1. **Shield Advanced** is not free service, it protects against more sophisticated attack on EC2, Elastic Load Balancer, CloudFront, Global Accelerator, and Route 53.
2. **AWS WAF – Web Application Firewall**, protect your web applications from common web exploits, works in layer 7 (HTTP). We can deploy it on
   * Application Load Balancer,
   * API Gateway,
   * CloudFront.

we can defend ourselves again for IP addresses, SQL injection, Cross-Site Scripting, size constrain of request queries, geo-match, rate-based rules, and DDoS protection. **AWS Firewall Manager** is used to manage rules in all account of an AWS organization.

1. **Amazon GuardDuty** - is an intelligent threat discovery service (monitor any malicious activity), by using machine learning algorithm, anomaly detection and 3rd party data. Input data to find the threat are,
   * CloudTrail Logs(Management Event and Data Event),
   * VPC Flow Logs,
   * DNS Logs.

Also, can protect against Cryptocurrency attack.

**Amazon GuardDuty** offers threat detection that enables you to continuously monitor and protect your AWS accounts, workloads, and data stored in Amazon S3.

1. **Amazon Inspector** is only for EC2 instances. Used for automated security assessments (check for any vulnerabilities on EC2 instances). We need to install the AWS Inspector agent must be installed on OS in EC2 instances. Then the assessment result will be sent to SNS topic for further operation. Network assessments (agentless), Host assessments (with Agent).
2. **Macie** is a fully managed data security and data privacy service that will use machine learning and pattern matching to discover and protect your sensitive data in AWS. More specifically, it will alert you around sensitive data, such a personally identifiable information, which is named PII.
3. To enable **In-flight Encryption** (In-Transit Encryption), we need to have an HTTP endpoint with an SSL certificate. In-flight Encryption = HTTPS, and HTTPS cannot be enabled without an SSL certificate.
4. KMS keys can be symmetric or asymmetric. A **symmetric KMS** key represents a 256-bit key used for encryption and decryption. An **asymmetric KMS** key represents an RSA key pair used for encryption and decryption or signing and verification, but not both. Or it represents an elliptic curve (ECC) key pair used for signing and verification.
5. **SSM Parameters Store** (serverless)can be used to store secrets and has built-in version tracking capability. Each time you edit the value of a parameter, SSM Parameter Store creates a new version of the parameter and retains the previous versions. You can view the details, including the values, of all versions in a parameter's history.
6. **KMS Key Policies** are used to control access to your KMS CMKs.
7. **AWS Firewall Manager** allows you to centrally manage EC2 Security Groups and AWS Shield Advanced across all AWS accounts in your AWS Organization.
8. **AWS Secrets Manager** is the most suitable AWS service for storing RDS DB passwords which also provides you automatic rotation.
9. CIDR – Classless Inter-Domain Routing, it has two components,

The base IP – IP contained in the range.

The Subnet – How many bits can change in IP.

1. /32- 32 bits are fixed so no IP can change – only one IP can use

/24 – 24 bits are fixed so Last IP can change

1. **Maximum CIDR** per VPC is 5, Min size is /28 = 16 IP address, Max size is /16 = 65536 IP address.
2. AWS will **reserve five IP addresses**, the first four and the last one in each subnet.
3. E.g.: CIDR Block 10.0.0.0/24, reserved IP are,

10.0.0.0: Network Address

10.0.0.1: Reserved by AWS for the VPC router

10.0.0.2: Reserved by AWS for mapping to Amazon-provided DNS

10.0.0.3: Future use

10.0.0.255: Network broadcast address. AWS does not support broadcast in a VPC; therefore, the address is reserved.

1. **Internet Gateway** helps our VPC instance to connect to the internet. Must be created separately from VPC. Route tables must also be edited. One VPC can only be attached to one Internet gateway and vice versa. It acts as a NAT (Network address translation) for the instance that have a public IPV4.
2. We have our instances in our public subnet that have internet connectivity by using internet gateway. But for our instances in our private subnet, they cannot access the internet. If they want to access it through the internet gateway, they would also be directly accessible from the internet. So, for this, we need a better solution, and that solution is a NAT. NAT stands for **Network Address Translation**.
3. For NAT instance we should disable Source/Destination Check. Other than NAT instance it should be enabled for all other instances. If this is a NAT instance, you must stop **source / destination checking**. A NAT instance must be able to send and receive traffic when the source or destination is not itself. Each EC2 instance performs source and destination checks by default. The instance must be the source or destination of all the traffic it sends and receives.
4. **Security groups** are stateful, that means, no matter what, If the Inbound rule passes then the outbound rule pass as well, even if there is a rule to deny any traffic out of the EC2 instance.
5. **Network access control list (NACL)** is stateless, means outbound traffic rules will get evaluated.
6. Therefore, the difference between Security group and Network Access Control, NACL will evaluate both inbound and outbound rules for all request, but the security group only check the inbound rules, if the inbound rules allowed to enter the traffic get into security group, then the outbound rule will allow the particular request to go out without checking it.
7. The **Security group** supports allow rules only, the **network ACL** allow both allow and deny rules.
8. A **VPC peering** allows you to connect two VPC privately by using AWS's network directly. Must not have a overlapping CIDR. Not transitive (~~A->B->C~~ / A->B, B->C, A->C). It also can work inter-region, cross account.
9. If a subnet's traffic is routed to an internet gateway, the subnet is known as a **Public Subnet**. If a subnet doesn't have a route to the internet gateway, the subnet is known as a **Private Subnet**.
10. **VPC Reachability Analyzer** - it's a network diagnostics tool that helps you troubleshoot network connectivity between two end points in your VPC. All of this is done by just analyzing network configuration, not by sending packets.
11. **VPC Flow Logs** – Capture information about IP traffic going into your interfaces.
12. **Direct connect (DX)**- it provides a dedicated private connection from the remote network into your VPC.
13. **Direct Connect Gateway –** If you want to setup a direct connect to one or more VPC in many different regions (Same account), You must use a direct connect Gateway.
14. **AWS PrivateLink (VPC Endpoint Services)** – Most secure & scalable way to expose a AWS service to 1000s of VPC (own or other account).
15. **Traffic Mirroring** – Allows you to capture and inspect network traffic in your VPC without disturbing the functionality of the device.
16. **Egress only Internet Gateway** – Used for IPV6 only, Similar to a NAT Gateway but for IPV6. Allow instances in your VPC outbound connections over IPV6 while preventing the internet to initiate an IPV6 connection to your instances.
17. Route tables must be updated in both VPCs that are peered.
18. **Amazon S3 and DynamoDB -** These two services using the VPC Gateway Endpoint (remember it), all the other ones using an Interface endpoint (powered by Private Link - means a private IP).
19. A **Dedicated Direct Connect** connection supports 1Gbps and 10Gbps.
20. AWS **VPN CloudHub** allows you to securely communicate with multiple sites using AWS VPN. It operates on a simple hub-and-spoke model that you can use with or without a VPC.
21. Using a **Direct Connect connection**, you can access both public and private AWS resources.
22. **AWS DataSync** (Simplify and accelerate secure (encrypted connection)data migrations) supports the following locations, EXCEPT Amazon EBS. It will support, Amazon S3, Amazon EFS, Amazon FSx for windows and NFS/SMB . It has DataSync Agent to install in the on-premises server to transfer the data. Can limit bandwidth. Replication tasks can be scheduled hourly, daily and weekly.
23. **Ongoing Replication / transfer** – Site -to-site VPN or DX or DMS or DataSync
24. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same subnet route table.
25. **Elastic Fabric Adapter (EFA)** is a network interface for Amazon EC2 instances that enables customers to run applications requiring high levels of inter-node communications at scale on AWS. Its custom-built operating system (OS) bypass hardware interface enhances the performance of inter-instance communications, which is critical to scaling these applications.
26. **AWS Trusted Advisor** service checks – cost optimization, performance, security, fault tolerance, service Limits.
27. In **EBS volumes (AZ locked) - gp2** (IO Increases if the disk size increases), io1(Increases IO independently) – only capable root volumes.
28. In **EFS** **(Multi AZ)** we need to pay only for how much we are using, But in EBS we need to provision the needed capacity while creating a disk, so we need to pay for whole provisioned memory.
29. An **Amazon EBS–optimized instance,** uses an optimized configuration stack and provides additional, dedicated capacity for Amazon EBS I/O. This optimization provides the best performance for your EBS volumes by minimizing contention between Amazon EBS I/O and other traffic from your instance.
30. **Burstable Instance (T2/T3)**– When the machine needs to process something unexpected (a spike in load for example) it can burst and CPU can be very good. Once the burst credits are over then it performs BAD.
31. When launching an EC2 instance, the EBS volume for root cannot be encrypted.
32. **S3 Cross region replication** cannot be enabled without enabling versioning.
33. **ECS Task Role** is the IAM Role used by the ECS task itself. Use when your container wants to call other AWS services like S3, SQS, etc. It will be defined in the task definition.
34. **EC2 Instance profile –** used by the ECS agent to make a call to ECS services likes sending container logs to CloudWatch Logs and PULL docker from ECR.
35. **ECS scaling –** have two types of scaling, **auto scaling** normally for scale-out the number of tasks (from CPU usage metrices). **Auto scaling Group with Scale ECS Capacity providers** if we are using the EC2 containerized services instead of ECS Fargate. we can also scale the ECS by using the number of tasks in the SQS queue metrics.
36. **Dynamic port mapping** allows an Application Load Balancer to redirect traffic to multiple ECS Tasks running on the same ECS Container instance.
37. **CloudWatch** (metrics) focuses on the activity of AWS services and resources, reporting on their health and performance. On the other hand, **CloudTrail** is a log of all actions that have taken place inside your AWS environment.
38. In **S3 Standard storage class**, there is no minimum storage duration charge and no retrieval fee. But S3 Intelligent-Tiering, S3 Standard-IA, and S3 One Zone-IA have a minimum storage duration charge of 30 days. S3 Standard-IA and S3 One Zone-IA also have retrieval charges.
39. **Here are some of the best practices while creating an AWS account root user:**

