Latest Version: 7.0

Question: 1

A company has deployed an e-commerce web application in a new AWS account. An Amazon RDS for MySQL Multi-AZ DB instance is part of this deployment with a database-1.xxxxxxxxxxxx.us-east-1.rds.amazonaws.com endpoint listening on port 3306. The company's Database Specialist is able to log in to MySQL and run queries from the bastion host using these details.
When users try to utilize the application hosted in the AWS account, they are presented with a generic error message. The application servers are logging a "could not connect to server: Connection times out" error message to Amazon CloudWatch Logs.
What is the cause of this error?

A. The user name and password the application is using are incorrect.
B. The security group assigned to the application servers does not have the necessary rules to allow inbound connections from the DB instance.
C. The security group assigned to the DB instance does not have the necessary rules to allow inbound connections from the application servers.
D. The user name and password are correct, but the user is not authorized to use the DB instance.

Answer: C

Reference: https://forums.aws.amazon.com/thread.jspa?threadID=129700

Question: 2

An AWS CloudFormation stack that included an Amazon RDS DB instance was accidentally deleted and recent data was lost. A Database Specialist needs to add RDS settings to the CloudFormation template to reduce the chance of accidental instance data loss in the future.
Which settings will meet this requirement? (Choose three.)

A. Set DeletionProtection to True
B. Set MultiAZ to True
C. Set TerminationProtection to True
D. Set DeleteAutomatedBackups to False
E. Set DeletionPolicy to Delete
F. Set DeletionPolicy to Retain

Answer: ACF

Reference: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html
https://aws.amazon.com/premiumsupport/knowledge-center/cloudformation-accidental-updates/

Question: 3

A Database Specialist is troubleshooting an application connection failure on an Amazon Aurora DB cluster with multiple Aurora Replicas that had been running with no issues for the past 2 months. The connection failure lasted for 5 minutes and corrected itself after that. The Database Specialist reviewed the Amazon RDS events and determined a failover event occurred at that time. The failover process took around 15 seconds to complete.
What is the MOST likely cause of the 5-minute connection outage?

A. After a database crash, Aurora needed to replay the redo log from the last database checkpoint
B. The client-side application is caching the DNS data and its TTL is set too high
C. After failover, the Aurora DB cluster needs time to warm up before accepting client connections
D. There were no active Aurora Replicas in the Aurora DB cluster

Answer: C

Question: 4

A company is deploying a solution in Amazon Aurora by migrating from an on-premises system. The IT department has established an AWS Direct Connect link from the company's data center. The company's Database Specialist has selected the option to require SSL/TLS for connectivity to prevent plaintext data from being set over the network. The migration appears to be working successfully, and the data can be queried from a desktop machine.
Two Data Analysts have been asked to query and validate the data in the new Aurora DB cluster. Both Analysts are unable to connect to Aurora. Their user names and passwords have been verified as valid and the Database Specialist can connect to the DB cluster using their accounts. The Database Specialist also verified that the security group configuration allows network from all corporate IP addresses.
What should the Database Specialist do to correct the Data Analysts' inability to connect?

A. Restart the DB cluster to apply the SSL change.
B. Instruct the Data Analysts to download the root certificate and use the SSL certificate on the connection string to connect.
C. Add explicit mappings between the Data Analysts' IP addresses and the instance in the security group assigned to the DB cluster.
D. Modify the Data Analysts' local client firewall to allow network traffic to AWS.

Answer: D

Question: 5

A company is concerned about the cost of a large-scale, transactional application using Amazon DynamoDB that only needs to store data for 2 days before it is deleted. In looking at the tables, a Database Specialist notices that much of the data is months old, and goes back to when the application was first deployed.
What can the Database Specialist do to reduce the overall cost?

A. Create a new attribute in each table to track the expiration time and create an AWS Glue transformation to delete entries more than 2 days old.
B. Create a new attribute in each table to track the expiration time and enable DynamoDB Streams on each table.
C. Create a new attribute in each table to track the expiration time and enable time to live (TTL) on each table.
D. Create an Amazon CloudWatch Events event to export the data to Amazon S3 daily using AWS Data Pipeline and then truncate the Amazon DynamoDB table.

Answer: A

Question: 6

A company has an on-premises system that tracks various database operations that occur over the lifetime of a database, including database shutdown, deletion, creation, and backup.
The company recently moved two databases to Amazon RDS and is looking at a solution that would satisfy these requirements. The data could be used by other systems within the company.
Which solution will meet these requirements with minimal effort?

