

Amazon-Web-Services

Exam Questions SCS-C02

AWS Certified Security - Specialty



NEW QUESTION 1

- (Exam Topic 1)

A Security Engineer has several thousand Amazon EC2 instances split across production and development environments. Each instance is tagged with its environment. The Engineer needs to analyze and patch all the development EC2 instances to ensure they are not currently exposed to any common vulnerabilities or exposures (CVEs)

Which combination of steps is the MOST efficient way for the Engineer to meet these requirements? (Select TWO.)

- A. Log on to each EC2 instance, check and export the different software versions installed, and verify this against a list of current CVEs.
- B. Install the Amazon Inspector agent on all development instances Build a custom rule package, and configure Inspector to perform a scan using this custom rule on all instances tagged as being in the development environment.
- C. Install the Amazon Inspector agent on all development instances Configure Inspector to perform a scan using the CVE rule package on all instances tagged as being in the development environment.
- D. Install the Amazon EC2 System Manager agent on all development instances Issue the Run command to EC2 System Manager to update all instances
- E. Use IAM Trusted Advisor to check that all EC2 instances have been patched to the most recent version of operating system and installed software.

Answer: CD

NEW QUESTION 2

- (Exam Topic 1)

A Developer reported that IAM CloudTrail was disabled on their account. A Security Engineer investigated the account and discovered the event was undetected by the current security solution. The Security Engineer must recommend a solution that will detect future changes to the CloudTrail configuration and send alerts when changes occur.

What should the Security Engineer do to meet these requirements?

- A. Use IAM Resource Access Manager (IAM RAM) to monitor the IAM CloudTrail configuratio
- B. Send notifications using Amazon SNS.
- C. Create an Amazon CloudWatch Events rule to monitor Amazon GuardDuty finding
- D. Send email notifications using Amazon SNS.
- E. Update security contact details in IAM account settings for IAM Support to send alerts when suspicious activity is detected.
- F. Use Amazon Inspector to automatically detect security issue
- G. Send alerts using Amazon SNS.

Answer: B

NEW QUESTION 3

- (Exam Topic 1)

Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Select THREE)

- A. Default IAM Certificate Manager certificate
- B. Custom SSL certificate stored in IAM KMS
- C. Default CloudFront certificate
- D. Custom SSL certificate stored in IAM Certificate Manager
- E. Default SSL certificate stored in IAM Secrets Manager
- F. Custom SSL certificate stored in IAM IAM

Answer: ACD

NEW QUESTION 4

- (Exam Topic 1)

An external Auditor finds that a company's user passwords have no minimum length. The company is currently using two identity providers:

- IAM IAM federated with on-premises Active Directory
- Amazon Cognito user pools to accessing an IAM Cloud application developed by the company Which combination o1 actions should the Security Engineer take to solve this issue? (Select TWO.)

- A. Update the password length policy In the on-premises Active Directory configuration.
- B. Update the password length policy In the IAM configuration.
- C. Enforce an IAM policy In Amazon Cognito and IAM IAM with a minimum password length condition.
- D. Update the password length policy in the Amazon Cognito configuration.
- E. Create an SCP with IAM Organizations that enforces a minimum password length for IAM IAM and Amazon Cognito.

Answer: AD

NEW QUESTION 5

- (Exam Topic 1)

A company's architecture requires that its three Amazon EC2 instances run behind an Application Load Balancer (ALB). The EC2 instances transmit sensitive data between each other Developers use SSL certificates to encrypt the traffic between the public users and the ALB However the Developers are unsure of how to encrypt the data in transit between the ALB and the EC2 instances and the traffic between the EC2 instances

Which combination of activities must the company implement to meet its encryption requirements'? (Select TWO)

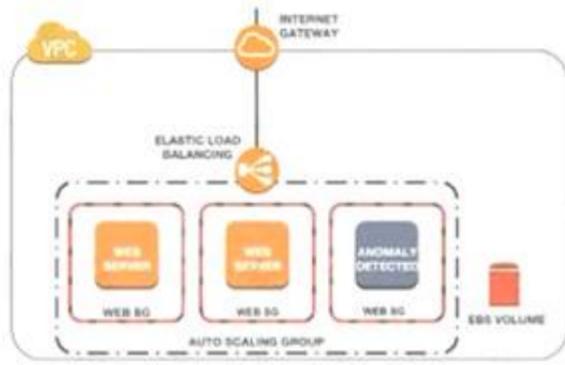
- A. Configure SSLTLS on the EC2 instances and configure the ALB target group to use HTTPS
- B. Ensure that all resources are in the same VPC so the default encryption provided by the VPC is used to encrypt the traffic between the EC2 instances.
- C. In the AL
- D. select the default encryption to encrypt the traffic between the ALB and the EC2 instances
- E. In the code for the application, include a cryptography library and encrypt the data before sending it between the EC2 instances
- F. Configure IAM Direct Connect to provide an encrypted tunnel between the EC2 instances

Answer: BC

NEW QUESTION 6

- (Exam Topic 1)

A Security Engineer noticed an anomaly within a company EC2 instance as shown in the image. The Engineer must now investigate what e causing the anomaly. What are the MOST effective steps to take lo ensure that the instance is not further manipulated while allowing the Engineer to understand what happened?



- A. Remove the instance from the Auto Scaling group Place the instance within an isolation security group, detach the EBS volume launch an EC2 instance with a forensic toolkit and attach the E8S volume to investigate
- B. Remove the instance from the Auto Scaling group and the Elastic Load Balancer Place the instance within an isolation security group, launch an EC2 instance with a forensic toolkit, and allow the forensic toolkit image to connect to the suspicious Instance to perform the Investigation.
- C. Remove the instance from the Auto Scaling group Place the Instance within an isolation security group, launch an EC2 Instance with a forensic toolkit and use the forensic toolkit imago to deploy an ENI as a network span port to inspect all traffic coming from the suspicious instance.
- D. Remove the instance from the Auto Scaling group and the Elastic Load Balancer Place the instance within an isolation security group, make a copy of the EBS volume from a new snapshot, launch an EC2 Instance with a forensic toolkit and attach the copy of the EBS volume to investigate.

Answer: B

NEW QUESTION 7

- (Exam Topic 1)

A company's development team is designing an application using IAM Lambda and Amazon Elastic Container Service (Amazon ECS). The development team needs to create IAM roles to support these systems. The company's security team wants to allow the developers to build IAM roles directly, but the security team wants to retain control over the permissions the developers can delegate to those roles. The development team needs access to more permissions than those required for the application's IAM services. The solution must minimize management overhead.

How should the security team prevent privilege escalation for both teams?

- A. Enable IAM CloudTrai
- B. Create a Lambda function that monitors the event history for privilege escalation events and notifies the security team.
- C. Create a managed IAM policy for the permissions require
- D. Reference the IAM policy as a permissions boundary within the development team's IAM role.
- E. Enable IAM Organizations Create an SCP that allows the IAM CreateUser action but that has a condition that prevents API calls other than those required by the development team
- F. Create an IAM policy with a deny on the IAMCreateUser action and assign the policy to the development tea
- G. Use a ticket system to allow the developers to request new IAM roles for their application
- H. The IAM roles will then be created by the security team.

Answer: A

NEW QUESTION 8

- (Exam Topic 1)

A company has recently recovered from a security incident that required the restoration of Amazon EC2 instances from snapshots. After performing a gap analysis of its disaster recovery procedures and backup strategies, the company is concerned that, next time, it will not be able to recover the EC2 instances if the IAM account was compromised and Amazon EBS snapshots were deleted. All EBS snapshots are encrypted using an IAM KMS CMK. Which solution would solve this problem?

- A. Create a new Amazon S3 bucket Use EBS lifecycle policies to move EBS snapshots to the new S3 bucke
- B. Move snapshots to Amazon S3 Glacier using lifecycle policies, and apply Glacier Vault Lock policies to prevent deletion
- C. Use IAM Systems Manager to distribute a configuration that performs local backups of all attached disks to Amazon S3.
- D. Create a new IAM account with limited privilege
- E. Allow the new account to access the IAM KMS key used to encrypt the EBS snapshots, and copy the encrypted snapshots to the new account on a recuning basis
- F. Use IAM Backup to copy EBS snapshots to Amazon S3.

Answer: A

NEW QUESTION 9

- (Exam Topic 1)

A company uses a third-party identity provider and SAML-based SSO for its IAM accounts After the third-party identity provider renewed an expired signing certificate users saw the following message when trying to log in:

```
Error: Response Signature Invalid (Service: AWSSecurityTokenService; Status Code: 400; Error Code: InvalidIdentityToken)
```

A security engineer needs to provide a solution that corrects the error and minimizes operational overhead Which solution meets these requirements?

- A. Upload the third-party signing certificate's new private key to the IAM identity provider entity defined in IAM identity and Access Management (IAM) by using the IAM Management Console
- B. Sign the identity provider's metadata file with the new public key Upload the signature to the IAM identity provider entity defined in IAM Identity and Access Management (IAM) by using the IAM CLI.
- C. Download the updated SAML metadata tile from the identity service provider Update the file in the IAM identity provider entity defined in IAM Identity and

Access Management (IAM) by using the IAM CLI

D. Configure the IAM identity provider entity defined in IAM Identity and Access Management (IAM) to synchronously fetch the new public key by using the IAM Management Console.

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

Unapproved changes were previously made to a company's Amazon S3 bucket. A security engineer configured IAM Config to record configuration changes made to the company's S3 buckets. The engineer discovers there are S3 configuration changes being made, but no Amazon SNS notifications are being sent. The engineer has already checked the configuration of the SNS topic and has confirmed the configuration is valid.

Which combination of steps should the security engineer take to resolve the issue? (Select TWO.)

- A. Configure the S3 bucket ACLs to allow IAM Config to record changes to the buckets.
- B. Configure policies attached to S3 buckets to allow IAM Config to record changes to the buckets.
- C. Attach the AmazonS3ReadOnlyAccess managed policy to the IAM user.
- D. Verify the security engineer's IAM user has an attached policy that allows all IAM Config actions.
- E. Assign the IAMConfigRole managed policy to the IAM Config role

Answer: BE

NEW QUESTION 10

- (Exam Topic 1)

A company requires that SSH commands used to access its IAM instance be traceable to the user who executed each command.

How should a Security Engineer accomplish this?

- A. Allow inbound access on port 22 at the security group attached to the instance Use IAM Systems Manager Session Manager for shell access to Amazon EC2 instances with the user tag defined Enable Amazon CloudWatch toggling for Systems Manager sessions
- B. Use Amazon S3 to securely store one Privacy Enhanced Mail Certificate (PEM file) for each user Allow Amazon EC2 to read from Amazon S3 and import every user that wants to use SSH to access EC2 instances Allow inbound access on port 22 at the security group attached to the instance Install the Amazon CloudWatch agent on the EC2 instance and configure it to ingest audit logs for the instance
- C. Deny inbound access on port 22 at the security group attached to the instance Use IAM Systems Manager Session Manager for shell access to Amazon EC2 instances with the user tag defined Enable Amazon CloudWatch toggling for Systems Manager sessions
- D. Use Amazon S3 to securely store one Privacy Enhanced Mail Certificate (PEM file) for each team or group Allow Amazon EC2 to read from Amazon S3 and import every user that wants to use SSH to access EC2 instances Allow inbound access on port 22 at the security group attached to the instance Install the Amazon CloudWatch agent on the EC2 instance and configure it to ingest audit logs for the instance

Answer: C

NEW QUESTION 13

- (Exam Topic 1)

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 block public S3 buckets without causing any outages on the existing websites The engineer has set up an Amazon CloudFront distribution (or each website)

Which set of steps should the security engineer implement next?

- A. 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
- B. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution Switch the DNS records for the websites to point to the CloudFront distribution Then, for each S3 bucket enable block public access settings
- C. 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
- D. Configure an S3 bucket as the origin for the 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 the account level

Answer: A

NEW QUESTION 15

- (Exam Topic 1)