1)Use a strong password to help protect account-level access to the AWS Management Console.

2) Never share your AWS account root user password or access keys with anyone.

3) If you do have an access key for your AWS account root user, delete it. If you must keep it, rotate (change) the access key regularly. You should not encrypt the access keys and save them on Amazon S3.

4) If you don't already have an access key for your AWS account root user, don't create one unless you absolutely need to.

5) Enable AWS multi-factor authentication (MFA) on your AWS account root user account.

1. ECS with EC2 launch type is charged based on EC2 instances and EBS volumes used. ECS with Fargate launch type is charged based on vCPU and memory resources that the containerized application requests.
2. **General Purpose SSD** (gp2), **Provisioned IOPS SSD** (io1), and **Instance Store** can be used as a boot volume.
3. A runtime is a version of a programming language or framework that you can use to write Lambda functions. **AWS Lambda supports runtimes for the following languages:**

C#/.NET, Go, Java, Node.js, Python, Ruby

1. You can use **Aurora replicas and CloudFront distribution** to make the application more resilient to spikes in request rates.
2. 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. 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.
3. AWS **Direct Connect** lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Using industry-standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces. AWS Direct Connect does not involve the Internet; instead, it uses dedicated, private network connections between your intranet and Amazon VPC.
4. Here are the **supported life cycle transitions for S3 storage classes** - The S3 Standard storage class to any other storage class. Any storage class to the S3 Glacier or S3 Glacier Deep Archive storage classes. The S3 Standard-IA storage class to the S3 Intelligent-Tiering or S3 One Zone-IA storage classes. The S3 Intelligent-Tiering storage class to the S3 One Zone-IA storage class. The S3 Glacier storage class to the S3 Glacier Deep Archive storage class.

Diagram

Description automatically generated

1. Kinesis Data Analytics cannot directly ingest data from the source as it ingests data either from Kinesis Data Streams or Kinesis Data Firehose,
2. **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. AWS Glue job is meant to be used for batch ETL data processing and it's not the right fit for a near real-time data processing use-case. It has metadata catalog feature.
3. **Amazon EMR** is a platform for processing and analyzing big data using open-source frameworks such as Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi and Presto. Amazon EMR uses Hadoop, an open-source framework, to distribute your data and processing across a resizable cluster of Amazon EC2 instances. Using an EMR cluster would imply managing the underlying infrastructure so it’s ruled out because the correct solution for the given use-case should require the least amount of infrastructure maintenance.
4. **Amazon RDS Multi-AZ** deployments provide enhanced availability and durability for RDS database (DB) instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Multi-AZ spans at least two Availability Zones within a single region.

**Amazon RDS Read Replicas** provide enhanced performance and durability for RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. For the MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server database engines, Amazon RDS creates a second DB instance using a snapshot of the source DB instance. It then uses the engines' native asynchronous replication to upda te the read replica whenever there is a change to the source DB instance. Amazon RDS replicates all databases in the source DB instance. Read replicas can be within an Availability Zone, Cross-AZ, or Cross-Region.

Graphical user interface, application

Description automatically generated

1. **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 offers two types of message queues **- Standard queues vs FIFO queues.** For FIFO queues, the order in which messages are sent and received is strictly preserved (i.e., First-In-First-Out). On the other hand, the standard SQS queues offer best-effort ordering. This means that occasionally, messages might be delivered in an order different from which they were sent.

By default, FIFO queues support up to 3,000 messages per second with batching, or up to 300 messages per second (300 send, receive, or delete operations per second) without batching. Therefore, using batching you can meet a throughput requirement of up to 3,000 messages per second.

