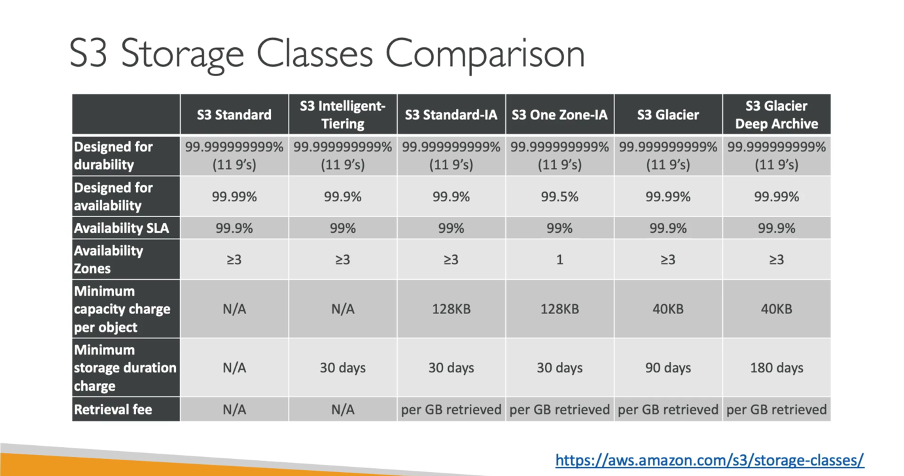
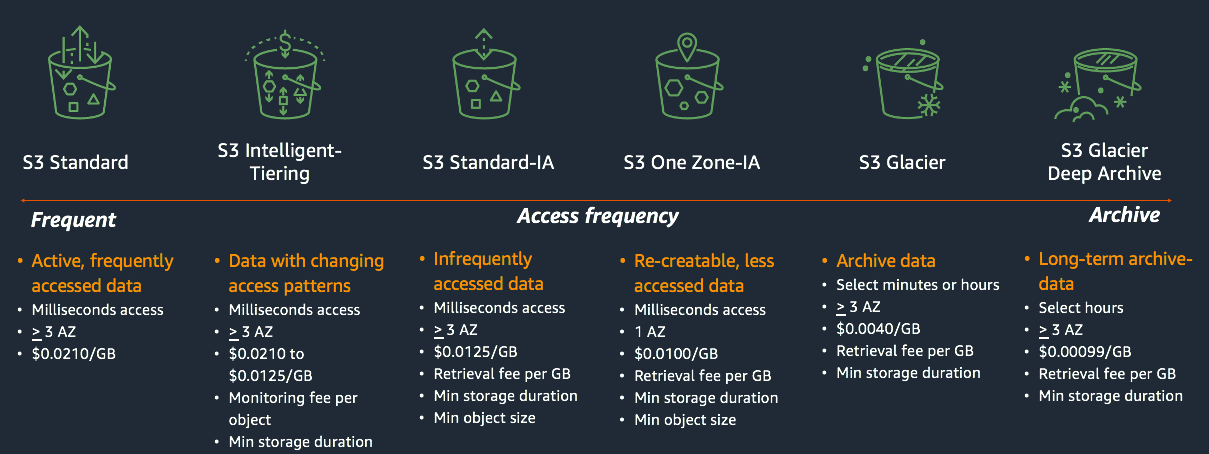
|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | An organization **wants to delegate access to a set of users** from the development environment so that they can access some resources in the production environment which is managed under another AWS account.  Answer:  Create a new IAM role with the required permissions to access the resources in the production environment. The users can then assume the IAM role while accessing the resources from the production environment. | IAM roles allow you to delegate access to users or services that normally don’t have access to your organizations AWS resources.  IAM users or AWS services can assume a role to obtain temporary security credentials that can be used to make AWS API calls.  Consequently, you don’t have to share long-term credentials for access to a resource. Using IAM roles, it is possible to access cross account resources. |
|  | The flagship application for a gaming company connects to an Amazon Aurora database and the entire technology stack is currently deployed in the United States. Now, the company has plans to expand to Europe and Asia for its operations. It needs the *games* table to be accessible globally but needs the *users* and *games\_played* tables to be regional only.  Answer:  Use an Amazon Global Database for the *games* table and use Amazon Aurora for the *users* and *games\_played* tables. | Aurora - Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases.  Amazon Aurora features a distributed, fault-tolerant, self-healing storage system that auto-scales up to 64TB per database instance. Aurora is not an in-memory database.  Amazon Aurora … is designed for globally distributed applications, allowing a single Amazon Aurora db to span multiple AWS regions. It replicates your data with no impact on db performance, enables fast local reads with low latency in each region, and provides disaster recovery from region-wide outages. Amazon Aurora Global Database is the correct choice for the given use-case.  For the given use-case, we, therefore, need to have two Aurora clusters, one for the global table (games table) and the other one for the local tables (users and games\_played tables). |
|  | The development team at an e-commerce startup has set up multiple microservices running on EC2 instances under an Application Load Balancer. The team wants to route traffic to multiple back-end services based on the URL path of the HTTP header. So it wants requests for the <https://www.examples.com/orders> to go to a specific microservice and requests for /products to go to another microservice.  Answer:  Path-base routing | Path-based routing  Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions.  If your application is composed of several individual services, an Application Load Balancer can route a request to a service based on the content of the request. Here are the different types –  Host-based routing:  You can route a client request based on the Host field of the HTTP header allowing you to route to multiple domains from the same load balancer. |
|  | A new DevOps engineer has just joined a development team and wants to understand the replication capabilities for RDS Multi-AZ as well as RDS Read-replicas.  Which of the following correctly summarizes these capabilities for the given database?  Answer:  Multi-AZ follows synchronous replication and spans at least two Availability Zones within a single Region. Read replicas follow ASYNCHRONOUS replication and can be within an Availability Zone, Cross-AZ, or Cross-Region. | Multi-AZ follows synchronous replication and spans at least two Availability Zones within a single region. Read replicas follow asynchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region  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 update 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. |
