* **Amazon API Gateway** is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. With a few clicks in the AWS Management Console, you can create an API that acts as a “front door” for applications to access data, business logic, or functionality from your back-end services, such as workloads running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, or any web application. **Since it can use AWS Lambda, you can run your APIs without servers.**
  + Amazon API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization, access control, monitoring, and API version management. Amazon API Gateway has no minimum fees or startup costs. You pay only for the API calls you receive and the amount of data transferred out.
  + Enables you to build **RESTful APIs and WebSocket APIs** that are optimized for **serverless workloads**
  + You pay only for **the API calls you receive** and the amount **of data transferred out.**
  + **AWS CloudWatch Event can trigger lambda**
* **AWS Global Accelerator(2 static ip)**
  + **Redirects users requests to the nearest edge location** and then routes the data to the Amazon global network,increasing the speed and security.It also **reroutes requests to healthy IPs if it fails and changes propagation.**
  + **AWS Global Accelerator** is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers or Amazon EC2 instances.
  + **Provides you with static anycast IP addresses that** serve as a fixed entry point to your applications hosted in one or more AWS Regions
  + AWS Global Accelerator uses the AWS global network to optimize the path from your users to your applications, improving the performance of your TCP and UDP traffic(**directs traffic to nearest app endpoint**). AWS Global Accelerator continually monitors the health of your application endpoints and will detect an unhealthy endpoint and redirect traffic to healthy endpoints in less than 1 minute.
* **SSD-**Small,random,I/O operations,Yes,Best for transactional workload,sCritical business application,Large databases MongoDB,Oracle,Microsoft SQL Server.IOPS
* **HDD**-Large,sequential I/O operations,No,Best for large streaming workloads,Big data,Data Warheouses,Log processing.Thoughput-orinented storage for large volumes of data that is infrequently accessed.Throughput(MiB/s)
  + EBS General Purpose SSD (gp2) is a General-purpose SSD volume costs more and it is mainly used for a wide variety of workloads. It is recommended to be used as system boot volumes, virtual desktops, low-latency interactive apps, and many more.
  + Provisioned IOPS SSD (io1) this costs more than Cold HDD and thus, It provides the highest performance SSD volume for mission-critical low-latency or high-throughput workloads,
  + Throughput Optimized HDD (st1) this is primarily used for **frequently accessed,** throughput-intensive workloads. In this scenario, Cold HDD perfectly fits the requirement as it is used for their infrequently accessed data and provides the lowest cost, unlike Throughput Optimized HDD.
* When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted(**ALL IS ENCRPTED)**
  + Data at rest inside the volume
  + All data moving between the volume and the instance
  + All snapshots created from the volume
  + All volumes created from those snapshot
* **Amazon Kinesis** makes it easy to **collect, process**, **and analyze real-time, streaming data** so you can get timely insights and react quickly to new information. With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications. Amazon Kinesis enables you to process and analyze data as it arrives and respond instantly instead of having to wait until all your data is collected before the processing can begin.
  + **Kinesis Data Streams** is a real-time data streaming service that requires the provisioning of shards. Amazon SQS is a cheaper option because you only pay for what you use. Since there is no **requirement for real-time processing** in the scenario given, **replacing Kinesis Data Streams with Amazon SQS would save more costs.**
  + **By default, records of a stream in Amazon Kinesis are accessible for up to 24 hours** from the time they are added to the stream. You can raise this **limit to up to 7 days** by enabling extended data retention.
  + **Kinesis Firehouse is a option to load data to analytic tools like redshift from multiple sources.(kinesis streams can’t directly upload)**
* **The AWS Step Functions** service lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly
  + **Also provides graphical way to visualize steps**
  + **It is good for short running activies(its serverless)(synchronius)**
* **Amazon SQS,** Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware, and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.(**SQS Is used for horizontal scaling)**
  + **you can configure the message retention period to a value from 1 minute to 14 days**. **The default is 4 days**. Once the message retention limit is reached, your messages are automatically deleted
  + **A single Amazon SQS message queue can contain an unlimited number of messages**. However, there is **a 120,000 limit for the number of inflight messages** for a standard queue and **20,000 for a FIFO queue.** Messages are inflight after they have been received from the queue by a consuming component, but have not yet been deleted from the que
  + **SQS limit is 2GB**
  + **The visibility timeout** is a period of time during which Amazon SQS **prevents other consuming components from receiving and processing a message.**
    - The default visibility **timeout for a message is 30 seconds.** The **maximum is 12 hours.**
  + **– Long polling** reduces the number of empty responses by allowing Amazon SQS to wait until a message is available in the queue before sending a response. Unless the connection times out, the response to the ReceiveMessage request contains at least one of the available messages, up to the maximum number of messages specified in the ReceiveMessage action.
  + **– Long polling** eliminates false empty responses by querying all (rather than a limited number) of the servers. Long polling returns messages as soon any message becomes available.
    - If it is set to a value **greater than zero, then it is Long polling.**
  + **Dead letter queue** should be **sleceted** as it designed to **isolate problematic** messages in the que