1. Text

   Description automatically generatedMaximum execution time: 900 sec (15min) anything other than this time is not a good use case for **lambda**.
2. **DynamoDB** maximum item size is 400KB (1 Row data)
3. **DynamoDB** – Basic, Provisioned throughput, DAX (DynamoDB Accelerator), Streams.
4. **DynamoDB streams** – The changes in DynamoDB (Create,Update,Delete) will be stored in streams for analytics, react to changes in real time. (With 24hrs of data retention)
5. Due to cost difference, **DynamoDB is best for** read more than write more use cases.
6. **DynamoDB global table** – cross region replication, must enable streams in DynamoDB.
7. An **Edge-Optimized API Gateway** is best for geographically distributed clients. API requests are routed to the nearest CloudFront Edge Location which improves latency. The API Gateway still lives in one AWS Region.
8. **The OAI** (Origin Access Identity) is a virtual user identity that will be used to give your CloudFront distribution permission to fetch a private object from your origin server (e.g., S3 bucket).
9. **Amazon redshift is not serverless.**
10. **AWS SSO** (Single Sign-On)- makes it easy to centrally manage SSO access to all of your AWS accounts and cloud applications. It helps you manage SSO access and user permissions across all your AWS accounts in AWS Organizations. It also helps when you manage access and permissions to commonly used 3rd party software as a service (SaaS) application, AWS SSO-integrated applications as well as custom applications that support Security Assertion Markup Language (SAML) 2.0. AWS SSO also includes built-in SAML integrations to many business applications, such as Salesforce, Box, and Office 365.
11. **Amazon Cognito** lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Apple, Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0 and OpenID Connect.
12. **Security Groups** cannot be attached to SQS queues.
13. When using a Lambda function with S3, the Lambda function would need to be triggered immediately and can't be postponed until tomorrow to be run.
14. **CloudFront Signed URL** – This will have security including IP address restriction.
15. **Amazon Elasticsearch** Service is now Amazon OpenSearch Service, from an exam perspective, they're both the same, and both leverage ElasticSearch, which was renamed in one for OpenSearch.
16. **RDS** – small down time in fail over, managed services,5- read replica, Multi AZ, Performance based on EC2 instance and EBS volume we provisioned, storage auto scaling but scaling of instance need to do manually, pay per hour based on EC2 and Instance.
17. **Aurora** – both provisioned and serverless (need to select minimum required instance and storage (on demand capacity), then it will auto scale for future) options are available, only MySQL and PostgreSQL compatibility, 6 replicas, across 3AZ, Multi AZ, Read Replica can be global (by selecting the option), Multi Master option for more writes fail over, auto-scales up to 64TB per database instance. Aurora is not an in-memory database.
18. **Elastic cache** – Managed Redis/Memcached (similar to RDS but for cache), In memory data store, must provisioned EC2 instance, Support clustering and multi-AZ, Redis Auth for authentication of the users, point in time recovery, snapshot, backup, key/value store, Frequent read and less write, read replicas for sharding, pay per hour based on EC2 and storage usage.
19. **DynamoDB** – Serverless, NoSQL DB, on demand capacity, auto scaling, Multi AZ by default, DAX for read cache, global table feature, pay per provisioned capacity and storage usage.
20. **S3** – cross region replication in S3 need to enable versioning, by creating 2 buckets in different region we can select one as a replica for other by enabling replication rule. S3 is good for static file, key value store for big files and website hosting, pay per storage usage, network cost, requests number.
21. **Athena** – fully serverless DB, used to query data in S3, pay per query/per TB of data scanned, output results back to S3, uses presto engine.
22. **Redshift** – Not serverless, PostgreSQL, NOT used for OLTP, used for OLAP – Online Analytics processing, Columnar DB (used to improve disk I/O performance), NO Multi AZ, cross-region snapshot copy, pay per node provisioned, Leader node (perform query planning and result aggregation), Compute node (perform queries, send to leader node).
23. **Redshift Spectrum** – Query data directly from S3 without loading it, must have redshift cluster (with leader node and compute node) to start query.
24. Diagram

    Description automatically generated**AWS Glue** – Fully serverless, ETL service, Useful to prepare and transform data for analytics.
25. **AWS Glue catalog** – Catalog for dataset.
26. **Neptune** – Fully managed graph-based DB, highly relationship data, 3 AZ, up to 15 read replicas, continues backup to amazon S3.
27. **Elastic search** – you can search on any field, even partial match, used with other DBs, cluster of instances, comes with Kibana (visualization) and Logstash (log ingestion), for search and indexing.
28. **CloudWatch** – gives metrics for every AWS service, Metrics is a variable to monitor (CPU performance, N/W performance, etc.,), will have timestamps.
29. For **custom CloudWatch metrics**, use the API call “PutMetricData”.
30. **Metric filters** define the terms and patterns to look for in log data as it is sent to CloudWatch Logs. CloudWatch Logs uses these metric filters to turn log data into numerical CloudWatch metrics that you can graph or set an alarm on.
31. By default, no logs from your EC2 machine will go to CloudWatch, you need to run a CloudWatch agent on EC2 to push the log files you want.
32. **Amazon EventBridge** – Amazon EventBridge is a serverless event bus service that makes it easy to connect your applications with data from a variety of sources. EventBridge delivers a stream of real-time data from your own applications, software-as-a-service (SaaS) applications, and AWS services and routes that data to targets such as AWS Lambda. You can set up routing rules to determine where to send your data to build application architectures that react in real time to all of your data sources. EventBridge enables you to build event-driven architectures that are loosely coupled and distributed.
33. **CloudTrail** – provides governance, compliance, and audit for your AWS account. If some resource is deleted in AWS, check the CloudTrail first. Exist only 90days, for more retention save it in S3. Later we can analyse with Athena on S3.
34. Diagram

    Description automatically generated with low confidenceTypes of **Events in CloudTrail** – Management Events (Default, Free), Data Events(pay), **CloudTrail Insight Events** (pay, out of lot of events it helps to detect the unusual activity).
35. **AWS Config** - Record and evaluate configurations of your AWS resources.
36. **How would you monitor your EC2 instance memory usage in CloudWatch?**

**Ans:** Use the Unified CloudWatch Agent to push memory usage as a custom metric to CloudWatch.

1. If you set an alarm on a high-resolution metric for CloudWatch Alarm, you can specify a high-resolution alarm with a period of 10 seconds or 30 seconds, or you can set a regular alarm with a period of any multiple of 60 seconds. ( used to trigger alarm)
2. **AWS Config Remediations** – Automatically re-configure (Check it)
3. **EC2 Detailed Monitoring** - This is a paid offering and is disabled by default. When enabled, the EC2 instance's metrics are available in 1-minute periods.
4. High-Resolution CloudWatch Custom Metrics can have a minimum resolution of 1second.( Used to send the metrics).
5. When you are using IAM Role, you must give up your original permission and take the permission assigned to the role, but the Resource based policies (S3 bucket policy, etc.,) the principle does not have to give up his permission.
6. AWS supports **permissions boundaries for IAM** entities (users or roles). A permissions boundary is an advanced feature for using a managed policy to set the maximum permissions that an identity-based policy can grant to an IAM entity. An entity's permissions boundary allows it to perform only the actions that are allowed by both its identity-based policies and its permissions boundaries.
7. **AWS Resource Access Manager (RAM)** – Share AWS resources that you own with other AWS accounts, share with any account or within your organization.
8. IAM policies allow or deny access to AWS services or API actions [that work with IAM](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html). An IAM policy can be applied only to [IAM identities (users, groups, or roles)](https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html). IAM policies can't restrict the [AWS account root user](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html).

