access to AWS programs & getting technical assistance from AWS experts.

Regions consist of 2 or more Availability Zones within a specific geographical area. These Availability Zones are physically isolated & connected via a low latency redundant link.

Logical Data Center within each region is called an Availability Zones instead of a Data Center.

Edge locations are used by CloudFront CDN to deliver content to users with low latency.

Regional Caches are used by CloudFront which sit between edge locations & origin servers providing additional caching.

Amazon Cognito web identity federation service acts as a broker that allows authenticated users to access AWS resources. After successful authentication on platforms such as Facebook, LinkedIn, or Google Mail, users receive a temporary authentication code from Amazon Cognito, thereby gaining temporary access.

Resiliency is the ability to recover from disruptions and mitigate disruptions.

Consistency involves more than one system storing information, to return the same result when queried.

Durability is the system’s ability to perform even upon the occurrence of unexpected events.

Latency is typically the measurement of delay between request and response.

AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances). AWS CloudFormation takes care of provisioning and configuring those resources for you. You don’t need to create and configure AWS resources individually and figure out what’s dependent on what. AWS CloudFormation handles all of that.

Amazon Connect is an omnichannel cloud contact centre which can be setup easily & with low cost. It has following features which helps to provide customers a superior service ,

Telephone as a service
High quality Audio
Omnichannel routing
Web & Mobile Chat
Task management
Contact Centre automation
Rules Engine.

AWS CodePipeline is a fully managed service that automates the release pipeline for application updates. For updates, it uses application code stored in AWS CodeCommit, performs testing using AWS CodeBuild, and uses AWS CodeDeploy for deployment.

AWS CodeCommit is used to store deployment codes.

AWS CodeDeploy is used for deployment of codes to resources.

AWS CodeBuild is used to test and build application code.

AWS Health Dashboard provides the overall status of AWS services where you can view personalized communications about your particular AWS account or organization.
It provides general awareness, such as an upcoming maintenance issue for a service in a Region.

Amazon WorkSpaces provides a secure managed service for virtual desktops for remote users. It supports both Windows & Linux based virtual desktops for a large number of users.

Amazon Cognito can be used to control access to AWS resources from an application.

Amazon AppStream 2.0 can be used to provide access to applications or a non-persistent desktop from any location.

Amazon WorkLink can be used by internal employees to securely access internal websites & applications using mobile phones.

AWS Professional Services is a global team of experts which provides assistance for deploying high performance computing systems using various services in AWS cloud. This team of experts works along with the customer team in achieving goals for business needs by adopting best practices within AWS cloud.

AWS Support helps customers to get quick support from AWS support personnel for any queries on AWS resources or products.

AWS Managed services can be used to operate AWS infrastructure in a secure & optimised way.

AWS IQ engages a freelance AWS expert to help customers in any project related to AWS cloud.

AWS Service Catalog can be used to create & deploy portfolio of products within AWS infrastructure. This helps to create consistent resources within AWS infrastructure with quick deployment. These catalogues can be used for deployment of single resource or a multi-tier web application consisting of web, application, & database layer resources.

AWS Service Catalog allows IT organizations to create a portfolio of products that end-users can use to deploy AWS resources as defined in the portfolio. For this, AWS Service Catalog uses AWS IAM & AWS CloudFormation.

MONITORING SERVICE :

- Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), IT managers, and product owners. CloudWatch provides you with data and actionable insights to monitor your applications, respond to system-wide performance changes, and optimize resource utilization.
- AWS Config is a service that you can use to assess, audit, and evaluate the configurations of your AWS resources.
- Amazon Managed Service for Prometheus is a Prometheus-compatible monitoring and alerting service that makes it easy to monitor containerized applications and infrastructure at scale.
- Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity. It also delivers detailed security findings for visibility and remediatio