* **AWS IoT Core** is a managed cloud service that lets connected devices easily and securely interact with cloud applications and other devices**. AWS IoT Core provides secure communication and data processing across different kinds of connected** devices and locations so you can easily build **IoT applications.**
* **By default, an Amazon SNS** topic subscriber receives every message published to the topic. You can **use Amazon SNS message filtering** to assign a filter policy to the topic subscription, and the subscriber will only receive a message that they are interested in. Using Amazon SNS and Amazon SQS together, messages can be delivered to applications that require immediate notification of an event. This method is known as fanout to Amazon SQS queues.
  + **SNS** can push **notification to the SQS endpoins**,it **uses publish/subscribe** model
* **Tape Gateway** enables you to replace using physical tapes on-premises with virtual tapes in AWS without changing existing backup workflows. Tape Gateway supports all leading backup applications and caches virtual tapes on-premises for low-latency data access. Tape Gateway encrypts data between the gateway and AWS for secure data transfer and compresses data and transitions virtual tapes between Amazon S3 and Amazon S3 Glacier, or Amazon S3 Glacier Deep Archive, to minimize storage costs.
* **AWS Storage Gateway** is a set **of hybrid cloud storage** services **that provide share and access data between your on-premise resources and AWS Resources**.It is not mainly designed to migrate data.All three storage gateway patterns are backed by S3(**ovo linkuje)**
  + **Nacin da se accesuje storage koji ne on premisses from on premisses na s3**
  + **Storage volumes up to 32TB in size and can attach iSCSI devices from your on premisses application servers.**
* **AWS Transit Gateway** is a service that enables customers to connect their Amazon **Clouds (VPCs**) and their on-premises networks to a single gateway. As you grow the number of workloads running on AWS, you need to be able to scale your networks across multiple accounts and Amazon VPCs to keep up with the growth.
  + **Transit Gateway acts as a hub** that controls how traffic is routed among all the connected networks which act like spokes. This hub and spoke model significantly simplifies management and reduces operational costs because each network only has to connect to the Transit Gateway and not to every other network. Any new VPC is simply connected to the Transit Gateway and is then automatically available to every other network that is connected to the Transit Gateway.
  + **A transit VPC** is primarily used to connect multiple VPCs and remote networks in order to create a global network transit center and not for establishing a dedicated connection to your on-premises network.
  + **Transit Gateway is used for interconnecting VPCs and on-premises networks through a central hub.**
  + **AWS Transit Gateway** also enables you to scale the IPsec VPN throughput with equal-cost multi-path (ECMP) routing support over multiple VPN tunnels. A single VPN tunnel still has a maximum throughput of 1.25 Gbps. If you establish multiple VPN tunnels to an **ECMP-enabled transit gateway,** it can scale beyond the default limit of 1.25 Gbps.
  + **Faster data** backup on vpn tunel:
    - **ENABLE ECMP** with multiple VPN tunnels assosiacted to a **transit gatewayfri**
  + **When traffic is outbound from the transit gateway subnet,nacl rules are not evaulted**
* **AWS DataSync** is an online data transfer service that simplifies, automates, and accelerates the process of copying large amounts of data to and from AWS storage services over the Internet or over AWS Direct Connect**.(Ovo kopira)**
  + **Disable verification during initial file transfer and enable it during the final cut-over**
* **Ftp is TCP 20/21 port number**
* **Here is a list of important information about EBS Volumes:**
  + When you create an EBS volume in an Availability Zone, it is automatically replicated within that zone to prevent data loss due to a failure of any single hardware component.
  + After you create a volume, you can attach it **to any EC2 instance in the same Availability Zone**.Amazon **EBS Multi-Attach** enables you to attach a **single Provisioned IOPS SSD (io1) volume to multiple Nitro-based instances that are in the same Availability Zone**. However, other EBS types are not supported.
  + An EBS volume is **off-instance storage** that can persist independently from the life of an instance. You can specify not to terminate the EBS volume when you terminate the EC2 instance during instance creation.
  + EBS volumes **support live configuration changes** while in production which means that you can modify the volume type, volume size, and IOPS capacity without service interruptions.
  + Amazon EBS encryption uses 256-bit Advanced Encryption Standard algorithms (AES-256)
  + EBS Volumes offer 99.999% SLA.
  + you can attach it only to the EC2 that is located in same AZ
  + EBS Volume Snapshot are stored in s3
  + There **is no access** to bucket **where snapshotys are automatically backed upon** and that’s why there is no option for cross-region replication.
  + You can **create point in time sn**apshots of volumes which we store **for you in S3,and** then you can copy **it from one region to another,or within the same region.**
  + **Amazon EBS is the persistent block storag**e volume among the options given. It is mainly used as the root volume to store the operating system of an EC2 instance. To encrypt an EBS volume at rest, yo**u can use AWS KMS customer master ke**ys for the encryption of both the boot and data volumes of an EC2 instance.
* **Here are the prerequisites for routing traffic to a website that is hosted in an Amazon S3 Bucket:**
  + An S3 bucket that is configured to host a static website. The bucket must have **the same name as your domain or subdomain.** For example, if you want to use the subdomain portal.tutorialsdojo.com, the name of the bucket must be portal.tutorialsdojo.com.
  + **A registered domain name**. You can use Route 53 as your domain registrar, or you can use a different registrar.
  + Route 53 as the DNS service for the domain. If you register your domain name by using Route 53, we automatically configure Route 53 as the DNS service for the domain
* **Amazon S3** can send event notification **to SNS,SQS,AWS Lambda,EVENTBRIDGE**