You can use SCPs to allow or deny access to AWS services for individual AWS accounts with AWS Organizations [member accounts](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html#account), or for groups of accounts within an [organizational unit (OU)](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_ous.html). The specified actions from an attached SCP affect all IAM identities including the [root user](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_example-scps.html) of the member account.

1. You have strong regulatory requirements to only allow fully internally audited AWS services in production. You still want to allow your teams to experiment in a development environment while services are being audited. How can you best set this up?

**Ans:** create an AWS Organization and create two prod and Dev OUs, then apply an SCP (service control policy) on the prod OU.

1. You have an on-premises Microsoft Active Directory setup, and you would like to provide access for your on-premises AD users to the multiple AWS accounts you have. The solution should be scalable for adding accounts in the future. What do you recommend?

**Ans:** Setup AWS Single Sign-On

1. **WAF** can be deployed in ALB, API Gateway, CloudFront.
2. **Kinesis Data Analytics** cannot directly ingest data from the source as it ingests data either from Kinesis Data Streams or Kinesis Data Firehose.
3. **Each DNS record** has a **TTL** (Time to Live) which orders clients for how long to cache these values and not overload the DNS Resolver with DNS requests. The TTL value should be set to strike a balance between how long the value should be cached vs. how many requests should go to the DNS Resolver.
4. There is no Security Group for network load balancer, but we can use WAF IP address filtering with it.
5. **Elastic Fibric Adapter** – Improved ENA (Elastic Network adapter – Higher bandwidth, Higher PPS, Low latency) for HPC, only works for Linux. Great for inter-node communications, tightly coupled workloads.
6. **ENA** – Elastic Network adapter(100Gbps). **EFA** - Elastic Fibric Adapter, **ENI** – Elastic Network Interface.
7. **DataSync** – Move large amount of data between on premise and S3, EFS, FSx for windows. We need to install DataSync Agent.
8. **AWS Batch** -supports multimode parallel jobs, which enables you to run a single job that span multiple EC2 instance.
9. **AWS ParallelCluster** – Open-source cluster management tool to deploy HPC on AWS, configure with text files, Automate creation of VPC, Subnet, Cluster type and instance type.
10. **Bastion Host** – used to SSH into a private EC2 instance. The Bastion host will be deployed in the public network. We need to use the network load balancer to route the traffic to Bastion host because application load balancer is deal with (Layer 7) HTTP traffic, but SSH is a low-level traffic, Network Load balancer is (layer 4) deal with lower traffics.
11. **CodeCommit** – is like GitHub where developer push their code to this repository.
12. **CodeBuild** (build & test)– is like Jenkins CI which test / build server to check the code as soon it’s pushed.

Graphical user interface, application, PowerPoint

Description automatically generated

1. **CloudFormation** - Speed up cloud provisioning with infrastructure as code
2. **CloudFormation StackSet** – Create, update, or delete stacks across multiple accounts and regions with a single operation.
3. **AWS Step Functions** – Build serverless visual workflow to orchestrate your Lambda functions. State Machine, workflow, Lambda orchestration.
4. **AWS SWF – (**Simple Workflow Service), Coordinate work among application. (Almost same like step function but it is bit old) code runs on EC2 (not serverless) Step Functions is recommended to be used for new applications expect if you need external signals or child processes then the SWF is best.
5. **AWS EMR – Elastic Map Reduce** – Helps creating Hadoop clusters (Big Data) to analyze and process vast amount of data also supports Apache Spark, HBase, Presto, Flink.
6. Logo, company name

   Description automatically generated**AWS Opsworks** – Managed chef and Puppet (chef and puppet help you perform server configuration automatically or repetitive actions / called as configuration as code). A picture containing text, clipart

   Description automatically generated
7. **AWS WorkSpaces** – Managed, Secure Cloud Desktop. Great to eliminate management of on-premises VDI (Virtual Desktop Infrastructure). Secure, Encrypted, Network Isolation.
8. **AWS AppSync –** Store and sync data across mobile and web apps in real-time. Make use of GraphQL (Mobile technology from Facebook).
9. **ElasticTranscoder -** managed media (video, music) converter service into various optimized formats.
10. **CodePipeline** - orchestrate the actions of your CICD pipelines (build stages, manual approvals, many deploys, etc.)
11. **AWS Cost Explor**er enables you to view and analyze your costs and usage. You can view data for up to the last 12 months, forecast how much you are likely to spend for the next 12 months, and get recommendations for what EC2 reserved instances to purchase.

**FROM QUESTION AND ANSWER**

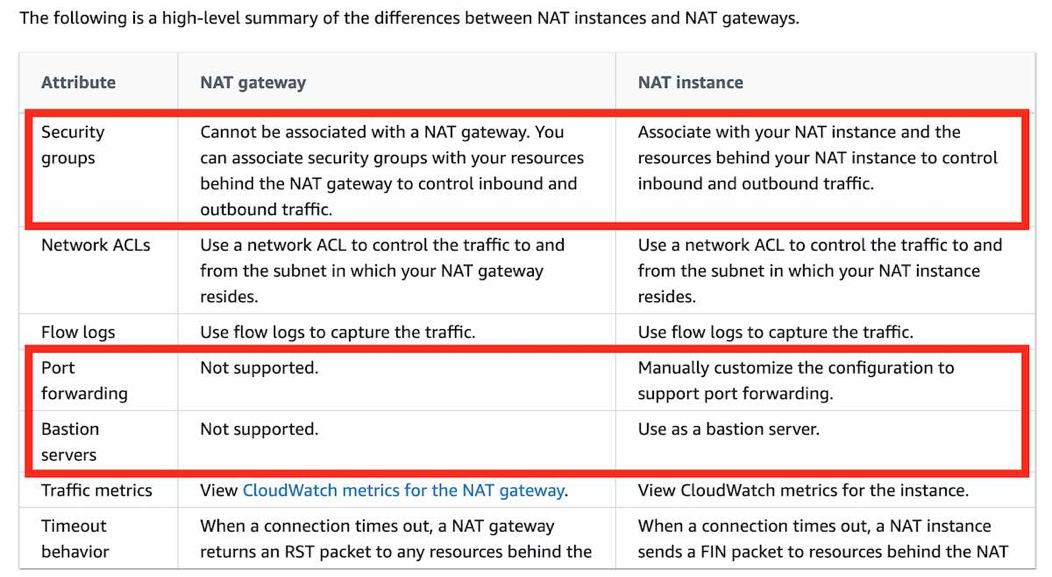
1. You control which EC2 instances can access your EFS file system by using VPC security group rules and AWS Identity and Access Management (IAM) policies. Use VPC security groups to control the network traffic to and from your file system. Attach an IAM policy to your file system to control which clients can mount your file system and with what permissions and use EFS Access Points to manage application access. Control access to files and directories with POSIX-compliant user and group-level permissions.