|  | A financial services company uses Amazon GuardDuty for analyzing its AWS account metadata to meet the compliance guidelines. However, the company has now decided to stop using GuardDuty service. All the existing findings have to be deleted and cannot persist anywhere on AWS Cloud.  Which of the following techniques will help the company meet this requirement?  Answer:  Disable the service in the general settings |  |
|  | A retail company uses Amazon EC2 instances, API Gateway, Amazon RDS, Elastic Load Balancer and CloudFront services. To improve the security of these services, the Risk Advisory group has suggested a feasibility check for using the Amazon GuardDuty service.  Which of the following would you identify as data sources supported by GuardDuty?  Answer:  VPC Flow Logs, DNS logs, CloudTrail events |  |
|  | A gaming company uses Amazon Aurora as its primary database service. The company has now deployed 5 multi-AZ read replicas to increase the read throughput and for use as failover target. The replicas have been assigned the following failover priority tiers and corresponding instance sizes are given in parentheses: tier-1 (16TB), tier-1 (32TB), tier-10 (16TB), tier-15 (16TB), tier-15 (32TB).  In the event of a failover, Amazon Aurora will promote which of the following read replicas?  Answer:  Tier-1 (32TB) |  |
|  | A file-hosting service uses Amazon S3 under the hood to power its storage offerings. Currently all the customer files are uploaded directly under a single S3 bucket. The engineering team has started seeing scalability issues where customer file uploads have started failing during the peak access hours with more than 5000 requests per second.  Which of the following is the MOST resource efficient and cost-optimal way of addressing this issue?  Answer:  Change the application architecture to create customer-specific custom prefixes within the single bucket and then upload the daily files into those prefixed locations. |  |
|  | The payroll department at a company initiates several computationally intensive workloads on EC2 instances at a designated hour on the last day of every month. The payroll department has noticed a trend of severe performance lag during this hour. The engineering team has figured out a solution by using Auto Scaling Group for these EC2 instances and making sure that 10 EC2 instances are available during this peak usage hour. For normal operations only 2 EC2 instances are enough to cater to the workload.  As a solutions architect, which of the following steps would you recommend to implement the solution?  Answer:  Configure your Auto Scaling group by creating a scheduled action that kicks-off at the designated hour on the last day of the month. Set the desired capacity of instances to 10. This causes the scale-out to happen before peak traffic kicks in at the designated hour. |  |
|  | A retail company has developed a REST API which is deployed in an Auto Scaling group behind an Application Load Balancer. The API stores the user data in DynamoDB and any static content, such as images, are served via S3. On analyzing the usage trends, it is found that 90% of the read requests are for commonly accessed data across all users.  As a Solutions Architect, which of the following would you suggest as the MOST efficient solution to improve the application performance?  Answer:  Enable DynamoDB Accelerator (DAX) for DynamoDB and CloudFront for S3 |  |
|  | The product team at a startup has figured out a market need to support both stateful and stateless client-server communications via the APIs developed using its platform. You have been hired by the startup as a solutions architect to build a solution to fulfill this market need using AWS API Gateway.  Which of the following would you identify as correct?  Answer:  API Gateway creates RESTful APIs that enable stateless client-server communication and API Gateway also creates WebSocket APIs that adhere to the WebSocket protocol, which enables stateful, full-duplex communication between client and server |  |
