Unit - 4

Q.1 1 Mark :-

1) full form : DNS
→ Domain Name System

2) Full form : VPC
→ Virtual private cloud

3) full form : RDS
→ Relational Database Service

4) What is Dynamodb?
→ DynamoDB is NoSQL database service offered by AWS that provides fast and scalable performance with low latency.

5) What is Route 53 ?
→ Route 53 is a Domain Name System web service offered by AWS.

6) Write Names of Routing policy.
→ Simple, weighted, latet latency, failover, Geolocation, multi value

7) What is Elasticache ?

→ fully managed in-memory caching service provided by AWS.

8) Write Types of Elasticache.

→ Memcached , Redis

Q.2 ~~& Mention~~ Sl:- Answer the followings :

1) Define web Hosting ?

→ Web hosting is service that allows individuals and organizations to make their website ~~access~~ accessible via the world wide web.

2) Explain Amazon Route 53 Health Checks ?

→ Amazon Route 53 Health ~~the~~ checks are a feature that continuously monitors the health and performance of your applications and resources.

DATE:
PAGE:

* Here's a detailed explanation:-

→ Monitoring :-

Amazon Route 53 Health checks continously monitor the health and performance of your web applications, web servers, APIs and other resources by sending automated requests at regular intervals, such as every 30 seconds.

→ Multiple protocols supported :-

Health checks supports multiple protocols including HTTP, HTTPS, TCP with string matching, allowing you to check the health of a wide range of endpoints.

→ Configurable Thresholds :-

you can configure thresholds for the check responses to determines whether the endpoint is healthy or unhealthy.

→ Geo-Location Based Health checks:-

You can configure health checks from different geographic locations to ensure that your application is performing well globally.

→ ~~Integra~~ ~~Int~~ Integration with DNS:-

Route 53 integrates health check status with DNS, allowing you to route traffic to healthy endpoints automatically and to fail over to healthy endpoints in case of failures, thus improving the availability and reliability of your applications.

→ Detailed Reporting and Notifications:-

Health checks provide detailed reporting and notifications via Amazon CloudWatch, Amazon SNS or AWS Lambda.

3) Explain Elasticache with its Types.

→ Amazon Elasticache is a fully managed in-memory caching service provided by AWS.

* Types of Elasticache :-

i) Memcached :-

→ Memcached is an in-memory key-value store that is commonly used for caching purposes.

→ It is simple to use and offers high-performance, distributed caching capabilities.

→ Memcached is suitable for use cases where simple caching of objects or data is required, without complex data structures or advanced features.

DATE:
PAGE:

3) Redis :-

→ Redis is an open-source, in-memory data structure store that supports various data structures such as strings, lists, sets, sorted sets, hashes and more.

→ It provides advanced features like replication, persistence, pub/sub messaging, and built-in data structures.

→ Redis is suitable for a wide range of use cases including caching, session management, real-time analytics, message queuing and more.

4) What is DNS?

→ DNS (Domain Name System) is distributed system that translates human-readable domain names (like example.com) into IP addresses and vice versa, facilitating the routing of Internet traffic by mapping domain names

to their corresponding IP addresses and enabling users to access websites and services using familiar domain names instead of numerical IP addresses.

5) Write Types of Monitoring Tools.

→ There are two categories of AWS monitoring tools: first-party and third party tools.

i) ~~First-party :-~~

* ii) first-party :-

i) AWS cloudTrail :-

→ AWS cloudTrail is a web service that records AWS API calls for monitoring, auditing, compliance, and investigative purposes.

DATE:
PAGE:

→ It provides a fully searchable log of who did what and when, enabling businesses to determine the responsible party for all actions taken on AWS infrastructure resources.

→ CloudTrail can be configured to send notifications when specific events occur, such creating a new Amazon EC2 instance or deleting a security group.

ii) AWS CloudWatch :-

→ AWS cloudWatch is a monitoring service provided by AWS that tracks metrics, logs, and events that can impact AWS resources and application running on them.

→ It offers real-time insight into the performance of applications running on AWS, including metrics such as CPU usage, memory usage, disk usage, and network traffic.

DATE:
PAGE:

* AWS Third-party :-

1) Middleware :-

→ Middleware is an all-in-one monitoring tool designed to monitor the performance of hybrid applications, including, those hosted on AWS.

→ It provides real-time application-level monitoring, offering businesses complete visibility into their AWS infrastructure.

2) Explain Dynamodb.

→ Amazon DynamoDB is a cloud-native NoSQL database primarily designed as a key-value store. Let's break down each aspect.

1) Cloud-Native :- Dynamo

DynamoDB operates exclusively on Amazon Web Services and does not have an on-premises or hybrid cloud deployment option.

→ This cloud-native nature allows it to leverage AWS's elastic infrastructure, meaning it can dynamically scale up or down based on demand without requiring upfront hardware investment from customers.

ii) NoSQL :-

→ DynamoDB is a NoSQL database, meaning it does not adhere to the traditional relational database model and does not support SQL queries, Instead, it offers a proprietary API based on JSON. This

iii) Key-Value Store :-

→ The core data model of DynamoDB revolves around key-value pairs stored in schemaless table.

→ Each table can contain a vast number of rows (records), and each consists of a key-value pair.