**Note:** Network ACLs operate at the subnet level and not at the instance level.

1. **Amazon API Gateway, Amazon SQS and Amazon Kinesis** – (to throttle the sudden spike) To prevent your API from being overwhelmed by too many requests, Amazon API Gateway throttles requests to your API using the token bucket algorithm, where a token counts for a request. Specifically, API Gateway sets a limit on a steady-state rate and a burst of request submissions against all APIs in your account. In the token bucket algorithm, the burst is the maximum bucket size.

**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. Amazon SQS offers buffer capabilities to smooth out temporary volume spikes without losing messages or increasing latency.

**Amazon Kinesis** - Amazon Kinesis is a fully managed, scalable service that can ingest, buffer, and process streaming data in real-time.

1. **Global Accelerator** improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. 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.
2. **AWS Global Accelerator and Amazon CloudFront** are separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable content (such as images and videos) and dynamic content (such as API acceleration and dynamic site delivery), while Global Accelerator improves performance for a wide range of applications over TCP or UDP.
3. ELB provides load balancing within one Region, AWS Global Accelerator provides traffic management across multiple Regions.
4. When you create a **Application load Balancer- target group**, you specify its target type, which can be an Instance, IP or a Lambda function. For IP address target type, you can route traffic using any private IP address from one or more network interfaces but not public routable IP address, so you can’t use Public IP in your target group.
5. **S3TA – S3 Transfer Accelerator** – S3TA improves transfer performance by routing traffic through Amazon Cloud Front’s globally distributed Edge Location and over AWS backbone network, and by using network protocol optimization. With S3TA, you pay only for transfer that are accelerated.
6. **AWS Global Accelerator** uses endpoint weights to determine the proportion of traffic that is directed to endpoints in an endpoint group, and traffic dials to control the percentage of traffic that is directed to an endpoint group (an AWS region where your application is deployed).
7. **Difference between NAT gateway vs NAT instance.**
8. The **AWS S3 sync command** uses the CopyObject APIs to copy objects between S3 buckets.
9. **AWS Cost Explorer** helps you identify under-utilized EC2 instances that may be downsized on an instance-by-instance basis within the same instance family, and also understand the potential impact on your AWS bill by taking into account your Reserved Instances and Savings Plans.

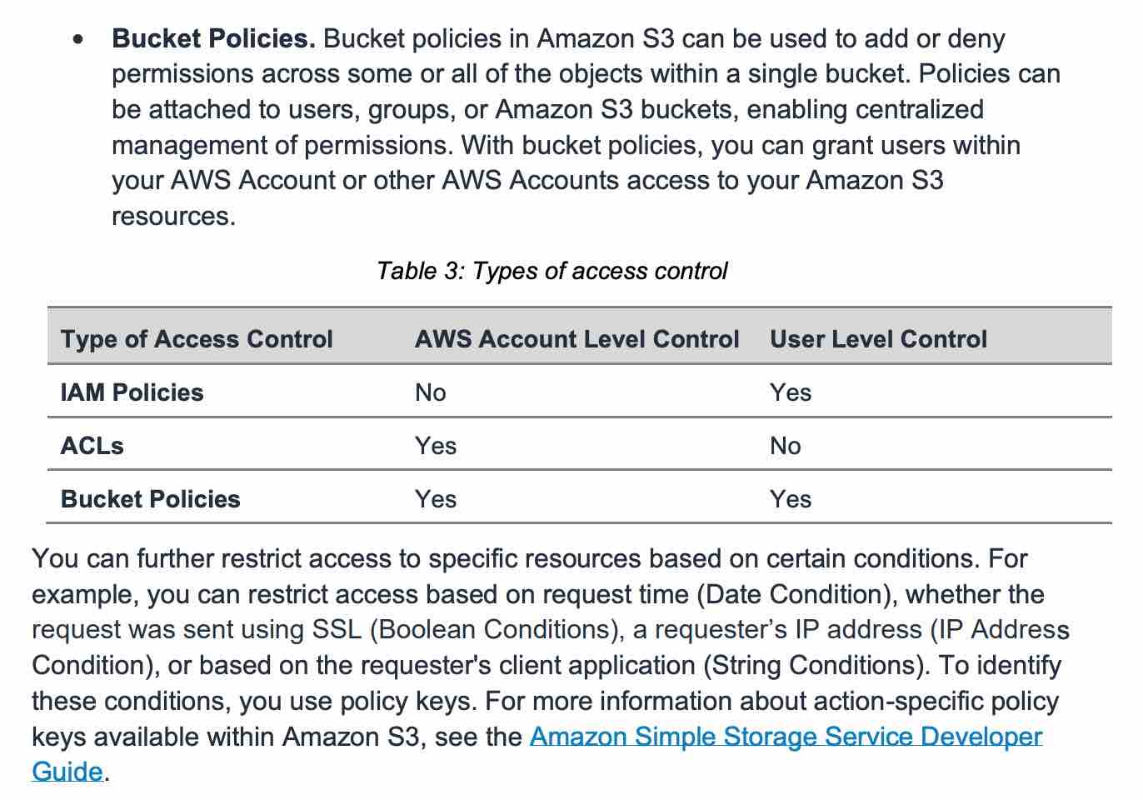
**AWS Compute Optimizer** recommends optimal AWS Compute resources for your workloads to reduce costs and improve performance by using machine learning to analyze historical utilization metrics. Compute Optimizer helps you choose the optimal Amazon EC2 instance types, including those that are part of an Amazon EC2 Auto Scaling group, based on your utilization data.

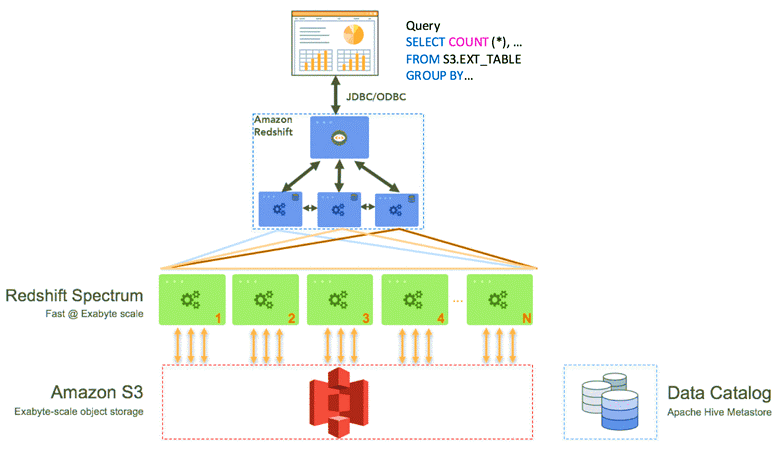
1. A **launch configuration** is an instance configuration template that an Auto Scaling group uses to launch EC2 instances. When you create a launch configuration, you specify information for the instances. Include the ID of the Amazon Machine Image (AMI), the instance type, a key pair, one or more security groups, and a block device mapping.
2. **A transit gateway** is a network transit hub that you can use to interconnect your virtual private clouds (VPC) and on-premises networks.
3. **Amazon ElastiCache** for Redis is HIPAA Eligible Service but Amazon Memcached is not a HIPPA Eligible service.
4. **DAX is tightly integrated with DynamoDB**—you simply provision a DAX cluster, use the DAX client SDK to point your existing DynamoDB API calls at the DAX cluster, and let DAX handle the rest. Because DAX is API-compatible with DynamoDB, you don't have to make any functional application code changes. DAX is used to natively cache DynamoDB reads.
5. **Kenesis Data Streams**.

