Amazon ECS doesn’t support resource-based policies. An example of a resource-based policy is the S3 bucket policy. An ECS task assumes an execution role (IAM role) to be able to call other AWS services like AWS Secrets Manager on your behalf.

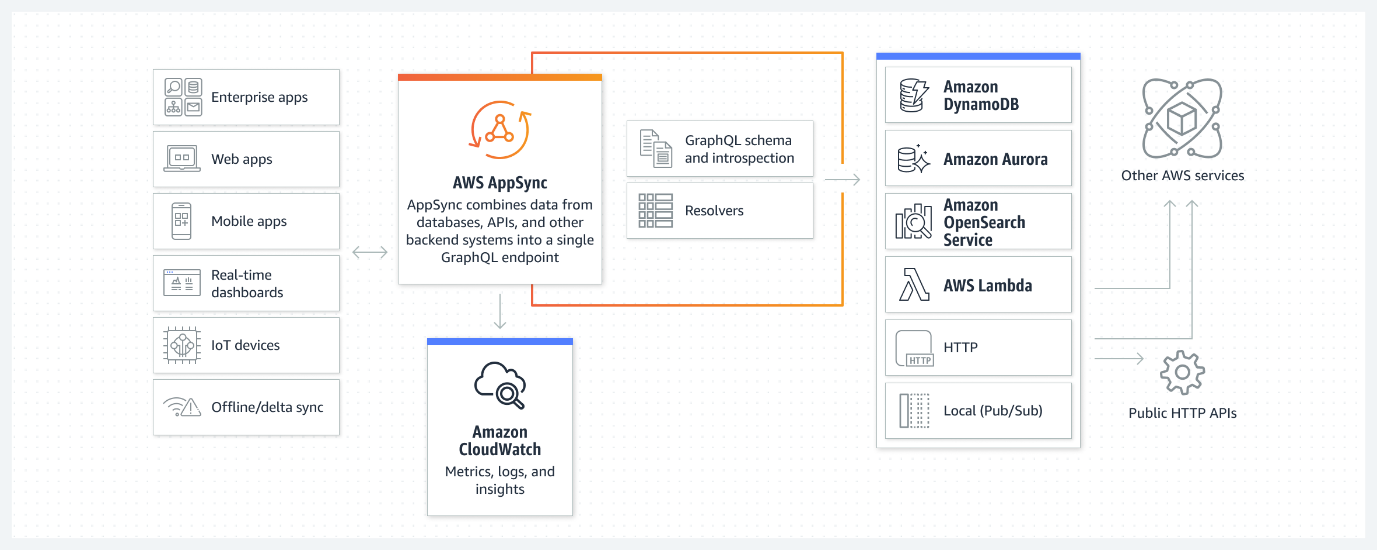
**AWS WAF** is a web application firewall that lets you monitor the HTTP(S) requests that are forwarded to an Amazon CloudFront distribution, an Amazon API Gateway , an Application Load Balancer, or an AWS AppSync GraphQL API. (eg SQL injection or cross-site scripting). It can block the requests based on:

* possible malicious scripts/ SQL code
* IP
* Geographic location
* length of specified parts of requests
* specified header or the query string
* regex pattern

**WAF rules across accounts/ region**

By setting up **AWS Firewall Manager**, you can centrally configure AWS WAF rules, which can be applied to multiple AWS accounts and Regions. This allows for efficient management and enforcement of security rules across accounts without the need for separate configuration in each individual Region.

AWS AppSync is a serverless GraphQL and Pub/Sub API service that simplifies building modern web and mobile applications. It provides a robust, scalable GraphQL interface for application developers to combine data from multiple sources, including Amazon DynamoDB, AWS Lambda, and HTTP APIs.



**AWS Database Migration Service (AWS DMS)** is a cloud service that makes it easy to migrate relational databases, data warehouses, NoSQL databases, and other types of data stores. You can use AWS DMS to migrate your data into the AWS Cloud or between combinations of cloud and on-premises setups.

Although using a combination of Security Groups and NACLs are valid to provide security to your VPC, this is not enough to mitigate a DDoS attack**. Use AWS Shield Advanced to detect and mitigate DDoS attacks**

AWS Network Firewall is a managed service that is primarily used to deploy essential network protections for all of your Amazon Virtual Private Clouds (VPCs) and not particularly to your Application Load Balancers

If you want to serve private content through CloudFront and you’re trying to decide whether to use signed URLs or signed cookies, consider the following:

Use **signed URLs** for the following cases:

– You want to use an RTMP distribution. Signed cookies aren’t supported for RTMP distributions.

– You want to restrict access to individual files, for example, an installation download for your application.

– Your users are using a client (for example, a custom HTTP client) that doesn’t support cookies.

Use **signed cookies** for the following cases:

– You want to provide access to multiple restricted files, for example, all of the files for a video in HLS format or all of the files in the subscribers’ area of a website.

– You don’t want to change your current URLs.

DynamoDB can handle frequent schema changes

VPC endpoint is the most suitable service that will allow you to use private IP addresses to access both DynamoDB and S3 without any exposure to the public internet

Cross-origin resource sharing (CORS) defines a way for client web applications that are loaded in one domain to interact with resources in a different domain.

AWS Lambda can handle a sudden burst of traffic within seconds and not minutes. Lambda automatically handles scaling the number of execution environments until you reach your account's concurrency limit.

Amazon RDS - replication

A screenshot of a computer

Description automatically generated with medium confidence

AWS Artifact is your go-to, central resource for compliance-related information that matters to you. Root users and IAM users with admin permissions can download all audit artifacts available to their accounts by agreeing to the associated terms and conditions.

AWS Storage Gateway is primarily used to integrate your on-premises network to AWS but not for migrating your applications

AWS Resource Access Manager (RAM) helps you securely share your resources across AWS accounts: share resources such as subnets or License Manager configurations with other accounts. This eliminates the need to provision duplicate resources in every account in a multi-account environment, reducing the operational overhead of managing those resources in every account.

**AWS Control Tower** simply offers the easiest way to set up ssa, multi-account AWS environment. This is not the most suitable service to use to securely share your resources across AWS accounts or within your Organization.

Maximum days for the EFS lifecycle policy is only 90 days. EBS costs more and is not as scalable as Amazon S3.

**sensitive information in Lambda**

Although Lambda does encrypt the environment variables in your function by default, the sensitive information would still be visible to other users who have access to the Lambda console. To secure your environment variables, The best option is to create a new KMS key and use it to enable encryption helpers that leverage on AWS Key Management Service to store and encrypt the sensitive information.

RDS events only provide operational events such as DB instance events, DB parameter group events, DB security group events, and DB snapshot events. What we need in the scenario is to capture data-modifying events (INSERT, DELETE, UPDATE) which can be achieved thru native functions or stored procedures

EFS is a POSIX-compliant shared file system, which can be accessed by Multiple Amazon EC2 instances.