→ Unlike relational databases, DynamoDB does not support traditional RDBMS features such as joins through foreign keys.

7) Explain Security in Amazon RDS.

→ ~~securi~~ Security in Amazon RDS follows the shared responsibility model, where AWS takes care of the security of the cloud infrastructure, while customers are responsible for security in the cloud, including access management and data protection.

* Here's how security is managed in Amazon RDS:

i) Security of the ~~co~~ cloud:

→ AWS is responsible for protecting the underlying infrastructure that powers Amazon RDS, including the data centers and network architecture.

DATE:
PAGE:

ii) Security in the cloud :-

→ Customers are responsible for managing access to their Amazon RDS resources and databases, as well as ensuring the security of their data.

* To manage access to Amazon RDS resources, customers can employ various methods :-

i) Amazon VPC ✓ ii) AWS IAM ✓
iii) Security Groups ✓ iv) SSL/TLS Connections ✓
v) Amazon RDS Encryption ✓
vi) Database Engine security features :-

i) Amazon VPC :-

→ Running RDS instances within a virtual Private Cloud provides the highest level of network access control. Customers can define subnets, route tables and network gateways to isolate their RDS instance within a private network.

...oud :-

...esponsible for managing ...esources ...Amazon RDS ...as well as ensuring ...their data.

...ss to Amazon RDS ...omers can employ various

ii) AWS IAM :-

iv) SSL/TLS Connections

...ption :-

security features :-

...tances within a ...ud provides the ... network access ... can define subnets ... network gateways ...tance within a ...rivate network

DATE
PAGE

2) What is AWS Monitoring ?

→ AWS monitoring refers to the process of collecting and analyzing metrics, logs, and event generated by various AWS services and resources to gain insights into their performance, health, and operational status. It involves using AWS monitoring tools and services to monitor the utilization, ~~avail~~ availability and performance of AWS infrastructure, applications and workloads. AWS monitoring helps organizations ensure the reliability, security and efficiency of their AWS environment by identifying issues, detecting anomalies, and optimizing resources usage.

DATE:
PAGE:

q) Explain AWS Monitoring Tools?

→ Amazon AWS offers a suite of monitoring tools and features that provide visibility into your AWS environment and help you ensure the security and reliability of your infrastructure and applications.

i) AWS CloudTrail?

→ AWS CloudTrail enables you to monitor your AWS deployments by tracking the history of API calls made in your accounts. It records API activity across various AWS services, including calls made through the management console, SDKs and command-line tools.

→ CloudTrail provides detailed information such as the user or account making the call, source IP address and the timestamp of the call.

ii) ~~Amazo~~ Amazon GuardDuty :-

→ Is a threat detection service that continuously monitors for malicious activity and unauthorized behavior in your AWS accounts and workloads. It uses machine learning algorithms and threat intelligence to analyze events and ~~dect~~ ~~dect~~ detect anomalies indicative of potential security threats.

iii) Amazon CloudWatch :-

→ Amazon CloudWatch provides a comprehensive monitoring solution that allows you to collect, visualize, and analyze metric and logs from your AWS resources in real-time.

DATE:
PAGE:

1a) Explain benefits of AWS Monitoring Tools ?

* benefits :-

i) Faster Issue Detection :-

→ AWS monitoring enables you to track the performance of your applications and infrastructure, allowing you to discover issues affecting the applications and take timely action to mitigate them.

ii) Better Performance :-

→ By tracking the performance of your applications, AWS monitoring helps you identify areas for improvement. Insights into network traffic and server activity allows you to optimize performance, enhancing customer and user experience.

iii) Heightened Security and compliance :-

→ AWS security Hub collects security alerts from various AWS security services, aiding in the identification of suspicious activity and threats.

iv) Cost Optimization :-

→ AWS monitoring assits in optimizing costs by identifying resource wastage and underutilization.

v) Increased Availability and Business Continuity :-

→ Properly configured AWS monitoring enables proactive identification and response to potential issues, preventing downtime and improving application performance.

DATE:
PAGE:

11) Write steps for Website Hosting?

1) Register a custom domain with Route 53:-

→ If you don't have a registered domain name, register one with Route 53.

2) create two buckets:-

→ Create one bucket for the root domain and another for the subdomain.

3) Configure the root domain bucket for website hosting:-

→ Enable static website hosting for the root domain bucket and specify the index document.

4) Configure the subdomain bucket for website redirect:-

→ Configure the subdomain bucket to redirect all request to track website traffic.

DATE:
PAGE:

5) Configure logging for website traffic:

→ Optionally enable server access logging for the root domain bucket to track website traffic.

6) Upload index and website content:

→ Upload the index document and other website content to the root domain bucket.

7) Upload an error document:

→ Upload an error document to handle errors on the website.

8) Edit S3 Block Public Access settings:

→ Edit block public access settings for the root domain bucket to allow public access.

9) Attach a bucket policy :-

→ Attach a bucket policy to the root domain bucket to grant public read access.

10) Test the domain endpoint :-

→ Test the website endpoint by navigating to the domain URL in a browser.

11) Add alias record records for the domain and subdomain :-

→ Add alias records to the hosted zone for the domain and subdomain in Route 53.

12) Test the website :-

→ Verify that website and redirect work correctly by accessing the domain and subdomain URLs.

Abdul Rahman
26/3/2024