Q1. A web application has two developers, Martha and Richard, who need full access to Amazon EC2 and Amazon S3 in the developer accounts (DevAccount1 and DevAccount2) and read-only access to EC2 and S3 resources in the production accounts (ProdAccount1 and ProdAccount2).

Find the correct order of steps to grant Martha and Richard permissions to the developer and production accounts.

Options

- (●) 1. Add users and groups in AWS SSO 2. Create permission sets 3. Assign groups to accounts and permission sets 4. Users sign into the User Portal to access accounts
- ( ) 1. Users sign into the User Portal to access accounts 2. Create permission sets 3. Assign groups to accounts and permission sets 4. Add users and groups in AWS SSO
- ( ) 1. Create permission sets 2. Assign groups to accounts and permission sets 3. Add users and groups in AWS SSO 4. Users sign into the User Portal to access accounts
- ( ) 1. Add users and groups in AWS SSO 2. Create permission sets 3. Users sign into the User Portal to access accounts 4. Assign groups to accounts and permission sets

2. Our requirement is to connect to MySQL RDS instance using credentials fetched from aws secrets. Find the correct order of steps to fulfil the equirement.

Options

1. Launch AWS mysql RDS instance in default VPC
 2. Create a user in IAM
 3. Launch an EC2 instance in default VPC with public ip enabled
 4. Store a new Secret as RDS database
 5. Modify RDS security group to provide inbound access to EC2 security group
 6. Create new IAM policy
 7. Attach the policy to IAM user
 8. SSH in EC2 instance, change to root user, install mysql, jquery and configure aws user
 9. Review and Stroe the key

1. Launch AWS mysql RDS instance in default VPC
 2. Launch an EC2 instance in default VPC with public ip enabled
 3. Modify RDS security group to provide inbound access to EC2 security group
 4. Create a user in IAM
 5. SSH in EC2 instance, change to root user, install mysql, jquery and configure aws user
 6. Create new IAM policy
 7. Attach the policy to IAM user
 8. Store a new Secret as RDS database
 9. Review and Stroe the key

1. SSH in EC2 instance, change to root user, install mysql, jquery and configure aws user
 2. Modify RDS security group to provide inbound access to EC2 security group
 3. Create new IAM policy
 4. Attach the policy to IAM user
 5. Store a new Secret as RDS database
 6. Create a user in IAM
 7. Launch AWS mysql RDS instance in default VPC
 8. Launch an EC2 instance in default VPC with public ip enabled
 9. Review and Stroe the key

1. Create a user in IAM
 2. Attach the policy to IAM user
 3. Create new IAM policy
 4. Launch an EC2 instance in default VPC with public ip enabled
 5. Store a new Secret as RDS database
 6. Launch AWS mysql RDS instance in default VPC
 7. Modify RDS security group to provide inbound access to EC2 security group
 8. SSH in EC2 instance, change to root user, install mysql, jquery and configure aws user
 9. Review and Stroe the key

Time Remaining: 02:55:12 Submit Assessment

Q3. Which of the following method will allow an application using an AWS SDK to be authenticated as a principal to access AWS Cloud services?

Options

- Create an IAM user and store the user name and password for the user in the application's configuration.Programmatic access is authenticated with user names/passwords, and not with an access key.
- Create an IAM user and store both parts of the access key for the user in the application's configuration.Programmatic access is authenticated with an access key, not with user names/passwords
- Run the application on an Amazon EC2 instance without an assigned IAM role.
- Make all the API calls over an SSL connection.No need to have an IAM user.

rrent Question

0

kipped

06

Q4. You are building a large-scale confidential documentation web server on AWS and all of its documentation will be stored on S3. One of the requirements is that it should not be publicly accessible from S3 directly, and CloudFront would be needed to accomplish this. Which of the methods listed below would satisfy the outlined requirements? Choose an answer from the options below.

Options

- Create an Identity and Access Management (IAM) user for CloudFront and grant access tothe objects in your S3 bucket to that IAM User.
- Create an Origin Access Identity (OAI) for CloudFront and grant access to the objectsin your S3 bucket to that OAI.
- Create individual policies for each bucket the documents are stored in, and grant access only to CloudFront in these policies.
- Create an S3 bucket policy that lists the CloudFront distribution ID as the Principaland the target bucket as the Amazon Resource Name (ARN).

Q5. As a security engineer, you refactored an application amd removes the hardcoded Amazon RDS database credential from the application and stored it to AWS Secrets Manager instead. The application works fine after the code change. For improved data security, you enabled rotation of the credential in Secrets Manager and then set the rotation to change every 30 days. The change was done successfully without any issues but after a short while, the application is getting an authentication error whenever it connects to the database.

What is the MOST likely cause of this issue?

Options

- The Security Engineer doesn't have the required AWS CloudHSM permissions. The AWS Secrets Manager encrypts the protected text of a secret by using AWS CloudHSM.
- Enabling rotation in AWS Secrets Manager causes the secret to rotate immediately.
- The Security Engineer doesn't have a SecretsManagerReadWrite permission.
- IAM DB Authentication was accidentally turned off.

Q6. _____ provides easy and seamless access to all enterprise resources with one set of credentials.
Amazon Web Services supports only Identity Provider initiated _____.

Find the correct option to complete above statements.

Options

- ○ SSO, IP Blocking
- ○ IP Blocking, SSO
- ○ IP Blocking, IP Blocking
- ◉ SSO, SSO