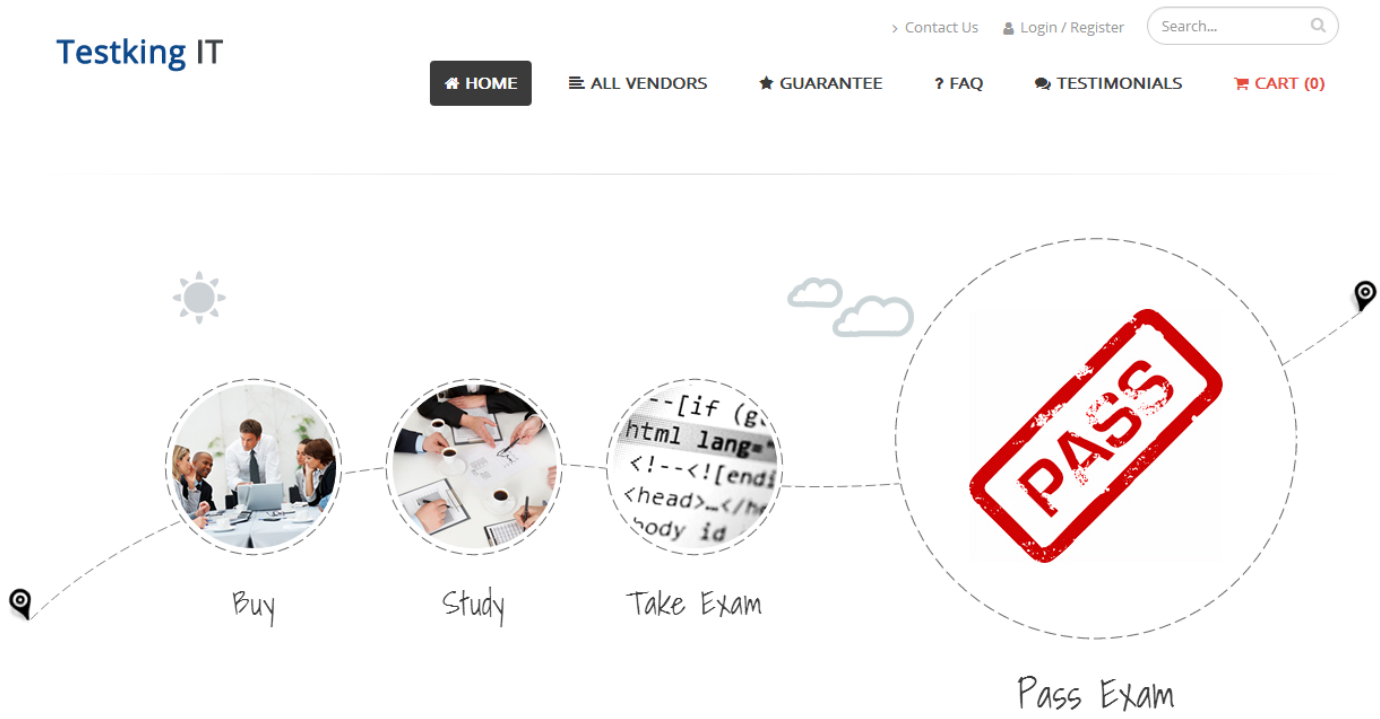
TestkingIT



Try **Desktop Test Engine** before you buy

We're not the only ones **happy** about TestKingsIT Practice Material ...

48236+ customers in 100+ countries use TestKingsIT Test Engine. Meet our customers.

iMessenger VOREED GetCustom JET ORANGE iCompany Paradoxx

http://www.testkingit.com/

Latest practice material - Exam Cram - TestKingIT

Exam : **SCS-C01**

Title : AWS Certified Security - Specialty

Vendor : Amazon

Version : DEMO

NO.1 You have just received an email from IAM Support stating that your IAM account might have been compromised. Which of the following steps would you look to carry out immediately. Choose 3 answers from the options below.
Please select:
A. Rotate all IAM access keys
B. Keep all resources running to avoid disruption
C. Change the root account password.
D. Change the password for all IAM users.
Answer: A,C,D
Explanation:
One of the articles from IAM mentions what should be done in such a scenario If you suspect that your account has been compromised, or if you have received a notification from IAM that the account has been compromised, perform the following tasks:
Change your IAM root account password and the passwords of any IAM users.
Delete or rotate all root and IAM Identity and Access Management (IAM) access keys.
Delete any resources on your account you didn't create, especially running EC2 instances, EC2 spot bids, or IAM users.
Respond to any notifications you received from IAM Support through the IAM Support Center.
Option C is invalid because there could be compromised instances or resources running on your environment. They should be shutdown or stopped immediately.
For more information on the article, please visit the below URL:
https://IAM.amazon.com/premiumsupport/knowledee-center/potential-account-compromise> The correct answers are: Change the root account password. Rotate all IAM access keys. Change the password for all IAM users. Submit your Feedback/Queries to our Experts