A. Create an Amazon Cloudwatch Events rule with the operations that need to be tracked on Amazon RDS. Create an AWS Lambda function to act on these rules and write the output to the tracking systems.
B. Create an AWS Lambda function to trigger on AWS CloudTrail API calls. Filter on specific RDS API calls and write the output to the tracking systems.
C. Create RDS event subscriptions. Have the tracking systems subscribe to specific RDS event system notifications.
D. Write RDS logs to Amazon Kinesis Data Firehose. Create an AWS Lambda function to act on these rules and write the output to the tracking systems.

Answer: C

Question: 7

A clothing company uses a custom ecommerce application and a PostgreSQL database to sell clothes to thousands of users from multiple countries. The company is migrating its application and database from its on- premises data center to the AWS Cloud. The company has selected Amazon EC2 for the application and Amazon RDS for PostgreSQL for the database. The company requires database passwords to be changed every 60 days. A Database Specialist needs to ensure that the credentials used by the web application to connect to the database are managed securely.

Which approach should the Database Specialist take to securely manage the database credentials?

A. Store the credentials in a text file in an Amazon S3 bucket. Restrict permissions on the bucket to the IAM role associated with the instance profile only. Modify the application to download the text file and retrieve the credentials on start up. Update the text file every 60 days.
B. Configure IAM database authentication for the application to connect to the database. Create an IAM user and map it to a separate database user for each ecommerce user. Require users to update their passwords every 60 days.
C. Store the credentials in AWS Secrets Manager. Restrict permissions on the secret to only the IAM role associated with the instance profile. Modify the application to retrieve the credentials from Secrets Manager on start up. Configure the rotation interval to 60 days.
D. Store the credentials in an encrypted text file in the application AMI. Use AWS KMS to store the key for decrypting the text file. Modify the application to decrypt the text file and retrieve the credentials on start up. Update the text file and publish a new AMI every 60 days.

Answer: B

Question: 8

A financial services company is developing a shared data service that supports different applications from throughout the company. A Database Specialist designed a solution to leverage Amazon ElastiCache for Redis with cluster mode enabled to enhance performance and scalability. The cluster is configured to listen on port 6379.
Which combination of steps should the Database Specialist take to secure the cache data and protect it from unauthorized access? (Choose three.)

A. Enable in-transit and at-rest encryption on the ElastiCache cluster.
B. Ensure that Amazon CloudWatch metrics are configured in the ElastiCache cluster.
C. Ensure the security group for the ElastiCache cluster allows all inbound traffic from itself and inbound traffic on TCP port 6379 from trusted clients only.
D. Create an IAM policy to allow the application service roles to access all ElastiCache API actions.
E. Ensure the security group for the ElastiCache clients authorize inbound TCP port 6379 and port 22 traffic from the trusted ElastiCache cluster's security group.
F. Ensure the cluster is created with the auth-token parameter and that the parameter is used in all subsequent commands.

Answer: ABE

Reference: https://aws.amazon.com/getting-started/tutorials/setting-up-a-redis-cluster-with-amazon-elasticache/

Question: 9

A company is running an Amazon RDS for PostgeSQL DB instance and wants to migrate it to an Amazon Aurora PostgreSQL DB cluster. The current database is 1 TB in size. The migration needs to have minimal downtime.
What is the FASTEST way to accomplish this?

A. Create an Aurora PostgreSQL DB cluster. Set up replication from the source RDS for PostgreSQL DB instance using AWS DMS to the target DB cluster.
B. Use the pg_dump and pg_restore utilities to extract and restore the RDS for PostgreSQL DB instance to the Aurora PostgreSQL DB cluster.
C. Create a database snapshot of the RDS for PostgreSQL DB instance and use this snapshot to create the Aurora PostgreSQL DB cluster.
D. Migrate data from the RDS for PostgreSQL DB instance to an Aurora PostgreSQL DB cluster using an Aurora Replica. Promote the replica during the cutover.

Answer: C

Question: 10

A Database Specialist is migrating a 2 TB Amazon RDS for Oracle DB instance to an RDS for PostgreSQL DB instance using AWS DMS. The source RDS Oracle DB instance is in a VPC in the us-east-1 Region. The target RDS for PostgreSQL DB instance is in a VPC in the use-west-2 Region.
Where should the AWS DMS replication instance be placed for the MOST optimal performance?

A. In the same Region and VPC of the source DB instance
B. In the same Region and VPC as the target DB instance
C. In the same VPC and Availability Zone as the target DB instance
D. In the same VPC and Availability Zone as the source DB instance

Answer: D