Tips for major AWS services

14 March 2024 15:40

1. Securing the Root Account: We discussed the importance of securing the root account by enabling multi-factor authentication (MFA) and minimizing its use for day-to-day administrative tasks.
2. Administrator Group and Users: We learned how to create an administrator group, assign appropriate permissions to it, and create user accounts for administrators. Users are added to groups to inherit permissions.
3. IAM Policy Documents: IAM permissions are managed using policy documents written in JSON format. We examined a basic policy document granting full administrative access.
4. Key Points for the Exam:
    - IAM is universal and not tied to specific regions.
    - The root account should be secured immediately, and its usage minimized.
    - New users have no permissions by default and must be added to groups or assigned policies.
    - Access keys and secret access keys are used for programmatic access and should be securely stored.
    - Password rotation policies should be implemented for enhanced security.
    - IAM Federation allows integrating existing user accounts with AWS using standards like SAML.
5. Next Steps: The next section of the course will focus on Amazon S3 (Simple Storage Service), one of the oldest and most commonly used services in AWS. Understanding S3 is essential for the exam and real-world AWS usage.
   By mastering IAM concepts and best practices, you're better equipped to manage access and security in your AWS environment.

From <https://chat.openai.com/c/d6fe90a1-a00b-4374-9bfc-54c5891880f3>

1. S3 Basics:
    - S3 is object-based storage suitable for files up to 5 terabytes in size.
    - Files are stored in buckets, and S3 provides a universal namespace.
    - Upon successful upload, the browser receives a HTTP 200 status code.
2. S3 Object Anatomy:
    - Key: Object name or file name.
    - Value: Data itself, consisting of bytes.
    - Version ID: Allows multiple versions of the same object.
    - Metadata: Data about stored objects, e.g., content type or modification time.
3. Securing S3 Buckets:
    - Buckets and objects are private by default.
    - Public access can be enabled through object ACLs or bucket policies.
    - Bucket policies allow making entire buckets public.
4. Hosting Static Websites with S3:
    - Static websites can be hosted on S3 using bucket policies.
    - S3 is suitable for static content, not dynamic content requiring database connections.
5. S3 Storage Classes:
    - Understand the use cases and retrieval times for different storage classes.
    - S3 Intelligent-Tiering uses machine learning to optimize storage costs.
6. Lifecycle Management:
    - Automates object movement between storage tiers based on defined rules.

- Can be used in conjunction with versioning.

7. S3 Object Lock:
   - Enables write-once-read-many (WORM) model for objects.
   - Available in governance and compliance modes.
8. Encryption with S3:
   - Encryption in transit (HTTPS) and at rest (server-side and client-side).
   - Can enforce encryption using bucket policies.
9. Performance Optimization:
   - Use prefixes (folders) to improve performance.
   - Multipart uploads and byte-range fetches enhance upload/download performance.
   - Understand limits and considerations for server-side encryption with KMS.
10. S3 Replication:
    - Replicates objects from one bucket to another, including cross-region replication.
    - Existing objects are not automatically replicated; delete markers may need replication.

Congratulations on completing the S3 section! The next topic is Amazon EC2, a fundamental service for provisioning virtual machines in the AWS cloud.