NO.2 A company is using IAM Organizations to manage multiple IAM member accounts. All of these accounts have Amazon GuardDuty enabled in all Regions. The company's IAM Security Operations Center has a centralized security account for logging and monitoring. One of the member accounts has received an excessively high bill A security engineer discovers that a compromised Amazon EC2 instance is being used to mine crypto currency. The Security Operations Center did not receive a GuardDuty finding in the central security account.
but there was a GuardDuty finding in the account containing the compromised EC2 instance. The security engineer needs to ensure an GuardDuty finding are available in the security account.
What should the security engineer do to resolve this issue?
A. Set up an Amazon CloudWatch Events rule to forward all GuardDuty findings to the security account Use an IAM Lambda function as a target to raise findings in IAM Security Hub
B. Set up an Amazon CloudWatch Event rule to forward ail GuardDuty findings to the security account Use an IAM Lambda function as a target to raise findings
C. Use the IAM GuardDuty get-members IAM CLI command m the security account to see if the account is listed Send an invitation from GuardDuty m the security account to GuardDuty in the compromised account Accept the invitation to forward all future GuardDuty findings
D. Check that GuardDuty in the security account is able to assume a role in the compromised account using the GuardDuty fast findings permission Schedule an Amazon CloudWatch Events rule and an IAM Lambda function to periodically check for GuardDuty findings
Answer: C

NO.3 A company has external vendors that must deliver files to the company. These vendors have cross-account that gives them permission to upload objects to one of the company's S3 buckets. What combination of steps must the vendor follow to successfully deliver a file to the company? Select 2 answers from the options given below Please select:

A. Attach an IAM role to the bucket that grants the bucket owner full permissions to the object

B. Encrypt the object with a KMS key controlled by the company.

C. Upload the file to the company's S3 bucket

D. Add a bucket policy to the bucket that grants the bucket owner full permissions to the object

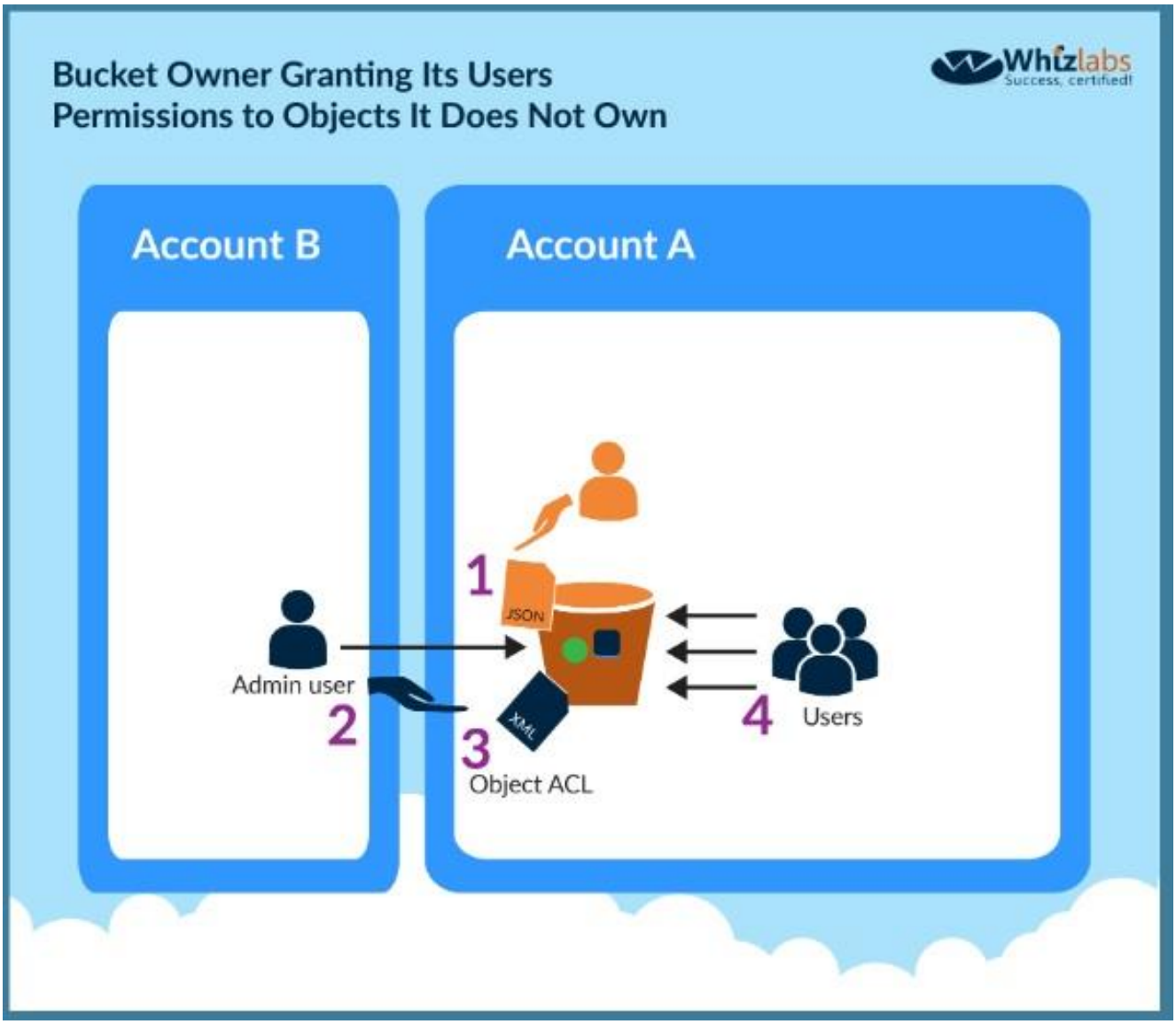
E. Add a grant to the objects ACL giving full permissions to bucket owner.