Diagram

Description automatically generatedDiagram

Description automatically generated

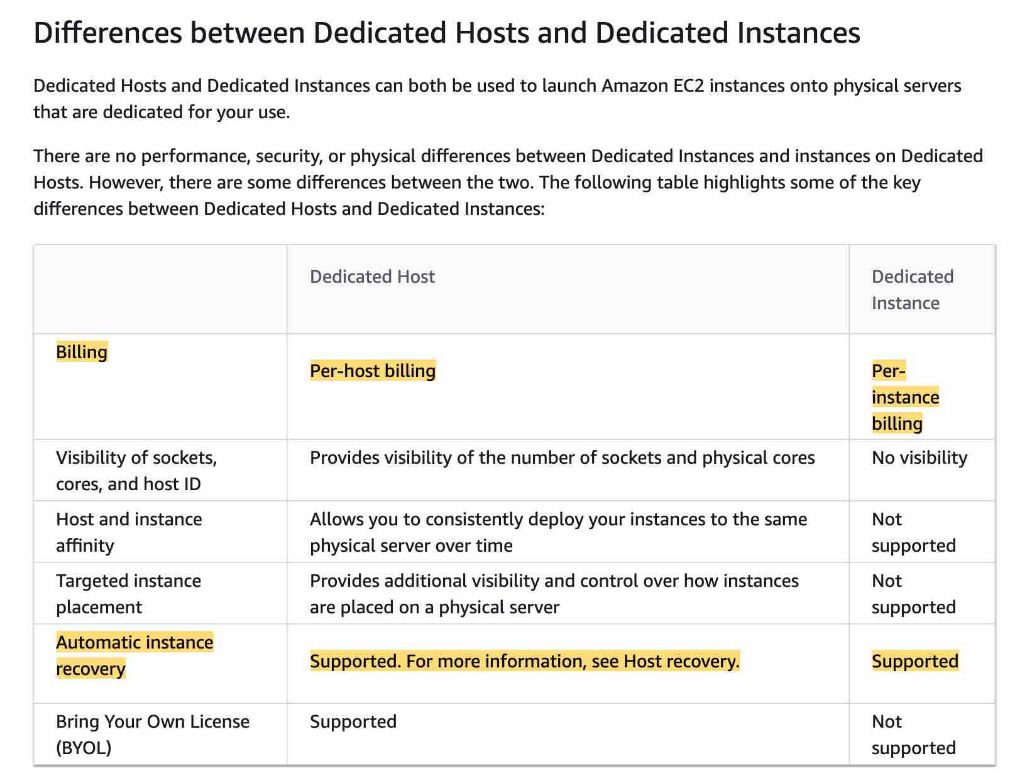
1. **Kinesis Data Firehose** can only write to S3, Redshift, Elasticsearch or Splunk. You can't have applications consuming data streams from Kinesis Data Firehose, that's the job of Kinesis Data Streams.
2. **S3 Standard** - The minimum storage duration is 30 days before you can transition objects from S3 Standard to S3 One Zone-IA.
3. **Auto Scaling group lifecycle hooks** enable you to perform custom actions as the Auto Scaling group launches or terminates instances. Lifecycle hooks enable you to perform custom actions by pausing instances as an Auto Scaling group launches or terminates them. When an instance is paused, it remains in a wait state either until you complete the lifecycle action using the complete-lifecycle-action command or the CompleteLifecycleAction operation, or until the timeout period ends (one hour by default). For example, you could install or configure software on newly launched instances or download log files from an instance before it terminates.
4. **An Application Load Balancer** functions at the application layer, the seventh layer of the Open Systems Interconnection (OSI) model. After the load balancer receives a request, it evaluates the listener rules in priority order to determine which rule to apply and then selects a target from the target group for the rule action. You can configure listener rules to route requests to different target groups based on the content of the application traffic.
5. A **spread placement group** can span multiple Availability Zones in the same Region. You can have a maximum of seven running instances per Availability Zone per group. Therefore, to deploy 15 EC2 instances in a single Spread placement group, the company needs to use 3 AZs.
6. Amazon S3 Bucket Policies:
7. **AWS X-Ray** helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors. X-Ray provides an end-to-end view of requests as they travel through your application and shows a map of your application’s underlying components. You can use X-Ray to collect data across AWS Accounts. The X-Ray agent can assume a role to publish data into an account different from the one in which it is running. This enables you to publish data from various components of your application into a central account.
8. **IPsec VPN connection** also called **site-to-site connection** (**aka VPN connection**) – Customer and gateway VPN - enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). You can securely extend your data center or branch office network to the cloud with an AWS Site-to-Site VPN connection. A VPC VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet. VPN Connections can be configured in minutes and are a good solution if you have an immediate need, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity.
9. **Amazon Redshift Spectrum -** you can efficiently query and retrieve structured and semi structured data from files in Amazon S3 without having to load the data into Amazon Redshift tables. Amazon Redshift Spectrum resides on dedicated Amazon Redshift servers that are independent of your cluster. Redshift Spectrum pushes many compute-intensive tasks, such as predicate filtering and aggregation, down to the Redshift Spectrum layer. Thus, Redshift Spectrum queries use much less of your cluster's processing capacity than other queries.
10. In Aurora, we don’t have any Multi AZ standby Instance, But in RDS we can configure the Multi AZ standby DB.



1. **VPC sharing** (part of Resource Access Manager) allows multiple AWS accounts to create their application resources such as EC2 instances, RDS databases, Redshift clusters, and Lambda functions, into shared and centrally managed Amazon Virtual Private Clouds (VPCs). To set this up, the account that owns the VPC (owner) shares one or more subnets with other accounts (participants) that belong to the same organization from AWS Organizations. After a subnet is shared, the participants can view, create, modify, and delete their application resources in the subnets shared with them. Participants cannot view, modify, or delete resources that belong to other participants or the VPC owner.
2. **Network Load Balancer** - Traffic is routed to instances using the primary private IP address specified in the primary network interface for the instance.
3. **Comparison vis-a-vis multi-AZ vs Read Replica for RDS**