AWS Transfer enables you to easily move your file transfer workloads that SFTP/ FTPS/ FTP

A screenshot of a computer

Description automatically generated with medium confidence

In **ElastiCache**, Using **Redis AUTH** command can improve data security by requiring the user to enter a password before they are granted permission to execute Redis commands on a passwowrd-protected Redis server.

You can set up an EventBridge rule that runs an Amazon ECS task whenever a file is uploaded to a certain Amazon S3 bucket using the Amazon S3 PUT operation.

You can authenticate to your DB instance using AWS Identity and Access Management (IAM) database authentication. This could ensure that your RDS database can only be accessed using the profile credentials specific to your EC2 instances via an authentication token.

**AWS Lake Formation** is a service that makes it easy to set up a secure data lake in days. A data lake is a centralized, curated, and secured repository that stores all your data, both in its original form and prepared for analysis. A d**ata lake enables you to break down data silos** and combine different types of analytics to gain insights and guide better business decisions. Data can be consolidated from multiple accounts into a single account.

You can configure any access point in S3 to accept requests only from a virtual private cloud (VPC) to restrict Amazon S3 data access to a private network

Although the Object Lock feature does provide write-once-read-many (WORM) storage, the Object Versioning feature must also be enabled too in order for this to work.

EC2 instance will be the first one to be terminated by your Auto Scaling group in priority:  
1. choose the Availability Zone with the most instances

2. oldest launch configuration

3. closest to the next billing hour

By default, instances that you launch into a virtual private cloud (VPC) can’t communicate with your own network. You can enable access to your network from your VPC by attaching a virtual private gateway to the VPC, creating a custom route table, updating your security group rules, and creating an AWS managed VPN connection.

A picture containing text, screenshot, diagram, design

Description automatically generated

**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.

To monitor the available swap space of each EC2 instance, Install the CloudWatch agent on each instance and monitor the SwapUtilization metric.

 You can transfer up to **100 TB** with a single Snowball Edge Storage Optimized device.

If a “Too Many Connections” error happens to a client connecting to a MySQL database, it means all available connections are in use by other clients. RDS Proxy comes in to maintain a connection pool that clients can reuse.

To obtain detailed logging information for object-level access in S3, Enable server access logging for all required Amazon S3 buckets.

You can’t assign an Elastic IP address to an Application Load Balancer. The alternative method you can do is assign an Elastic IP address to a Network Load Balancer

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.

Encryption of EBS:

* When attaching EBS to EC2, following data is encrypted by AES-256:

– 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 snapshots

– Encryption of EBS is regional specific

– Beware Server-Side Encryption and Client-Side Encryption are relate only to S3, not EBS

– You cannot directly encrypt existing unencrypted volumes or snapshots. However, you can create encrypted volumes or snapshots from unencrypted volumes or snapshots

– Apart from default, you can also encrypt EBS by using Amazon-managed keys/ customized keys in AWS KMS, when creating the volume

If one of your instances serving a particular function fails/ terminated, its network interface can be attached to a replacement or hot standby instance pre-configured for the same role in order to rapidly recover the service.

Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover.

IN S3, Cross-origin resource sharing (CORS) defines a way for client web applications that are loaded in one domain to interact with resources in a different domain

Amazon ECS is an AWS proprietary managed container orchestration service. You should use Amazon EKS since Kubernetes is an open-source platform and is considered cloud-agnostic. With Kubernetes, you can use the same configuration and tools that you’re currently using in AWS even if you move your containers to another cloud service provider.

Although you can copy data from on-premises to AWS with Storage Gateway, it is not suitable for transferring large sets of data to AWS. Storage Gateway is mainly used in providing low-latency access to data by caching frequently accessed data on-premises while storing archive data securely and durably in Amazon cloud storage services. Storage Gateway optimizes data transfer to AWS by sending only changed data and compressing data.

A Gateway endpoint is a type of VPC endpoint that provides reliable connectivity to Amazon S3 and DynamoDB without requiring an internet gateway or a NAT device for your VPC.  It would take you a lot of time to configure a bucket policy for each S3 bucket instead of using a single endpoint policy. Therefore, you should use an endpoint policy to control the traffic to the trusted Amazon S3 buckets.

 AWS Glue is just a serverless ETL service that crawls your data, builds a data catalog, performs data preparation, data transformation, and data ingestion. It won’t allow you to utilize different big data frameworks effectively, unlike Amazon EMR. In addition, the S3 Select feature in Amazon S3 can only run simple SQL queries against a subset of data from a specific S3 object. To perform queries in the S3 bucket, you need to use Amazon Athena.

After you or AWS applies tags to your AWS resources (such as Amazon EC2 instances or Amazon S3 buckets) and you activate the tags in the Billing and Cost Management console, AWS generates a cost allocation report as a comma-separated value (CSV file) with your usage and costs grouped by your active tags. You can apply tags that represent business categories (such as cost centers, application names, or owners) to organize your costs across multiple services.

Network ACL is much suitable to control the traffic that goes in and out of your entire VPC and not just on one EC2 instance. A **security group** acts as a virtual firewall that controls the traffic for one or more instances.

A Lambda function's execution role is an AWS Identity and Access Management (IAM) role that grants the function permission to access AWS services and resources. A resource-based policy is added to the Lambda function, which allows the specified principal (eg events.amazonaws.com) to invoke the function. The lambda:InvokeFunction action provides the necessary permission for the Amazon EventBridge rule to trigger the Lambda function.

A screenshot of a computer

Description automatically generated with low confidence

Elastic Fabric Adapter is just 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 AWS.

AppFlow is simply an integration service for transferring data securely between Software-as-a-Service (SaaS) applications like Salesforce, SAP, Zendesk, Slack, ServiceNow, and AWS services. While AWS AppSync Connect apps to data and events with secure, serverless, and performant GraphQL and Pub/Sub APIs

Amazon EBS root device volumes are automatically deleted when the instance terminates. To preserve the root volume when an instance terminates, change the DeleteOnTermination attribute for the root volume to False.

In cases where your EC2 instance cannot be accessed from the Internet (or vice versa), you usually have to check two things:

– Does it have an EIP or public IP address?

– Is the route table properly configured?

**customer gateway (CGW)**  is used when you are setting up a VPN

Use the following tagging strategies to help identify and manage AWS resources, can be governed by AWS Config Rules,

* resource organization
* cost allocation
* automation
* access control

you cannot integrate DynamoDB table with CloudFront as these two are incompatible.

**Amazon API Gateway** lets you create an API that acts as a “front door” for applications to access data, business logic, or functionality from your back-end services (eg dynamoDB). improve its overall performance and make it more scalable from millions of read and write request

**API Gateway REST API**

A REST API in API Gateway is a collection of resources and methods that are integrated with backend HTTP endpoints, Lambda functions, or other AWS services. You can use API Gateway features to help you with all aspects of the API lifecycle, from creation through monitoring your production APIs.