Answer: C,E

Explanation:

This scenario is given in the IAM Documentation

A bucket owner can enable other IAM accounts to upload objects. These objects are owned by the accounts that created them. The bucket owner does not own objects that were not created by the bucket owner. Therefore, for the bucket owner to grant access to these objects, the object owner must first grant permission to the bucket owner using an object ACL. The bucket owner can then delegate those permissions via a bucket policy. In this example, the bucket owner delegates permission to users in its own account.



Option A and D are invalid because bucket ACL's are used to give grants to bucket Option C is not required since encryption is not part of the requirement For more information on this scenario please see the below Link:
https://docs.IAM.amazon.com/AmazonS3/latest/dev/example-walkthroushs-manaeing-access-example3.htmll The correct answers are: Add a grant to the objects ACL giving full permissions to bucket owner., Upload the file to the company's S3 bucket Submit your Feedback/Queries to our Experts

NO.4 An application has a requirement to be resilient across not only Availability Zones within the application's primary region but also be available within another region altogether.
Which of the following supports this requirement for IAM resources that are encrypted by IAM KMS?
A. Copy the application's IAM KMS CMK from the source region to the target region so that it can be used to decrypt the resource after it is copied to the target region.
B. Configure the target region's IAM service to communicate with the source region's IAM KMS so that it can decrypt the resource in the target region.
C. Configure IAM KMS to automatically synchronize the CMK between regions so that it can be used to decrypt the resource in the target region.
D. Use IAM services that replicate data across regions, and re-wrap the data encryption key created

in the source region by using the CMK in the target region so that the target region's CMK can decrypt the database encryption key.

Answer: D

NO.5 You are trying to use the Systems Manager to patch a set of EC2 systems. Some of the systems are not getting covered in the patching process. Which of the following can be used to troubleshoot the issue? Choose 3 answers from the options given below.

Please select:

A. Check the Instance status by using the Health API.

B. Ensure that agent is running on the instances.

C. Check to see if the IAM user has the right permissions for EC2

D. Check to see if the right role has been assigned to the EC2 instances

Answer: A,B,D

Explanation:

For ensuring that the instances are configured properly you need to ensure the followi .

1) You installed the latest version of the SSM Agent on your instance

2) Your instance is configured with an IAM Identity and Access Management (IAM) role that enables the instance to communicate with the Systems Manager API

3) You can use the Amazon EC2 Health API to quickly determine the following information about Amazon EC2 instances The status of one or more instances The last time the instance sent a heartbeat value The version of the SSM Agent The operating system The version of the EC2Config service (Windows) The status of the EC2Config service (Windows) Option B is invalid because IAM users are not supposed to be directly granted permissions to EC2 Instances For more information on troubleshooting IAM SSM, please visit the following URL:

https://docs.IAM.amazon.com/systems-manager/latest/userguide/troubleshooting-remote-commands.html The correct answers are: Check to see if the right role has been assigned to the EC2 Instances, Ensure that agent is running on the Instances., Check the Instance status by using the Health API.

Submit your Feedback/Queries to our Experts

NO.6 A company is building an application on IAM that will store sensitive Information. The company has a support team with access to the IT infrastructure, including databases. The company's security engineer must introduce measures to protect the sensitive data against any data breach while minimizing management overhead. The credentials must be regularly rotated.

What should the security engineer recommend?

A. Install a database on an Amazon EC2 Instance. Enable third-party disk encryption to encrypt the Amazon Elastic Block Store (Amazon EBS) volume. Store the database credentials in IAM CloudHSM with automatic rotation. Set up TLS for the connection to the database.

B. Enable Amazon RDS encryption to encrypt the database and snapshots. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instances. Include the database credential in the EC2 user data field. Use an IAM Lambda function to rotate database credentials. Set up TLS for the connection to the database.

C. Enable Amazon RDS encryption to encrypt the database and snapshots. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instances. Store the database credentials in IAM Secrets Manager with automatic rotation. Set up TLS for the connection to the RDS hosted

database.

D. Set up an IAM CloudHSM cluster with IAM Key Management Service (IAM KMS) to store KMS keys. Set up Amazon RDS encryption using IAM KMS to encrypt the database. Store database credentials in the IAM Systems Manager Parameter Store with automatic rotation. Set up TLS for the connection to the RDS hosted database.

Answer: C

NO.7 An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing.

Which steps should be taken to troubleshoot the issue? (Choose two.)

A. Verify that the permissions used by the agent allow creation of log groups/streams and to put log events.

B. Verify that the time zone on the application servers is in UTC.

C. Check that the trust relationship grants the service "cwlogs.amazonIAM.com" permission to write objects to the Amazon S3 staging bucket.