**Route53:**

* + **MX record** specifies the mail server responsible for accepting email messages on behalf of a domain name
  + A Record Type – the value for an A record is an IPv4 address in dotted decimal notation.
  + CNAME Record Type – a CNAME Value element is the same format as a domain name.
  + **Enable Cross-Origin Resource Sharing (CORS)(S3)** when your client’s web application on one domain interacts with the resources in a different domain
    - **CORS support metod: GET,PUT,POST,DELETE AND HEAD**
  + To create an **active-passive failover** configuration with one primary record and one secondary record, you just create the records and specify Failover for the routing policy
  + **Weighted routing** simply lets you associate multiple resources with a single domain name (tutorialsdojo.com) or subdomain name (blog.tutorialsdojo.com) and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load balancing and testing new versions of software, but not for a failover configuration
    - **Its ideal for using blue-green deployment**
  + **Geolocation routing** lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from. For example, you might want all queries from Europe to be routed to an ELB load balancer in the Frankfurt region.
  + **Multivalue routing policy,** use when you want Route53 to respond to DNS queries with up to eight healthy records selected randomly.
* **Amazon Guard​Duty** is just a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.
* **AWS Firewall Manager** just simplifies your AWS WAF and AWS Shield Advanced administration and maintenance tasks across multiple accounts and resources.
* **AWS Athena if you want to save money:**
  + Partiotion data based **upon date&location** and create separate **workgroups** based upon user group
* **AWS WAF** is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer. AWS WAF also lets you control access to your content. Based on conditions that you specify, such as the **IP addresses** that requests originate from or the values of query strings, API **Gateway, CloudFront or an Application Load Balancer** responds to requests either with the requested content or with an HTTP 403 status code (Forbidden). You also can configure CloudFront to return a custom error page when a request is blocked. At the simplest level, AWS
* **WAF lets you choose one of the following behaviors:**
  + **Allow all requests except the ones that you specify** – This is useful when you want CloudFront or an Application Load Balancer to serve content for a public website, but you also want to block requests from attackers.
  + **Block all requests except the ones that you specify** – This is useful when you want to serve content for a restricted website whose users are readily identifiable by properties in web requests, such as the IP addresses that they use to browse to the website.
  + **Count the requests that match the properties that you specify** – When you want to allow or block requests based on new properties in web requests, you first can configure AWS WAF to count the requests that match those properties without allowing or blocking those requests. This lets you confirm that you didn’t accidentally configure AWS WAF to block all the traffic to your website. When you’re confident that you specified the correct properties, you can change the behavior to allow or block requests.
* **AWS Direct Connect** is primarily used to establish a dedicated network connection from your premises network to AWS. This is not suitable for one-time data transfer tasks.
  + For IPsec you need direct connect +VPN
  + Create multiple Direct Connections with LAG enabled in active mode to provide **redudancy**
* **AMAZON S3**
  + **Expedited retrievals** allow you to quickly access your data when occasional urgent requests for a subset of archives are required. For all but the largest archives (250 MB+), data accessed using Expedited retrievals are typically made available **within 1–5 minutes**. Provisioned Capacity ensures that retrieval capacity for Expedited retrievals is available when you need it.
  + **Provisioned capacity** ensures that your retrieval capacity for expedited retrievals is available when you need it. Each unit of capacity provides that at least three expedited retrievals can be performed every five minutes and provides up to 150 MB/s of retrieval throughput. You should purchase provisioned retrieval capacity if your workload requires highly reliable and predictable access to a subset of your data in minutes. Without provisioned capacity Expedited retrievals are accepted, except for rare situations of unusually high demand. However, if you require access to Expedited retrievals under all circumstances, you must purchase provisioned retrieval capacity.
  + **Bulk** retrievals typically complete within 5–12 hours hence
  + **Amazon S3 Multipart Upload**, this feature simply enables you to upload large objects in multiple parts. It still uses the same Internet connection of the company, which means that the transfer will still take time due to its current bandwidth allocation.
    - **You can create s3 lifecycle configuration to abort incomplited multiparts uploads**
  + **CORS simply** defines a way for client web applications that are loaded in **one domain to** interact with resources in **a different domain**, **and not on a different AWS account.**
  + S3 delivers **strong read-after-write** and list consistency automatically
* **AWS Glue** is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. **It does not provide scalability or elasticity to your instances.**
* **You can authenticate to your DB instance using AWS Identity and Access Management (IAM) database authentication. IAM database authentication works with MySQL and PostgreSQL. With this authentication method, you don’t need to use a password when you connect to a DB instance.**
  + An authentication token is a string of characters that you use instead of a password. After you generate an authentication token, it’s valid for 15 minutes before it expires. If you try to connect using an expired token, the connection request is denied.