Graphical user interface, text, table

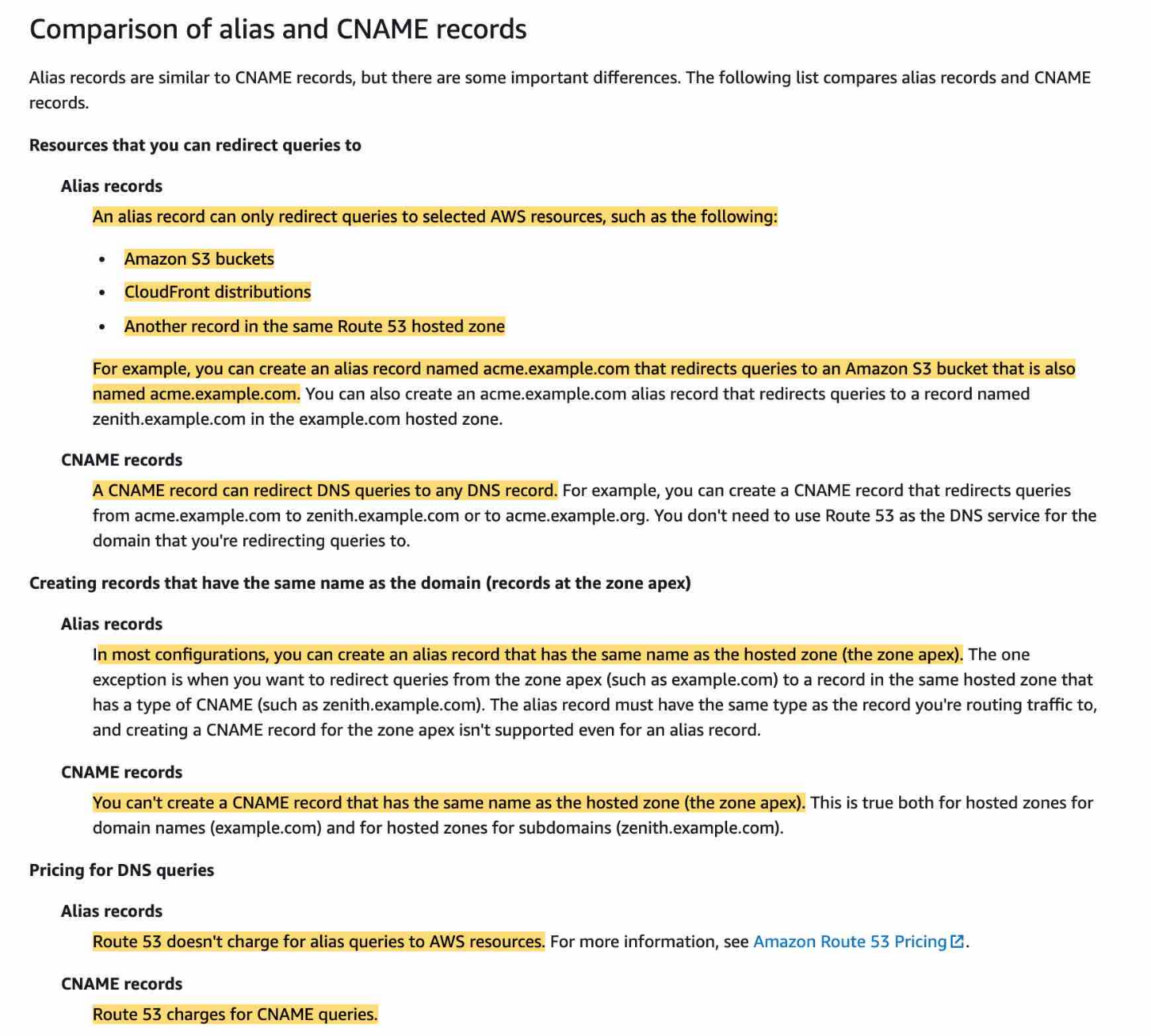
Description automatically generated

1. You can't host a website on Lambda. Also, you can't have CloudFront in front of Lambda.
2. **AWS Secrets Manager** helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text. Secrets Manager offers secret rotation with built-in integration for Amazon RDS, Amazon Redshift, and Amazon DocumentDB. The correct answer here is Secrets Manager.
3. **SSM Parameter Store** - AWS Systems Manager Parameter Store (aka SSM Parameter Store) provides secure, hierarchical storage for configuration data management and secrets management. You can store data such as passwords, database strings, EC2 instance IDs, Amazon Machine Image (AMI) IDs, and license codes as parameter values. You can store values as plain text or encrypted data. You can reference Systems Manager parameters in your scripts, commands, SSM documents, and configuration and automation workflows by using the unique name that you specified when you created the parameter. SSM Parameter Store can serve as a secrets store, but you must rotate the secrets yourself, it doesn't have an automatic capability for this.
4. **Kinesis Agent** is a stand-alone Java software application that offers an easy way to collect and send data to Kinesis Data Streams or Kinesis Firehose. Kinesis Agent cannot write to a Kinesis Firehose for which the delivery stream source is already set as Kinesis Data. When a Kinesis data stream is configured as the source of a Firehose delivery stream, Firehose’s PutRecord and PutRecordBatch operations are disabled, and Kinesis Agent cannot write to Firehose delivery stream directly. Data needs to be added to the Kinesis data stream through the Kinesis Data Streams PutRecord and PutRecords operations instead.
5. You can create a **VPC peering** connection between your VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection). VPC Peering helps connect two VPCs and is not transitive.
6. **Private Link** - AWS PrivateLink simplifies the security of data shared with cloud-based applications by eliminating the exposure of data to the public Internet. AWS PrivateLink provides private connectivity between VPCs, AWS services, and on-premises applications, securely on the Amazon network. Private Link is utilized to create a private connection between an application that is fronted by an NLB in an account, and an Elastic Network Interface (ENI) in another account, without the need of VPC peering, and allowing the connections between the two to remain within the AWS network.
7. **Dedicated host vs dedicated instance**
8. The two main components of Amazon Cognito are user pools and identity pools. Identity pools provide AWS credentials to grant your users access to other AWS services. To enable users in your user pool to access AWS resources, you can configure an identity pool to exchange user pool tokens for AWS credentials. So, identity pools aren't an authentication mechanism.