After a recent security audit involving Amazon S3, a company has asked assistance reviewing its S3 buckets to determine whether data is properly secured. The first S3 bucket on the list has the following bucket policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [
            "10.10.10.0/24"
          ]
        }
      }
    }
  ]
}
```

Is this bucket policy sufficient to ensure that the data is not publicly accessible?

- A. Yes, the bucket policy makes the whole bucket publicly accessible despite now the S3 bucket ACL or object ACLs are configured.
- B. Yes, none of the data in the bucket is publicly accessible, regardless of how the S3 bucket ACL and object ACLs are configured.
- C. No, the IAM user policy would need to be examined first to determine whether any data is publicly accessible.
- D. No, the S3 bucket ACL and object ACLs need to be examined first to determine whether any data is publicly accessible.

Answer: A

NEW QUESTION 20

- (Exam Topic 1)

A global company must mitigate and respond to DDoS attacks at Layers 3, 4 and 7 All of the company's IAM applications are serverless with static content hosted on Amazon S3 using Amazon CloudFront and Amazon Route 53

Which solution will meet these requirements?

- A. Use IAM WAF with an upgrade to the IAM Business support plan
- B. Use IAM Certificate Manager with an Application Load Balancer configured with an origin access identity
- C. Use IAM Shield Advanced
- D. Use IAM WAF to protect IAM Lambda functions encrypted with IAM KMS and a NACL restricting all Ingress traffic

Answer: C

NEW QUESTION 25

- (Exam Topic 1)

A company's application runs on Amazon EC2 and stores data in an Amazon S3 bucket The company wants additional security controls in place to limit the likelihood of accidental exposure of data to external parties

Which combination of actions will meet this requirement? (Select THREE.)

- A. Encrypt the data in Amazon S3 using server-side encryption with Amazon S3 managed encryption keys (SSE-S3)
- B. Encrypt the data in Amazon S3 using server-side encryption with IAM KMS managed encryption keys (SSE-KMS)
- C. Create a new Amazon S3 VPC endpoint and modify the VPC's routing tables to use the new endpoint
- D. Use the Amazon S3 Block Public Access feature.
- E. Configure the bucket policy to allow access from the application instances only
- F. Use a NACL to filter traffic to Amazon S3

Answer: BCE

NEW QUESTION 30

- (Exam Topic 1)

A Security Engineer is looking for a way to control access to data that is being encrypted under a CMK. The Engineer is also looking to use additional authenticated data (AAD) to prevent tampering with ciphertext.

Which action would provide the required functionality?

- A. Pass the key alias to IAM KMS when calling Encrypt and Decrypt API actions.
- B. Use IAM policies to restrict access to Encrypt and Decrypt API actions.
- C. Use kms:EncryptionContext as a condition when defining IAM policies for the CMK.
- D. Use key policies to restrict access to the appropriate IAM groups.

Answer: C

Explanation:

<https://IAM.amazon.com/blogs/security/how-to-protect-the-integrity-of-your-encrypted-data-by-using-IAM-key> One of the most important and critical concepts in IAM Key Management Service (KMS) for advanced and secure data usage is EncryptionContext. Using EncryptionContext properly can help significantly improve the security of your applications. EncryptionContext is a key-value map (both strings) that is provided to KMS with each encryption and decryption request. EncryptionContext provides three benefits: Additional authenticated data (AAD), Audit trail, Authorization context

NEW QUESTION 33

- (Exam Topic 1)

A company uses multiple IAM accounts managed with IAM Organizations Security engineers have created a standard set of security groups for all these accounts. The security policy requires that these security groups be used for all applications and delegates modification authority to the security team only.

A recent security audit found that the security groups are inconsistency implemented across accounts and that unauthorized changes have been made to the security groups. A security engineer needs to recommend a solution to improve consistency and to prevent unauthorized changes in the individual accounts in the future.

Which solution should the security engineer recommend?

- A. Use IAM Resource Access Manager to create shared resources for each required security group and apply an IAM policy that permits read-only access to the security groups only.
- B. Create an IAM CloudFormation template that creates the required security groups Execute the template as part of configuring new accounts Enable Amazon Simple Notification Service (Amazon SNS) notifications when changes occur
- C. Use IAM Firewall Manager to create a security group policy, enable the policy feature to identify and revert local changes, and enable automatic remediation
- D. Use IAM Control Tower to edit the account factory template to enable the snare security groups option Apply an SCP to the OU or individual accounts that prohibits security group modifications from local account users

Answer: B

NEW QUESTION 36

- (Exam Topic 1)

A company has several critical applications running on a large fleet of Amazon EC2 instances. As part of a security operations review, the company needs to apply a critical operating system patch to EC2 instances within 24 hours of the patch becoming available from the operating system vendor. The company does not have a patching solution deployed on IAM, but does have IAM Systems Manager configured. The solution must also minimize administrative overhead.

What should a security engineer recommend to meet these requirements?

- A. Create an IAM Config rule defining the patch as a required configuration for EC2 instances.
- B. Use the IAM Systems Manager Run Command to patch affected instances.
- C. Use an IAM Systems Manager Patch Manager predefined baseline to patch affected instances.
- D. Use IAM Systems Manager Session Manager to log in to each affected instance and apply the patch.

Answer: B

NEW QUESTION 40

- (Exam Topic 1)

To meet regulatory requirements, a Security Engineer needs to implement an IAM policy that restricts the use of IAM services to the us-east-1 Region.

What policy should the Engineer implement?

A

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}
```

B

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:Region": "us-east-1"
        }
      }
    }
  ]
}
```

C

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}
```

D

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "NotAction": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

NEW QUESTION 41

- (Exam Topic 1)

A company's Developers plan to migrate their on-premises applications to Amazon EC2 instances running Amazon Linux AMIs. The applications are accessed by a group of partner companies. The Security Engineer needs to implement the following host-based security measures for these instances:

- Block traffic from documented known bad IP addresses
- Detect known software vulnerabilities and CIS Benchmarks compliance. Which solution addresses these requirements?

- A. Launch the EC2 instances with an IAM role attached
- B. Include a user data script that uses the IAM CLI to retrieve the list of bad IP addresses from IAM Secrets Manager and uploads it as a threat list in Amazon GuardDuty. Use Amazon Inspector to scan the instances for known software vulnerabilities and CIS Benchmarks compliance
- C. Launch the EC2 instances with an IAM role attached. Include a user data script that uses the IAM CLI to create NACLs blocking ingress traffic from the known bad IP addresses in the EC2 instance's subnets. Use IAM Systems Manager to scan the instances for known software vulnerabilities, and IAM Trusted Advisor to check instances for CIS Benchmarks compliance
- D. Launch the EC2 instances with an IAM role attached. Include a user data script that uses the IAM CLI to create and attach security groups that only allow an allow-listed source IP address range inbound
- E. Use Amazon Inspector to scan the instances for known software vulnerabilities, and IAM Trusted Advisor to check instances for CIS Benchmarks compliance
- F. Launch the EC2 instances with an IAM role attached. Include a user data script that creates a cron job to periodically retrieve the list of bad IP addresses from Amazon S3, and configures iptables on the instances blocking the list of bad IP addresses. Use Amazon Inspector to scan the instances for known software vulnerabilities and CIS Benchmarks compliance.

Answer: D

NEW QUESTION 42

- (Exam Topic 1)

A Security Engineer for a large company is managing a data processing application used by 1,500 subsidiary companies. The parent and subsidiary companies all use IAM. The application uses TCP port 443 and runs on Amazon EC2 behind a Network Load Balancer (NLB). For compliance reasons, the application should only be accessible to the subsidiaries and should not be available on the public internet. To meet the compliance requirements for restricted access, the Engineer has received the public and private CIDR block ranges for each subsidiary.

What solution should the Engineer use to implement the appropriate access restrictions for the application?

- A. Create a NACL to allow access on TCP port 443 from the 1,500 subsidiary CIDR block ranges. Associate the NACL to both the NLB and EC2 instances
- B. Create an IAM security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range
- C. Associate the security group to the NLB
- D. Create a second security group for EC2 instances with access on TCP port 443 from the NLB security group.
- E. Create an IAM PrivateLink endpoint service in the parent company account attached to the NLB
- F. Create an IAM security group for the instances to allow access on TCP port 443 from the IAM PrivateLink endpoint
- G. Use IAM PrivateLink interface endpoints in the 1,500 subsidiary IAM accounts to connect to the data processing application.
- H. Create an IAM security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range
- I. Associate the security group with EC2 instances.

Answer: D

NEW QUESTION 44

- (Exam Topic 1)

A Security Engineer is setting up an IAM CloudTrail trail for all regions in an IAM account. For added security, the logs are stored using server-side encryption with IAM KMS-managed keys (SSE-KMS) and have log integrity validation enabled.

While testing the solution, the Security Engineer discovers that the digest files are readable, but the log files are not. What is the MOST likely cause?

- A. The log files fail integrity validation and automatically are marked as unavailable.
- B. The KMS key policy does not grant the Security Engineer's IAM user or role permissions to decrypt with it.
- C. The bucket is set up to use server-side encryption with Amazon S3-managed keys (SSE-S3) as the default and does not allow SSE-KMS-encrypted files.

D. An IAM policy applicable to the Security Engineer's IAM user or role denies access to the "CloudTrail/" prefix in the Amazon S3 bucket

Answer: B

Explanation:

Enabling server-side encryption encrypts the log files but not the digest files with SSE-KMS. Digest files are encrypted with Amazon S3-managed encryption keys (SSE-S3). <https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-IAM-kms.htm>

NEW QUESTION 46

- (Exam Topic 1)

A Security Engineer has launched multiple Amazon EC2 instances from a private AMI using an IAM CloudFormation template. The Engineer notices instances terminating right after they are launched.

What could be causing these terminations?

- A. The IAM user launching those instances is missing ec2:Runinstances permission.
- B. The AMI used as encrypted and the IAM does not have the required IAM KMS permissions.
- C. The instance profile used with the EC2 instances is unable to query instance metadata.
- D. IAM currently does not have sufficient capacity in the Region.

Answer: B

Explanation:

<https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/troubleshooting-launch.html>

NEW QUESTION 51

- (Exam Topic 1)

A company uses SAML federation with IAM Identity and Access Management (IAM) to provide internal users with SSO for their IAM accounts. The company's identity provider certificate was rotated as part of its normal lifecycle. Shortly after, users started receiving the following error when attempting to log in:

"Error: Response Signature Invalid (Service: IAMSecurityTokenService; Status Code: 400; Error Code: InvalidIdentityToken)"

A security engineer needs to address the immediate issue and ensure that it will not occur again. Which combination of steps should the security engineer take to accomplish this? (Select TWO.)

- A. Download a new copy of the SAML metadata file from the identity provider Create a new IAM identity provider entit
- B. Upload the new metadata file to the new IAM identity provider entity.
- C. During the next certificate rotation period and before the current certificate expires, add a new certificate as the secondary to the identity provide
- D. Generate a new metadata file and upload it to the IAM identity provider entit
- E. Perform automated or manual rotation of the certificate when required.
- F. Download a new copy of the SAML metadata file from the identity provider Upload the new metadata to the IAM identity provider entity configured for the SAML integration in question.
- G. During the next certificate rotation period and before the current certificate expires, add a new certificateas the secondary to the identity provide
- H. Generate a new copy of the metadata file and create a new IAM identity provider entit
- I. Upload the metadata file to the new IAM identity provider entit
- J. Perform automated or manual rotation of the certificate when required.
- K. Download a new copy of the SAML metadata file from the identity provider Create a new IAM identity provider entit
- L. Upload the new metadata file to the new IAM identity provider entit
- M. Update the identity provider configurations to pass a new IAM identity provider entity name in the SAML assertion.

Answer: AD

NEW QUESTION 54

- (Exam Topic 1)

A Security Engineer has discovered that, although encryption was enabled on the Amazon S3 bucket example bucket, anyone who has access to the bucket has the ability to retrieve the files. The Engineer wants to limit access to each IAM user can access an assigned folder only.

What should the Security Engineer do to achieve this?

- A. Use envelope encryption with the IAM-managed CMK IAM/s3.
- B. Create a customer-managed CMK with a key policy granting "kms:Decrypt" based on the "\${IAM:username}" variable.
- C. Create a customer-managed CMK for each use
- D. Add each user as a key user in their corresponding key policy.
- E. Change the applicable IAM policy to grant S3 access to "Resource": "arn:IAM:s3:::examplebucket/\${IAM:username}/*"

Answer: B

Explanation:

Reference: <https://IAM.amazon.com/premiumsupport/knowledge-center/iam-s3-user-specific-folder/>

NEW QUESTION 55

- (Exam Topic 1)

A Security Engineer is troubleshooting a connectivity issue between a web server that is writing log files to the logging server in another VPC. The Engineer has confirmed that a peering relationship exists between the two VPCs. VPC flow logs show that requests sent from the web server are accepted by the toggging server but the web server never receives a reply

Which of the following actions could fix this issue1?

- A. Add an inbound rule to the security group associated with the logging server that allows requests from the web server
- B. Add an outbound rule to the security group associated with the web server that allows requests to the logging server.
- C. Add a route to the route table associated with the subnet that hosts the logging server that targets the peering connection
- D. Add a route to the route table associated with the subnet that hosts the web server that targets the peering connection

Answer: C

NEW QUESTION 58

- (Exam Topic 1)

A security engineer has been tasked with implementing a solution that allows the company's development team to have interactive command line access to Amazon EC2 Linux instances using the IAM Management Console.

Which steps should the security engineer take to satisfy this requirement while maintaining least privilege?

- A. Enable IAM Systems Manager in the IAM Management Console and configure for access to EC2 instances using the default AmazonEC2RoleforSSM role
- B. Install the Systems Manager Agent on all EC2 Linux instances that need interactive access
- C. Configure IAM user policies to allow development team access to the Systems Manager Session Manager and attach to the team's IAM users.
- D. Enable console SSH access in the EC2 console
- E. Configure IAM user policies to allow development team access to the IAM Systems Manager Session Manager and attach to the development team's IAM users.
- F. Enable IAM Systems Manager in the IAM Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM role
- G. Install the Systems Manager Agent on all EC2 Linux instances that need interactive access
- H. Configure a security group that allows SSH port 22 from all published IP addresses
- I. Configure IAM user policies to allow development team access to the IAM Systems Manager Session Manager and attach to the team's IAM users.
- J. Enable IAM Systems Manager in the IAM Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM role. Install the Systems Manager Agent on all EC2 Linux instances that need interactive access
- K. Configure IAM policies to allow development team access to the EC2 console and attach to the team's IAM users.

Answer: A

NEW QUESTION 59

- (Exam Topic 1)

A company's web application is hosted on Amazon EC2 instances running behind an Application Load Balancer (ALB) in an Auto Scaling group. An IAM WAF web ACL is associated with the ALB. IAM CloudTrail is enabled, and stores logs in Amazon S3 and Amazon CloudWatch Logs.

The operations team has observed some EC2 instances reboot at random. After rebooting, all access logs on the instances have been deleted. During an investigation, the operations team found that each reboot happened just after a PHP error occurred on the new-user-creation.php file. The operations team needs to view log information to determine if the company is being attacked.

Which set of actions will identify the suspect attacker's IP address for future occurrences?