  + Use IAM DB Authentication and create database accounts using the AWS-provided AWSAuthenticationPlugin plugin in MySQL.
* **DynamoDB** is a fully managed service which automatically scales its storage, without setting it up manually
  + **Enabling In-Memory Acceleration with DynamoDB Accelerator (DAX)** is primarily used for read performance improvement of your DynamoDB table from **milliseconds response time to microseconds.**
  + **If the shard iterator expires immediately before you can use it**, this might indicate that the DynamoDB table used by Kinesis does not have enough capacity to store the lease data. This situation is more likely to happen if you have a large number of shards. To solve this problem, increase the write capacity assigned to the shard table.
  + **Amazon DynamoDB is integrated with AWS Lambda** so that you can create triggers—pieces of code that automatically respond to events in DynamoDB Streams. With triggers, you can build applications that react to data modifications in DynamoDB tables.
  + **If you enable DynamoDB Streams on a table**, you can associate the stream ARN with a Lambda function that you write. Immediately after an item in the table is modified, a new record appears in the table’s stream. AWS Lambda polls the stream and invokes your Lambda function synchronously when it detects new stream records.
    - **You can monitor changes in DynamoDB table with it**
  + **Data in DynamoDB**  is stored in **JSON** format.
  + **DynamoDb plus ElastiCache** are usually used for storing a seasion data.
  + **You can use DynamoDB Stream to monitor to monitor changes to dynamo db table**
  + **DynamoDb is ideal to store metadata**
* **RDS**
  + In a **Multi-AZ deployment**, Amazon RDS automatically provisions and maintains a **synchronous standby replica in** a different Availability Zone. The primary DB instance is **synchronously replicated across Availability Zones** to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups
  + **Amazon RDS simply flips the canonical name record (CNAME)** for your DB instance to point at the standby, which is in turn promoted to become the new primary.
  + Multi-AZ:
    - Provides **synchronous replication** and **automatic failover** in the case of Availability Zone service failures
    - In multi-az you cannot promote instance cannot be promoted to be a read relica
  + **The high-availability feature is not a scaling solution for** read-only scenarios; you cannot use a standby replica to serve read traffic. To service read-only traffic, you should use a **Read Replica.**
  + **Read replicas: they provide >multiple seconds replication(use amazon aurora read replicas for <1milisiceond time)**
    - It **elastically scales out** beyond the capacity constraints of a single DB instance for **read-heavy database workloads.**
    - Provides **asynchronou**s replication and improves the performance of the primary database by taking read-heavy database workloads from it.
    - Read Replicas are primarily used to offload read-only operations from the primary database instance.
  + Amazon **RDS automatically performs a failover** in the event of any of the following:
    - Loss of availability in primary Availability Zone.
    - Loss of network connectivity to primary.
    - Compute unit failure on primary.
    - Storage failure on primary.
  + **RDS Storage Auto Scaling** automatically scales storage capacity in response to growing database workloads, with zero downtime.
  + **If you want all data in flight to be secured between web server and rds you should:**
    - Download the Amazon RDS Root CA certificate. Import the certificate to your servers and configure your application to use SSL to encrypt the connection to RDS.
    - Force all connections to your DB instance to use SSL by setting the rds.force\_ssl parameter to true. Once done, reboot your DB instance.
  + Automated Snapshots Creation:
    - AWS creates a storage volume snapshot of database instance during backup period once a day,and captures transational logs and stores them in s3
  + You cannot encrypt an unecrypted directly
  + You can use SQS Queues to cache the pending database writes so that the database can handle the load properly(**queue database writes)**
  + **AWS Migration Hub** is used to track the **progress of migrations in AWS**.
  + If you want to increase **number of connection** you create a **new parameter group**,attach it **to db instance and change settings.**
* **Load Balancing**
  + Classic Load Balancer does not support Server Name Indication (SNI). You have to use an Application Load Balancer instead or a CloudFront web distribution to allow the SNI feature.
  + If you are using NLB,and you need to **negotiate TLS connection** with clients,NLB uses a security policy that **consist of protocls & ciphers(default)**
    - It **does not** support **custom policies**
  + **ALB support server name indicatin(SNI),enabling hosting multiple domain names with diffirent tls certification behind single alb**
* **The Amazon Simple Workflow Service (Amazon SWF**) makes it easy to build applications that coordinate work across distributed components. In Amazon SWF, a task represents a logical unit of work that is performed by a component of your application. Coordinating tasks across the application involves managing intertask dependencies, scheduling, and concurrency in accordance with the logical flow of the application(**SWF is fit for long running tasks)(async)(support integration with other aws services)**
  + Amazon Simple Queue Service (SQS) and Amazon Simple Workflow Service (SWF) are the services that you can use for creating a decoupled architecture in AWS. Decoupled architecture is a type of computing architecture that enables computing components or layers to execute independently while still interfacing with each other.
* **Instance metadata** is the data about your instance that you can use to configure or manage the running instance. You can get the instance ID, public keys, public IP address and many other information from the instance metadata by firing a URL command in your instance to this URL:

<http://169.254.169.254/latest/meta-data/>

* + Curl or get to get latest meta-data if you need ip adresses
* **Instance user data** is mainly used to perform common automated configuration tasks and run scripts after the instance starts.
* **AWS Security Token Service (AWS STS)** is the service that you can use to create and provide trusted users with temporary security credentials that can control access to your AWS resources. Temporary security credentials work almost identically to the long-term access key credentials that your IAM users can use.
  + In this diagram, IAM user Alice in the Dev account (the role-assuming account) needs to access the Prod account (the role-owning account). Here’s how it works:
  + Alice in the Dev account assumes an IAM role (WriteAccess) in the Prod account by calling AssumeRole.
  + STS returns a set of temporary security credentials.
  + Alice uses the temporary security credentials to access services and resources in the Prod account. Alice could, for example, make calls to Amazon S3 and Amazon EC2, which are granted by the WriteAccess role.
* **Amazon EMR** is a managed cluster platform that simplifies running big data frameworks, such as Apache Hadoop and Apache Spark, on AWS to process and analyze vast amounts of data. By using these frameworks and related open-source projects, such as Apache Hive and Apache Pig, you can process data for analytics purposes and business intelligence workloads. Additionally, you can use Amazon EMR to transform and move large amounts of data into and out of other AWS data stores and databases.
  + **EMR IS NOT RECIVING DATA**
  + **KINESIS DATA STREAM TO INGEST THEN CUSTOM APP TO ANALYZE AND THEN MOVE OUTCOMES TO REDSHFIT**
* **Amazon Redshift** is the most widely used **cloud data warehouse**. It makes it fast, simple and cost-effective to analyze all your data **using standard SQL and y**our existing **Business Intelligence (BI)** tools. It allows you to run complex analytic queries against terabytes to petabytes of structured and semi-structured data, using sophisticated query optimization, columnar storage on high-performance storage, and massively parallel query execution.
  + **Amazon Redshift** also includes Redshift Spectrum, allowing you to directly run SQL queries against exabytes of unstructured data in Amazon S3. No loading or transformation is required, and you can use open data formats, including Avro, CSV, Grok, ORC, Parquet, RCFile, RegexSerDe, SequenceFile, TextFile, and TSV. Redshift Spectrum automatically scales query compute capacity based on the data being retrieved, so queries against Amazon S3 run fast, regardless of data set size.
  + **You can configure Amazon Redshift to copy snapshots for a cluster to another region**. To configure cross-region snapshot copy, you need to enable this copy feature for each cluster and configure where to copy snapshots and how long to keep copied automated snapshots in the destination region. When cross-region copy is enabled for a cluster, all new manual and automatic snapshots are copied to the specified region.
  + **Amazon Redshift Enhanced VPC** Routing provides VPC resources access to Redshift,Redshift is not able to access s3 VPC endpoints without enabling this.
    - **If you use this,Redshift forces all COPY and UNLOAD traffic between your cluster and your data repositories though your amazon VPC(it will not go though internet)**
  + **You can**  **configure cross-regional snapshots** when you want Amazon Redshift to **automatically copy snapshots(automated or manual**) to another region for backup purposes.)
  + **It supports OLAP and not OLTP**
  + **Encyption shoud be enabled at cluster level**
* **AWS Config** is a service that enables you to **assess, audit, and evaluate the** configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.
* Y**ou can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation,** retention, and deletion of snapshots taken to back up your Amazon EBS volumes. Automating snapshot management helps you to:
  + Protect valuable data by enforcing a regular backup schedule.
  + Retain backups as required by auditors or internal compliance.
  + Reduce storage costs by deleting outdated backups.

Combined with the monitoring features of Amazon CloudWatch Events and AWS CloudTrail, Amazon DLM provides a complete backup solution for EBS volumes at no additional cost.