Data transition  
A picture containing text, diagram, design

Description automatically generated

* direct connect: on your on-premises data center
* transfer acceleration: leverages Edge Location. Between cloud and all users around the world

VPC endpoints for Amazon S3 simplify access to S3 from within a VPC by providing configurable and highly reliable secure connections to S3 that do not require an internet gateway or Network Address Translation (NAT) device You can use two types of VPC endpoints to access Amazon S3: **gateway endpoints and interface endpoints:  
-** A gateway endpoint is a gateway that you specify in your route table to access Amazon S3 from your VPC over the AWS network.

* Interface endpoints extend the functionality of gateway endpoints by using private IP addresses to route requests to Amazon S3 from within your VPC, on-premises, or from a different AWS Region

When a client initiates a connection to a server on port 443, the client's operating system dynamically selects an ephemeral port from a range of available ports. It is necessary to configure ephemeral ports on a NACL to enable the return traffic for outbound connections

Kinesis Data Streams supports changes to the data record retention period of your stream.By default, the data records are only accessible for 24 hours from the time they are added to a Kinesis stream.

Hibernation of EC2 provides the convenience of pausing and resuming the instances, saves time by reducing the startup time taken by applications, and saves effort in setting up the environment or applications all over again. While the instance is in hibernation, you pay only for the EBS volumes and Elastic IP Addresses attached to it; there are no other hourly charges (just like any other stopped instance).

**Amazon EMR** provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances. It securely and reliably handles a broad set of big data use cases, including log analysis, web indexing, data transformations (ETL), machine learning, financial analysis, scientific simulation, and bioinformatics.

**Retrieve the required data from Glacier:**

**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.

**Expedited retrievals** allow you to quickly access your data when occasional urgent requests for a subset of archives are required, getting you your data in minutes rather than hours. Expedited will incur a premium charge.

**Stop a instance**

If you stopped an EBS-backed EC2 instance, the volume is preserved, but the data in any attached instance store volume will be erased. Keep in mind that an EC2 instance has an underlying physical host computer. If the instance is stopped, AWS usually moves the instance to a new host computer.

**Standard queue vs FIFO queue**

A screenshot of a computer

Description automatically generated

**Import third-party certificate**

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. You can then upload these certificate into CloudFront. But you cannot import the third-party certificate into CloudFront directly

The IAM Policy that enforces MFA authentication can then be attached to an IAM Group to quickly apply to all IAM Users.

For RDS, Maximum backup retention period for automated backup is only 35 days. You cannot directly download or export an automated snapshot in RDS to Amazon S3. To implement a 90-day backup retention policy, **create an AWS Backup plan to take daily snapshots with a retention period of 90 days.**

You are limited to running On-Demand Instances per your vCPU-based On-Demand Instance limit per region. You can **submit the limit increase form to AWS**

**DNS Failover**

You can use **Route 53 health checking** to configure active-active and active-passive failover configurations.

**Active-Active Failover**

Use this failover configuration when you want **all of your resources** to be available the majority of the time. When a resource becomes unavailable, Route 53 can detect that it’s unhealthy and stop including it when responding to queries.

In active-active failover, all the records that have the same name, the same type (such as A or AAAA), and the same routing policy (such as weighted or latency) are active unless Route 53 considers them unhealthy.

**Active-Passive Failover**

Use an active-passive failover configuration when you want a primary resource or group of resources to be available the majority of the time and you want a **secondary resource or group of resources to be on standby** in case all the primary resources become unavailable. When responding to queries, Route 53 includes only the healthy primary resources. If all the primary resources are unhealthy, Route 53 begins to include only the healthy secondary resources in response to DNS queries.

ELB is designed to only run in one region and not across multiple regions.

 The AWS VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. It uses an Amazon VPC virtual private gateway with multiple customer gateways, each using unique BGP autonomous system numbers (ASNs).  It is only for **VPNs** and not for VPCs

A picture containing text, screenshot, diagram, font

Description automatically generated

Host multiple website

* wildcard certificate can only handle multiple sub-domains but not different domains.
* To host different domains, you can upload all SSL certificates of the domains in the ALB using the console and bind multiple certificates to the same secure listener on your load balancer. ALB will automatically choose the optimal TLS certificate for each client using Server Name Indication (SNI).

**Health Dashboard**

The AWS **Service Health Dashboard** provides a complete **health check of all services in all regions at any one time**, and this can be accessed through the following link. It shows public events that may affect several customers in particular regions. It doesn’t show events related to specific EC2 instances on individual AWS accounts. You have to check the events on the AWS Personal Health Dashboard instead. **The Personal Health Dashboard** differs to that of the Service Health Dashboard, in that it will notify you of any services interruptions that may affect the resources and services that you are using **within your own AWS account.**

**Prevent duplication of message:**

Use an Amazon SQS FIFO Queue instead.

Replace Amazon SQS and instead, use Amazon Simple Workflow service.

An **Amazon S3 Glacier vault** can have one resource-based vault access policy and one Vault Lock policy attached to it. You can create a Vault Lock policy that denies users permission to delete an archive until the archive has existed for x year.

**Control access to S3 in cloudfront**

When you create or update a distribution in CloudFront, you can add an origin access identity (OAI) and automatically update the bucket policy to give the origin access identity permission to access your bucket. Alternatively, you can choose to manually change the bucket policy or change ACLs, which control permissions on individual objects in your bucket. It also prevents direct navigation to the S3 URL

Kinesis data stream ensure the sequence of data arrival in large data volume

If you got your certificate from a third-party CA, import the certificate into **ACM** or upload it to the **IAM certificate store**

If your identity store is not compatible with SAML 2.0 then you can build a custom identity broker application to perform a similar function.

In AWS CloudFront, the term "origin" refers to the source location from which CloudFront retrieves the content. It represents the original server or storage location where your content is stored or generated. CloudFront acts as a content delivery network (CDN) and caches your content in edge locations worldwide, allowing for faster content delivery to end users.

In Redshift, to implement a disaster recovery plan for their systems, enable Cross-Region Snapshots Copy in your Amazon Redshift Cluster.

**AWS Application Migration Service (AWS MGN)** is the primary migration service recommended for lift-and-shift migrations to AWS. Implementation begins by installing the **AWS Replication Agent** on your source servers. When you launch Test or Cutover instances, AWS Application Migration Service automatically converts your source servers to boot and run natively on AWS.

**EC2 type and selection**

A picture containing text, screenshot, font, document

Description automatically generated

**Fastest storage option with high I/O performance for the temporary files.**

RAID 0 configuration enables you to improve your storage volumes’ performance by distributing the I/O across the volumes in a stripe. Therefore, if you add a storage volume, you get the straight addition of throughput and IOPS. This configuration can be implemented on both EBS or instance store volumes

Regular Amazon RDS Metrics in CloudWatch: **CPU Utilization, Database Connections,**and**Freeable Memory**

Enhanced Monitoring metrics: **RDS processes, OS processes**

**Transit Gateway – equal-cost multi-path (ECMP)**

* The maximum tunnel for a VPN connection is two
* 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**.