Diagram

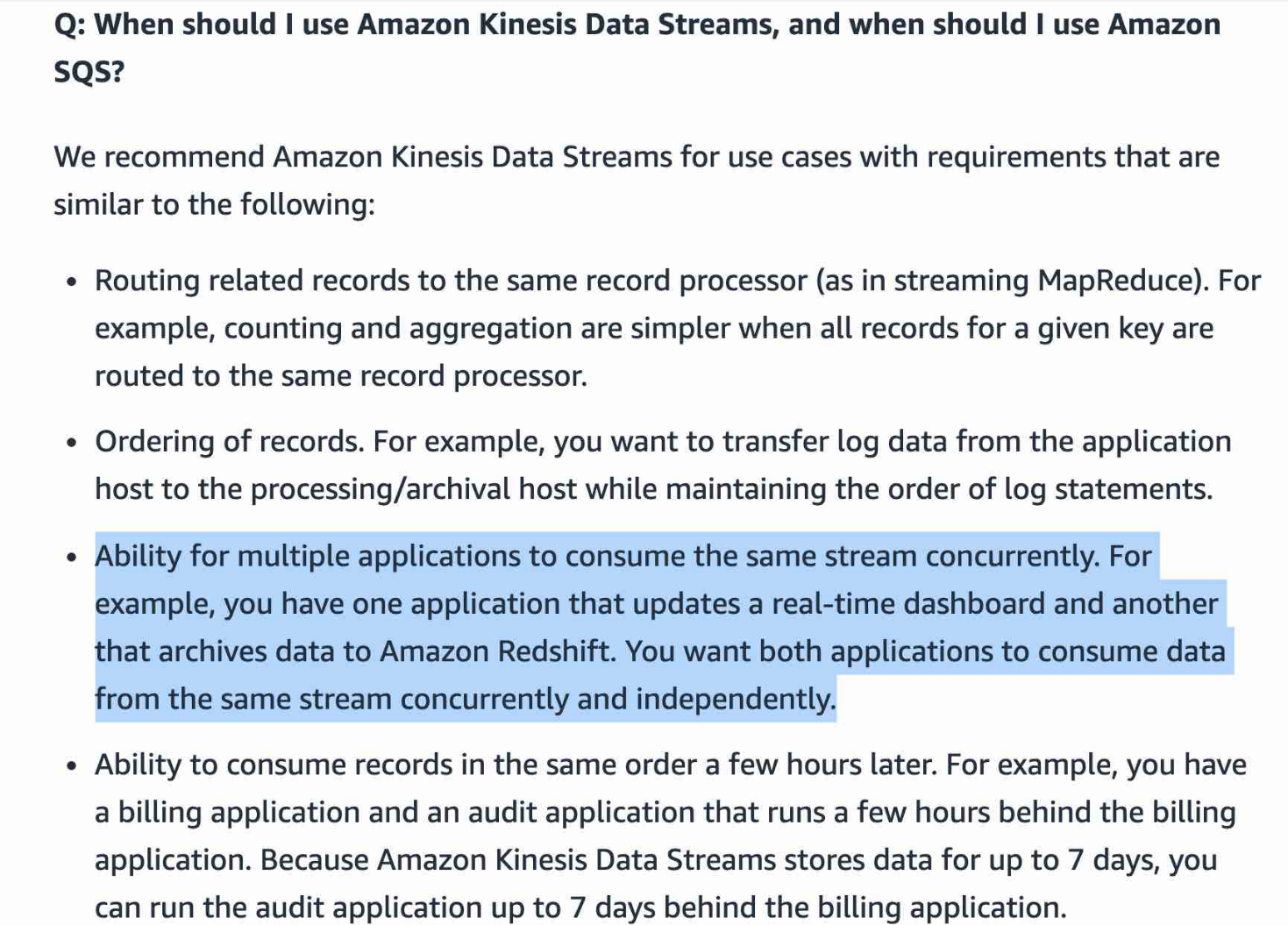
Description automatically generated

1. **AWS Resource Access Manager (RAM)** is a service that enables you to easily and securely share AWS resources with any AWS account or within your AWS Organization. You can share AWS Transit Gateways, Subnets, AWS License Manager configurations, and Amazon Route 53 Resolver rules resources with RAM. RAM eliminates the need to create duplicate resources in multiple accounts, reducing the operational overhead of managing those resources in every single account you own. You can create resources centrally in a multi-account environment and use RAM to share those resources across accounts in three simple steps: create a Resource Share, specify resources, and specify accounts. RAM is available to you at no additional charge.
2. **IAM permission boundary** can only be applied to roles or users, not IAM groups.
3. The aws:SourceIP in this condition always represents the IP of the caller of the API
4. Launch template is similar to launch configuration which usually Auto Scaling group uses to launch EC2 instances. However, defining a launch template instead of a launch configuration allows you to have multiple versions of a template. AWS recommend that we should use launch templates instead of launch configurations to ensure that we can leverage the latest features of Amazon EC2, such as T2 Unlimited instances.
5. Most kinds of **Aurora clusters** are single-master clusters. For example, provisioned, Aurora Serverless, parallel query, and Global Database clusters are all single-master clusters. In a single-master cluster, a single B instance performs all write operations and any other DB instances are read-only. If the writer DB instance becomes unavailable, a failover mechanism promotes one of the read-only instances to be the new writer. In a multi-master cluster, all DB instances can perform write operations. The notions of a single read/write primary instance and multiple read-only Aurora Replicas don't apply. There isn't any failover when a writer DB instance becomes unavailable because another writer DB instance is immediately available to take over the work of the failed instance.
6. A **CNAME record** maps DNS queries for the name of the current record, such as acme.example.com, to another domain (example.com or example.net) or subdomain (acme.example.com or zenith.example.org). CNAME records can be used to map one domain name to another. Although you should keep in mind that the DNS protocol does not allow you to create a CNAME record for the top node of a DNS namespace, also known as the zone apex. For example, if you register the DNS name example.com, the zone apex is example.com. You cannot create a CNAME record for example.com, but you can create CNAME records for www.example.com, newproduct.example.com, and so on.





1. **Create an A record in Router 53** - Used to point a domain or subdomain to an IP address. 'A record' cannot be used to map one domain name to another.
2. **Create a PTR record in Router 53**  - A Pointer (PTR) record resolves an IP address to a fully-qualified domain name (FQDN) as an opposite to what A record does. PTR records are also called Reverse DNS records. 'PTR record' cannot be used to map one domain name to another.



1. Please remember that Kinesis Data Firehose is used to load streaming data into data stores (Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk) whereas Kinesis Data Streams provides support for real-time processing of streaming data. It provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple downstream Amazon Kinesis Applications.
2. SQS FIFO queues are designed to guarantee that messages are processed exactly once, in the exact order that they are sent. For SQS, you cannot have the same message being consumed by multiple consumers at the same time.
3. You can use **message timers** to set an initial invisibility period for a message added to a queue. So, if you send a message with a 60-second timer, the message isn't visible to consumers for its first 60 seconds in the queue. The default (minimum) delay for a message is 0 seconds. The maximum is 15 minutes. Therefore, you should use message timers to postpone the delivery of certain messages to the queue by one minute.
4. **Delay queues** let you postpone the delivery of all new messages to a queue for several seconds, for example, when your consumer application needs additional time to process messages. If you create a delay queue, any messages that you send to the queue remain invisible to consumers for the duration of the delay period. The default (minimum) delay for a queue is 0 seconds. The maximum is 15 minutes.
5. You can create an Amazon CloudWatch alarm to automatically recover the Amazon EC2 instance if it becomes impaired due to an underlying hardware failure or a problem that requires AWS involvement to repair. Terminated instances cannot be recovered. A recovered instance is identical to the original instance, including the instance ID, private IP addresses, Elastic IP addresses, and all instance metadata. If the impaired instance is in a placement group, the recovered instance runs in the placement group. If your instance has a public IPv4 address, it retains the public IPv4 address after recovery. During instance recovery, the instance is migrated during an instance reboot, and any data that is in-memory is lost.