D. Use an EC2 run command to confirm that the "IAMlogs" service is running on all instances.

E. Check whether any application log entries were rejected because of invalid time stamps by reviewing /var/cwlogs/rejects.log.

Answer: A,D

Explanation:

EC2 run command - can run scripts, install software, collect metrics and log files, manage patches and more. Bringing these two services together - can create CloudWatch Events rules that use EC2 Run Command to perform actions on EC2 instances or on-premises servers.

NO.8 A company's on-premises networks are connected to VPCs using an IAM Direct Connect gateway. The company's on-premises application needs to stream data using an existing Amazon Kinesis Data Firehose delivery stream. The company's security policy requires that data be encrypted in transit using a private network.

How should the company meet these requirements?

A. Peer the on-premises network with the Kinesis Data Firehose VPC using Direct Connect. Configure the application to connect to the existing Firehose delivery stream.

B. Create a VPC endpoint tor Kinesis Data Firehose. Configure the application to connect to the VPC endpoint.

C. Create a new TLS certificate in IAM Certificate Manager (ACM). Create a public-facing Network Load Balancer (NLB) and select the newly created TLS certificate. Configure the NLB to forward all traffic to Kinesis Data Firehose. Configure the application to connect to the NLB.

D. Configure an IAM policy to restrict access to Kinesis Data Firehose using a source IP condition. Configure the application to connect to the existing Firehose delivery stream.

Answer: B

NO.9 A company needs to store multiple years of financial records. The company wants to use Amazon S3 to store copies of these documents. The company must implement a solution to prevent

the documents from being edited, replaced, or deleted for 7 years after the documents are stored in Amazon S3. The solution must also encrypt the documents at rest.
A security engineer creates a new S3 bucket to store the documents.
What should the security engineer do next to meet these requirements?
A. Configure S3 server-side encryption. Configure S3 Versioning on the S3 bucket. Configure S3 Object Lock to use compliance mode with a retention period of 7 years.
B. Configure S3 server-side encryption. Create an S3 bucket policy that has an explicit deny rule for all users for s3:DeleteObject and s3:PutObject API calls. Configure S3 Object Lock to use governance mode with a retention period of 7 years.
C. Set up S3 Event Notifications and use S3 server-side encryption. Configure S3 Event Notifications to target an AWS Lambda function that will review any S3 API call to the S3 bucket and deny the s3:DeleteObject and s3:PutObject API calls. Remove the S3 event notification after 7 years.
D. Configure S3 Versioning. Configure S3 Intelligent-Tiering on the S3 bucket to move the documents to S3 Glacier Deep Archive storage. Use S3 server-side encryption immediately. Expire the objects after 7 years.
Answer: A

NO.10 You are trying to use the IAM Systems Manager run command on a set of Instances. The run command on a set of Instances. What can you do to diagnose the issue? Choose 2 answers from the options given Please select:
A. Ensure the right AMI is used for the Instance
B. Check the /var/log/amazon/ssm/errors.log file
C. Ensure the security groups allow outbound communication for the instance
D. Ensure that the SSM agent is running on the target machine
Answer: B,D
Explanation:
The IAM Documentation mentions the following
If you experience problems executing commands using Run Command, there might be a problem with the SSM Agent. Use the following information to help you troubleshoot the agent View Agent Logs The SSM Agent logs information in the following files. The information in these files can help you troubleshoot problems.
On Windows
%PROGRAMDATA%\Amazon\SSM\Logs\amazon-ssm-agent.log
%PROGRAMDATA%\Amazon\SSM\Logs\error.log
The default filename of the seelog is seelog-xml.template. If you modify a seelog, you must rename the file to seelog.xml.
On Linux
/var/log/amazon/ssm/amazon-ssm-agentlog /var/log/amazon/ssm/errors.log
Option C is invalid because the right AMI has nothing to do with the issues. The agent which is used to execute run commands can run on a variety of AMI'S Option D is invalid because security groups does not come into the picture with the communication between the agent and the SSM service For more information on troubleshooting IAM SSM, please visit the following URL:
https://docs.IAM.amazon.com/systems-manaeer/latest/userguide/troubleshootine-remote-commands.htmll The correct answers are: Ensure that the SSM agent is running on the target machine. Check the /var/log/amazon/ssm/errors.log file Submit your Feedback/Queries to our

Experts

NO.11 You have a bucket and a VPC defined in IAM. You need to ensure that the bucket can only be accessed by the VPC endpoint. How can you accomplish this?
Please select:

A. Modify the route tables to allow access for the VPC endpoint

B. Modify the security groups for the VPC to allow access to the 53 bucket

C. Modify the IAM Policy for the bucket to allow access for the VPC endpoint

D. Modify the bucket Policy for the bucket to allow access for the VPC endpoint

Answer: D

Explanation:
This is mentioned in the IAM Documentation
Restricting Access to a Specific VPC Endpoint
The following is an example of an S3 bucket policy that restricts access to a specific bucket, examplebucket only from the VPC endpoint with the ID vpce-la2b3c4d. The policy denies all access to the bucket if the specified endpoint is not being used. The IAM:sourceVpce condition is used to the specify the endpoint. The IAM:sourceVpce condition does not require an ARN for the VPC endpoint resource, only the VPC endpoint ID. For more information about using conditions in a policy, see Specifying Conditions in a Policy.