1. EC2 Basics:
   - EC2 provides virtual machines hosted in AWS, allowing flexible capacity provisioning.
   - Pricing options include On-Demand, Spot, Reserved, and Dedicated instances, each suited for different use cases.
2. AWS Command Line Interface (CLI):
   - Users should be granted least privilege access.
   - IAM groups and policies should be used for managing permissions.
   - Secret access keys should be kept secure and not shared.
3. Roles and Policies:
   - Roles are preferred over hardcoding credentials in code.
   - Policies control role permissions and can be updated and attached/detached without stopping instances.
4. Security Groups:
   - Security groups control inbound/outbound traffic and changes take effect immediately.
   - Multiple security groups can be attached to EC2 instances.
5. Bootstrap Scripts and Metadata:
   - Bootstrap scripts run at instance launch, passing user data and accessing metadata.
   - User data is used for bootstrap scripts, while metadata provides information about EC2 instances.
6. Networking with EC2:
   - Understand ENIs, Enhanced Networking, and EFAs for different networking requirements.
   - Placement groups allow logical grouping of EC2 instances for specific use cases.
7. Dedicated Hosts:
   - Dedicated Hosts provide physical servers dedicated to a single customer, suitable for special licensing or compliance requirements.
8. Spot Instances and Fleets:
   - Spot Instances offer savings of up to 90% compared to On-Demand instances and can be blocked from termination using Spot block.
   - Spot Fleets combine Spot and On-Demand instances for flexibility and cost optimization.
9. Newer Topics:
   - vCenter on AWS allows extending private VMware clouds to the AWS public cloud.

- AWS Outposts bring AWS infrastructure to on-premises data centers, available in rack and server form factors.

Ensure understanding of these concepts for the exam and practical application in real-world scenarios.

1. EBS Volume Types:
   - General Purpose SSD (gp2): Suitable for boot volumes and general applications, offering up to 16,000 IOPS per volume.
   - Provisioned IOPS SSD (io1/io2): High-performance volumes for latency-sensitive applications, offering up to 64,000 IOPS per volume. io2 provides 5 nines durability.
   - Throughput Optimized HDD (st1): Suitable for big data, data warehouses, and ETL applications, with a maximum throughput of 500 MB/s per volume.
   - Cold HDD (sc1): Designed for less frequently accessed data, offering a max throughput of 250 MB/s per volume.
2. Volume and Snapshot Management:
   - Volumes exist on EBS, while snapshots exist on S3. Snapshots are incremental and point-in-time backups.
   - Consistent snapshots are recommended to be taken after stopping and detaching the volume.
   - Snapshots can be shared between AWS accounts and regions. Volumes can be resized and changed in types (e.g., gp2 to gp3).
3. EBS vs. Instance Store (Ephemeral Storage):
   - EBS volumes provide persistent storage, allowing instances to be stopped without data loss.
   - Instance store volumes are ephemeral and cannot be stopped. Data loss occurs if the underlying host fails.
4. Encrypted Volumes:
   - Data-at-rest is encrypted inside the volume, and data-in-flight is encrypted between the instance and volumes.
   - Snapshots and volumes created from snapshots are also encrypted.
5. EC2 Hibernation:
   - Preserves in-memory RAM on persistent storage (EBS), enabling faster boot times.
   - Available for specific instance families and operating systems, with a maximum hibernation duration of 60 days.
6. Amazon EFS (Elastic File System):
   - Supports NFSv4 protocol and provides scalable, shared storage for Linux instances.
   - Automatically scales up/down based on storage usage and provides read-after-write consistency.
7. Comparing Storage Options:
   - Understanding the use cases for S3, Glacier, EFS, FSx (Lustre and Windows), EBS, and Instance Store is crucial for selecting the appropriate storage solution.
8. AWS Backup:
   - Centralized backup solution for various AWS services, offering automation, lifecycle management, and compliance enforcement.
   - Can be integrated with AWS Organizations for managing backups across multiple AWS accounts.

Ensure comprehension of these concepts for the exam, as there may be scenario-based questions requiring you to choose the correct storage solution

1. Amazon RDS (Relational Database Service):
   - Supports SQL Server, Oracle, MySQL, PostgreSQL, MariaDB, and Amazon Aurora.

- Primarily used for online transaction processing (OLTP) workloads.
- Offers Multi-AZ deployments for disaster recovery and read replicas for scaling read performance.