**Enhanced networking, Elastic Network Adapter (ENA) & Elastic Fabric Adapter (EFA)**

* Enhanced networking uses single root I/O virtualization (SR-IOV) to provide SR-IOV to provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces
* Enhanced networking provides
  + **higher bandwidth**
  + higher bandwidth, higher packet per second (PPS) performance
  + consistently lower inter-instance latencies
* Amazon EC2 provides enhanced networking capabilities through the **Elastic Network Adapter (ENA).**
* An **Elastic Fabric Adapter (EFA)** is simply an Elastic Network Adapter (ENA) with added capabilities. It provides all of the functionality of an ENA, with additional OS-bypass functionality. OS-bypass is an access model that allows HPC and machine learning applications to communicate directly with the network interface hardware to provide low-latency, reliable transport functionality.The OS-bypass capabilities of EFAs are not supported on Windows instances.

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.

**Amazon EBS**

**General Purpose (SSD)** is the new, SSD-backed, general purpose EBS volume type that is recommended as the default choice for customers. General Purpose (SSD) volumes are suitable for a broad range of workloads, including **small to medium-sized databases**, development and test environments, and **boot volumes**.

**Provisioned IOPS (SSD)** volumes offer storage with consistent and low-latency performance and are designed for I/O intensive applications such as **large relational or NoSQL databases.** Magnetic volumes provide the lowest cost per gigabyte of all EBS volume types.

**Magnetic volumes** are ideal for workloads where data are **accessed infrequently**, and applications where the lowest storage cost is important. Take note that this is a Previous Generation Volume. The latest low-cost magnetic storage types are Cold HDD (sc1) and Throughput Optimized HDD (st1) volumes.

**S3 Requester Pays**

In general, bucket owners pay for all Amazon S3 storage and data transfer costs that are associated with their bucket. However, you can configure a bucket to be a Requester Pays bucket. With Requester Pays buckets, the requester instead of the bucket owner pays the cost of the request and the data download from the bucket. The bucket owner always pays the cost of storing data.

**Permissions of EKS**

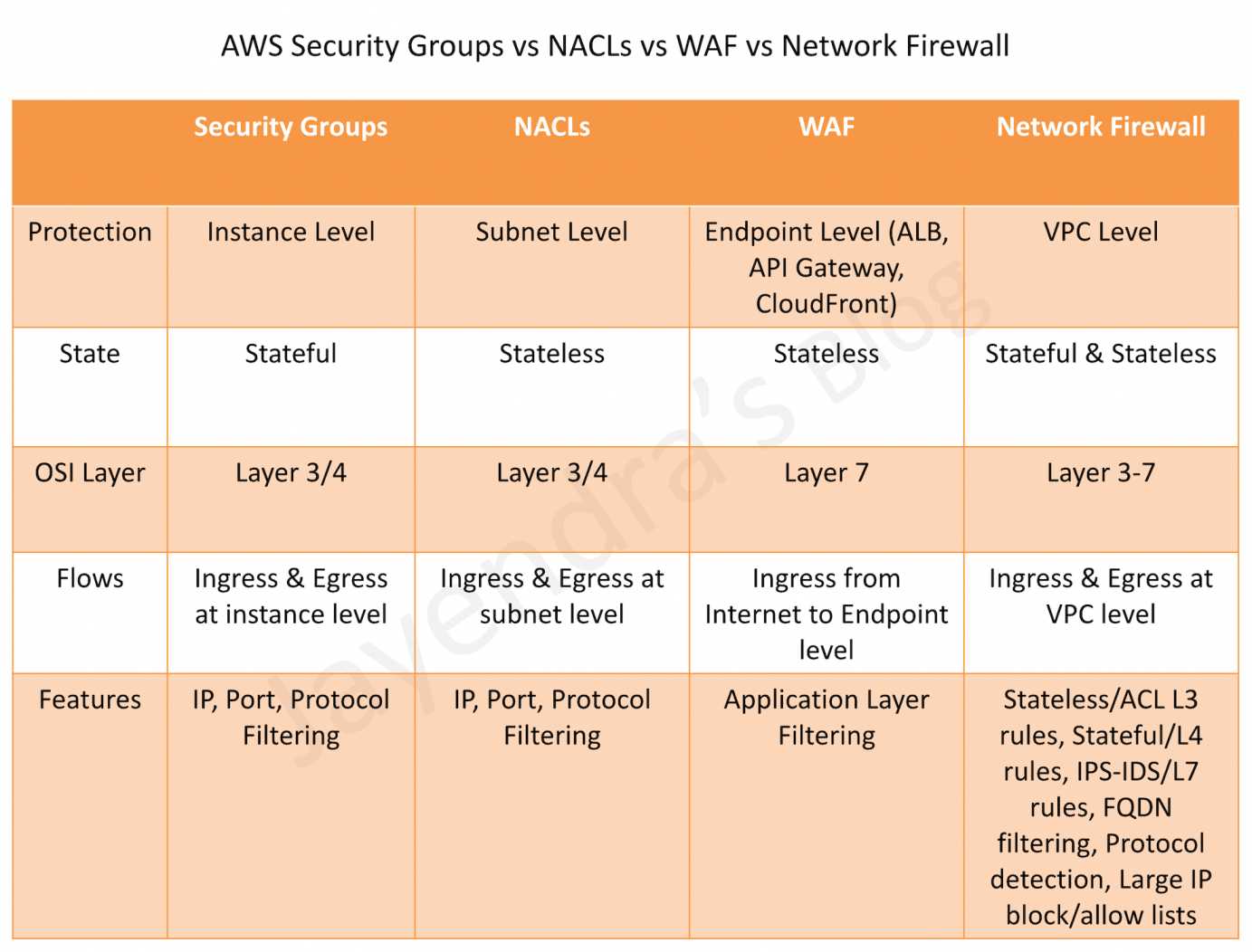
Amazon EKS uses IAM to provide authentication to your Kubernetes cluster, but it still relies on native Kubernetes Role-Based Access Control (RBAC) for authorization. This means that IAM is only used for the authentication of valid IAM entities. All permissions for interacting with your Amazon EKS cluster’s Kubernetes API are managed through the native Kubernetes RBAC system.

**Use EBS during snapshotting**

In EBS Snapshots occur asynchronously, the point-in-time snapshot is created immediately, but the status of the snapshot is pending until the snapshot is completed. While it is completing, an in-progress snapshot is not affected by ongoing reads and writes to the volume hence, you can still use the EBS volume normally.

A screenshot of a computer

Description automatically generated with medium confidence



Always remember that you should associate IAM roles to EC2 instances. an IAM policy is used to define permissions for an IAM user or group, not for an EC2 instance.

Gateway Load Balancer endpoints are configured in spoke VPCs originating or receiving traffic from the Internet. This architecture allows you to perform inline inspection of traffic from multiple spoke VPCs in a simplified and scalable fashion while still centralizing your virtual appliances.

You can share your CloudWatch dashboards with people who do not have direct access to your AWS account.