- A. Configure VPC Flow Logs on the subnet where the ALB is located, and stream the data to CloudWatch. Search for the new-user-creation.php occurrences in CloudWatch.
- B. Configure the CloudWatch agent on the ALB. Configure the agent to send application logs to CloudWatch. Update the instance role to allow CloudWatch Logs access.
- C. Export the logs to CloudWatch. Search for the new-user-creation.php occurrences in CloudWatch.
- D. Configure the ALB to export access logs to an Amazon Elasticsearch Service cluster, and use the service to search for the new-user-creation.php occurrences.
- E. Configure the web ACL to send logs to Amazon Kinesis Data Firehose, which delivers the logs to an S3 bucket. Use Amazon Athena to query the logs and find the new-user-creation.php occurrences.

Answer: D

Explanation:

You send logs from your web ACL to an Amazon Kinesis Data Firehose with a configured storage destination. After you enable logging, IAM WAF delivers logs to your storage destination through the HTTPS endpoint of Kinesis Data Firehose. <https://docs.IAM.amazon.com/waf/latest/developerguide/logging.html>

NEW QUESTION 64

- (Exam Topic 1)

A company's data lake uses Amazon S3 and Amazon Athena. The company's security engineer has been asked to design an encryption solution that meets the company's data protection requirements. The encryption solution must work with Amazon S3 and keys managed by the company. The encryption solution must be protected in a hardware security module that is validated to Federal Information Processing Standards (FIPS) 140-2 Level 3.

Which solution meets these requirements?

- A. Use client-side encryption with an IAM KMS customer-managed key implemented with the IAM Encryption SDK
- B. Use IAM CloudHSM to store the keys and perform cryptographic operations. Save the encrypted text in Amazon S3
- C. Use an IAM KMS customer-managed key that is backed by a custom key store using IAM CloudHSM
- D. Use an IAM KMS customer-managed key with the bring your own key (BYOK) feature to import a key stored in IAM CloudHSM

Answer: B

NEW QUESTION 65

- (Exam Topic 1)

A company wants to encrypt data locally while meeting regulatory requirements related to key exhaustion. The encryption key can be no more than 10 days old or encrypt more than 2¹⁶ objects. Any encryption key must be generated on a FIPS-validated hardware security module (HSM). The company is cost-conscious, as plans to upload an average of 100 objects to Amazon S3 each second for sustained operations across 5 data producers.

Which approach MOST efficiently meets the company's needs?

- A. Use the IAM Encryption SDK and set the maximum age to 10 days and the minimum number of messages encrypted to 2¹⁶. Use IAM Key Management Service (IAM KMS) to generate the master key and data key. Use data key caching with the Encryption SDK during the encryption process.
- B. Use IAM Key Management Service (IAM KMS) to generate an IAM managed CMK
- C. Then use Amazon S3 client-side encryption configured to automatically rotate with every object
- D. Use IAM CloudHSM to generate the master key and data key
- E. Then use Boto 3 and Python to locally encrypt data before uploading the object. Rotate the data key every 10 days or after 2¹⁶ objects have been uploaded to Amazon S3
- F. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) and set the master key to automatically rotate.

Answer: A

NEW QUESTION 68

- (Exam Topic 1)

A Developer signed in to a new account within an IAM Organizations organizations unit (OU) containing multiple accounts. Access to the Amazon S3 service is restricted with the following SCP:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

How can the Security Engineer provide the Developer with Amazon S3 access without affecting other accounts?

- A. Move the SCP to the root OU of Organizations to remove the restriction to access Amazon S3.
- B. Add an IAM policy for the Developer, which grants S3 access.
- C. Create a new OU without applying the SCP restricting S3 access.
- D. Move the Developer account to this new OU.
- E. Add an allow list for the Developer account for the S3 service.

Answer: C

NEW QUESTION 72

- (Exam Topic 1)

A company hosts its public website on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an EC2 Auto Scaling group across multiple Availability Zones. The website is under a DDoS attack by a specific IoT device brand that is visible in the user agent. A security engineer needs to mitigate the attack without impacting the availability of the public website.

What should the security engineer do to accomplish this?

- A. Configure a web ACL rule for IAM WAF to block requests with a string match condition for the user agent of the IoT device.
- B. Associate the web ACL with the ALB.
- C. Configure an Amazon CloudFront distribution to use the ALB as an origin.
- D. Configure a web ACL rule for IAM WAF to block requests with a string match condition for the user agent of the IoT device.
- E. Associate the web ACL with the ALB. Change the public DNS entry of the website to point to the CloudFront distribution.
- F. Configure an Amazon CloudFront distribution to use a new ALB as an origin.
- G. Configure a web ACL rule for IAM WAF to block requests with a string match condition for the user agent of the IoT device.
- H. Change the ALB security group to allow access from CloudFront IP address ranges only. Change the public DNS entry of the website to point to the CloudFront distribution.
- I. Activate IAM Shield Advanced to enable DDoS protection.
- J. Apply an IAM WAF ACL to the ALB.
- K. Configure a listener rule on the ALB to block IoT devices based on the user agent.

Answer: D

NEW QUESTION 73

- (Exam Topic 1)

A Solutions Architect is designing a web application that uses Amazon CloudFront, an Elastic Load Balancing Application Load Balancer, and an Auto Scaling group of Amazon EC2 instances. The load balancer and EC2 instances are in the US West (Oregon) region. It has been decided that encryption in transit is necessary by using a customer-branded domain name from the client to CloudFront and from CloudFront to the load balancer.

Assuming that IAM Certificate Manager is used, how many certificates will need to be generated?

- A. One in the US West (Oregon) region and one in the US East (Virginia) region.
- B. Two in the US West (Oregon) region and none in the US East (Virginia) region.
- C. One in the US West (Oregon) region and none in the US East (Virginia) region.
- D. Two in the US East (Virginia) region and none in the US West (Oregon) region.

Answer: A

Explanation:

Why? If you want to require HTTPS between viewers and CloudFront, you must change the IAM Region to US East (N. Virginia) in the IAM Certificate Manager console before you request or import a certificate. If you want to require HTTPS between CloudFront and your origin, and you're using an ELB load balancer as your origin, you can request or import a certificate in any Region.

<https://docs.IAM.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html>

NEW QUESTION 75

- (Exam Topic 1)

A company is operating an open-source software platform that is internet facing. The legacy software platform no longer receives security updates. The software platform operates using Amazon Route 53 weighted load balancing to send traffic to two Amazon EC2 instances that connect to an Amazon RDS cluster. A recent report suggests this software platform is vulnerable to SQL injection attacks, with samples of attacks provided. The company's security engineer must secure this system against SQL injection attacks within 24 hours. The security engineer's solution involves the least amount of effort and maintain normal operations during implementation.

What should the security engineer do to meet these requirements?

- A. Create an Application Load Balancer with the existing EC2 instances as a target group. Create an IAM WAF web ACL containing rules that protect the application from this attack.

- B. then apply it to the ALB Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to the ALB Update security groups on the EC2 instances to prevent direct access from the internet
- C. Create an Amazon CloudFront distribution specifying one EC2 instance as an origin Create an IAM WAF web ACL containing rules that protect the application from this attack, then apply it to the distribution Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to CloudFront
- D. Obtain the latest source code for the platform and make the necessary updates Test the updated code to ensure that the vulnerability has been mitigated, then deploy the patched version of the platform to the EC2 instances
- E. Update the security group that is attached to the EC2 instances, removing access from the internet to the TCP port used by the SQL database Create an IAM WAF web ACL containing rules that protect the application from this attack, then apply it to the EC2 instances Test to ensure the vulnerability has been mitigated
- F. then restore the security group to the original setting

Answer: A

NEW QUESTION 77

- (Exam Topic 1)

An IAM account administrator created an IAM group and applied the following managed policy to require that each individual user authenticate using multi-factor authentication:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    },
    {
      "Sid": "BlockAnyAccessUnlessSignedInWithMFA",
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "BoolIfExists": {
          "aws:MultiFactorAuthPresent": false
        }
      }
    }
  ]
}
```

After implementing the policy, the administrator receives reports that users are unable to perform Amazon EC2 commands using the IAM CLI. What should the administrator do to resolve this problem while still enforcing multi-factor authentication?

- A. Change the value of IAM MultiFactorAuthPresent to true.
- B. Instruct users to run the IAM sts get-session-token CLI command and pass the multi-factor authentication `--serial-number` and `--token-code` parameter
- C. Use these resulting values to make API/CLI calls
- D. Implement federated API/CLI access using SAML 2.0, then configure the identity provider to enforce multi-factor authentication.
- E. Create a role and enforce multi-factor authentication in the role trust policy Instruct users to run the sts assume-role CLI command and pass `--serial-number` and `--token-code` parameters Store the resulting values in environment variable
- F. Add sts:AssumeRole to NotAction in the policy.

Answer: B

NEW QUESTION 81

- (Exam Topic 1)

A company plans to use custom AMIs to launch Amazon EC2 instances across multiple IAM accounts in a single Region to perform security monitoring and analytics tasks. The EC2 instances are launched in EC2 Auto Scaling groups. To increase the security of the solution, a Security Engineer will manage the lifecycle of the custom AMIs in a centralized account and will encrypt them with a centrally managed IAM KMS CMK. The Security Engineer configured the KMS key policy to allow cross-account access. However, the EC2 instances are still not being properly launched by the EC2 Auto Scaling groups.

Which combination of configuration steps should the Security Engineer take to ensure the EC2 Auto Scaling groups have been granted the proper permissions to execute tasks?

- A. Create a customer-managed CMK in the centralized account
- B. Allow other applicable accounts to use that key for cryptographic operations by applying proper cross-account permissions in the key policy
- C. Create an IAM role in all applicable accounts and configure its access policy to allow the use of the centrally managed CMK for cryptographic operation
- D. Configure EC2 Auto Scaling groups within each applicable account to use the created IAM role to launch EC2 instances.
- E. Create a customer-managed CMK in the centralized account
- F. Allow other applicable accounts to use that key for cryptographic operations by applying proper cross-account permissions in the key policy
- G. Create an IAM role in all applicable accounts and configure its access policy with permissions to create grants for the centrally managed CMK
- H. Use this IAM role to create a grant for the centrally managed CMK with permissions to perform cryptographic operations and with the EC2 Auto Scaling service-linked role defined as the grantee principal.
- I. Create a customer-managed CMK or an IAM managed CMK in the centralized account
- J. Allow other applicable accounts to use that key for cryptographic operations by applying proper cross-account permissions in the key policy
- K. Use the CMK administrator to create a CMK grant that includes permissions to perform cryptographic operations that define EC2 Auto Scaling service-linked roles from all other accounts as the grantee principal.
- L. Create a customer-managed CMK or an IAM managed CMK in the centralized account
- M. Allow other applicable accounts to use that key for cryptographic operations by applying proper cross-account permissions in the key policy
- N. Modify the access policy for the EC2 Auto Scaling roles to perform cryptographic operations against the centrally managed CMK.

Answer: B

NEW QUESTION 86

- (Exam Topic 1)

A financial institution has the following security requirements:

- > Cloud-based users must be contained in a separate authentication domain.
- > Cloud-based users cannot access on-premises systems.

As part of standing up a cloud environment, the financial institution is creating a number of Amazon managed databases and Amazon EC2 instances. An Active Directory service exists on-premises that has all the administrator accounts, and these must be able to access the databases and instances.

How would the organization manage its resources in the MOST secure manner? (Choose two.)

- A. Configure an IAM Managed Microsoft AD to manage the cloud resources.
- B. Configure an additional on-premises Active Directory service to manage the cloud resources.
- C. Establish a one-way trust relationship from the existing Active Directory to the new Active Directory service.
- D. Establish a one-way trust relationship from the new Active Directory to the existing Active Directory service.
- E. Establish a two-way trust between the new and existing Active Directory services.

Answer: AD

Explanation:

Deploy a new forest/domain on IAM with one-way trust. If you are planning on leveraging credentials from an on-premises AD on IAM member servers, you must establish at least a one-way trust to the Active Directory running on IAM. In this model, the IAM domain becomes the resource domain where computer objects are located and on-premises domain becomes the account domain. Ref: <https://d1.IAMstatic.com/whitepapers/adds-on-IAM.pdf>
https://docs.IAM.amazon.com/directoryservice/latest/admin-guide/directory_microsoft_ad.html

NEW QUESTION 90

- (Exam Topic 2)

Your IT Security department has mandated that all data on EBS volumes created for underlying EC2 Instances need to be encrypted. Which of the following can help achieve this?

Please select:

- A. IAM KMS API
- B. IAM Certificate Manager
- C. API Gateway with STS
- D. IAM Access Key

Answer: A

Explanation:

The IAM Documentation mentions the following on IAM KMS

IAM Key Management Service (IAM KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. IAM KMS is integrated with other IAM services including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Redshift Amazon Elastic Transcoder, Amazon WorkMail, Amazon Relational Database Service (Amazon RDS), and others to make it simple to encrypt your data with encryption keys that you manage

Option B is incorrect - The IAM Certificate manager can be used to generate SSL certificates that can be used to encrypt traffic transit, but not at rest

Option C is incorrect is again used for issuing tokens when using API gateway for traffic in transit. Option D is used for secure access to EC2 Instances

For more information on IAM KMS, please visit the following URL: <https://docs.IAM.amazon.com/kms/latest/developerguide/overview.html> The correct answer is: IAM KMS API

Submit your Feedback/Queries to our Experts

NEW QUESTION 92

- (Exam Topic 2)

The Security Engineer created a new IAM Key Management Service (IAM KMS) key with the following key policy:

```
{
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
  "Action": "kms:*";
  "Resource": "*"
}
```

What are the effects of the key policy? (Choose two.)

- A. The policy allows access for the IAM account 111122223333 to manage key access through IAM policies.
- B. The policy allows all IAM users in account 111122223333 to have full access to the KMS key.
- C. The policy allows the root user in account 111122223333 to have full access to the KMS key.
- D. The policy allows the KMS service-linked role in account 111122223333 to have full access to the KMS key.
- E. The policy allows all IAM roles in account 111122223333 to have full access to the KMS key.

Answer: AC

Explanation:

Giving the IAM account full access to the CMK does this; it enables you to use IAM policies to give IAM users and roles in the account access to the CMK. It does not by itself give any IAM users or roles access to the CMK, but it enables you to use IAM policies to do so.

<https://docs.IAM.amazon.com/kms/latest/developerguide/key-policies.html#key-policy-default-allow-root-enabl>

NEW QUESTION 97

- (Exam Topic 2)

A company plans to migrate a sensitive dataset to Amazon S3. A Security Engineer must ensure that the data is encrypted at rest. The encryption solution must enable the company to generate its own keys without needing to manage key storage or the encryption process.

What should the Security Engineer use to accomplish this?

- A. Server-side encryption with Amazon S3-managed keys (SSE-S3)
- B. Server-side encryption with IAM KMS-managed keys (SSE-KMS)

- C. Server-side encryption with customer-provided keys (SSE-C)
- D. Client-side encryption with an IAM KMS-managed CMK

Answer: B

Explanation:

Reference <https://IAM.amazon.com/s3/faqs/>

NEW QUESTION 99

- (Exam Topic 2)

You want to get a list of vulnerabilities for an EC2 Instance as per the guidelines set by the Center of Internet Security. How can you go about doing this? Please select:

- A. Enable IAM Guard Duty for the Instance
- B. Use IAM Trusted Advisor
- C. Use IAM inspector
- D. Use IAM Macie

Answer: C

Explanation:

The IAM Inspector service can inspect EC2 Instances based on specific Rules. One of the rules packages is based on the guidelines set by the Center of Internet Security

Center for Internet security (CIS) Benchmarks

The CIS Security Benchmarks program provides well-defined, un-biased and consensus-based industry best practices to help organizations assess and improve their security. Amazon Web Services is a CIS Security Benchmarks Member company and the list of Amazon Inspector certifications can be viewed here.

Option A is invalid because this can be used to protect an instance but not give the list of vulnerabilities Options B and D are invalid because these services cannot give a list of vulnerabilities For more information

on the guidelines, please visit the below URL:

* https://docs.IAM.amazon.com/inspector/latest/userguide/inspector_cis.html The correct answer is: Use IAM Inspector

Submit your Feedback/Queries to our Experts

NEW QUESTION 102

- (Exam Topic 2)

Example.com hosts its internal document repository on Amazon EC2 instances. The application runs on EC2 instances and previously stored the documents on encrypted Amazon EBS volumes. To optimize the application for scale, example.com has moved the files to Amazon S3. The security team has mandated that all the files are securely deleted from the EBS volume, and it must certify that the data is unreadable before releasing the underlying disks.

Which of the following methods will ensure that the data is unreadable by anyone else?

- A. Change the volume encryption on the EBS volume to use a different encryption mechanism
- B. Then, release the EBS volumes back to IAM.
- C. Release the volumes back to IA
- D. IAM immediately wipes the disk after it is deprovisioned.
- E. Delete the encryption key used to encrypt the EBS volume
- F. Then, release the EBS volumes back to IAM.
- G. Delete the data by using the operating system delete command
- H. Run Quick Format on the drive and then release the EBS volumes back to IAM.

Answer: D

Explanation:

Amazon EBS volumes are presented to you as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs immediately before reuse so that you can be assured that the wipe process completed. If you have procedures requiring that all data be wiped via a specific method, such as those detailed in NIST 800-88 ("Guidelines for Media Sanitization"), you have the ability to do so on Amazon EBS. You should conduct a specialized wipe procedure prior to deleting the volume for compliance with your established requirements.

<https://d0.IAMstatic.com/whitepapers/IAM-security-whitepaper.pdf>

NEW QUESTION 104

- (Exam Topic 2)

The Security Engineer has discovered that a new application that deals with highly sensitive data is storing Amazon S3 objects with the following key pattern, which itself contains highly sensitive data.

Pattern: "randomID_datestamp_PII.csv" Example:

"1234567_12302017_000-00-0000 csv"

The bucket where these objects are being stored is using server-side encryption (SSE). Which solution is the most secure and cost-effective option to protect the sensitive data?

- A. Remove the sensitive data from the object name, and store the sensitive data using S3 user-defined metadata.
- B. Add an S3 bucket policy that denies the action s3:GetObject
- C. Use a random and unique S3 object key, and create an S3 metadata index in Amazon DynamoDB using client-side encrypted attributes.
- D. Store all sensitive objects in Binary Large Objects (BLOBS) in an encrypted Amazon RDS instance.

Answer: C

Explanation:

<https://docs.IAM.amazon.com/AmazonS3/latest/dev/UsingMetadata.html> <https://IAM.amazon.com/blogs/database/best-practices-for-securing-sensitive-data-in-IAM-data-stores/>

NEW QUESTION 106

- (Exam Topic 2)

The Security Engineer for a mobile game has to implement a method to authenticate users so that they can save their progress. Because most of the users are part of the same OpenID-Connect compatible social media website, the Security Engineer would like to use that as the identity provider. Which solution is the SIMPLEST way to allow the authentication of users using their social media identities?

- A. Amazon Cognito
- B. AssumeRoleWithWebIdentity API
- C. Amazon Cloud Directory
- D. Active Directory (AD) Connector

Answer: A

NEW QUESTION 110

- (Exam Topic 2)

Which of the following is the most efficient way to automate the encryption of IAM CloudTrail logs using a Customer Master Key (CMK) in IAM KMS?

- A. Use the KMS direct encrypt function on the log data every time a CloudTrail log is generated.
- B. Use the default Amazon S3 server-side encryption with S3-managed keys to encrypt and decrypt the CloudTrail logs.
- C. Configure CloudTrail to use server-side encryption using KMS-managed keys to encrypt and decrypt CloudTrail logs.
- D. Use encrypted API endpoints so that all IAM API calls generate encrypted CloudTrail log entries using the TLS certificate from the encrypted API call.

Answer: C

Explanation:

<https://docs.IAM.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html>

NEW QUESTION 113

- (Exam Topic 2)

A Security Engineer is working with a Product team building a web application on IAM. The application uses Amazon S3 to host the static content, Amazon API Gateway to provide RESTful services; and Amazon DynamoDB as the backend data store. The users already exist in a directory that is exposed through a SAML identity provider.

Which combination of the following actions should the Engineer take to enable users to be authenticated into the web application and call APIs? (Choose three.)

- A. Create a custom authorization service using IAM Lambda.
- B. Configure a SAML identity provider in Amazon Cognito to map attributes to the Amazon Cognito user pool attributes.
- C. Configure the SAML identity provider to add the Amazon Cognito user pool as a relying party.
- D. Configure an Amazon Cognito identity pool to integrate with social login providers.
- E. Update DynamoDB to store the user email addresses and passwords.
- F. Update API Gateway to use a COGNITO_USER_POOLS authorizer.

Answer: BDE

NEW QUESTION 118

- (Exam Topic 2)

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack? Please select:

- A. Change the Inbound Security Groups to deny access from the suspecting IP
- B. Change the Outbound Security Groups to deny access from the suspecting IP
- C. Change the Inbound NACL to deny access from the suspecting IP
- D. Change the Outbound NACL to deny access from the suspecting IP

Answer: C

Explanation:

Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL's as an additional security layer for the subnet to deny traffic.

Option D is invalid since just changing the Inbound Rules is sufficient The IAM Documentation mentions the following

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for

controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

The correct answer is: Change the Inbound NACL to deny access from the suspecting IP

NEW QUESTION 120

- (Exam Topic 2)

A Software Engineer is trying to figure out why network connectivity to an Amazon EC2 instance does not appear to be working correctly. Its security group allows inbound HTTP traffic from 0.0.0.0/0, and the outbound rules have not been modified from the default. A custom network ACL associated with its subnet allows inbound HTTP traffic from 0.0.0.0/0 and has no outbound rules.

What would resolve the connectivity issue?

- A. The outbound rules on the security group do not allow the response to be sent to the client on the ephemeral port range.
- B. The outbound rules on the security group do not allow the response to be sent to the client on the HTTP port.
- C. An outbound rule must be added to the network ACL to allow the response to be sent to the client on the ephemeral port range.
- D. An outbound rule must be added to the network ACL to allow the response to be sent to the client on the HTTP port.

Answer: C

Explanation:

<https://docs.IAM.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

NEW QUESTION 121

- (Exam Topic 2)

A company plans to move most of its IT infrastructure to IAM. They want to leverage their existing on-premises Active Directory as an identity provider for IAM. Which combination of steps should a Security Engineer take to federate the company's on-premises Active Directory with IAM? (Choose two.)

- A. Create IAM roles with permissions corresponding to each Active Directory group.
- B. Create IAM groups with permissions corresponding to each Active Directory group.
- C. Configure Amazon Cloud Directory to support a SAML provider.
- D. Configure Active Directory to add relying party trust between Active Directory and IAM.
- E. Configure Amazon Cognito to add relying party trust between Active Directory and IAM.

Answer: AD

Explanation:

<https://IAM.amazon.com/blogs/security/how-to-establish-federated-access-to-your-IAM-resources-by-using-acti>

NEW QUESTION 123

- (Exam Topic 2)

A company is using CloudTrail to log all IAM API activity for all regions in all of its accounts. The CISO has asked that additional steps be taken to protect the integrity of the log files.

What combination of steps will protect the log files from intentional or unintentional alteration? Choose 2 answers from the options given below Please select:

- A. Create an S3 bucket in a dedicated log account and grant the other accounts write only access
- B. Deliver all log files from every account to this S3 bucket.
- C. Write a Lambda function that queries the Trusted Advisor Cloud Trail check
- D. Run the function every 10 minutes.
- E. Enable CloudTrail log file integrity validation
- F. Use Systems Manager Configuration Compliance to continually monitor the access policies of S3 buckets containing Cloud Trail logs.
- G. Create a Security Group that blocks all traffic except calls from the CloudTrail service
- H. Associate the security group with) all the Cloud Trail destination S3 buckets.

Answer: AC

Explanation:

The IAM Documentation mentions the following

To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log file integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.

Option B is invalid because there is no such thing as Trusted Advisor Cloud Trail checks Option D is invalid because Systems Manager cannot be used for this purpose.

Option E is invalid because Security Groups cannot be used to block calls from other services For more information on Cloudtrail log file validation, please visit the below URL:

<https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-loc-file-validation-intro.html> For more information on delivering Cloudtrail logs from multiple accounts, please visit the below URL:

<https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-receive-logs-from-multiple-accounts.ht>

The correct answers are: Create an S3 bucket in a dedicated log account and grant the other accounts write only access. Deliver all log files from every account to this S3 bucket, Enable Cloud Trail log file integrity validation

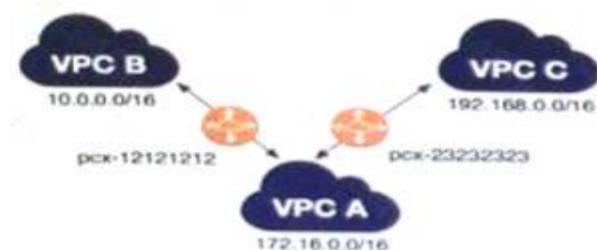
Submit your Feedback/Queries to our Experts

NEW QUESTION 124

- (Exam Topic 2)

A company has multiple VPCs in their account that are peered, as shown in the diagram. A Security Engineer wants to perform penetration tests of the Amazon EC2 instances in all three VPCs.

How can this be accomplished? (Choose two.)



- A. Deploy a pre-authorized scanning engine from the IAM Marketplace into VPC B, and use it to scan instances in all three VPC
- B. Do not complete the penetration test request form.
- C. Deploy a pre-authorized scanning engine from the Marketplace into each VPC, and scan instances in each VPC from the scanning engine in that VP
- D. Do not complete the penetration test request form.
- E. Create a VPN connection from the data center to VPC
- F. Use an on-premises scanning engine to scan the instances in all three VPC
- G. Complete the penetration test request form for all three VPCs.
- H. Create a VPN connection from the data center to each of the three VPC
- I. Use an on-premises scanning engine to scan the instances in each VP
- J. Do not complete the penetration test request form.
- K. Create a VPN connection from the data center to each of the three VPC
- L. Use an on-premises scanning engine to scan the instances in each VP
- M. Complete the penetration test request form for all three VPCs.

Answer: BD

Explanation:

<https://IAM.amazon.com/security/penetration-testing/>

NEW QUESTION 126

- (Exam Topic 2)

A company's security policy requires that VPC Flow Logs are enabled on all VPCs. A Security Engineer is looking to automate the process of auditing the VPC resources for compliance.

What combination of actions should the Engineer take? (Choose two.)

- A. Create an IAM Lambda function that determines whether Flow Logs are enabled for a given VPC.
- B. Create an IAM Config configuration item for each VPC in the company IAM account.
- C. Create an IAM Config managed rule with a resource type of IAM:: Lambda:: Function.
- D. Create an Amazon CloudWatch Event rule that triggers on events emitted by IAM Config.
- E. Create an IAM Config custom rule, and associate it with an IAM Lambda function that contains the evaluating logic.

Answer: AE

Explanation:

<https://medium.com/mudita-misra/how-to-audit-your-aws-resources-for-security-compliance-by-using-custom-l>

NEW QUESTION 129

- (Exam Topic 2)

An IAM user with full EC2 permissions could not start an Amazon EC2 instance after it was stopped for a maintenance task. Upon starting the instance, the instance state would change to "Pending", but after a few seconds, it would switch back to "Stopped".

An inspection revealed that the instance has attached Amazon EBS volumes that were encrypted by using a Customer Master Key (CMK). When these encrypted volumes were detached, the IAM user was able to start the EC2 instances.

The IAM user policy is as follows:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        <Action>
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:012345678910:key/ebs-encryption-key"
      ]
    }
  ]
}
```

What additional items need to be added to the IAM user policy? (Choose two.)