2. Amazon Aurora:
   - Proprietary database compatible with MySQL and PostgreSQL.
   - Provides two copies of data in each availability zone and supports up to 15 read replicas.
   - Aurora Serverless is suitable for infrequent or unpredictable workloads.
3. Amazon DynamoDB:
   - NoSQL database stored on SSD storage and spread across three geographically distinct data centers.
   - Supports eventually consistent and strongly consistent reads.
   - DynamoDB transactions offer atomicity, consistency, isolation, and durability (ACID).
   - On-demand backups and point-in-time recovery provide backup and restore capabilities.
   - DynamoDB streams enable capturing and processing item-level changes in real-time.
   - Global tables allow multi-master, multi-region replication for global applications.
4. Amazon DocumentDB:
   - Used for MongoDB workloads on AWS.
5. Amazon Keyspaces:
   - Used for Cassandra workloads on AWS.
6. Amazon Neptune:
   - Graph database service used for graph-related workloads.
7. Amazon QLDB (Quantum Ledger Database):
   - Immutable database service for maintaining a complete and verifiable history of data changes.
8. Amazon Timestream:
   - Database service for storing and analyzing time series data, such as IoT sensor data.

Ensure understanding of these concepts for the exam, as scenario-based questions may require you to choose the appropriate database solution based on specific requirements.

1. VPC Components:
   - VPC acts as a logical data center in AWS and includes components like internet gateways, virtual private gateways, route tables, network access control lists (NACLs), subnets, and security groups.
   - Each subnet is associated with one availability zone and cannot span multiple zones.
2. NAT Gateways:
   - Provide outbound internet access for instances in private subnets.
   - Redundant within an availability zone and automatically assigned a public IP address.
3. Security Groups:
   - Act as virtual firewalls for EC2 instances.
   - Stateful, allowing inbound traffic response regardless of inbound security group rules.
4. Network ACLs (NACLs):
   - Control traffic at the subnet level.
   - Stateless, meaning responses to allowed inbound traffic are subject to outbound rules.
5. Direct Connect:
   - Provides a dedicated network connection between on-premises networks and AWS.
   - Suitable for high-throughput and stable connections.
6. VPC Endpoints:

- Allow connections to AWS services without leaving the Amazon network.
- Two types: interface endpoints and gateway endpoints.

7. VPC Peering:
   - Connects one VPC to another via a direct network route using private IP addresses.
   - Peering is done in a star configuration, and transitive peering is not supported.
8. AWS PrivateLink:
   - Allows access to AWS services without VPC peering.
   - Requires a network load balancer on the service VPC and an ENI on the customer VPC.
9. Transit Gateways:
   - Simplify network topology by connecting multiple VPCs, VPN connections, and Direct Connect gateways.
   - Supports IP multicast and helps in simplifying network topology.
10. VPN Hub:
    - Simplifies VPN network topology by allowing communication between different offices connected via VPN connections.
11. AWS Wavelength:
    - Provides ultra-low latency for mobile and 5G applications by running AWS services at the edge of the network.

Understanding these concepts thoroughly will be beneficial for the exam, as networking questions are often considered challenging. Practice building VPCs from memory to solidify your understanding further.

1. Alias Records vs. CNAME:
   - Alias records are unique to AWS and are preferred over CNAME records, as they can map both naked domain names and subdomains to AWS resources.
   - CNAME records only allow mapping of subdomains.
2. Common DNS Record Types:
   - Start of Authority (SOA), CNAME, NS, and A records are commonly used DNS record types.
   - A records translate domain names into IP addresses.
3. Routing Policies:
   - Simple routing policy returns all values in a record set to users in a random order.
   - Weighted routing policy distributes traffic based on specified weights.
   - Latency-based routing policy directs users to the AWS region with the lowest latency.
   - Failover routing policy automatically switches traffic from an active to a passive resource based on health checks.
   - Geolocation routing policy routes users to resources based on their geographic location.
   - Geoproximity routing policy routes traffic based on the geographic location of both users and resources.
   - Multivalue answer routing policy returns multiple healthy records in response to DNS queries.
4. Health Checks:
   - Health checks monitor the health of individual record sets and remove unhealthy records from Route 53 until they pass the health check.
   - SNS notifications can be configured to alert about failed health checks.
5. Route 53 Traffic Flow:
   - Route 53 Traffic Flow is used for complex routing architectures and works with geoproximity routing.
   - It allows for the configuration of sophisticated routing policies through a graphical interface.