|  | A video analytics organization has been acquired by a leading media company. The analytics organization has 10 independent applications with an on-premises data footprint of about 70TB for each application. The CTO of the media company has set a timeline of two weeks to carry out the data migration from on-premises data center to AWS Cloud and establish connectivity.  Which of the following are the MOST cost-effective options for completing the data transfer and establishing connectivity? (Select two)  Answer:  B. Setup Site-to-Site VPN to establish connectivity between the on-premises data center and AWS Cloud. C. Order 10 Snowball Edge Storage Optimized devices to complete the one-time data transfer. |  |
|  | As part of a pilot program, a biotechnology company wants to integrate data files from its on-premises analytical application with AWS Cloud via an NFS interface.  Which of the following AWS service is the MOST efficient solution for the given use-case?  Answer:  AWS Storage Gateway – File Gateway |  |
|  | A new DevOps engineer has joined a large financial services company recently. As part of his onboarding, the IT department is conducting a review of the checklist for tasks related to AWS Identity and Access Management.  As a solutions architect, which best practices would you recommend (Select two)?  Answer:   1. Configure AWS CloudTrail to log all IAM actions. 2. Enable MFA for privileged users. |  |
|  | The engineering team at a data analytics company has observed that its flagship application functions at its peak performance when the underlying EC2 instances have a CPU utilization of about 50%. The application is built on a fleet of EC2 instances managed under an Auto Scaling group. The workflow requests are handled by an internal Application Load Balancer that routes the requests to the instances.  As a solutions architect, what would you recommend so that the application runs near its peak performance state?  Answer:  Configure the Auto Scaling group to use target tracking policy and set the CPU utilization as the target metric with a target value of 50%. |  |
|  | The sourcing team at the US headquarters of a global e-commerce company is preparing a spreadsheet of the new product catalog. The spreadsheet is saved on an EFS file system created in us-east-1 region. The sourcing team counterparts from other AWS regions such as Asia Pacific and Europe also want to collaborate on this spreadsheet.  As a solutions architect, what is your recommendation to enable this collaboration with the LEAST amount of operational overhead?  Answer:  The spreadsheet on the EFS file system can be accessed from EC2 instances running in other AWS regions by using an inter-region VPC peering connection. |  |
|  | An IT consultant is helping the owner of a medium-sized business set up an AWS account. What are the security recommendations he must follow while creating the AWS account root user? (Select two)  Answer:  B. Enable Multi Factor Authentication (MFA) for the AWS account root user account.  C. Create a strong password for the AWS account root user. |  |
|  | A gaming company is developing a mobile game that streams score updates to a backend processor and then publishes results on a leaderboard. The company has hired you as an AWS Certified Solutions Architect Associate to design a solution that can handle major traffic spikes, process the mobile game updates in the order of receipt, and store the processed updates in a highly available database. The company wants to minimize the management overhead required to maintain the solution.  Which of the following will you recommend to meet these requirements?  Answer:  Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue. Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SQS queue. Store the processed updates in an Amazon RDS Multi-AZ DB instance. |  |