Options A and B are incorrect because using Security Groups nor route tables will help to allow access specifically for that bucke via the VPC endpoint Here you specifically need to ensure the bucket policy is changed.
Option C is incorrect because it is the bucket policy that needs to be changed and not the IAM policy.
For more information on example bucket policies for VPC endpoints, please refer to below URL:
https://docs.IAM.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html
The correct answer is: Modify the bucket Policy for the bucket to allow access for the VPC endpoint
Submit your Feedback/Queries to our Experts

NO.12 Due to new compliance requirements, a Security Engineer must enable encryption with

customer-provided keys on corporate data that is stored in DynamoDB. The company wants to retain full control of the encryption keys.
Which DynamoDB feature should the Engineer use to achieve compliance'?
A. Enable S3 server-side encryption with the customer-provided keys. Upload the data to Amazon S3, and then use S3Copy to move all data to DynamoDB
B. Create a KMS master key. Generate per-record data keys and use them to encrypt data prior to uploading it to DynamoDS. Dispose of the cleartext and encrypted data keys after encryption without storing.
C. Use the DynamoDB Java encryption client to encrypt data prior to uploading it to DynamoDB.
D. Use IAM Certificate Manager to request a certificate. Use that certificate to encrypt data prior to uploading it to DynamoDB.
Answer: C
Explanation:
Follow the link: https://docs.IAM.amazon.com/dynamodb-encryption-client/latest/devguide/what-is-ddb-encrypt.html

NO.13 A company's policy requires that all API keys be encrypted and stored separately from source code in a centralized security account. This security account is managed by the company's security team However, an audit revealed that an API key is steed with the source code of an IAM Lambda function m an IAM CodeCommit repository in the DevOps account How should the security learn securely store the API key?
A. Create an encrypted environment variable for the Lambda function to store the API key using IAM Key Management Service (IAM KMS) tor encryption Grant access to the IAM role used by the Lambda function so that the function can decrypt the key at runtime
B. Create a secret in IAM Secrets Manager in the security account to store the API key using IAM Key Management Service (IAM KMS) tor encryption Grant access to the IAM role used by the Lambda function so that the function can retrieve the key from Secrets Manager and call the API
C. Store the API key in an Amazon S3 bucket in the security account using server-side encryption with Amazon S3 managed encryption keys (SSE-S3) to encrypt the key Create a resigned URL tor the S3 key. and specify the URL m a Lambda environmental variable in the IAM CloudFormation template Update the Lambda function code to retrieve the key using the URL and call the API
D. Create a CodeCommit repository in the security account using IAM Key Management Service (IAM KMS) tor encryption Require the development team to migrate the Lambda source code to this repository
Answer: B

NO.14 A company's security engineer is configuring Amazon S3 permissions to ban all current and future public buckets However, the company hosts several websites directly off S3 buckets with public access enabled The engineer needs to bock me pubic S3 buckets without causing any outages on me easting websites The engineer has set up an Amazon CloudFrom distribution (or each website Which set or steps should the security engineer implement next?
A. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution Switch the ONS records tor the websites to point to the CloudFront disinfection Then, tor each S3 bucket enable block public access settings

B. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution Enable block public access settings at the account level

C. Configure an S3 bucket as the origin for me CloudFront distribution Configure the S3 bucket policy to accept connections from the CloudFront points of presence only Switch the DNS records for the websites to point to the CloudFront distribution Enable block public access settings at me account level

D. Configure an S3 bucket as the origin an origin access identity (OAI) for the CloudFront distribution Switch the DNS records from websites to point to the CloudFront distribution Enable Nock public access settings at the account level

Answer: D

NO.15 A company's Security Engineer has been asked to monitor and report all IAM account root user activities.

Which of the following would enable the Security Engineer to monitor and report all root user activities? (Select TWO)

A. Using Amazon SNS to notify the target group

B. Configuring Amazon Inspector to scan the IAM account for any root user activity

C. Configuring IAM Trusted Advisor to send an email to the Security team when the root user logs in to the console

D. Creating an Amazon CloudWatch Events rule that will trigger when any API call from the root user is reported

E. Configuring IAM Organizations to monitor root user API calls on the paying account

Answer: A,D

NO.16 You need to ensure that the cloudtrail logs which are being delivered in your IAM account is encrypted. How can this be achieved in the easiest way possible?