* **In Auto Scaling**, the following statements are correct regarding **the cooldown period:**
  + It ensures that the Auto Scaling group does not launch or terminate additional EC2 instances before the previous scaling activity takes effect.
  + Its **default value is 300 seconds.**
  + It is a configurable setting for your Auto Scaling group.
  + **Lifecycle Hooks** puts the instance into a wait state before termination.Default Wait perioid is 1h
  + **Termination policy** is used to specify which instance to terminate first during scale-in.
  + **Scalling:**
  + **Target tracking scaling policy increases or decreases the current** capacity of the group based on a target value for a specific metric, instead of a set of scaling adjustments.
  + **Simple scaling is** incorrect because the simple scaling policy increases or decreases the current capacity of the group based on a single scaling adjustment, instead of a set of scaling adjustments.
  + **Scheduled Scaling** is incorrect because the scheduled scaling policy is based on a schedule that allows you to set your own scaling schedule for predictable load changes. This is not considered as one of the types of dynamic scaling.
  + **Step scaling** – Increase or decrease the current capacity of the group based on a set of scaling adjustments, known as step adjustments, that vary based on the size of the alarm breach.
    - If you are scaling based on a utilization metric that increases or decreases proportionally to the number of instances in an Auto Scaling group, then it is recommended that you use target tracking scaling policies. Otherwise, it is better to use step scaling policies instead.
  + Sqs plus ASG can scale if you have parameter **ApproximateNumberOfMessegesVisible**
* **Amazon S3 Transfer Acceleration** enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket. Transfer Acceleration leverages **Amazon CloudFront’s globally distributed AWS Edge Locations**. As data arrives at an AWS Edge Location, data is routed to your Amazon S3 bucket over an optimized network path.
* **ACL:** 
  + Rules are evaluated starting with the lowest numbered rule. As soon as a rule matches traffic, it’s applied immediately regardless of any higher-numbered rule that may contradict it.
* **Lambda**
  + If you **get EC2ThrottledException erros:**
    - You only specified one subnet in your Lambda function configuration. That single subnet runs out of available IP addresses and there is no other subnet or Availability Zone which can handle the peak load.
    - Your VPC does not have sufficient subnet ENIs or subnet Ips.
    - Lamba function **is statless by** nature
    - Encyption helpers make your lambda function more secure,by ecnprinting evniroment variable before they are sent to lambda
    - Lambda key configuration allows you to have your lambda functions use and ecnpytion key.AWS KMS
    - Lambda layers are used to package common code such as libriareis,fongiraution files or custom runtime images.
    - Lambda aliasesa are used to refer to a specific version of your lambda function(you have to deploy new code to create a new version)
* **AWS Backup** is a centralized backup service that makes it easy and cost-effective for you to backup your application data across AWS services in the AWS Cloud, helping you meet your business and regulatory backup compliance requirements. AWS Backup makes protecting your AWS storage volumes, databases, and file systems simple by providing a central place where you can configure and audit the AWS resources you want to backup, automate backup scheduling, set retention policies, and monitor all recent backup and restore activity.
* **AWS App Mesh** is just a service mesh that provides application-level networking to make it easy for your services to communicate with each other across multiple types of compute infrastructure.
* **AWS Cloud Map** is simply a cloud resource discovery service that enables you to name your application resources with custom names and automatically update the locations of your dynamically changing resources.
* **Amazon ElastiCache** is a fully managed, in-memory caching service supporting flexible, real-time use cases. You can use ElastiCache for [caching](https://aws.amazon.com/caching/), which accelerates application and database performance, or as a primary data store for use cases that don’t require durability like session stores, gaming leaderboards, streaming, and analytics. ElastiCache is compatible with Redis and Memcached.
* **An Elastic Fabric Adapter (EFA)** is a network device that you can attach to your Amazon EC2 instance to accelerate High Performance Computing (HPC) and machine learning applications. EFA enables you to achieve the application performance of an on-premises HPC cluster, with the scalability, flexibility, and elasticity provided by the AWS Cloud. (**os-bypass capabilietes are not supported on windows instances)**
  + Enables you to run applications requiring high levels of inter-node communications at scale on AWS through its custom-built operating system (OS) bypass hardware interface
  + **Elastic Network Adapter**  same without OS-bypass capabilities
  + **Elastic Network Interface** is just a logical network card
  + **Private Virtual Interface** just allows you to connect to your VPC resources on your private Ip address or endpoint
* **CloudFront can’t work with Anycast static IP Address**
  + **Cloudfront origin can be: s3,ELB,Ec2,lambda@edge for custom code**
* **Lambda@Edge** is a feature of Amazon CloudFront that lets you run code closer to users of your application, which improves performance and reduces latency. With Lambda@Edge, you don’t have to provision or manage infrastructure in multiple locations around the world. You pay only for the compute time you consume – there is no charge when your code is not running.
  + **Lambda Edge needs to created in one region and then replicated to all regions**