- A. kms:GenerateDataKey
- B. kms:Decrypt
- C. kms:CreateGrant
- D. "Condition": {"Bool": {"kms:ViaService": "ec2.us-west-2.amazonaws.com"}}
- E. "Condition": {"Bool": {"kms:GrantsForIAMResource": true}}

Answer: CE

Explanation:

The EBS which is IAM resource service is encrypted with CMK and to allow EC2 to decrypt, the IAM user should create a grant (action) and a boolean condition for the IAM resource. This link explains how IAM keys work. <https://docs.IAM.amazon.com/kms/latest/developerguide/key-policies.html>

NEW QUESTION 134

- (Exam Topic 2)

Which of the following are valid event sources that are associated with web access control lists that trigger IAM WAF rules? (Choose two.)

- A. Amazon S3 static web hosting
- B. Amazon CloudFront distribution
- C. Application Load Balancer
- D. Amazon Route 53
- E. VPC Flow Logs

Answer: BC

Explanation:

A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon API Gateway API, Amazon CloudFront distribution or Application Load Balancer responds to.

NEW QUESTION 137

- (Exam Topic 2)

What is the function of the following IAM Key Management Service (KMS) key policy attached to a customer master key (CMK)?

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:GenerateDataKey*",
    "kms:CreateGrant",
    "kms:ListGrants"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": [
        "workmail.us-west-2.amazonaws.com",
        "ses.us-west-2.amazonaws.com"
      ]
    }
  }
}
```

- A. The Amazon WorkMail and Amazon SES services have delegated KMS encrypt and decrypt permissions to the ExampleUser principal in the 111122223333 account.
- B. The ExampleUser principal can transparently encrypt and decrypt email exchanges specifically between ExampleUser and IAM.
- C. The CMK is to be used for encrypting and decrypting only when the principal is ExampleUser and the request comes from WorkMail or SES in the specified region.
- D. The key policy allows WorkMail or SES to encrypt or decrypt on behalf of the user for any CMK in the account.

Answer: C

NEW QUESTION 140

- (Exam Topic 2)

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. Use IAM Config to detect whether an Internet Gateway is added and use an IAM Lambda function to provide auto-remediation.
- B. Within the Amazon VPC configuration, mark the VPC as private and disable Elastic IP addresses.
- C. Use IPv6 addressing exclusively on the EC2 hosts, as this prevents the hosts from being accessed from the internet.
- D. Move the workload to a Dedicated Host, as this provides additional network security controls and monitorin

Answer: A

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.

NEW QUESTION 145

- (Exam Topic 2)

The Security Engineer is given the following requirements for an application that is running on Amazon EC2 and managed by using IAM CloudFormation templates with EC2 Auto Scaling groups:

- Have the EC2 instances bootstrapped to connect to a backend database.
- Ensure that the database credentials are handled securely.
- Ensure that retrievals of database credentials are logged.

Which of the following is the MOST efficient way to meet these requirements?

- A. Pass databases credentials to EC2 by using CloudFormation stack parameters with the property set to tru
- B. Ensure that the instance is configured to log to Amazon CloudWatch Logs.
- C. Store database passwords in IAM Systems Manager Parameter Store by using SecureString parameters.Set the IAM role for the EC2 instance profile to allow access to the parameters.
- D. Create an IAM Lambda that ingests the database password and persists it to Amazon S3 with server-side encryptio
- E. Have the EC2 instances retrieve the S3 object on startup, and log all script invocations to syslog.
- F. Write a script that is passed in as UserData so that it is executed upon launch of the EC2 instance.Ensure that the instance is configured to log to Amazon CloudWatch Logs.

Answer: B

NEW QUESTION 149

- (Exam Topic 2)

A Software Engineer wrote a customized reporting service that will run on a fleet of Amazon EC2 instances. The company security policy states that application logs for the reporting service must be centrally collected.

What is the MOST efficient way to meet these requirements?

- A. Write an IAM Lambda function that logs into the EC2 instance to pull the application logs from the EC2 instance and persists them into an Amazon S3 bucket.
- B. Enable IAM CloudTrail logging for the IAM account, create a new Amazon S3 bucket, and then configure Amazon CloudWatch Logs to receive the application logs from CloudTrail.
- C. Create a simple cron job on the EC2 instances that synchronizes the application logs to an Amazon S3 bucket by using rsync.
- D. Install the Amazon CloudWatch Logs Agent on the EC2 instances, and configure it to send the application logs to CloudWatch Logs.

Answer: D

Explanation:

<https://IAM.amazon.com/blogs/IAM/cloudwatch-log-service/>

NEW QUESTION 150

- (Exam Topic 2)

The Information Technology department has stopped using Classic Load Balancers and switched to Application Load Balancers to save costs. After the switch, some users on older devices are no longer able to connect to the website.

What is causing this situation?

- A. Application Load Balancers do not support older web browsers.
- B. The Perfect Forward Secrecy settings are not configured correctly.
- C. The intermediate certificate is installed within the Application Load Balancer.
- D. The cipher suites on the Application Load Balancers are blocking connections.

Answer: D

Explanation:

<https://docs.IAM.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html>

NEW QUESTION 153

- (Exam Topic 2)

A Lambda function reads metadata from an S3 object and stores the metadata in a DynamoDB table. The function is triggered whenever an object is stored within the S3 bucket.

How should the Lambda function be given access to the DynamoDB table? Please select:

- A. Create a VPC endpoint for DynamoDB within a VP
- B. Configure the Lambda function to access resources in the VPC.
- C. Create a resource policy that grants the Lambda function permissions to write to the DynamoDB table. Attach the policy to the DynamoDB table.
- D. Create an IAM user with permissions to write to the DynamoDB table.
- E. Store an access key for that user in the Lambda environment variables.
- F. Create an IAM service role with permissions to write to the DynamoDB table.
- G. Associate that role with the Lambda function.

Answer: D

Explanation:

The ideal way is to create an IAM role which has the required permissions and then associate it with the Lambda function

The IAM Documentation additionally mentions the following

Each Lambda function has an IAM role (execution role) associated with it. You specify the IAM role when you create your Lambda function. Permissions you grant to this role determine what IAM Lambda can do when it assumes the role. There are two types of permissions that you grant to the IAM role:

If your Lambda function code accesses other IAM resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role.

If the event source is stream-based (Amazon Kinesis Data Streams and DynamoDB streams), IAM Lambda polls these streams on your behalf. IAM Lambda needs permissions to poll the stream and read new records on the stream so you need to grant the relevant permissions to this role.

Option A is invalid because the VPC endpoint allows access instances in a private subnet to access DynamoDB

Option B is invalid because resource policies are present for resources such as S3 and KMS, but not IAM Lambda

Option C is invalid because IAM Roles should be used and not IAM Users

For more information on the Lambda permission model, please visit the below URL: <https://docs.IAM.amazon.com/lambda/latest/dg/intro-permission-model.html>

The correct answer is: Create an IAM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.

Submit your Feedback/Queries to our Exp

NEW QUESTION 157

- (Exam Topic 2)

A company uses IAM Organization to manage 50 IAM accounts. The finance staff members log in as IAM IAM users in the FinanceDept IAM account. The staff members need to read the consolidated billing information in the MasterPayer IAM account. They should not be able to view any other resources in the MasterPayer IAM account. IAM access to billing has been enabled in the MasterPayer account.

Which of the following approaches grants the finance staff the permissions they require without granting any unnecessary permissions?

- A. Create an IAM group for the finance users in the FinanceDept account, then attach the IAM managed ReadOnlyAccess IAM policy to the group.
- B. Create an IAM group for the finance users in the MasterPayer account, then attach the IAM managed ReadOnlyAccess IAM policy to the group.
- C. Create an IAM IAM role in the FinanceDept account with the ViewBilling permission, then grant the finance users in the MasterPayer account the permission to assume that role.
- D. Create an IAM IAM role in the MasterPayer account with the ViewBilling permission, then grant the finance users in the FinanceDept account the permission to assume that role.

Answer: D

Explanation:

IAM Region that You Request a Certificate In (for IAM Certificate Manager) If you want to require HTTPS between viewers and CloudFront, you must change the IAM region to US East (N. Virginia) in the IAM Certificate Manager console before you request or import a certificate. If you want to require HTTPS between CloudFront and your origin, and you're using an ELB load balancer as your origin, you can request or import a certificate in any region.
<https://docs.IAM.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html>

NEW QUESTION 160

- (Exam Topic 2)

Which of the following minimizes the potential attack surface for applications?

- A. Use security groups to provide stateful firewalls for Amazon EC2 instances at the hypervisor level.
- B. Use network ACLs to provide stateful firewalls at the VPC level to prevent access to any specific IAM resource.
- C. Use IAM Direct Connect for secure trusted connections between EC2 instances within private subnets.
- D. Design network security in a single layer within the perimeter network (also known as DMZ, demilitarized zone, and screened subnet) to facilitate quicker responses to threats.

Answer: A

Explanation:

<https://IAM.amazon.com/answers/networking/vpc-security-capabilities/> Security Group is stateful and hypervisor level.

NEW QUESTION 164

- (Exam Topic 2)

You have enabled Cloudtrail logs for your company's IAM account. In addition, the IT Security department has mentioned that the logs need to be encrypted. How can this be achieved?

Please select:

- A. Enable SSL certificates for the Cloudtrail logs
- B. There is no need to do anything since the logs will already be encrypted
- C. Enable Server side encryption for the trail
- D. Enable Server side encryption for the destination S3 bucket

Answer: B

Explanation:

The IAM Documentation mentions the following.

By default CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encryption your log files with an IAM Key Management Service (IAM KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about lo file delivery and validation, you can set up Amazon SNS notifications.

Option A.C and D are not valid since logs will already be encrypted

For more information on how Cloudtrail works, please visit the following URL: <https://docs.IAM.amazon.com/IAMcloudtrail/latest/useruide/how-cloudtrail-works.html>

The correct answer is: There is no need to do anything since the logs will already be encrypted

Submit your Feedback/Queries to our Experts

NEW QUESTION 168

- (Exam Topic 2)

A company has a forensic logging use case whereby several hundred applications running on Docker on EC2 need to send logs to a central location. The Security Engineer must create a logging solution that is able to perform real-time analytics on the log files, grants the ability to replay events, and persists data.

Which IAM Services, together, can satisfy this use case? (Select two.)

- A. Amazon Elasticsearch
- B. Amazon Kinesis
- C. Amazon SQS
- D. Amazon CloudWatch
- E. Amazon Athena

Answer: AB

Explanation:

<https://docs.aws.amazon.com/whitepapers/latest/IAM-overview/analytics.html#amazon-athena>

NEW QUESTION 171

- (Exam Topic 2)

A company has deployed a custom DNS server in IAM. The Security Engineer wants to ensure that Amazon EC2 instances cannot use the Amazon-provided DNS.

How can the Security Engineer block access to the Amazon-provided DNS in the VPC?

- A. Deny access to the Amazon DNS IP within all security groups.
- B. Add a rule to all network access control lists that deny access to the Amazon DNS IP.
- C. Add a route to all route tables that black holes traffic to the Amazon DNS IP.
- D. Disable DNS resolution within the VPC configuration.

Answer: D

Explanation:

<https://docs.IAM.amazon.com/vpc/latest/userguide/vpc-dns.html>

NEW QUESTION 173

- (Exam Topic 2)

An organization wants to be alerted when an unauthorized Amazon EC2 instance in its VPC performs a network port scan against other instances in the VPC. When the Security team performs its own internal tests in a separate account by using pre-approved third-party scanners from the IAM Marketplace, the Security team also then receives multiple Amazon GuardDuty events from Amazon CloudWatch alerting on its test activities. How can the Security team suppress alerts about authorized security tests while still receiving alerts about the unauthorized activity?

- A. Use a filter in IAM CloudTrail to exclude the IP addresses of the Security team's EC2 instances.
- B. Add the Elastic IP addresses of the Security team's EC2 instances to a trusted IP list in Amazon GuardDuty.
- C. Install the Amazon Inspector agent on the EC2 instances that the Security team uses.
- D. Grant the Security team's EC2 instances a role with permissions to call Amazon GuardDuty API operations.

Answer: B

Explanation:

Trusted IP lists consist of IP addresses that you have whitelisted for secure communication with your IAM infrastructure and applications. GuardDuty does not generate findings for IP addresses on trusted IP lists. At any given time, you can have only one uploaded trusted IP list per IAM account per region. Threat lists consist of known malicious IP addresses. GuardDuty generates findings based on threat lists. At any given time, you can have up to six uploaded threat lists per IAM account per region. https://docs.IAM.amazon.com/guardduty/latest/ug/guardduty_upload_lists.html

NEW QUESTION 174

- (Exam Topic 2)

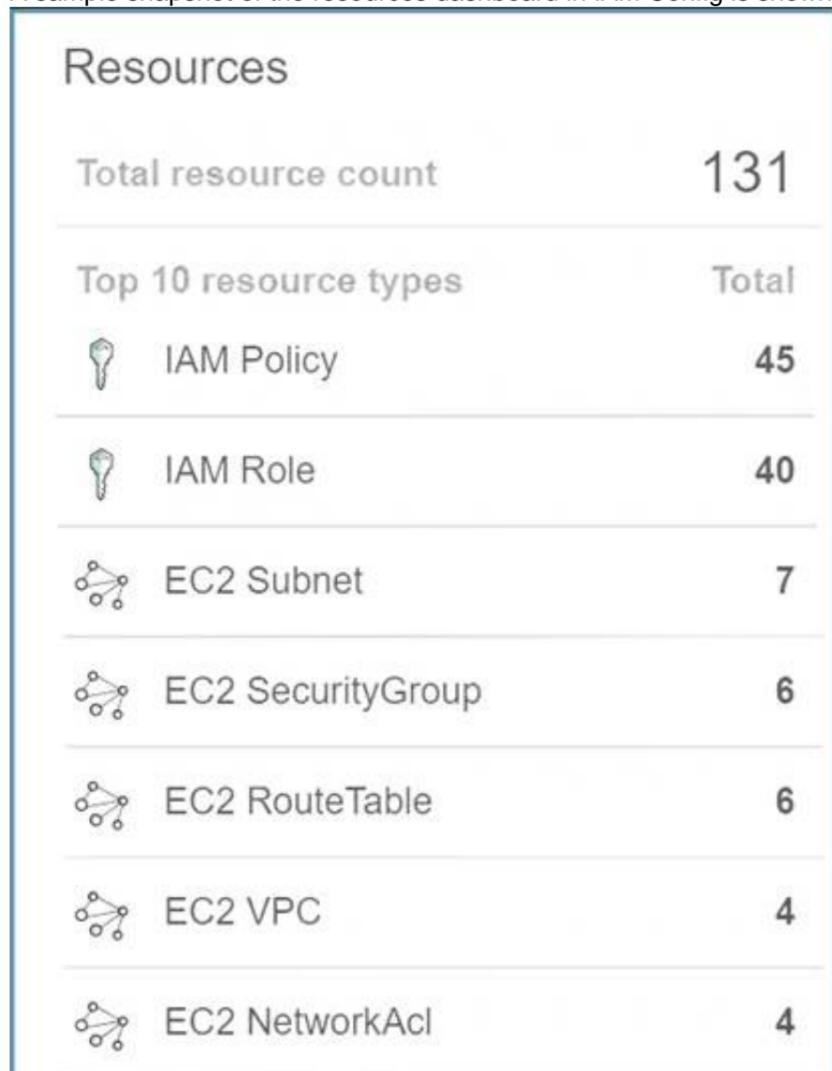
Your company has a set of resources defined in the IAM Cloud. Their IT audit department has requested to get a list of resources that have been defined across the account. How can this be achieved in the easiest manner? Please select:

- A. Create a powershell script using the IAM CL
- B. Query for all resources with the tag of production.
- C. Create a bash shell script with the IAM CL
- D. Query for all resources in all region
- E. Store the results in an S3 bucket.
- F. Use Cloud Trail to get the list of all resources
- G. Use IAM Config to get the list of all resources

Answer: D

Explanation:

The most feasible option is to use IAM Config. When you turn on IAM Config, you will get a list of resources defined in your IAM Account. A sample snapshot of the resources dashboard in IAM Config is shown below <C:\Users\wk\Desktop\mudassar\Untitled.jpg>



Resources	
Total resource count	131
Top 10 resource types	Total
 IAM Policy	45
 IAM Role	40
 EC2 Subnet	7
 EC2 SecurityGroup	6
 EC2 RouteTable	6
 EC2 VPC	4
 EC2 NetworkAcl	4

Option A is incorrect because this would give the list of production based resources and now all resources Option B is partially correct But this will just add more maintenance overhead.

Option C is incorrect because this can be used to log API activities but not give an account of all resou For more information on IAM Config, please visit the below URL: <https://docs.IAM.amazon.com/config/latest/developereuide/how-does-confie-work.html>

The correct answer is: Use IAM Config to get the list of all resources

Submit your Feedback/Queries to our Experts

NEW QUESTION 179

- (Exam Topic 2)

A Security Engineer is trying to determine whether the encryption keys used in an IAM service are in compliance with certain regulatory standards. Which of the following actions should the Engineer perform to get further guidance?

- A. Read the IAM Customer Agreement.
- B. Use IAM Artifact to access IAM compliance reports.
- C. Post the question on the IAM Discussion Forums.
- D. Run IAM Config and evaluate the configuration outputs.

Answer: B

Explanation:

<https://IAM.amazon.com/artifact/>

Third-party auditors assess the security and compliance of IAM Key Management Service as part of multiple IAM compliance programs. These include SOC, PCI, FedRAMP, HIPPA, and others. The compliance document is found in IAM Artifact.

NEW QUESTION 180

- (Exam Topic 2)

A company maintains sensitive data in an Amazon S3 bucket that must be protected using an IAM KMS CMK. The company requires that keys be rotated automatically every year. How should the bucket be configured?

- A. Select server-side encryption with Amazon S3-managed keys (SSE-S3) and select an IAM-managed CMK.
- B. Select Amazon S3-IAM KMS managed encryption keys (S3-KMS) and select a customer-managed CMK with key rotation enabled.
- C. Select server-side encryption with Amazon S3-managed keys (SSE-S3) and select a customer-managed CMK that has imported key material.
- D. Select server-side encryption with IAM KMS-managed keys (SSE-KMS) and select an alias to an IAM-managed CMK.

Answer: B

NEW QUESTION 184

- (Exam Topic 2)

A company uses user data scripts that contain sensitive information to bootstrap Amazon EC2 instances. A Security Engineer discovers that this sensitive information is viewable by people who should not have access to it.

What is the MOST secure way to protect the sensitive information used to bootstrap the instances?

- A. Store the scripts in the AMI and encrypt the sensitive data using IAM KMS Use the instance role profile to control access to the KMS keys needed to decrypt the data.
- B. Store the sensitive data in IAM Systems Manager Parameter Store using the encrypted string parameter and assign the GetParameters permission to the EC2 instance role.
- C. Externalize the bootstrap scripts in Amazon S3 and encrypt them using IAM KM
- D. Remove the scripts from the instance and clear the logs after the instance is configured.
- E. Block user access of the EC2 instance's metadata service using IAM policie
- F. Remove all scripts and clear the logs after execution.

Answer: B

NEW QUESTION 187

- (Exam Topic 2)

You are devising a policy to allow users to have the ability to access objects in a bucket called appbucket. You define the below custom bucket policy