Please select:

A. Don't do anything since CloudTrail logs are automatically encrypted.

B. Enable S3-KMS for the underlying bucket which receives the log files

C. Enable S3-SSE for the underlying bucket which receives the log files

D. Enable KMS encryption for the logs which are sent to Cloudwatch

Answer: A

Explanation:

The IAM Documentation mentions the following

By default the log files delivered by CloudTrail to your bucket are encrypted by Amazon server-side encryption with Amazon S3-managed encryption keys (SSE-S3) Option B,C and D are all invalid because by default all logs are encrypted when they sent by Cloudtrail to S3 buckets For more information on IAM Cloudtrail log encryption, please visit the following URL: https://docs.IAM.amazon.com/IAMcloudtrail/latest/usereuide/encryptine-cloudtrail-loe-files-with-IAM-kms.htmll The correct answer is: Don't do anything since CloudTrail logs are automatically encrypted. Submit your Feedback/Queries to our Experts

NO.17 A company has an AWS account that includes an Amazon S3 bucket. The S3 bucket uses server-side encryption with AWS KMS keys (SSE-KMS) to encrypt all the objects at rest by using a

customer managed key. The S3 bucket does not have a bucket policy.
An IAM role in the same account has an IAM policy that allows s3 List* and s3 Get' permissions for the S3 bucket. When the IAM role attempts to access an object in the S3 bucket the role receives an access denied message.
Why does the IAM rote not have access to the objects that are in the S3 bucket?

A. The S3 bucket lacks a policy that allows access to the customer managed key that encrypts the objects.

B. The ACL of the S3 objects does not allow read access for the objects when the objects ace encrypted at rest.

C. The IAM rote does not have permission to use the customer managed key that encrypts the objects that are in the S3 bucket.

D. The IAM rote does not have permission to use the KMS CreateKey operation.

Answer: C

Explanation:
When using server-side encryption with AWS KMS keys (SSE-KMS), the requester must have both Amazon S3 permissions and AWS KMS permissions to access the objects. The Amazon S3 permissions are for the bucket and object operations, such as s3:ListBucket and s3:GetObject. The AWS KMS permissions are for the key operations, such as kms:GenerateDataKey and kms:Decrypt. In this case, the IAM role has the necessary Amazon S3 permissions, but not the AWS KMS permissions to use the customer managed key that encrypts the objects. Therefore, the IAM role receives an access denied message when trying to access the objects. Verified Reference:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/troubleshoot-403-errors.html
https://repost.aws/knowledge-center/s3-access-denied-error-kms
https://repost.aws/knowledge-center/cross-account-access-denied-error-s3

NO.18 A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The public subnet uses CIDR 20.0.1.0/24. The user is planning to host a web server in the public subnet with port 80 and a Database server in the private subnet with port 3306. The user is configuring a security group for the public subnet (WebSecGrp) and the private subnet (DBSecGrp). which of the below mentioned entries is required in the private subnet database security group DBSecGrp?
Please select:

A. Allow Inbound on port 3306 from source 20.0.0.0/16

B. Allow Inbound on port 3306 for Source Web Server Security Group WebSecGrp.

C. Allow Outbound on port 3306 for Destination Web Server Security Group WebSecGrp.

D. Allow Outbound on port 80 for Destination NAT Instance IP

Answer: B

Explanation:
Since the Web server needs to talk to the database server on port 3306 that means that the database server should allow incoming traffic on port 3306. The below table from the IAM documentation shows how the security groups should be set up.

DBServerSG: Recommended Rules

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
The ID of your WebServerSG security group	TCP	1433	Allow inbound Microsoft SQL Server access from the web servers associated with the WebServerSG security group.
The ID of your WebServerSG security group	TCP	3306	Allow inbound MySQL Server access from the web servers associated with the WebServerSG security group.
Outbound			
Destination	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	TCP	80	Allow outbound HTTP access to the Internet over IPv4 (for example, for software updates).
0.0.0.0/0	TCP	443	Allow outbound HTTPS access to the Internet over IPv4 (for example, for software updates).

Option B is invalid because you need to allow incoming access for the database server from the WebSecGrp security group.
Options C and D are invalid because you need to allow Outbound traffic and not inbound traffic For more information on security groups please visit the below Link:
http://docs.IAM.amazon.com/AmazonVPC/latest/UserGuide/VPC Scenario2.html The correct answer is: Allow Inbound on port 3306 for Source Web Server Security Group WebSecGrp. Submit your Feedback/Queries to our Experts

NO.19 Your company has a set of EBS volumes defined in IAM. The security mandate is that all EBS volumes are encrypted. What can be done to notify the IT admin staff if there are any unencrypted volumes in the account.
Please select:
A. Use IAM Lambda to check for the unencrypted EBS volumes
B. Use IAM Inspector to inspect all the EBS volumes
C. Use IAM Guard duty to check for the unencrypted EBS volumes
D. Use IAM Config to check for unencrypted EBS volumes
Answer: D
Explanation:
The enc
config rule for IAM Config can be used to check for unencrypted volumes.
encrypted-volurrn
5 volumes that are in an attached state are encrypted. If you specify the ID of a KMS key for encryptio using the kmsld parameter, the rule checks if the EBS volumes in an attached state are encrypted with that KMS key*1.
Options A and C are incorrect since these services cannot be used to check for unencrypted EBS volumes Option D is incorrect because even though this is possible, trying to implement the solution alone with just the Lambda servk would be too difficult For more information on IAM Config and encrypted volumes, please refer to below URL:
https://docs.IAM.amazon.com/config/latest/developerguide/encrypted-volumes.html Submit your Feedback/Queries to our Experts

NO.20 A company uses AWS Organizations to manage several AWs accounts. The company processes a large volume of sensitive dat a. The company uses a serverless approach to

microservices. The company stores all the data in either Amazon S3 or Amazon DynamoDB. The company reads the data by using either AWS lambda functions or container-based services that the company hosts on Amazon Elastic Kubernetes Service (Amazon EKS) on AWS Fargate.
The company must implement a solution to encrypt all the data at rest and enforce least privilege data access controls. The company creates an AWS Key Management Service (AWS KMS) customer managed key.
What should the company do next to meet these requirements?