* **Amazon MQ is a managed message** broker service for Apache ActiveMQ that makes it easy to set up and operate message brokers in the cloud. Connecting your current applications to Amazon MQ is easy because it uses industry-standard APIs and protocols for messaging, including **JMS, NMS, AMQP, STOMP, MQTT, and WebSocket**. Using standards means that in most cases, there’s no need to rewrite any messaging code when you migrate to AWS.
  + **JMS APIS,AMQP,MQTT**
* You can use **AWS X-Ray** to trace and analyze user requests as they travel through your Amazon API Gateway APIs to the underlying services. API Gateway supports AWS X-Ray tracing for all API Gateway endpoint types: regional, edge-optimized, and private. You can use AWS X-Ray with Amazon API Gateway in all regions where X-Ray is available.
  + **X-ray colets data,analysis and debug of microservice app.**
* **RAID 0 is** used for improved performance of your storage volumes
* **RAID 1 is** used for data mirroring
* If you got your certificate from a third-party CA, import the certificate into ACM or upload it to the IAM certificate store. Hence, **AWS Certificate Manager and IAM certificate store** are the correct answers.
* **AWS Elastic Beanstalk** is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.
  + **It is not used to store data only to provision and managed/deploy**
  + Application files are stored in S3. The server log files can also optionally be stored in S3 or in CloudWatch Logs.
* **AWS VPN links** on-premise network to AWS network.
* **AWS Lake** is used to manage a large amount of data in AWS
* **VPC Flow logs** is a feature that enables you to capture information about **the IP traffic going to and** from network interfaces in your VPC.Flow log data is stored in CloudWatchLogs.
* **Amazon FSx for Lustre file system is** an open-source,parallel file system that can be used for **HPC applications.In** **amazon FSx,** users can quickly launch a Luster file system at a low **cost.(utomat S3)**
  + AMAZON FSx for Luster doesn’t support WINDOWS BASED application and WINDOWS Server**s**
  + **There is Amazon Fsx for Windows File Server** that does the same but supports windows
    - **Can connect to Manage Active Drirectory and to Windows instance,inside managed active directory.**
  + FSX for Lustre can **read data from s3 and** connect to **multiple instance** at the same time( it can **read/write at same time**)
* **Amazon Elastic File System (EFS)** is incorrect because although the EFS service can be used for HPC applications, it doesn’t natively work with Amazon S3. It doesn’t have the capability to easily process your S3 data with a high-performance POSIX interface, unlike Amazon FSx for Lustre.
  + **If you want to encypt data in transit while accessing data from amazon efs you need to use:**
    - **EFS mount helper to encypt data in transit (tls1.2)**
* **Amazon FSx for Windows File Server** is incorrect because although this service is a type of Amazon FSx, it does not work natively with Amazon S3. This service is a fully managed native Microsoft Windows file system that is primarily used for your Windows-based applications that require shared file storage to AWS.
* **Amazon Neptune is a fast,** reliable, fully-managed **graph database** service that makes it easy to build and run applications that work with highly connected datasets.
* **AWS Schema Conversion Tool** is used to convert source scheam ut application code to match target database.
  + **You transfer it to s3 then for saving before uploading it**
* You can use **Run Command** from the console to configure instances without having to login to each EC2 instance.
* **File Gateway** is used to store and retrieve Amazon S3 objects **through NFS and SMB protocols.**
* **Volume Gateway in stored mode** is incorrect because the requirement is to provide low latency access to the frequently accessed data subsets locally. Stored Volumes are used if you need low-latency access to your entire dataset.
  + **There is also Volume Gateawy in cached mode**
* **Amazon WorkSpaces** is a fully managed desktop virtualization service for Windows and Linux that enables you to access resources from any supported device.
* With web identity federation, you don’t need to create custom sign-in code or manage your own user identities. Instead, users of your app can sign in using a well-known identity provider (IdP) —such as Login with Amazon, Facebook, Google, or any other OpenID Connect (OIDC)-compatible IdP, receive an authentication token.
* **On-Demand Capacity Reservations enable** you to reserve compute capacity for your Amazon EC2 instances in a specific Availability Zone for any duration. This gives you the ability to create and manage Capacity Reservations independently from the billing discounts offered by Savings Plans or Regional Reserved Instances.
  + When you create a Capacity Reservation, you specify:
    - – The Availability Zone in which to reserve the capacity
    - – The number of instances for which to reserve capacity
    - – The instance attributes, including the instance type, tenancy, and platform/OS
* The key to managing sticky sessions is determining how long your load balancer should consistently route the user’s request to the same target.
* Federated identity provides are used to **authenticate users**.Then Cognito identity pool provides temporary token that authorizes users to access aws resources
  + Open ID connect OIDC,Identity providers are supported in cognito,along with social and samlb ased identity providers.
* KMS is USED TO encrypt data at rest
* **Amazon QuickSight is a BI services** you can use to buil**d visualizations,perform ad hoc** analysis,and get business insights from your data.It can utomatically discover AWS data sources and also works with your data utomat.Scales to hundres of thounsands of users and deliver reposnive utomaticall using robust inmemory engine(spice)
* **User data can be used to run automation at start of instance**
* S3 **and Dynamodb are serverless in aws and** you don’t need to maintain servers for them
* **Gateway endpoints are for s3 and dynamodb** other are i**nterface**