```
{ "ID": "Policy1502987489630",  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "Stmt1502987487640",  
      "Action": [  
        "s3:GetObject",  
        "s3:GetObjectVersion"  
      ],  
      "Effect": "Allow",  
      "Resource": "arn:aws:s3:::appbucket",  
      "Principal": "*"   
    }  
  ]  
}
```

But when you try to apply the policy you get the error "Action does not apply to any resource(s) in statement." What should be done to rectify the error Please select:

- A. Change the IAM permissions by applying PutBucketPolicy permissions.
- B. Verify that the policy has the same name as the bucket nam
- C. If no
- D. make it the same.
- E. Change the Resource section to "arn:IAM:s3:::appbucket/*".
- F. Create the bucket "appbucket" and then apply the policy.

Answer: C

Explanation:

When you define access to objects in a bucket you need to ensure that you specify to which objects in the bucket access needs to be given to. In this case, the * can be used to assign the permission to all objects in the bucket

Option A is invalid because the right permissions are already provided as per the question requirement Option B is invalid because it is not necessary that the policy has the same name as the bucket

Option D is invalid because this should be the default flow for applying the policy For more information on bucket policies please visit the below URL:

<https://docs.IAM.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

The correct answer is: Change the Resource section to "arn:IAM:s3:::appbucket/" Submit your Feedback/Queries to our Experts

NEW QUESTION 192

- (Exam Topic 2)

A Systems Engineer has been tasked with configuring outbound mail through Simple Email Service (SES) and requires compliance with current TLS standards. The mail application should be configured to connect to which of the following endpoints and corresponding ports?

- A. email.us-east-1.amazonIAM.com over port 8080
- B. email-pop3.us-east-1.amazonIAM.com over port 995
- C. email-smtp.us-east-1.amazonIAM.com over port 587
- D. email-imap.us-east-1.amazonIAM.com over port 993

Answer: C

Explanation:

<https://docs.IAM.amazon.com/ses/latest/DeveloperGuide/smtp-connect.html>

NEW QUESTION 195

- (Exam Topic 2)

A Security Architect is evaluating managed solutions for storage of encryption keys. The requirements are:

-Storage is accessible by using only VPCs.

-Service has tamper-evident controls.

-Access logging is enabled.

-Storage has high availability.

Which of the following services meets these requirements?

- A. Amazon S3 with default encryption
- B. IAM CloudHSM
- C. Amazon DynamoDB with server-side encryption
- D. IAM Systems Manager Parameter Store

Answer: B

NEW QUESTION 199

- (Exam Topic 2)

A company has five IAM accounts and wants to use IAM CloudTrail to log API calls. The log files must be stored in an Amazon S3 bucket that resides in a new account specifically built for centralized services with a unique top-level prefix for each trail. The configuration must also enable detection of any modification to the logs.

Which of the following steps will implement these requirements? (Choose three.)

- A. Create a new S3 bucket in a separate IAM account for centralized storage of CloudTrail logs, and enable "Log File Validation" on all trails.
- B. Use an existing S3 bucket in one of the accounts, apply a bucket policy to the new centralized S3 bucket that permits the CloudTrail service to use the "s3:PutObject" action and the "s3:GetBucketACL" action, and specify the appropriate resource ARNs for the CloudTrail trails.
- C. Apply a bucket policy to the new centralized S3 bucket that permits the CloudTrail service to use the "s3:PutObject" action and the "s3:GetBucketACL" action, and specify the appropriate resource ARNs for the CloudTrail trails.
- D. Use unique log file prefixes for trails in each IAM account.
- E. Configure CloudTrail in the centralized account to log all accounts to the new centralized S3 bucket.
- F. Enable encryption of the log files by using IAM Key Management Service

Answer: ACE

Explanation:

<https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/best-practices-security.html>

If you have created an organization in IAM Organizations, you can create a trail that will log all events for all IAM accounts in that organization. This is sometimes referred to as an organization trail. You can also choose to edit an existing trail in the master account and apply it to an organization, making it an organization trail.

Organization trails log events for the master account and all member accounts in the organization. For more information about IAM Organizations, see Organizations Terminology and Concepts. Note Reference: <https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/creating-trail-organization.html> You must be logged in with the master account for the organization in order to create an organization trail. You must also have sufficient permissions for the IAM user or role in the master account in order to successfully create an organization trail. If you do not have sufficient permissions, you will not see the option to apply a trail to an organization.

NEW QUESTION 201

- (Exam Topic 2)

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. Copy the data directly from the EBS encrypted volume before the volume is detached from the EC2 instance.
- B. Recover the data from the EBS encrypted volume using an earlier version of the KMS backing key.

- C. Make a request to IAM Support to recover the S3 encrypted data.
- D. Make a request to IAM Support to restore the deleted CMK, and use it to recover the data.

Answer: A

Explanation:

<https://docs.IAM.amazon.com/kms/latest/developerguide/deleting-keys.html#deleting-keys-how-it-works>

NEW QUESTION 202

- (Exam Topic 2)

A security alert has been raised for an Amazon EC2 instance in a customer account that is exhibiting strange behavior. The Security Engineer must first isolate the EC2 instance and then use tools for further investigation.

What should the Security Engineer use to isolate and research this event? (Choose three.)

- A. IAM CloudTrail
- B. Amazon Athena
- C. IAM Key Management Service (IAM KMS)
- D. VPC Flow Logs
- E. IAM Firewall Manager
- F. Security groups

Answer: ADF

Explanation:

https://github.com/IAMlabs/aws-well-architected-labs/blob/master/Security/300_Incident_Response_with_IAM

NEW QUESTION 203

- (Exam Topic 2)

An IAM Lambda function was misused to alter data, and a Security Engineer must identify who invoked the function and what output was produced. The Engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs.

Which of the following explains why the logs are not available?

- A. The execution role for the Lambda function did not grant permissions to write log data to CloudWatch Logs.
- B. The Lambda function was executed by using Amazon API Gateway, so the logs are not stored in CloudWatch Logs.
- C. The execution role for the Lambda function did not grant permissions to write to the Amazon S3 bucket where CloudWatch Logs stores the logs.
- D. The version of the Lambda function that was executed was not current.

Answer: A

NEW QUESTION 206

- (Exam Topic 2)

Your company has defined a number of EC2 Instances over a period of 6 months. They want to know if any of the security groups allow unrestricted access to a resource. What is the best option to accomplish this requirement?

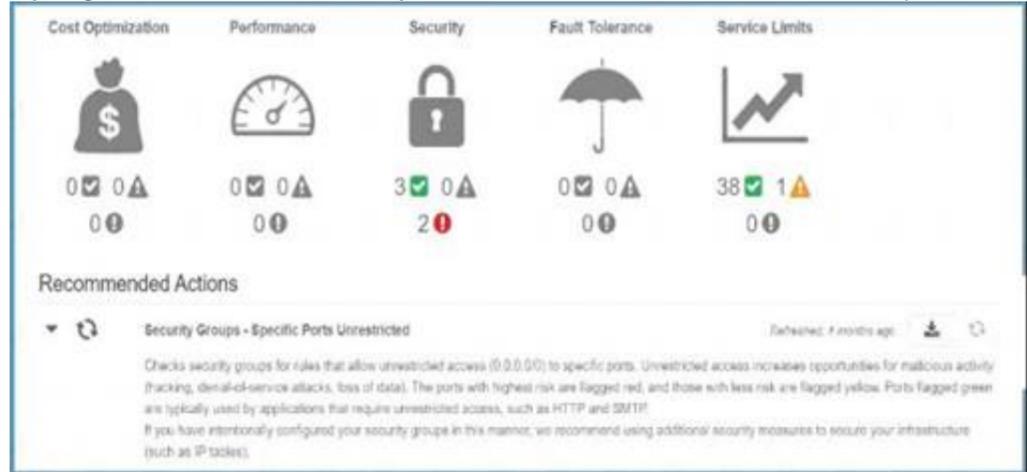
Please select:

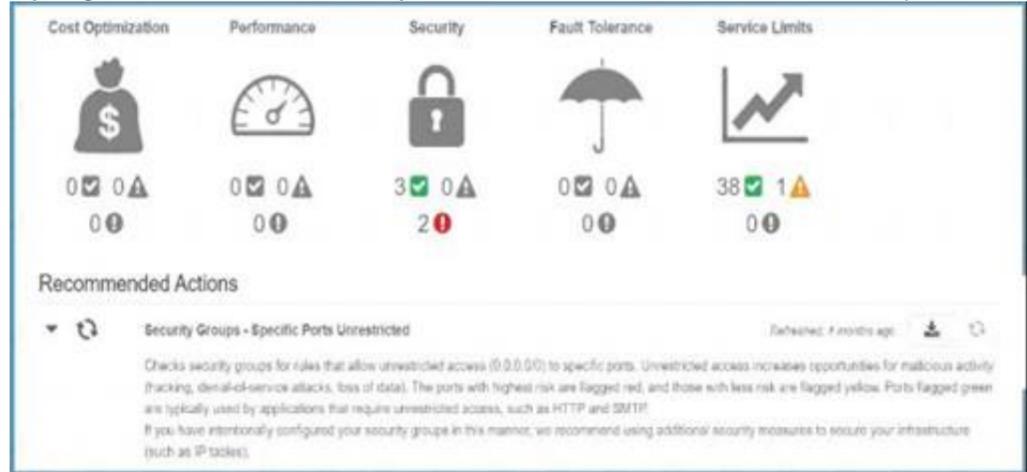
- A. Use IAM Inspector to inspect all the security Groups
- B. Use the IAM Trusted Advisor to see which security groups have compromised access.
- C. Use IAM Config to see which security groups have compromised access.
- D. Use the IAM CLI to query the security groups and then filter for the rules which have unrestricted access

Answer: B

Explanation:

The IAM Trusted Advisor can check security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).

If you go to IAM Trusted Advisor, you can see the details  C:\Users\wk\Desktop\mudassar\Untitled.jpg



Option A is invalid because IAM Inspector is used to detect security vulnerabilities in instances and not for security groups.

Option C is invalid because this can be used to detect changes in security groups but not show you security groups that have compromised access.

Option D is partially valid but would just be a maintenance overhead

For more information on the IAM Trusted Advisor, please visit the below URL: <https://IAM.amazon.com/premiumsupport/trustedadvisor/best-practices>;

The correct answer is: Use the IAM Trusted Advisor to see which security groups have compromised access. Submit your Feedback/Queries to our Experts

NEW QUESTION 207

- (Exam Topic 2)

An Amazon EC2 instance is part of an EC2 Auto Scaling group that is behind an Application Load Balancer (ALB). It is suspected that the EC2 instance has been compromised.

Which steps should be taken to investigate the suspected compromise? (Choose three.)

- A. Detach the elastic network interface from the EC2 instance.
- B. Initiate an Amazon Elastic Block Store volume snapshot of all volumes on the EC2 instance.
- C. Disable any Amazon Route 53 health checks associated with the EC2 instance.
- D. De-register the EC2 instance from the ALB and detach it from the Auto Scaling group.
- E. Attach a security group that has restrictive ingress and egress rules to the EC2 instance.
- F. Add a rule to an IAM WAF to block access to the EC2 instance.

Answer: BDE

Explanation:

https://d1.IAMstatic.com/whitepapers/IAM_security_incident_response.pdf

NEW QUESTION 210

- (Exam Topic 2)

An organization is moving non-business-critical applications to IAM while maintaining a mission-critical application in an on-premises data center. An on-premises application must share limited confidential information with the applications in IAM. The internet performance is unpredictable.

Which configuration will ensure continued connectivity between sites MOST securely?

- A. VPN and a cached storage gateway
- B. IAM Snowball Edge
- C. VPN Gateway over IAM Direct Connect
- D. IAM Direct Connect

Answer: C

Explanation:

<https://docs.IAM.amazon.com/whitepapers/latest/IAM-vpc-connectivity-options/IAM-direct-connect-plus-vpn-n>

NEW QUESTION 215

- (Exam Topic 2)

A Development team has asked for help configuring the IAM roles and policies in a new IAM account. The team using the account expects to have hundreds of master keys and therefore does not want to manage access control for customer master keys (CMKs).

Which of the following will allow the team to manage IAM KMS permissions in IAM without the complexity of editing individual key policies?

- A. The account's CMK key policy must allow the account's IAM roles to perform KMS EnableKey.
- B. Newly created CMKs must have a key policy that allows the root principal to perform all actions.
- C. Newly created CMKs must allow the root principal to perform the kms CreateGrant API operation.
- D. Newly created CMKs must mirror the IAM policy of the KMS key administrator.

Answer: B

Explanation:

<https://docs.IAM.amazon.com/kms/latest/developerguide/key-policies.html#key-policy-default-allow-root-enabl>

NEW QUESTION 216

- (Exam Topic 2)

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 modify-instance-attribute API to change the key on any EC2 instance that is using the key.
- C. Use the EC2 RunCommand to modify the authorized_keys file on any EC2 instance that is using the key.
- D. Update the key pair in any AMI used to launch the EC2 instances, then restart the EC2 instances.

Answer: C

NEW QUESTION 218

- (Exam Topic 2)

A Security Engineer must design a solution that enables the Incident Response team to audit for changes to a user's IAM permissions in the case of a security incident.

How can this be accomplished?

- A. Use IAM Config to review the IAM policy assigned to users before and after the incident.
- B. Run the GenerateCredentialReport via the IAM CLI, and copy the output to Amazon S3 daily for auditing purposes.
- C. Copy IAM CloudFormation templates to S3, and audit for changes from the template.
- D. Use Amazon EC2 Systems Manager to deploy images, and review IAM CloudTrail logs for changes.

Answer: A

Explanation:

<https://IAM.amazon.com/blogs/security/how-to-record-and-govern-your-iam-resource-configurations-using-IAM>

NEW QUESTION 222

- (Exam Topic 2)

A Security Engineer is working with the development team to design a supply chain application that stores sensitive inventory data in an Amazon S3 bucket. The application will use an IAM KMS customer master key (CMK) to encrypt the data on Amazon S3. The inventory data on Amazon S3 will be shared of vendors. All vendors will use IAM principals from their own IAM accounts to access the data on Amazon S3. The vendor list may change weekly, and the solution must support cross-account access.

What is the MOST efficient way to manage access control for the KMS CMK?

- A. Use KMS grants to manage key acces
- B. Programmatically create and revoke grants to manage vendor access.
- C. Use an IAM role to manage key acces
- D. Programmatically update the IAM role policies to manage vendor access.
- E. Use KMS key policies to manage key acces
- F. Programmatically update the KMS key policies to manage vendor access.
- G. Use delegated access across IAM accounts by using IAM roles to manage key acces
- H. Programmatically update the IAM trust policy to manage cross-account vendor access.

Answer: A

NEW QUESTION 224

- (Exam Topic 2)

A Developer who is following IAM best practices for secure code development requires an application to encrypt sensitive data to be stored at rest, locally in the application, using IAM KMS. What is the simplest and MOST secure way to decrypt this data when required?

- A. Request KMS to provide the stored unencrypted data key and then use the retrieved data key to decrypt the data.
- B. Keep the plaintext data key stored in Amazon DynamoDB protected with IAM policie
- C. Query DynamoDB to retrieve the data key to decrypt the data
- D. Use the Encrypt API to store an encrypted version of the data key with another customer managed key. Decrypt the data key and use it to decrypt the data when required.
- E. Store the encrypted data key alongside the encrypted dat
- F. Use the Decrypt API to retrieve the data key to decrypt the data when required.

Answer: D

Explanation:

We recommend that you use the following pattern to locally encrypt data: call the GenerateDataKey API, use the key returned in the Plaintext response field to locally encrypt data, and then erase the plaintext data key from memory. Store the encrypted data key (contained in the CiphertextBlob field) alongside of the locally encrypted data. The Decrypt API returns the plaintext key from the encrypted key.

<https://docs.IAM.amazon.com/sdkfornet/latest/apidocs/items/MKeyManagementServiceKeyManagementService>

NEW QUESTION 225

- (Exam Topic 2)

A Security Administrator is configuring an Amazon S3 bucket and must meet the following security requirements:

- > Encryption in transit
- > Encryption at rest
- > Logging of all object retrievals in IAM CloudTrail

Which of the following meet these security requirements? (Choose three.)

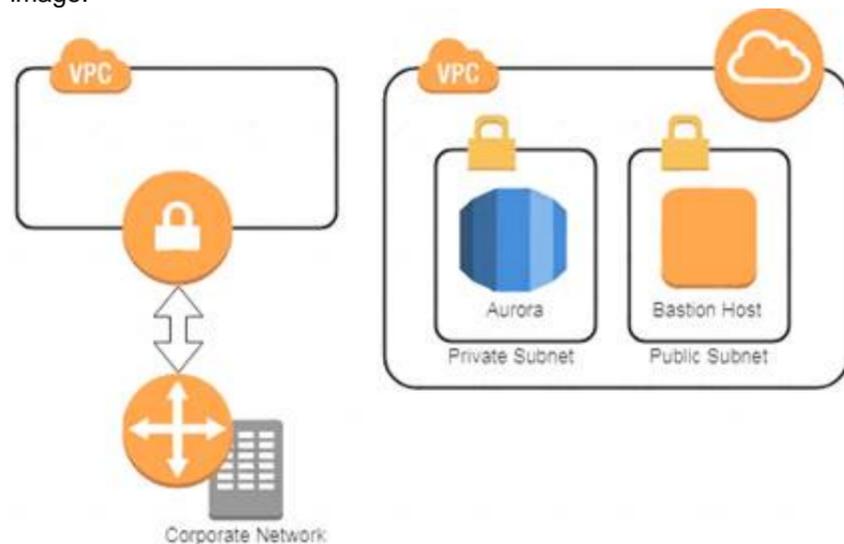
- A. Specify "IAM:SecureTransport": "true" within a condition in the S3 bucket policy.
- B. Enable a security group for the S3 bucket that allows port 443, but not port 80.
- C. Set up default encryption for the S3 bucket.
- D. Enable Amazon CloudWatch Logs for the IAM account.
- E. Enable API logging of data events for all S3 objects.
- F. Enable S3 object versioning for the S3 bucket.

Answer: ACE

NEW QUESTION 227

- (Exam Topic 2)

A company has two IAM accounts, each containing one VPC. The first VPC has a VPN connection with its corporate network. The second VPC, without a VPN, hosts an Amazon Aurora database cluster in private subnets. Developers manage the Aurora database from a bastion host in a public subnet as shown in the image.



A security review has flagged this architecture as vulnerable, and a Security Engineer has been asked to make this design more secure. The company has a short

deadline and a second VPN connection to the Aurora account is not possible.
 How can a Security Engineer securely set up the bastion host?

- A. Move the bastion host to the VPC with VPN connectivity
- B. Create a VPC peering relationship between the bastion host VPC and Aurora VPC.
- C. Create a SSH port forwarding tunnel on the Developer's workstation to the bastion host to ensure that only authorized SSH clients can access the bastion host.
- D. Move the bastion host to the VPC with VPN connectivity
- E. Create a cross-account trust relationship between the bastion VPC and Aurora VPC, and update the Aurora security group for the relationship.
- F. Create an IAM Direct Connect connection between the corporate network and the Aurora account, and adjust the Aurora security group for this connection.

Answer: A

NEW QUESTION 231

- (Exam Topic 2)

A Security Engineer must enforce the use of only Amazon EC2, Amazon S3, Amazon RDS, Amazon DynamoDB, and IAM STS in specific accounts.
 What is a scalable and efficient approach to meet this requirement?

- A Set up an AWS Organizations hierarchy, and replace the FullAWSAccess policy with the following Service Control Policy for the governed organization units:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "dynamodb:*", "rds:*", "ec2:*",
        "s3:*", "sts:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

- B Create multiple IAM users for the regulated accounts, and attach the following policy statement to restrict services as required:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": *
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "NotAction": [
        "dynamodb:*", "rds:*", "ec2:*",
        "s3:*", "sts:*"
      ],
      "Effect": "Deny",
      "Resource": "*"
    }
  ]
}
```