* Share a single dashboard and designate specific email addresses of the people who can view the dashboard. Each of these users creates their own password that they must enter to view the dashboard.
* Share a single dashboard publicly, so that anyone who has the link can view the dashboard.
* Share all the CloudWatch dashboards in your account and specify a third-party single sign-on (SSO) provider for dashboard access.

**Avoid Regional data transfer charges by gateway endpoint**

Deploying a gateway VPC endpoint for Amazon S3 is the most cost-effective way for the company to avoid Regional data transfer charges. A gateway VPC endpoint is a network gateway that allows communication between instances in a VPC and a service, such as Amazon S3, without requiring an Internet gateway or a NAT device. Data transfer between the VPC and the service through a gateway VPC endpoint is free of charge, while data transfer between the VPC and the Internet through an Internet gateway or NAT device is subject to data transfer charges.

**Overcome internet bandwidth limitations**

AWS Direct Connect is a network service that allows you to establish a dedicated network connection from your on-premises data center to AWS. This connection bypasses the public Internet and can provide more reliable, lower-latency communication between your on-premises application and Amazon S3. By directing backup traffic through the AWS Direct Connect connection, you can minimize the impact on your internet bandwidth and ensure timely backups to S3.

Ensure the lambda wouldn’t miss a job:

* Create an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe it to the SNS topic
* Modify the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue

AWS SSO which requires two way trust.

AWS Systems Manager **Run Command** allows the company to run commands or scripts on multiple EC2 instances. By using Run Command, the company can quickly and easily apply the patch to all 1,000 EC2 instances to remediate the security vulnerability.

To automatically rotate the database credentials on a regular basis and  not hardcode database credentials in the application, Store the database credentials as a secret in AWS Secrets Manager. Turn on automatic rotation for the secret. Attach the required permission to the EC2 role to grant access to the secret.

The visibility timeout is the duration during which SQS prevents other consumers from receiving and processing the same message. By increasing the visibility timeout, you allow more time for the processing of a message to complete before it becomes visible to other consumers.

**Backup solution existing in DynamoDB (continuously)**

[Amazon DynamoDB](https://aws.amazon.com/dynamodb/) offers two types of backups: point-in-time recovery (PITR) and on-demand backups. PITR is used to recover your table to any point in time in a rolling 35 day window, which is used to help customers mitigate accidental deletes or writes to their tables from bad code, malicious access, or user error. On demand backups are designed for long-term archiving and retention, which is typically used to help customers meet compliance and regulatory requirements.

**DynamoDB on-demand and provisioned capacity**

**Provisioned capacity** is best if you have relatively predictable application traffic, run applications whose traffic is consistent, and ramps up or down gradually. **On-demand capacity mode** is best when you have unknown workloads, unpredictable application traffic and also if you only want to pay exactly for what you use. The on-demand pricing model is ideal for bursty

**Gateway endpoints for S3 without** travel across the internet.

Gateway endpoints provide reliable connectivity to Amazon S3 and DynamoDB without requiring an internet gateway or a NAT device for your VPC

**Backup with mysqldump**

Populating the staging database by implementing a backup and restore process that uses the **mysqldump** utility is not the recommended solution because it involves taking a full export of the production database, which can cause unacceptable application latency. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Use database cloning to create the staging database on-demand.

# SQS message duplication

Setting the visibility timeout ensure the downstream process (like Lambda) has enough time to process the message and be invisible to other consumers. Prevent the message being consumed again, if lambda cannot finish the message and delete the message from the queue. While using a FIFO queue can prevent duplicates, it requires additional configuration and therefore may have higher operational overhead.

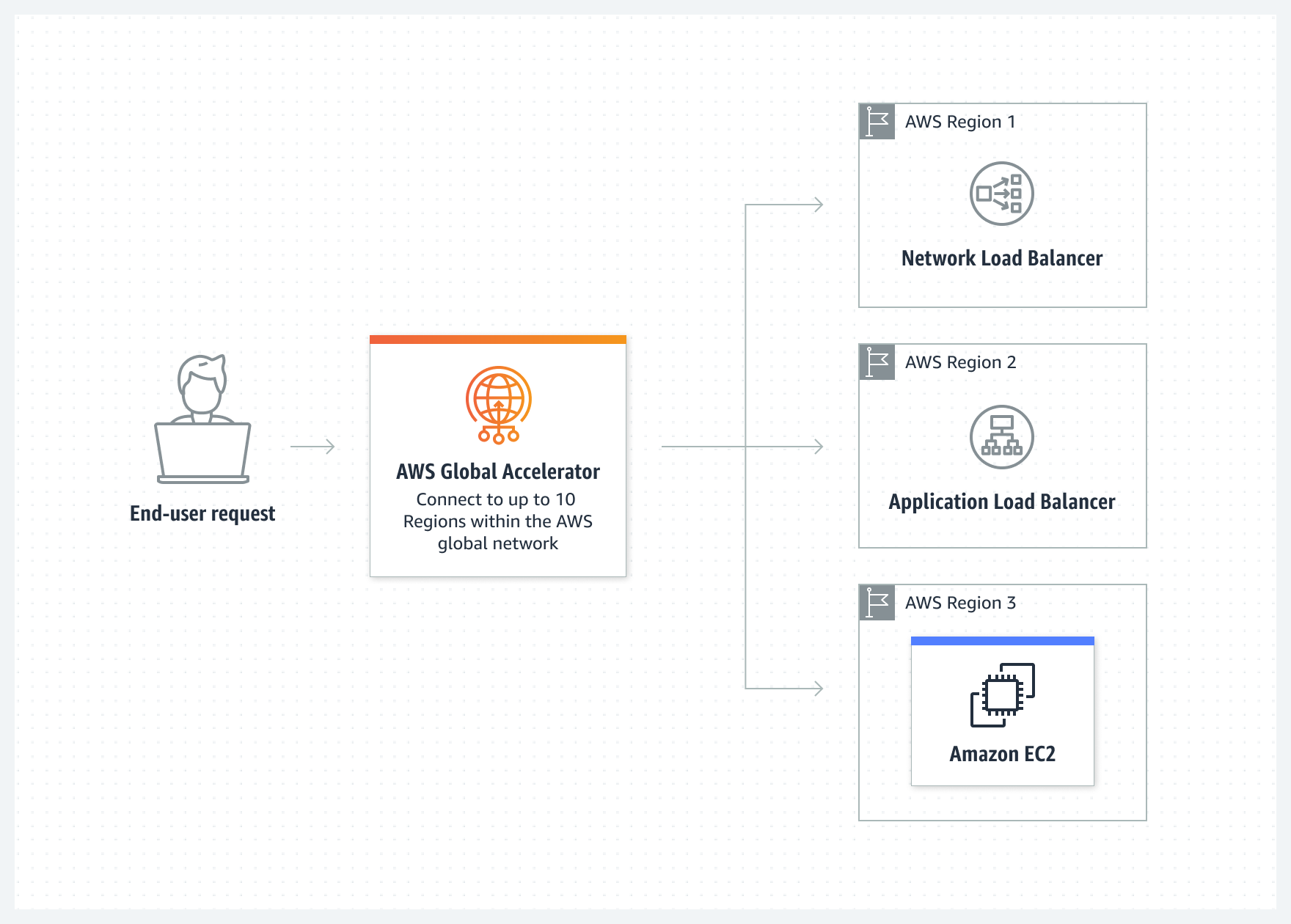
AWS Glue – job bookmarks

AWS Glue tracks data that has already been processed during a previous run of an ETL job by persisting state information from the job run. This persisted state information is called a job bookmark. Job bookmarks help AWS Glue maintain state information and **prevent the reprocessing of old data.**

**Protect EC2 instance from DDOS**

* Use AWS Shield Advanced to stop the DDoS attack.
* using CloudFront, the solutions architect can distribute the website's content across multiple edge locations, which can help absorb the impact of a DDoS attack and reduce the risk of downtime for the website.