**Table

Description automatically generated**

**EBS Provisioned IOPS SSD (io1)** is incorrect because Amazon EBS Provisioned IOPS SSD is not the most cost-effective EBS type and is primarily used for critical business applications that require sustained IOPS performance.

**EBS General Purpose SSD (gp2)** is incorrect. Although an Amazon EBS General Purpose SSD volume balances price and performance for a wide variety of workloads, it is not suitable for frequently accessed, throughput-intensive workloads. Throughput Optimized HDD is a more suitable option to use than General Purpose SSD.

**EBS Cold HDD (sc1)** is incorrect. Although this provides lower cost HDD volume compared to General Purpose SSD, it is much suitable for **less** frequently accessed workloads.

When you create ebs with ec2 it must remain in same az as ec2,if you want to copy it to other az you need to create a snapshot and then create a volume from the snapshot

* Throughput Optimized HDD (st1) volumes, though similar to Cold HDD (sc1) volumes, are designed to support frequently accessed data.
* **Throughput Optimized HDD (st1)** volumes provide low-cost magnetic storage that defines performance in terms of throughput rather than IOPS. This volume type is a good fit for large, sequential workloads such as Amazon EMR, ETL, data warehouses, and log processing. Bootable st1 volumes are not supported.

**EBS-maintain a single snapshot:latest snapshot is both incremental and complete version**

**Memory Optimized Instances** is incorrect because these are designed to deliver fast performance for workloads that process large data sets in memory, which is quite different from handling high read and write capacity on local storage.

**Compute Optimized Instances** is incorrect because these are ideal for compute-bound applications that benefit from high-performance processors, such as batch processing workloads and media transcoding.

**General Purpose Instances** is incorrect because these are the most basic type of instances. They provide a balance of compute, memory, and networking resources, and can be used for a variety of workloads. Since you are requiring higher read and write capacity, storage optimized instances should be selected instead.

**Storage optimized instances** are designed for workloads that require high, sequential read and write access to very large data sets on local storage. They are optimized to deliver tens of thousands of low-latency, random I/O operations per second (IOPS) to applications.

* Vpc Peering keep in mind:
  + Ensuring that Vpc **don’t have overlaping** CIDR block
  + **Transitive** peering is not supported
  + **It support peering across reigons also**
* **VPC peering site to site(on premises to vpc cloud) prerequsites:**
  + A **public ip address** on the **customer gateway** for the on premises network
  + A **virtual private** gateway atttache to the **VPC**
* **When ec2 is in hibernate state you only pay for: EBS volumes and Elastic Ip adress attache to it**
* **S3 encyption**
  + **SSE-S3**  requires that amazon s3 manage the data and master encyption keys.
  + **SSE-c** reuqies that you manage the encyption key(customer)
  + **SSE-KMS** requiers that AWS manage the data key,but you manage the master key in AWS KMS
    - **Key policy size is 32kb max**

Graphical user interface

Description automatically generated

* S3 that objects must be stored at least 30 days in the current storage class before you can transition them to STANDARD\_IA or ONEZONE\_IA. You cannot create a lifecycle rule to transition objects to either STANDARD\_IA or ONEZONE\_IA storage class 7 days after you create them because you can only do this after the 30-day period has elapsed.
  + For Glacier you can do it sooner in sooner 7days or 1day not sure
* Amazon S3 now provides increased performance to support at **least 3,500 requests** per second to add data **and 5,500 requests per** second to retrieve data, which can save significant processing time for no additional charge. Each S3 prefix can support these request rates, making it simple to increase performance significantly.

Minimum storage duration for standard is 0,OneZone Standard IA 30,glacier 90 I deep arhicved 180

* For Glacier Deep Archive you cannot moved data directly to another storage class,you have to restore them first and then move them with S3 Console (copy) to other tier like Intelligent-Tiering
* **Amazon s3 Select**:uses **simple SQL,objects** needs to be stored in **CSV,JSON or Apache Perquet format.GZIP BZIP2 compreesion** is supported with **CSV or JSON** format with server side encryption.
* **With S3 Versioning,**  each version of an object can have a different retention period.
* **CDN-Content delivery network** will improve time of your files and pages to the customer but is not a hostin solution
* **To determain if** log file **was modfied,deleted or unchanged after cloudtrail** delivered it you can use **CloudTrail log file integrity validation**.(compliance)
* **To** back up AWS CloudHSm data to s3 in same region,CloudHSm generates a unique EBK to encypt all data using AES 256-bit.This EBK is further encypted using Persistent Backup pbk also aes256-bit
* S3 **object lock** should be enabled to store **object using write once read many models(WORM)**
* SSO **minimum(default**) period to be log in **is 1h and max is 12h**,you can create custom permission set and increase time **from 1 to max of 12h**
* CloudTrail can be created to be one for all regions
* Using AD connector,customers can use existing AD deployed at on premises servers.

Trusted Advisor includes an ever-expanding list of checks in the following five categories:

**Cost Optimization**– recommendations that can potentially save you money by highlighting unused resources and opportunities to reduce your bill.

**Security** – identification of security settings that could make your AWS solution less secure.

**Fault Tolerance** – recommendations that help increase the resiliency of your AWS solution by highlighting redundancy shortfalls, current service limits, and over-utilized resources.

**Performance** – recommendations that can help to improve the speed and responsiveness of your applications.

**Service Limits** – recommendations that will tell you when service usage is more than 80% of the service limit.

* Well architected framework:
  + Monitoring cloudwatch and cloudtrail
* Reliability pillar:
  + Non overlapiing Private ip
* Performance efficiency pillar
  + Designh with elasticity

Graphical user interface, application

Description automatically generated

* **Cloudformation:**
  + **Resources**-main resourse
  + **Parametars-parametar** that can be taken during template deployment
  + **Mappings-used** to map key-value pairs in template
  + **Outputs-Allows ELB** Dns to return once stack is created

Graphical user interface, text, application, email

Description automatically generated