- C Set up an Organizations hierarchy, replace the global FullAWSAccess with the following Service Control Policy at the top level:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "dynamodb:*", "rds:*", "ec2:*",
        "s3:*", "sts:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

D Set up all users in the Active Directory for federated access to all accounts in the company. Associate Active Directory groups with IAM groups, and attach the following policy statement to restrict services as required:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": *
      "Effect": "Allow",
      "Resource": "*"
    }
  ],
  "NotAction": [
    "dynamodb:*", "rds:*", "ec2:*",
    "s3:*", "sts:*"
  ],
  "Effect": "Deny ",
  "Resource": "*"
}
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

It says specific accounts which mean specific governed OUs under your organization and you apply specific service control policy to these OUs.

NEW QUESTION 234

- (Exam Topic 2)

Your IT Security team has advised to carry out a penetration test on the resources in their company's IAM Account. This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?

Please select:

- A. Turn on Cloud trail and carry out the penetration test
- B. Turn on VPC Flow Logs and carry out the penetration test
- C. Submit a request to IAM Support
- D. Use a custom IAM Marketplace solution for conducting the penetration test

Answer: C

Explanation:

This concept is given in the IAM Documentation

How do I submit a penetration testing request for my IAM resources? Issue

I want to run a penetration test or other simulated event on my IAM architecture. How do I get permission from IAM to do that?

Resolution

Before performing security testing on IAM resources, you must obtain approval from IAM. After you submit your request IAM will reply in about two business days. IAM might have additional questions about your test which can extend the approval process, so plan accordingly and be sure that your initial request is as detailed as possible.