Global accelerator connect multiple load balancer/ EC2 at once



Encrypted  an unencrypted Amazon RDS DB instance

"You can enable encryption for an Amazon RDS DB instance when you create it, but not after it's created. However, you can add encryption to an unencrypted DB instance by creating a snapshot of your DB instance, and then creating an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot to get an encrypted copy of your original DB instance."

SSL offloading

If SSL encryption and decryption is causing the compute capacity of the web servers, using ACM to manage the SSL certificate and configuring an ALB with HTTPS listener, the SSL termination will be handled by the load balancer instead of the web servers

# Amazon RDS Custom

# Amazon RDS Custom brings the benefits of Amazon RDS to a market that can't easily move to a fully managed service because of customizations that are required with third-party applications. Amazon RDS Custom saves administrative time, is durable, and scales with your business.

# DB cost

# Aurora Serverless scales the database up or down based on the workload, which helps to minimize costs during idle periods.

# When you implement Amazon RDS for MySQL for the database, you pay for the computing and storage resources whether or not you are actively using them. This means you would be charged even during idle periods,

**Aurora Failover**

In the event of system failure on the primary database instance, If you have an Amazon Aurora Replica in the same or a different Availability Zone, when failing over, Amazon Aurora **flips the canonical name record (CNAME) for your DB Instance** to point at the healthy replica, which in turn is promoted to become the new primary. Start-to-finish failover typically completes within 30 seconds. If you do not have an Amazon Aurora Replica (i.e., single instance) and are not running Aurora Serverless, Aurora will attempt to create a new DB Instance in the same Availability Zone as the original instance. This replacement of the original instance is done on a best-effort basis and may not succeed, for example, if there is an issue that is broadly affecting the Availability Zone.

**Amazon Aurora** typically involves a cluster of DB instances instead of a single instance. Each connection is handled by a specific DB instance. When you connect to an Aurora cluster, the hostname and port that you specify point to an intermediate handler called an endpoint. Aurora uses the endpoint mechanism to abstract these connections. Thus, you don’t have to hardcode all the hostnames or write your own logic for load-balancing and rerouting connections when some DB instances aren’t available.

Aurora Global Database supports storage-based replication that has a latency of less than 1 second

**Direct Read/ write Traffic in Aurora**

Create a custom endpoint in Aurora based on the specified criteria for the production traffic and another custom endpoint to handle the reporting queries.

# **Reserved Instances**

# - Unused Standard Reserved Instances can later be sold at the Reserved Instance Marketplace.

# - Convertible Reserved Instances allow you to exchange for another convertible reserved instance of a different instance family.

# identity federation - a single sign-on (SSO) capability

**- Setup a Federation proxy or an Identity provider**

**- Setup an AWS Security Token Service to generate temporary tokens**

**- Configure an IAM role and an IAM Policy to access the bucket.**

# S3 Event Notifications

Currently, Amazon S3 can publish notifications for the following events and send to **SNS, SQS, lambda & EventBridge**:

* New object created events
* Object removal events
* Restore object events
* Reduced Redundancy Storage (RRS) object lost events
* Replication events
* S3 Lifecycle expiration events
* S3 Lifecycle transition events
* S3 Intelligent-Tiering automatic archival events
* Object tagging events
* Object ACL PUT events

Monolithic/ micro-service -> ECS is needed

DB instances for Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and Microsoft SQL Server use Amazon Elastic Block Store (Amazon EBS) volumes for database and log storage.

**General Purpose SSD** – medium-sized DB instances, best suited for development and testing environments.

**Provisioned IOPS SSD** –designed to meet the needs of I/O-intensive workloads, particularly database workloads, that require low I/O latency and consistent I/O throughput. Provisioned IOPS storage is best suited for production environments.

**Magnetic** – Amazon RDS also supports magnetic storage for backward compatibility. We recommend that you use General Purpose SSD or Provisioned IOPS SSD for any new storage needs. The maximum amount of storage allowed for DB instances on magnetic storage is less than that of the other storage types. For more information, see [Magnetic storage](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html#CHAP_Storage.Magnetic).

**Ensure resource only on 1 specific regions:**

With Control Tower’s new **data residency guardrails** you can specify the AWS Region or Regions your **customer data** is stored and processed in, and if you need even more granular control, you can choose from 17 new guardrails that are purpose-built to enable data residency controls, such as "Disallow Amazon Virtual Private Network (VPN) connections”, or “Disallow internet access for an Amazon VPC instance”. You can see the compliance status of the guardrails and whether your data residency requirements are being met in the AWS Control Tower console.

**Prevent any VPC that doesn't already have internet access from getting it**

This SCP prevents users or roles in any affected account from changing the configuration of your Amazon EC2 virtual private clouds (VPCs) to grant them direct access to the internet. It doesn't block existing direct access or any access that routes through your on-premises network environment.

Egress-only internet gateways is only for IPv6

**"automated backup" = AWS Backup**

AWS Backup provides a centralized console, automated backup scheduling, backup retention management, and backup monitoring and alerting. AWS Backup offers advanced features such as lifecycle policies to transition backups to a low-cost storage tier. It also includes backup storage and encryption independent from its source data, audit and compliance reporting capabilities with AWS Backup Audit Manager, and delete protection with AWS Backup Vault Lock.

**Global Accelerator – for non-HTTP use cases!!!**

While Global Accelerator can improve global application performance, it is primarily used for accelerating TCP and UDP traffic, such as gaming and real-time applications, rather than serving static media files.

**Host dynamic content**

using Amazon API Gateway and AWS Lambda. Use Amazon DynamoDB (a severless DB)/ RDS (a server-based DB) with on-demand capacity for the database

**Amazon ElastiCache**

* Use **Redis** most of the time. But If multi-thread is needed, choose **Memcached**
* provide a shared data storage for sessions that can be accessed from any individual web server, when using with auto Discovery

**Amazon DynamoDB Time to Live (TTL)**

allows you to define a per-item timestamp to determine when an item is no longer needed, eg application needs only data from the last 30 days, set TTL as current timestamp + 30 days and the data will be delete afterward

**Two-Way Messaging**

With **Amazon Pinpoint**, you can create automatic responses when customers send you messages that contain certain keywords. Anytime you see marketing or campaign, just pick AWS Pinpoint.