Remembering these concepts and policies will be crucial for the exam. Practice scenarios and understanding how each routing policy works in different situations will help reinforce your knowledge

1. Elastic Load Balancer Types:

- Application Load Balancers (ALBs): Operate at Layer 7 (Application Layer) and support intelligent routing decisions based on the content of the request. Used for HTTP and HTTPS traffic.
- Network Load Balancers (NLBs): Operate at Layer 4 (Transport Layer) and are designed for extreme performance, handling millions of requests per second. Used for TCP, TLS, and UDP traffic.
- Gateway Load Balancers (GWLBs): Operate at Layer 3 (Network Layer) and are used for inline virtual appliances, such as firewalls, intrusion detection systems (IDS), etc.
- Classic Load Balancers: Operate at a combination of Layers 4 and 7, primarily used for existing applications running in the EC2-Classic network mode. Less commonly used compared to ALBs and NLBs.

2. Listener, Rules, and Target Groups (for ALBs):
   - Listener: Listens for connection requests from clients on a specific protocol and port.
   - Rules: Determine how the load balancer routes requests to registered targets based on conditions.
   - Target Groups: Route requests to one or more registered targets, such as EC2 instances, using specified protocols and port numbers.
3. Health Checks:
   - Used to monitor the health of registered targets.
   - Route traffic only to healthy instances or targets.
4. Sticky Sessions:
   - Enable users to stick to the same EC2 instance for subsequent requests.
   - Useful for maintaining session state if needed by the application.
5. Deregistration Delay (or Connection Draining):
   - Keeps existing connections open for a specified duration when an instance is deregistered or becomes unhealthy.
   - Helps to ensure smooth transition during instance removal from the load balancer.

Understanding these concepts and features will be essential for managing and configuring load balancers effectively. Practice scenarios and ensure familiarity with the different types of load balancers and their use cases to excel in the exam.

1. Introduction to CloudWatch Logs:
   - CloudWatch Logs is a service provided by AWS for effectively monitoring, storing, and accessing log files from various sources within your AWS environment, including on-premise solutions.
   - It allows you to collect and centralize log data for easy analysis and troubleshooting, providing methods to search, filter, and visualize log information.
2. Log Terms:
   - Log Events: Fundamental records of what happened, containing a timestamp and associated data. Think of them as individual log entries.
   - Log Streams: Sequences of log events originating from the same source, such as a single instance or component. Log streams provide context for events.
   - Log Groups: Logical groupings of related log streams, enabling effective organization and management of log data.
3. Features of CloudWatch Logs:
   - Filter Patterns: Used to extract and analyze specific log events or data based on defined patterns, helping to monitor for relevant information and identify patterns or trends.
   - CloudWatch Logs Insights: A powerful tool for querying and analyzing log data using SQL-like query languages, facilitating flexible and efficient exploration and gaining insights from log data.
   - CloudWatch Alarms: Enable proactive response to critical events by defining thresholds and conditions that trigger automated actions, such as sending

notifications or initiating remediation processes.

4. Demo:
   - Demonstrated the process of deploying an EC2 instance, installing the CloudWatch agent, configuring log files to be sent to CloudWatch, and setting up a subscription filter to detect specific log events.
5. Exam Tips:
   - Favor CloudWatch Logs as the primary logging solution for AWS services and custom applications.
   - Understand the use of filter patterns, CloudWatch Logs Insights, and CloudWatch Alarms for effective log management, analysis, and alerting.
   - Remember to use the CloudWatch agent for sending custom log files to CloudWatch.
   - Consider CloudWatch Logs Insights when SQL-like querying of log data is mentioned in exam scenarios.

   By mastering these concepts and practices, you'll be well-equipped to handle application monitoring using CloudWatch Logs effectively.

From <https://chat.openai.com/c/d6fe90a1-a00b-4374-9bfc-54c5891880f3>