If your request is approved, you'll receive an authorization number.

Option A.B and D are all invalid because the first step is to get prior authorization from IAM for penetration tests

For more information on penetration testing, please visit the below URL

* <https://IAM.amazon.com/security/penetration-testing/>

* <https://IAM.amazon.com/premiumsupport/knowledge-center/penetration-testing/> (

The correct answer is: Submit a request to IAM Support Submit your Feedback/Queries to our Experts

NEW QUESTION 235

- (Exam Topic 2)

Compliance requirements state that all communications between company on-premises hosts and EC2 instances be encrypted in transit. Hosts use custom proprietary protocols for their communication, and EC2 instances need to be fronted by a load balancer for increased availability.

Which of the following solutions will meet these requirements?

- A. Offload SSL termination onto an SSL listener on a Classic Load Balancer, and use a TCP connection between the load balancer and the EC2 instances.
- B. Route all traffic through a TCP listener on a Classic Load Balancer, and terminate the TLS connection on the EC2 instances.
- C. Create an HTTPS listener using an Application Load Balancer, and route all of the communication through that load balancer.
- D. Offload SSL termination onto an SSL listener using an Application Load Balancer, and re-spawn and SSL connection between the load balancer and the EC2 instances.

Answer: B

Explanation:

<https://IAM.amazon.com/blogs/compute/maintaining-transport-layer-security-all-the-way-to-your-container-usin>

NEW QUESTION 240

- (Exam Topic 2)

An application makes calls to IAM services using the IAM SDK. The application runs on Amazon EC2 instances with an associated IAM role. When the application attempts to access an object within an Amazon S3 bucket; the Administrator receives the following error message: HTTP 403: Access Denied. Which combination of steps should the Administrator take to troubleshoot this issue? (Select three.)

- A. Confirm that the EC2 instance's security group authorizes S3 access.
- B. Verify that the KMS key policy allows decrypt access for the KMS key for this IAM principle.
- C. Check the S3 bucket policy for statements that deny access to objects.
- D. Confirm that the EC2 instance is using the correct key pair.
- E. Confirm that the IAM role associated with the EC2 instance has the proper privileges.
- F. Confirm that the instance and the S3 bucket are in the same Region.

Answer: BCE

NEW QUESTION 243

- (Exam Topic 2)

A Systems Administrator has written the following Amazon S3 bucket policy designed to allow access to an S3 bucket for only an authorized IAM IAM user from the IP address range 10.10.10.0/24:

```
{
  "Version": "2012-10-17",
  "Id": "S3Policy1",
  "Statement": [
    {
      "Sid": ["OfficeAllowIP"],
      "Effect": ["Allow"],
      "Principal": ["*"],
      "Action": ["s3:*"],
      "Resource": ["arn:aws:s3:::Bucket"],
      "Condition": {
        "IpAddress": [
          {
            "aws:SourceIp": "10.10.10.0/24"
          }
        ]
      }
    }
  ]
}
```

When trying to download an object from the S3 bucket from 10.10.10.40, the IAM user receives an access denied message. What does the Administrator need to change to grant access to the user?

- A. Change the "Resource" from "arn: IAM:s3:::Bucket" to "arn:IAM:s3:::Bucket/*".
- B. Change the "Principal" from "*" to {"IAM:"arn:IAM:iam: : account-number: user/username"}
- C. Change the "Version" from "2012-10-17" to the last revised date of the policy
- D. Change the "Action" from ["s3:*"] to ["s3:GetObject", "s3:ListBucket"]

Answer: A

NEW QUESTION 247

- (Exam Topic 2)

An organization is using IAM CloudTrail, Amazon CloudWatch Logs, and Amazon CloudWatch to send alerts when new access keys are created. However, the alerts are no longer appearing in the Security Operations mail box. Which of the following actions would resolve this issue?

- A. In CloudTrail, verify that the trail logging bucket has a log prefix configured.
- B. In Amazon SNS, determine whether the "Account spend limit" has been reached for this alert.
- C. In SNS, ensure that the subscription used by these alerts has not been deleted.
- D. In CloudWatch, verify that the alarm threshold "consecutive periods" value is equal to, or greater than 1.

Answer: C

NEW QUESTION 252

- (Exam Topic 2)

Which of the following is not a best practice for carrying out a security audit? Please select:

- A. Conduct an audit on a yearly basis
- B. Conduct an audit if application instances have been added to your account
- C. Conduct an audit if you ever suspect that an unauthorized person might have accessed your account
- D. Whenever there are changes in your organization

Answer: A

Explanation:

A year's time is generally too long a gap for conducting security audits The IAM Documentation mentions the following

You should audit your security configuration in the following situations: On a periodic basis.

If there are changes in your organization, such as people leaving.

If you have stopped using one or more individual IAM services. This is important for removing permissions that users in your account no longer need.

If you've added or removed software in your accounts, such as applications on Amazon EC2 instances, IAM OpsWorks stacks, IAM CloudFormation templates, etc.

If you ever suspect that an unauthorized person might have accessed your account.

Option B, C and D are all the right ways and recommended best practices when it comes to conducting audits. For more information on Security Audit guideline, please visit the below URL:

<https://docs.IAM.amazon.com/eeneral/latest/gr/IAM-security-audit-euide.html>

The correct answer is: Conduct an audit on a yearly basis. Submit your Feedback/Queries to our Experts

NEW QUESTION 253

- (Exam Topic 2)

The IAM Systems Manager Parameter Store is being used to store database passwords used by an IAM Lambda function. Because this is sensitive data, the parameters are stored as type SecureString and protected by an IAM KMS key that allows access through IAM. When the function executes, this parameter cannot be retrieved as the result of an access denied error.

Which of the following actions will resolve the access denied error?

- A. Update the ssm.amazonaws.com principal in the KMS key policy to allow kms: Decrypt.
- B. Update the Lambda configuration to launch the function in a VPC.
- C. Add a policy to the role that the Lambda function uses, allowing kms: Decrypt for the KMS key.
- D. Add lambda.amazonaws.com as a trusted entity on the IAM role that the Lambda function uses.

Answer: C

Explanation:

https://docs.amazonaws.cn/en_us/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Authorizin

NEW QUESTION 255

- (Exam Topic 2)

A company has complex connectivity rules governing ingress, egress, and communications between Amazon EC2 instances. The rules are so complex that they cannot be implemented within the limits of the maximum number of security groups and network access control lists (network ACLs).

What mechanism will allow the company to implement all required network rules without incurring additional cost?

- A. Configure IAM WAF rules to implement the required rules.
- B. Use the operating system built-in, host-based firewall to implement the required rules.
- C. Use a NAT gateway to control ingress and egress according to the requirements.
- D. Launch an EC2-based firewall product from the IAM Marketplace, and implement the required rules in that product.

Answer: B

NEW QUESTION 259

- (Exam Topic 2)

A company is hosting a website that must be accessible to users for HTTPS traffic. Also port 22 should be open for administrative purposes. The administrator's workstation has a static IP address of 203.0.113.1/32. Which of the following security group configurations are the MOST secure but still functional to support these requirements? Choose 2 answers from the options given below.

Please select:

- A. Port 443 coming from 0.0.0.0/0
- B. Port 443 coming from 10.0.0.0/16
- C. Port 22 coming from 0.0.0.0/0
- D. Port 22 coming from 203.0.113.1/32

Answer: AD

Explanation:

Since HTTPS traffic is required for all users on the Internet, Port 443 should be open on all IP addresses. For port 22, the traffic should be restricted to an internal subnet.

Option B is invalid, because this only allow traffic from a particular CIDR block and not from the internet. Option C is invalid because allowing port 22 from the internet is a security risk.

For more information on IAM Security Groups, please visit the following URL:

<https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/usins-network-security.html>

The correct answers are: Port 443 coming from 0.0.0.0/0, Port 22 coming from 203.0.113.1 /32. Submit your Feedback/Queries to our Experts

NEW QUESTION 261

- (Exam Topic 2)

A company has a customer master key (CMK) with imported key materials. Company policy requires that all encryption keys must be rotated every year.

What can be done to implement the above policy?

- A. Enable automatic key rotation annually for the CMK.
- B. Use IAM Command Line Interface to create an IAM Lambda function to rotate the existing CMK annually.
- C. Import new key material to the existing CMK and manually rotate the CMK.
- D. Create a new CMK, import new key material to it, and point the key alias to the new CMK.

Answer: D

Explanation:

https://docs.IAM.amazon.com/en_pv/kms/latest/developerguide/rotate-keys.html#rotate-keys-manually "You might prefer to rotate keys manually so you can control the rotation frequency. It's also a good solution

for CMKs that are not eligible for automatic key rotation, such as asymmetric CMKs, CMKs in custom key stores and CMKs with imported key material. Because

the new CMK is a different resource from the current CMK, it has a different key ID and ARN. When you change CMKs, you need to update references to the CMK ID or ARN in your applications. Aliases, which associate a friendly name with a CMK, make this process easier. Use an alias to refer to a CMK in your applications. Then, when you want to change the CMK that the application uses, change the target CMK of the alias. To update the target CMK of an alias, use UpdateAlias operation in the IAM KMS API. "

NEW QUESTION 266

- (Exam Topic 2)

Amazon CloudWatch Logs agent is successfully delivering logs to the CloudWatch Logs service. However, logs stop being delivered after the associated log stream has been active for a specific number of hours.

What steps are necessary to identify the cause of this phenomenon? (Choose two.)

- A. Ensure that file permissions for monitored files that allow the CloudWatch Logs agent to read the file have not been modified.
- B. Verify that the OS Log rotation rules are compatible with the configuration requirements for agent streaming.
- C. Configure an Amazon Kinesis producer to first put the logs into Amazon Kinesis Streams.
- D. Create a CloudWatch Logs metric to isolate a value that changes at least once during the period before logging stops.
- E. Use IAM CloudFormation to dynamically create and maintain the configuration file for the CloudWatch Logs agent.

Answer: AB

Explanation:

https://acloud.guru/forums/IAM-certified-security-specialty/discussion/-Lm5A3w6_NybQPhh6tRP/Cloudwatch

NEW QUESTION 270

- (Exam Topic 2)

A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of "Sensitive," "Confidential," and "Restricted."

The security solution must meet all of the following requirements:

- > Each object must be encrypted using a unique key.
- > Items that are stored in the "Restricted" bucket require two-factor authentication for decryption.
- > IAM KMS must automatically rotate encryption keys annually.

Which of the following meets these requirements?

- A. Create a Customer Master Key (CMK) for each data classification type, and enable the rotation of it annual
- B. For the "Restricted" CMK, define the MFA policy within the key polic
- C. Use S3 SSE-KMS to encrypt the objects.
- D. Create a CMK grant for each data classification type with EnableKeyRotation and MultiFactorAuthPresent set to tru
- E. S3 can then use the grants to encrypt each object with a unique CMK.
- F. Create a CMK for each data classification type, and within the CMK policy, enable rotation of it annually, and define the MFA polic
- G. S3 can then create DEK grants to uniquely encrypt each object within the S3 bucket.
- H. Create a CMK with unique imported key material for each data classification type, and rotate them annual
- I. For the "Restricted" key material, define the MFA policy in the key polic
- J. Use S3 SSE-KMS to encrypt the objects.

Answer: A

Explanation:

CMKs that are not eligible for automatic key rotation, including asymmetric CMKs, CMKs in custom key stores, and CMKs with imported key material.

NEW QUESTION 272

- (Exam Topic 2)

A Security Engineer must design a system that can detect whether a file on an Amazon EC2 host has been modified. The system must then alert the Security Engineer of the modification.

What is the MOST efficient way to meet these requirements?

- A. Install antivirus software and ensure that signatures are up-to-dat
- B. Configure Amazon CloudWatch alarms to send alerts for security events.
- C. Install host-based IDS software to check for file integrit
- D. Export the logs to Amazon CloudWatch Logs for monitoring and alerting.
- E. Export system log files to Amazon S3. Parse the log files using an IAM Lambda function that will send alerts of any unauthorized system login attempts through Amazon SNS.
- F. Use Amazon CloudWatch Logs to detect file system change
- G. If a change is detected, automatically terminate and recreate the instance from the most recent AM
- H. Use Amazon SNS to send notification of the event.

Answer: B

NEW QUESTION 276

- (Exam Topic 2)

You have a vendor that needs access to an IAM resource. You create an IAM user account. You want to restrict access to the resource using a policy for just that user over a brief period. Which of the following would be an ideal policy to use?

Please select:

- A. An IAM Managed Policy
- B. An Inline Policy
- C. A Bucket Policy
- D. A bucket ACL

Answer: B

Explanation:

The IAM Documentation gives an example on such a case

Inline policies are useful if you want to maintain a strict one-to-one relationship between a policy and the principal entity that it's applied to. For example, you want to be sure that the permissions in a policy are not inadvertently assigned to a principal entity other than the one they're intended for. When you use an inline policy, the permissions in the policy cannot be inadvertently attached to the wrong principal entity. In addition, when you use the IAM Management Console to delete that principal entity, the policies embedded in the principal entity are deleted as well. That's because they are part of the principal entity.

Option A is invalid because IAM Managed Policies are ok for a group of users, but for individual users, inline policies are better.

Option C and D are invalid because they are specifically meant for access to S3 buckets. For more information on policies, please visit the following URL:

<https://docs.IAM.amazonaws.com/IAM/latest/UserGuide/access-managed-vs-inline>

The correct answer is: An Inline Policy. Submit your Feedback/Queries to our Experts

NEW QUESTION 281

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SCS-C02 Practice Exam Features:

- * SCS-C02 Questions and Answers Updated Frequently
- * SCS-C02 Practice Questions Verified by Expert Senior Certified Staff
- * SCS-C02 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SCS-C02 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SCS-C02 Practice Test Here](#)