**Lake Formation for manage fine-grained data permissions**

Lake Formation enables the creation of a secure and scalable data lake on AWS, **allowing centralized access controls for both S3 and RDS data**. By using Lake Formation, the company can manage permissions effectively and integrate RDS data through the AWS Glue JDBC connection. Registering the S3 in Lake Formation ensures unified access control. This solution **reduces operational overhead while providing fine-grained permissions management.**

Improve querying in Athena

**Amazon Athena** supports a wide variety of data formats like CSV, TSV, JSON, or Textfiles and also supports open-source columnar formats such as Apache ORC and Apache Parquet. Athena also supports compressed data in Snappy, Zlib, LZO, and GZIP formats. By compressing, partitioning, and using columnar formats you can improve performance and reduce your costs. **Apache Parquet** is an open-source columnar storage format that is 2x faster to unload and takes up 6x less storage in Amazon S3 as compared to other text formats

# Monitor AMI events using Amazon EventBridge

When the state of an Amazon Machine Image (AMI) changes, Amazon EC2 generates an event that is sent to Amazon EventBridge (formerly known as Amazon CloudWatch Events). You can use Amazon EventBridge to detect and react to these events. You do this by creating rules in EventBridge that trigger an action in response to an event. For example, you can create an **EventBridge rule that detects when the AMI creation process** has completed and then **invokes an Amazon SNS topic to send an email notification** to you.

**Distributed session data management across multiple Availability Zones**

Use Amazon ElastiCache to manage and store session data

AWS Glue allows fully managed CSV to Parquet conversion jobs

**Amazon Route 53 multivalue answer routing policy**

Multivalue answer routing distributes DNS responses across multiple IP addresses. If a web server becomes unavailable after a resolver caches a response, a client can try up to eight other IP addresses from the response to avoid downtime. Multivalue answer routing is not a substitute for Elastic Load Balancing (ELB). Route 53 randomly selects any eight records

**Notification when RDP or SSH access to an environment has been established**

Publish VPC flow logs to Amazon CloudWatch Logs. Create required metric filters. Create an Amazon CloudWatch metric alarm with a notification action for when the alarm is in the ALARM state. **Most Voted**

we need AWS Schema Conversion Tool to convert from Oracle to Aurora PostgreSQL

VPC Peering can use across account.

**Procedure before adding read replicas**

Before adding read replicas, one needs to allow long-running transactions to complete on the source DB instance otherwise you might end up interrupting transactions. The, you should enable automatic backups on the source instance and set the backup retention period to a value other than 0.

**FSx-AD integration**

Amazon FSx works with Microsoft Active Directory (AD) to integrate with your existing Microsoft Windows environments. Active Directory is the Microsoft directory service used to store information about objects on the network and make this information easy for administrators and users to find and use. These objects typically include shared resources such as file servers and network user and computer accounts.

IAM roles are global services that are available to all regions hence

**How to configure the DNS zone apex record to point to the load balancer?**

Create an A record aliased to the load balancer DNS name in Route 53. AWS Route 53 Alias targets any AWS resource that has a publicly resolvable DNS name, which updates automatically if the IP address of the AWS resource changes

Tranfer data between ec2 instances in the VPCs in two different regions:

* Set up a VPC peering connection between the VPCs.
* Re-configure the route table’s target and destination of the instances’ subnet.

Out of service from the load balancer

* The health check configuration is not properly defined.

CloudTrail log files

By default, CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encrypt your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about log file delivery and validation, you can set up Amazon SNS notifications.

**Amazon CloudWatch Application Insights**

facilitates observability for your applications and underlying AWS resources. It helps you set up the best monitors for your application resources to continuously analyze data for signs of problems with your applications. Application Insights, which is powered by SageMaker and other AWS technologies, provides automated dashboards that show potential problems with monitored applications, which help you to quickly isolate ongoing issues with your applications and infrastructure. The enhanced visibility into the health of your applications that Application Insights provides helps reduce the “mean time to repair” (MTTR) to troubleshoot your application issues.

**ELB access log**

Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client’s IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues.

**IAM Identity Center**

* AWS IAM Identity Center (successor to AWS Single Sign-On) provides single sign-on access for all of your AWS accounts and cloud applications
* Supported identity sources include Microsoft Active Directory Domain Services, and external identity providers such as Okta Universal Directory or Microsoft Azure AD.
* You can use multi-account permissions to assign your workforce users access to AWS accounts.
* you can grant your workforce users in IAM Identity Center single sign-on access to SAML 2.0 applications

**EC2 state charging**

* running
* termination for researved instance
* hibernate stopping (but not for stopped) + EBS storage for any Amazon EBS volumes

Network vs application load balancer

DynamoDB table with CloudFront as these two are incompatible.



Amazon EKS - containerized applications with current tools

since Kubernetes is an open-source platform and is considered **cloud-agnostic**. With Kubernetes, you can use the same configuration and tools that you're currently using in AWS even if you move your containers to another cloud service provider.

AWS X-Ray

AWS X-Ray is a service that collects data about requests that your application serves, and provides tools that you can use to view, filter, and gain insights into that data to identify issues and opportunities for optimization. For any traced request to your application, you can see detailed information not only about the request and response, but also about calls that your application makes to downstream AWS resources, microservices, databases, and web APIs.

**Storage optimized instances** are designed for workloads that require high, sequential read and write access to very large data sets on local storage.

**Memory Optimized Instances** are designed to deliver fast performance for workloads that process large data sets in memory.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | FSx for Window | FSx for lustre | File gateway |  | EFS | |
| protocol | **SMB/ NFS** |  | **NFS/ SMB** |  | NFS | |
| **Integrates with AD** | yes |  |  |  |  | |
| system | window | **Linux – POXIS** | Any |  | **Linux – POXIS** | |
|  | Integrate with same access method |  | S3 as file system |  |  | |
|  |  |  |  |  |  | |
|  |  |  |  |  |  | |
|  |  |  |  |  | |  |

**lifecycle hook of Auto Scaling group**

A picture containing text, screenshot, diagram, font

Description automatically generated

**Traffic routing between AWS and external system (on-premise/ other VPCs)**

* Use Application Elastic Load balancer with Weighted Target Groups, OR
* Use Route 53 with Weighted routing policy
* Connection to on-premises IP is required (e.g. via a peered VPC/ Direct Connect/ VPN)

**Short-lived authentication token to connect to the RDS-DB**

Use IAM DB Authentication and create database accounts using the AWS-provided AWSAuthenticationPlugin plugin in MySQL, only supported in MySQL and PostgreSQL

**prevent traffic from traversing to the public internet**

Using a Network Access Control List (NACL) alone is not sufficient to prevent traffic from traversing to the public internet in AWS because NACLs operate at the subnet level and control inbound and outbound traffic based on IP addresses, whereas the internet gateway and route tables handle the actual routing of traffic.

**Trusted Advisor**

Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. It only provides you alerts on areas where you do not adhere to best practices and tells you how to improve them. It does not assist in maintaining governance over your AWS accounts.