A. Create a key policy that allows the kms:Decrypt action only for Amazon S3, DynamoDB, Lambda, and Amazon EKS. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.

B. Create a key policy that allows the kms:Decrypt action only for Amazon S3 and DynamoDB. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.

C. Create an 1AM policy that denies the kms:Decrypt action for the key. Create a Lambda function than runs on a schedule to attach the policy to any new roles. Create an AWS Config rule to send alerts for resources that are not encrypted with the key.

D. Create a key policy that allows the kms:Decrypt action only for Amazon S3, DynamoDB, Lambda, and Amazon EKS. Create an AWS Config rule to send alerts for resources that are not encrypted with the key.

Answer: C

NO.21 A company's IAM account consists of approximately 300 IAM users. Now there is a mandate that an access change is required for 100 IAM users to have unlimited privileges to S3.As a system administrator, how can you implement this effectively so that there is no need to apply the policy at the individual user level?
Please select:

A. Create an S3 bucket policy with unlimited access which includes each user's IAM account ID

B. Create a policy and apply it to multiple users using a JSON script

C. Create a new role and add each user to the IAM role

D. Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group

Answer: D
Explanation:
Option A is incorrect since you don't add a user to the IAM Role
Option C is incorrect since you don't assign multiple users to a policy Option D is incorrect since this is not an ideal approach An IAM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group For more information on IAM Groups, just browse to the below URL:
https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_eroups.html
The correct answer is: Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group Submit your Feedback/Queries to our Experts

NO.22 A Developer's laptop was stolen. The laptop was not encrypted, and it contained the SSH key used to access multiple Amazon EC2 instances. A Security Engineer has verified that the key has not

been used, and has blocked port 22 to all EC2 instances while developing a response plan.
How can the Security Engineer further protect currently running instances?
A. Delete the key-pair key from the EC2 console, then create a new key pair.
B. Use the EC2 RunCommand to modify the authorized_keys file on any EC2 instance that is using the key.
C. Update the key pair in any AMI used to launch the EC2 instances, then restart the EC2 instances.
D. Use the modify-instance-attribute API to change the key on any EC2 instance that is using the key.
Answer: B

NO.23 Some highly sensitive analytics workloads are to be moved to Amazon EC2 hosts. Threat modeling has found that a risk exists where a subnet could be maliciously or accidentally exposed to the internet.
Which of the following mitigations should be recommended?
A. Within the Amazon VPC configuration, mark the VPC as private and disable Elastic IP addresses.
B. Use IAM Config to detect whether an Internet Gateway is added and use an IAM Lambda function to provide auto-remediation.
C. Move the workload to a Dedicated Host, as this provides additional network security controls and monitoring.
D. Use IPv6 addressing exclusively on the EC2 hosts, as this prevents the hosts from being accessed from the internet.
Answer: B
Explanation:
By default, Private instance has a private IP address, but no public IP address. These instances can communicate with each other, but can't access the Internet. You can enable Internet access for an instance launched into a nondefault subnet by attaching an Internet gateway to its VPC (if its VPC is not a default VPC) and associating an Elastic IP address with the instance. Alternatively, to allow an instance in your VPC to initiate outbound connections to the Internet but prevent unsolicited inbound connections from the Internet, you can use a network address translation (NAT) instance. NAT maps multiple private IP addresses to a single public IP address. A NAT instance has an Elastic IP address and is connected to the Internet through an Internet gateway.You can connect an instance in a private subnet to the Internet through the NAT instance, which routes traffic from the instance to the Internet gateway, and routes any responses to the instance.

NO.24 A company has implemented IAM WAF and Amazon CloudFront for an application. The application runs on Amazon EC2 instances that are part of an Auto Scaling group. The Auto Scaling group is behind an Application Load Balancer (ALB).
The IAM WAF web ACL uses an IAM Managed Rules rule group and is associated with the CloudFront distribution. CloudFront receives the request from IAM WAF and then uses the ALB as the distribution's origin.
During a security review, a security engineer discovers that the infrastructure is susceptible to a large, layer 7 DDoS attack.
How can the security engineer improve the security at the edge of the solution to defend against this type of attack?
A. Configure IAM WAF with a rate-based rule that imposes a rate limit that automatically blocks requests when the rate limit is exceeded.