|  | The engineering team at an in-home fitness company is evaluating multiple in-memory data stores with the ability to power its on-demand, live leaderboard. The company's leaderboard requires high availability, low latency, and real-time processing to deliver customizable user data for the community of users working out together virtually from the comfort of their home.  As a solutions architect, which of the following solutions would you recommend? (Select two)  Answer:  Power the on-demand, live leaderboard using ElastiCache Redis as it meets the in-memory, high availability, low latency requirements.  Power the on-demand, live leaderboard using DynamoDB with DynamoDB Accelerator (DAX) as it meets the in-memory, high availability, low latency requirements. |  |
|  | A company has moved its business critical data to Amazon EFS file system which will be accessed by multiple EC2 instances.  As an AWS Certified Solutions Architect Associate, which of the following would you recommend to exercise access control such that only the permitted EC2 instances can read from the EFS file system? (Select three)  Answer: |  |
|  | The development team at an e-commerce startup has set up multiple microservices running on EC2 instances under an Application Load Balancer. The team wants to route traffic to multiple back-end services based on the URL path of the HTTP header. So it wants requests for https://www.example.com/orders to go to a specific microservice and requests for https://www.example.com/products to go to another microservice.  Which of the following features of Application Load Balancers can be used for this use-case?  Answer:  Path-based Routing. |  |
|  | A US-based healthcare startup is building an interactive diagnostic tool for COVID-19 related assessments. The users would be required to capture their personal health records via this tool. As this is sensitive health information, the backup of the user data must be kept encrypted in S3. The startup does not want to provide its own encryption keys but still wants to maintain an audit trail of when an encryption key was used and by whom.  Which of the following is the BEST solution for this use-case?  Answer:  Use SSE-KMS to encrypt the user data on S3. |  |
|  | An audit department generates and accesses the audit reports only twice in a financial year. The department uses AWS Step Functions to orchestrate the report creating process that has failover and retry scenarios built into the solution. The underlying data to create these audit reports is stored on S3, runs into hundreds of Terabytes and should be available with millisecond latency.  As a solutions architect, which is the MOST cost-effective storage class that you would recommend to be used for this use-case?  Answer:  Amazon S3 Standard-Infrequent Access (S3 Standard-IA)  Explanation: Since the data is accessed only twice in a financial year but needs rapid access when required, the most cost-effective storage class for this use-case is S3 Standard-IA |  |
|  | An IT Company wants to move all the compute components of its AWS Cloud infrastructure into serverless architecture. Their development stack comprises a mix of backend programming languages and the company would like to explore the support offered by the AWS Lambda runtime for their programming languages stack.  Can you identify the programming languages supported by the Lambda runtime? (Select two) |  |
|  | An Electronic Design Automation (EDA) application produces massive volumes of data that can be divided into two categories. The 'hot data' needs to be both processed and stored quickly in a parallel and distributed fashion. The 'cold data' needs to be kept for reference with quick access for reads and updates at a low cost.  Which of the following AWS services is BEST suited to accelerate the aforementioned chip design process?  Answer:  Amazon FSx for Lustre. |  |
