Free Questions for SCS-C01 by go4braindumps

Shared by Rhodes on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

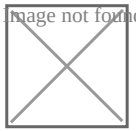
A company created an IAM account for its developers to use for testing and learning purposes Because MM account will be shared among multiple teams of developers, the company wants to restrict the ability to stop and terminate Amazon EC2 instances so that a team can perform these actions only on the instances it owns.

Developers were Instructed to tag al their instances with a Team tag key and use the team name in the tag value One of the first teams to use this account is Business Intelligence A security engineer needs to develop a highly scalable solution for providing developers with access to the appropriate resources within the account The security engineer has already created individual IAM roles for each team.

Which additional configuration steps should the security engineer take to complete the task?

A.

For each team, create an AM policy similar to the one that fellows Populate the ec2: ResourceTag/Team condition key with a proper team name Attach resulting policies to the corresponding IAM roles.



B.

For each team create an IAM policy similar to the one that follows Populate the IAM TagKeys/Team condition key with a proper team name. Attach the resuming policies to the corresponding IAM roles.

Image not found or type unknown

C.

Tag each IAM role with a Team lag key. and use the team name in the tag value. Create an IAM policy similar to the one that follows, and attach 4 to all the IAM roles used by developers.

Image not found or type unknown

D.

Tag each IAM role with the Team key, and use the team name in the tag value. Create an IAM policy similar to the one that follows, and it to all the IAM roles used by developers.

Image not found or type unknown

Options:

A) Option A

B) Option B

C) Option C

D) Option D

Answer:

A

Question 2

Question Type: **MultipleChoice**

A company's security team is building a solution for logging and visualization. The solution will assist the company with the large variety and velocity of data that it receives from IAM across multiple accounts. The security team has enabled IAM CloudTrail and VPC Flow Logs in all of its accounts In addition, the company has an organization in IAM Organizations and has an IAM Security Hub master account.

The security team wants to use Amazon Detective However the security team cannot enable Detective and is unsure why

What must the security team do to enable Detective?

Options:

A) Enable Amazon Macie so that Secunty H jb will allow Detective to process findings from Macie.

B) Disable IAM Key Management Service (IAM KMS) encryption on CtoudTrail logs in every member account of the organization

C) Enable Amazon GuardDuty on all member accounts Try to enable Detective in 48 hours

D) Ensure that the principal that launches Detective has the organizations ListAccounts permission

Answer:

D

Question 3

Question Type: MultipleChoice

A company has a website with an Amazon CloudFront HTTPS distribution, an Application Load Balancer (ALB) with multiple web instances for dynamic website content, and an Amazon S3 bucket for static website content. The company's security engineer recently updated the website security requirements:

* HTTPS needs to be enforced for all data in transit with specific ciphers.

* The CloudFront distribution needs to be accessible from the internet only.

Which solution will meet these requirements?

A company Is trying to replace its on-premises bastion hosts used to access on-premises Linux servers with AWS Systems Manager Session Manager. A security engineer has installed the Systems Manager Agent on all servers. The security engineer verifies that the agent is running on all the servers, but Session Manager cannot connect to them. The security engineer needs to perform verification steps before Session Manager will work on the servers.

Which combination of steps should the security engineer perform? (Select THREE.)

Options:

A) Open inbound port 22 to 0 0.0.0/0 on all Linux servers.

B) Enable the advanced-instances tier in Systems Manager.

C) Create a managed-instance activation for the on-premises servers.

D) Reconfigure the Systems Manager Agent with the activation code and ID.

E) Assign an IAM role to all of the on-premises servers.

F) Initiate an inventory collection with Systems Manager on the on-premises servers

Answer:

C, E, F

Question 4

Question Type: MultipleChoice

A company is using AWS Organizations to manage multiple AWS accounts. The company has an application that allows users to assume the AppUser IAM role to download files from an Amazon S3 bucket that is encrypted with an AWS KMS CMK However when users try to access the files in the S3 bucket they get an access denied error.

What should a Security Engineer do to troubleshoot this error? (Select THREE)

Options:

A) Ensure the KMS policy allows the AppUser role to have permission to decrypt for the CMK

B) Ensure the S3 bucket policy allows the AppUser role to have permission to get objects for the S3 bucket

C) Ensure the CMK was created before the S3 bucket.

D) Ensure the S3 block public access feature is enabled for the S3 bucket.

E) Ensure that automatic key rotation is disabled for the CMK

F) Ensure the SCPs within Organizations allow access to the S3 bucket.

Answer:

A, B, F

Question 5

Question Type: MultipleChoice

A company's information security team wants to analyze Amazon EC2 performance and utilization data in the near-real time for anomalies. A Sec Engineer is responsible for log aggregation. The Engineer must collect logs from all of the company's AWS accounts in centralized location to perform the analysis.

How should the Security Engineer do this?

Log in to each account four te a day and filter the AWS CloudTrail log data, then copy and paste the logs in to the Amazon S3 bucket in the destination account.

Options:

A) Set up Amazon CloudWatch to stream data to an Amazon S3 bucket in each source account. Set up bucket replication for each source account into a centralized bucket owned by the security Engineer.

B) Set up an AWS Config aggregator to collect AWS configuration data from multiple sources.

C) Set up an AWS config aggregator to collect AWS configuration data from multiple sources.

D) Set up Amazon CloudWatch cross-account log data sharing with subscriptions in each account. Send the logs to Amazon Kinesis Data Firehose in the Security Engineer's account.

Answer:

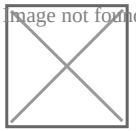
A

Question 6

Question Type: MultipleChoice

A Security Engineer manages AWS Organizations for a company. The Engineer would like to restrict AWS usage to allow Amazon S3 only in one of the organizational units (OUs). The Engineer adds the following SCP to the OU:

Image not found or type unknown



The next day. API calls to AWS IAM appear in AWS CloudTrail logs In an account under that OU. How should the Security Engineer resolve this issue?

Options:

A) Move the account to a new OU and deny IAM:* permissions.

B) Add a Deny policy for all non-S3 services at the account level.

C) Change the policy to:

{

"Version": "2012-10-17",

''Statement'': [
{
''Sid'': ''AllowS3'',
'Effect': 'Allow',
'Action': 's3:*',
'Resource': '*/*
}
]
}

D) Detach the default FullAWSAccess SCP

Answer:

C