B. Configure the CloudFront distribution to use the Lambda@Edge feature. Create an IAM Lambda function that imposes a rate limit on CloudFront viewer requests. Block the request if the rate limit is exceeded.
C. Configure the IAM WAF web ACL so that the web ACL has more capacity units to process all IAM WAF rules faster.
D. Configure the CloudFront distribution to use IAM WAF as its origin instead of the ALB.
Answer: A

NO.25 A Security Engineer is defining the logging solution for a newly developed product. Systems Administrators and Developers need to have appropriate access to event log files in IAM CloudTrail to support and troubleshoot the product.
Which combination of controls should be used to protect against tampering with and unauthorized access to log files? (Choose two.)
A. Ensure that Systems Administrators and Developers with job-related need-to-know requirements only are capable of viewing-but not modifying-the log files.
B. Ensure that all log files are stored on Amazon EC2 instances that allow SSH access from the internal corporate network only.
C. Ensure that the log file integrity validation mechanism is enabled.
D. Ensure that all log files are written to at least two separate Amazon S3 buckets in the same account.
E. Ensure that Systems Administrators and Developers can edit log files, but prevent any other access.
Answer: A,C

NO.26 A Web Administrator for the website example.com has created an Amazon CloudFront distribution for dev.example.com, with a requirement to configure HTTPS using a custom TLS certificate imported to IAM Certificate Manager.
Which combination of steps is required to ensure availability of the certificate in the CloudFront console? (Choose two.)
A. Call UploadServerCertificate with /cloudfront/dev/ in the path parameter.
B. Import the certificate in the us-east-1 (N. Virginia) Region.
C. Ensure that the certificate, private key, and certificate chain are PEM-encoded.
D. Import the certificate with a 4,096-bit RSA public key.
E. Ensure that the certificate, private key, and certificate chain are PKCS #12-encoded.
Answer: B,C

NO.27 A company wants to deploy a distributed web application on a fleet of EC2 instances. The fleet will be fronted by a Classic Load Balancer that will be configured to terminate the TLS connection The company wants to make sure that all past and current TLS traffic to the Classic Load Balancer stays secure even if the certificate private key is leaked.
To ensure the company meets these requirements, a Security Engineer can configure a Classic Load Balancer with:
A. A TCP listener that uses a custom security policy that allows only perfect forward secrecy cipher suites.

B. An HTTPS listener that uses a custom security policy that allows only perfect forward secrecy cipher suites
C. An HTTPS listener that uses the latest IAM predefined ELBSecuntyPolicy-TLS-1 -2-2017-01 security policy
D. An HTTPS listener that uses a certificate that is managed by Amazon Certification Manager.
Answer: B

NO.28 A company is configuring three Amazon EC2 instances with each instance in a separate Availability Zone. The EC2 instances wilt be used as transparent proxies for outbound internet traffic for ports 80 and 443 so the proxies can block traffic to certain internet destinations as required by the company's security policies. A Security Engineer completed the following:
* Set up the proxy software on the EC2 instances.
* Modified the route tables on the private subnets to use the proxy EC2 instances as the default route.
* Created a security group rule opening inbound port 80 and 443 TCP protocols on the proxy EC2 instance security group.
However, the proxy EC2 instances are not successfully forwarding traffic to the internet.
What should the Security Engineer do to make the proxy EC2 instances route traffic to the internet?
A. Change the VPC's DHCP domain-name-server's options set to the IP addresses of proxy EC2 instances.
B. Disable source and destination checks on the proxy EC2 instances.
C. Open all inbound ports on the proxy EC2 instance security group.
D. Put all the proxy EC2 instances in a cluster placement group.
Answer: B

NO.29 A company stores data on an Amazon EBS volume attached to an Amazon EC2 instance. The data is asynchronously replicated to an Amazon S3 bucket. Both the EBS volume and the S3 bucket are encrypted with the same IAM KMS Customer Master Key (CMK). A former employee scheduled a deletion of that CMK before leaving the company.
The company's Developer Operations department learns about this only after the CMK has been deleted.
Which steps must be taken to address this situation?
A. Make a request to IAM Support to recover the S3 encrypted data.
B. Recover the data from the EBS encrypted volume using an earlier version of the KMS backing key.
C. Copy the data directly from the EBS encrypted volume before the volume is detached from the EC2 instance.
D. Make a request to IAM Support to restore the deleted CMK, and use it to recover the data.
Answer: C
Explanation:
https://docs.IAM.amazon.com/kms/latest/developerguide/deleting-keys.html#deleting-keys-how-it-works

NO.30 Your company manages thousands of EC2 Instances. There is a mandate to ensure that all servers don't have any critical security flIAM. Which of the following can be done to ensure this?

Choose 2 answers from the options given below.
Please select:

A. Use IAM SSM to patch the servers

B. Use IAM inspector to patch the servers

C. Use IAM Config to ensure that the servers have no critical flIAM.

D. Use IAM inspector to ensure that the servers have no critical flIAM.

Answer: A,D

Explanation:

The IAM Documentation mentions the following on IAM Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on IAM. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.

Option A is invalid because the IAM Config service is not used to check the vulnerabilities on servers

Option C is invalid because the IAM Inspector service is not used to patch servers For more information on IAM Inspector, please visit the following URL:

https://IAM.amazon.com/inspector>

Once you understand the list of servers which require critical updates, you can rectify them by installing the required patches via the SSM tool.

For more information on the Systems Manager, please visit the following URL:

https://docs.IAM.amazon.com/systems-manager/latest/APIReference/Welcome.html The correct answers are: Use IAM Inspector to ensure that the servers have no critical flIAM.. Use IAM SSM to patch the servers (