|  | A company uses DynamoDB as a data store for various kinds of customer data, such as user profiles, user events, clicks, and visited links. Some of these use-cases require a high request rate (millions of requests per second), low predictable latency, and reliability. The company now wants to add a caching layer to support high read volumes.  As a solutions architect, which of the following AWS services would you recommend as a caching layer for this use-case? (Select two)  Answer:  a. DynamoDB Accelerator (DAX)  b. ElastiCache |  |
|  | An IT company wants to review its security best-practices after an incident was reported where a new developer on the team was assigned full access to DynamoDB. The developer accidentally deleted a couple of tables from the production environment while building out a new feature.  Which is the MOST effective way to address this issue so that such incidents do not recur?  Answer:  Use permissions boundary to control the maximum permissions employees can grant to the IAM principals. |  |
|  | CloudFront offers a multi-tier cache in the form of regional edge caches that improve latency. However, there are certain content types that bypass the regional edge cache, and go directly to the origin.  Which of the following content types skip the regional edge cache? (Select two)  Answer:  a. Dynamic content, as determined at request time (cache-behavior configured to forward all headers)  b. Proxy methods PUT/POST/PATCH/OPTIONS/DELETE go directly to the origin |  |
|  | A data analytics company measures what the consumers watch and what advertising they’re exposed to. This real-time data is ingested into its on-premises data center and subsequently, the daily data feed is compressed into a single file and uploaded on Amazon S3 for backup. The typical compressed file size is around 2 GB.  Which of the following is the fastest way to upload the daily compressed file into S3?  Answer:  Upload the compressed file using multipart upload with S3 transfer acceleration |  |
|  | A development team requires permissions to list an S3 bucket and delete objects from that bucket. A systems administrator has created the following IAM policy to provide access to the bucket and applied that policy to the group. The group is not able to delete objects in the bucket. The company follows the principle of least privilege.    Answer: |  |
|  | A social gaming startup has its flagship application hosted on a fleet of EC2 servers running behind an Elastic Load Balancer. These servers are part of an Auto Scaling Group. 90% of the users start logging into the system at 6 pm every day and continue till midnight. The engineering team at the startup has observed that there is a significant performance lag during the initial hour from 6 pm to 7 pm. The application is able to function normally thereafter.  As a solutions architect, which of the following steps would you recommend addressing the performance bottleneck during that initial hour of traffic spike?  Answer:  Configure your Auto Scaling group by creating a scheduled action that kicks-off before 6 pm. This causes the scale-out to happen even before peak traffic kicks in at 6 pm. |  |
|  | The IT department at a consulting firm is conducting a training workshop for new developers. As part of an evaluation exercise on Amazon S3, the new developers were asked to identify the invalid storage class lifecycle transitions for objects stored on S3.  Can you spot the INVALID lifecycle transitions from the options below? (Select two)  Answer:  B. S3 Intelligent-Tiering S3 Standard.  C. S3 One Zone-IA => S3 Standard-IA. |  |
|  | A healthcare startup needs to enforce compliance and regulatory guidelines for objects stored in Amazon S3. One of the key requirements is to provide adequate protection against accidental deletion of objects.  As a solutions architect, what are your recommendations to address these guidelines? (Select two)  Answer:  A. Enable versioning on the bucket.  B. Enable MFA delete on the bucket. |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Storage Classes