AWS Global Accelerator 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.

**Transparent data encryption** (TDE) is primarily used to encrypt stored data on your DB instances running Microsoft SQL Server, does not protect data in transit nor data in use.

Notification before the expiration of the SSL certificates in ACM (2 ways)

* **Create an Amazon EventBridge (Amazon CloudWatch Events) rule that will check AWS Health or ACM expiration events related to ACM certificates. Send an alert notification to an Amazon Simple Notification Service (Amazon SNS) topic when a certificate is going to expire in 30 days**
* **Create an Amazon EventBridge (Amazon CloudWatch Events) rule and schedule it to run every day to identify the expiring ACM certificates. Configure to rule to check the DaysToExpiry metric of all ACM certificates in Amazon CloudWatch. Send an alert notification to an Amazon Simple Notification Service (Amazon SNS) topic when a certificate is going to expire in 30 days.**

**AWS Elastic Beanstalk** log

Application files are stored in S3. The server log files can also optionally be stored in S3 or in CloudWatch Logs.

AWS Elastic Beanstalk simply sets up the infrastructure (EC2 instance, load balancer, auto-scaling group) for your application. Elastic Beanstalk supports applications developed in Go, Java, .NET, Node.js, PHP, Python, and Ruby.

**Amazon S3 IA (standard/ one-zone)**

this storage class has a minimum storage duration of at least 30 days, not suitable for temporary storage

**bastion host**

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. If you have a bastion host in AWS, it is basically just an EC2 instance. It should be in a public subnet with either a public or Elastic IP address with sufficient RDP or SSH access defined in the security group. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets.

A diagram of a server

Description automatically generated

**Lambda function URLs** are HTTP(S) endpoints dedicated to your Lambda function. You can easily create and set up a function URL using the Lambda console or API. Once created, Lambda generates a unique URL endpoint for your use (by sending an HTTP POST request to trigger the function.). This also simplifies the architecture since there is no need to set up and manage an intermediary service such as API Gateway.

shards of the Kinesis stream can be scaled by UpdateShardCount command to respond in real time to changes in your streaming data needs

origin failover in CloudFront

you must have at least two origins to set up an origin failover in CloudFront. In addition, you can’t directly use a single Auto Scaling group as an origin.

EC2 placement group

If you try to add more instances to the placement group later, or if you try to launch more than one instance type in the placement group, you increase your chances of getting an insufficient capacity error. Stop and restart the instances in the Placement group and then try the launch again can resolve this issue.

S3 Object Ownership

By default, an S3 object is owned by the AWS account that uploaded it even though the bucket is owned by another account. To get full access to the object, the object owner must explicitly grant the bucket owner access. You can create a bucket policy to require external users to grant bucket-owner-full-control when uploading objects so the bucket owner can have full access to the objects.

A drawing of a bucket

Description automatically generated

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. You can create Capacity Reservations at any time, without entering into a one-year or three-year term commitment, and the capacity is available immediately.

A screenshot of a computer

Description automatically generated

To reduce the data transfer costs between EC2 instances, deploy the Amazon EC2 instances in the same Availability Zone

**Amazon Inspector, GuardDuty, detective, Trusted Advisor**

* **Inspector** Performs active vulnerability scans of EC2 instances. It looks for software vulnerabilities, unintended network accessibility, and other security issues (agent is required)
* **GuardDuty** specializes in real-time threat detection and monitoring, eg unusual API calls, unauthorized infrastructure deployments, or compromised EC2 instances. It uses machine learning and behavioral analysis of logs. visualize the graph model to correlate events (agent is not required)
* **Detective** aids in security investigations and analysis of **collected logs**
* **Trusted Advisor** provides security recommendations based on the infrastructure

**Amazon GuardDuty**

* can detect potential threats by analysing VPC flow logs, it can’t prevent those threats from entering or leaving your VPC
* is just a threat detection service. You should use AWS WAF’s rate-based rules for mitigating HTTP flood attacks
* cannot directly be integrated with the Application Load Balancer

**AWS Network Firewall**

- is a stateful, managed, network firewall, and intrusion detection and prevention service for your virtual private cloud (VPC)

- enables you to define custom security rules and policies to monitor and control the traffic flow passing to and from your VPC. You can use Network Firewall to monitor and protect your Amazon VPC traffic in a number of ways, including the following:

- Pass traffic through only from known AWS service domains or IP address endpoints, such as Amazon S3.

* Use custom lists of known bad domains to limit the types of domain names that your applications can access.
* Perform deep packet inspection on traffic entering or leaving your VPC.
* Use stateful protocol detection to filter protocols like HTTPS, independent of the port used
* monitor both incoming and outgoing VPC traffic and block any malicious connections.

**CloudTrail log file validation**

This helps to determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it.

**Read IAM policies:**  
[Condition] is [allow/deny] the [action] in [resource]

**AWS Compute Optimizer** recommends optimal AWS resources for your workloads to reduce costs and improve performance by using machine learning to analyze historical utilization metrics. It helps to strike a good amount of resource provision. Cloudwatch metric can do the work but it requires many entails a lot of manual work for each instance

**CloudWatch Logs subscription**

You can use subscriptions to get access to a real-time feed of log events from CloudWatch Logs and have it delivered to other services such as an Amazon Kinesis stream, an Amazon Kinesis Data Firehose stream, or AWS Lambda for custom processing, analysis, or loading to other systems.

**AWS Proton =** deployment on standard templates (CI/CD)

**AWS Proton** allows you to deploy any serverless or container-based application with increased efficiency, consistency, and control. You can define infrastructure standards and effective continuous delivery pipelines for your organization. Proton breaks down the infrastructure into environment and service (“infrastructure as code” templates). As a developer, you select a standardized service template that AWS Proton uses to create a service that deploys and manages your application in a service instance. An AWS Proton service is an instantiation of a service template, which normally includes several service instances and a pipeline.

For shared storage between Linux and windows you need to implement Amazon FSx for NetApp ONTAP

**Dynamic Contact Forms for S3 Static Websites**

* Using AWS Lambda, Amazon API Gateway, and Amazon SES
* [**https://aws.amazon.com/blogs/architecture/create-dynamic-contact-forms-for-s3-static-websites-using-aws-lambda-amazon-api-gateway-and-amazon-ses/**](https://aws.amazon.com/blogs/architecture/create-dynamic-contact-forms-for-s3-static-websites-using-aws-lambda-amazon-api-gateway-and-amazon-ses/)
* A diagram of a logo

  Description automatically generated

Data transformation can be done in Amazon Kinesis Data Analytics as well, not only AWS Glue

S3 Storage Lens is a fully managed S3 storage analytics solution that provides a comprehensive view of object storage usage, activity trends, and recommendations to optimize costs. Storage Lens allows you to analyze object access patterns across all of your S3 buckets and generate detailed metrics and reports.

### **[Amazon Elastic Transcoder](https://aws.amazon.com/elastictranscoder/)**

# Application Auto Scaling