Multi-AZ Deployments, Multi-Region Deployments, and Read-ReplicasGraphical user interface, text, application, email

Description automatically generated

|  |  |  |
| --- | --- | --- |
| Multi-AZ Dep | Multi-Region Dep | Read-Replicas |
| Main purpose:  High availability | Main purpose:  Disaster recovery and local performance | Main purpose:  Scalability |
| Non-Aurora:  Synchronous replication  Aurora:  Asynchronous replication |  |  |
| Non-Aurora:  Automated backups are taken from standby.  Aurora:  Automated backups are taken from shared storage layer. |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Definitions:

## Aurora:

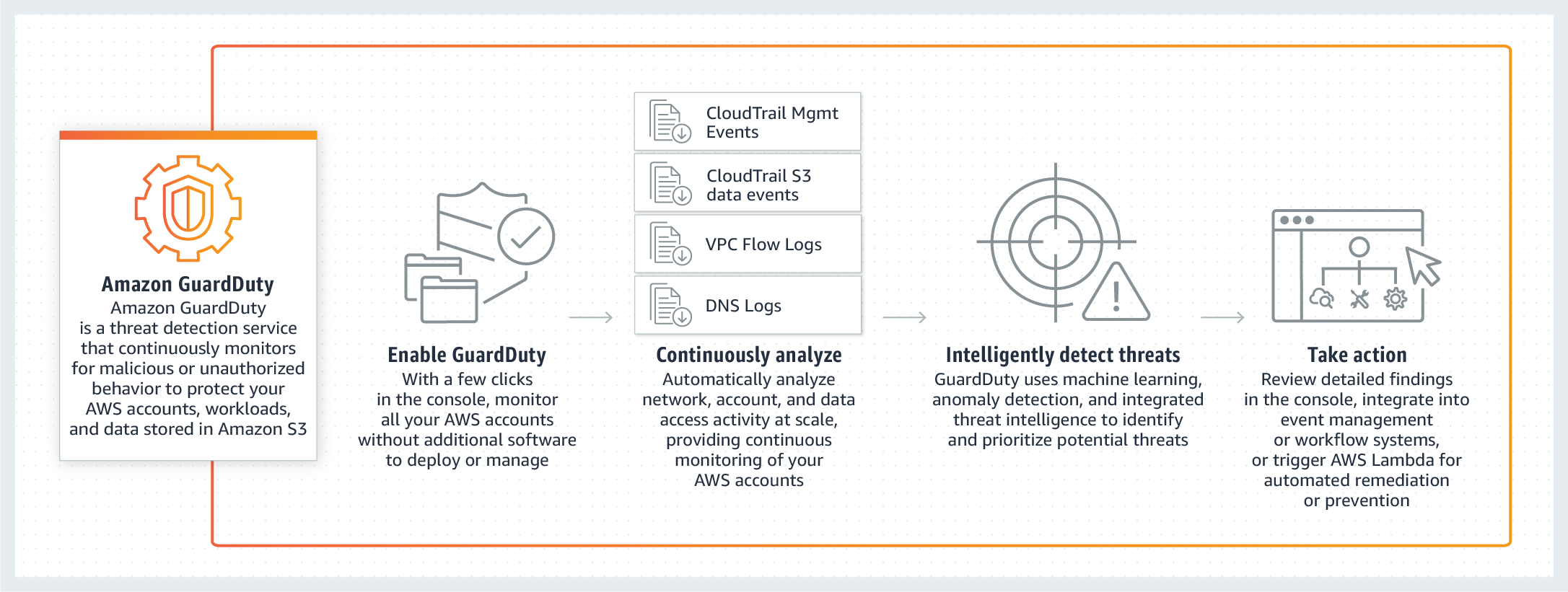
Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases.

Amazon Aurora is up to five times faster than standard MySQL databases and three times faster than standard PostgreSQL databases. It provides the security, availability, and reliability of commercial databases at 1/10th the cost. Amazon Aurora is fully managed by Amazon Relational Database Service (RDS), which automates time-consuming administration tasks like hardware provisioning, database setup, patching, and backups.

Amazon Aurora features a distributed, fault-tolerant, self-healing storage system that auto-scales up to 128TB per database instance. It delivers high performance and availability with up to 15 low-latency read replicas, point-in-time recovery, continuous backup to Amazon S3, and replication across three Availability Zones.

## AWS Guard Duty:

Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.



## High Availability:

High availability (HA) is a component of a technology system that eliminates single points of failure to ensure continuous operations or uptime for an extended period. High Availability ensures your systems, databases, and applications operate when and as needed.

* AWS Highly Available Services:
* EC2 – Elastic Compute Cloud.
* AWS RDS – Relational Database.
* AS – Auto Scaling.
* ELB – Elastic Load Balancer.
* SNS – Simple Notification Service.
* VPC – Virtual Private Cloud.
* Route53 – DNS service.
* AMI – Amazon Machine Image.

## Synchronous vs. Asynchronous Replication

Synchronous replication - Synchronous replication is the process of copying data over a storage area network, local area network or wide area network so there are multiple, current copies of the data. Synchronous replication is mainly used for high-end transactional applications that need instant failover if the primary node fails.   
Synchronous replication requires the bandwidth of a LAN between the servers, possibly with an extended LAN in two geographically remote computer zones. ... It can work between two SQL Servers Enterprise in on-premise network or between two EC2 SQL Servers Enterprise in same AWS region.

Synchronous vs. asynchronous replication

The primary difference between synchronous replication and asynchronous replication is the way in which data is written to the replica. Most synchronous replication products write data to primary storage and the replica simultaneously. As such, the primary copy and the replica should always remain synchronized.

In contrast, asynchronous replication products copy the data to the replica after the data is already written to the primary storage. Although the replication process may occur in near-real-time, it is more common for replication to occur on a scheduled basis. For instance, write operations may be transmitted to the replica in batches on a periodic basis (for example, every one minute). In case of a fail-over event, some data loss may occur.

Source: <https://cloudbasic.net/white-papers/synchronous-vs-asynchronous-replication/>