- **Vendor:** Amazon
- **Exam Code:** SCS-C02
- **Exam Name:** AWS Certified Security - Specialty (SCS-C02)
- **New Updated Questions from Braindump2go**
- **(Updated in December/2023)**

QUESTION 91
A company is using Amazon Route 53 Resolver for its hybrid DNS infrastructure. The company has set up Route 53 Resolver forwarding rules for authoritative domains that are hosted on on-premises DNS servers.
A new security mandate requires the company to implement a solution to log and query DNS traffic that goes to the on-premises DNS servers. The logs must show details of the source IP address of the instance from which the query originated. The logs also must show the DNS name that was requested in Route 53 Resolver.
Which solution will meet these requirements?

A. Use VPC Traffic Mirroring. Configure all relevant elastic network interfaces as the traffic source, include amazon-dns in the mirror filter, and set Amazon CloudWatch Logs as the mirror target. Use CloudWatch Insights on the mirror session logs to run queries on the source IP address and DNS name.
B. Configure VPC flow logs on all relevant VPCs. Send the logs to an Amazon S3 bucket. Use Amazon Athena to run SQL queries on the source IP address and DNS name.
C. Configure Route 53 Resolver query logging on all relevant VPCs. Send the logs to Amazon CloudWatch Logs. Use CloudWatch Insights to run queries on the source IP address and DNS name.
D. Modify the Route 53 Resolver rules on the authoritative domains that forward to the on-premises DNS servers. Send the logs to an Amazon S3 bucket. Use Amazon Athena to run SQL queries on the source IP address and DNS name.

Answer: C
Explanation:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-query-logs.html

QUESTION 92
A security engineer is configuring account-based access control (ABAC) to allow only specific principals to put objects into an Amazon S3 bucket. The principals already have access to Amazon S3.
The security engineer needs to configure a bucket policy that allows principals to put objects into the S3 bucket only if the value of the Team tag on the object matches the value of the Team tag that is associated with the principal. During testing, the security engineer notices that a principal can still put objects into the S3 bucket when the tag values do not match.
Which combination of factors are causing the PutObject operation to succeed when the tag values are different? (Choose two.)

A. The principal's identity-based policy grants access to put objects into the S3 bucket with no conditions.
B. The principal's identity-based policy overrides the condition because the identity-based policy contains an explicit allow.

C. The S3 bucket's resource policy does not deny access to put objects.
D. The S3 bucket's resource policy cannot allow actions to the principal.
E. The bucket policy does not apply to principals in the same zone of trust.

Answer: AC

QUESTION 93
A company is hosting multiple applications within a single VPC in its AWS account. The applications are running behind an Application Load Balancer that is associated with an AWS WAF web ACL. The company's security team has identified that multiple port scans are originating from a specific range of IP addresses on the internet.
A security engineer needs to deny access from the offending IP addresses.
Which solution will meet these requirements?

A. Modify the AWS WAF web ACL with an IP set match rule statement to deny incoming requests from the IP address range.
B. Add a rule to all security groups to deny the incoming requests from the IP address range.
C. Modify the AWS WAF web ACL with a rate-based rule statement to deny the incoming requests from the IP address range.
D. Configure the AWS WAF web ACL with regex match conditions. Specify a pattern set to deny the incoming requests based on the match condition.

Answer: A

QUESTION 94
A company has contracted with a third party to audit several AWS accounts. To enable the audit, cross-account IAM roles have been created in each account targeted for audit. The auditor is having trouble accessing some of the accounts.
Which of the following may be causing this problem? (Choose three.)

A. The external ID used by the auditor is missing or incorrect.
B. The auditor is using the incorrect password.
C. The auditor has not been granted sts:AssumeRole for the role in the destination account.
D. The Amazon EC2 role used by the auditor must be set to the destination account role.
E. The secret key used by the auditor is missing or incorrect.
F. The role ARN used by the auditor is missing or incorrect.

Answer: ACF

QUESTION 95
A security engineer needs to configure an Amazon S3 bucket policy to restrict access to an S3 bucket that is named DOC-EXAMPLE-BUCKET. The policy must allow access to only DOC-EXAMPLE-BUCKET from only the following endpoint: vpce-1a2b3c4d. The policy must deny all access to DOC-EXAMPLE-BUCKET if the specified endpoint is not used.
Which bucket policy statement meets these requirements?

A.

```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Allow",
        "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                     "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"],
        "Condition": {
            "StringNotEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

B.

```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                     "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"],
        "Condition": {
            "StringNotEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

C.

```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                     "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"],
        "Condition": {
            "StringEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

D.

```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Allow",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

Answer: B

QUESTION 96
A company has a group of Amazon EC2 instances in a single private subnet of a VPC with no internet gateway attached. A security engineer has installed the Amazon CloudWatch agent on all instances in that subnet to capture logs from a specific application. To ensure that the logs flow securely, the company's networking team has created VPC endpoints for CloudWatch monitoring and CloudWatch logs. The networking team has attached the endpoints to the VPC.
The application is generating logs However, when the security engineer queries CloudWatch, the logs do not appear.
Which combination of steps should the security engineer take to troubleshoot this issue? (Choose three.)

A. Ensure that the EC2 instance profile that is attached to the EC2 instances has permissions to create log streams and write logs.
B. Create a metric filter on the logs so that they can be viewed in the AWS Management Console.
C. Check the CloudWatch agent configuration file on each EC2 instance to make sure that the CloudWatch agent is collecting the proper log files.
D. Check the VPC endpoint policies of both VPC endpoints to ensure that the EC2 instances have permissions to use them.
E. Create a NAT gateway in the subnet so that the EC2 instances can communicate with CloudWatch.
F. Ensure that the security groups allow all the EC2 instances to communicate with each other to aggregate logs before sending.

Answer: ACD

QUESTION 97
A company uses AWS Signer with all of the company's AWS Lambda functions. A developer recently stopped working for the company. The company wants to ensure that all the code that the developer wrote can no longer be deployed to the Lambda functions.
Which solution will meet this requirement?

A. Revoke all versions of the signing profile assigned to the developer.
B. Examine the developer's IAM roles. Remove all permissions that grant access to Signer.
C. Re-encrypt all source code with a new AWS Key Management Service (AWS KMS) key.
D. Use Amazon CodeGuru to profile all the code that the Lambda functions use.

Answer: A
Explanation:
https://docs.aws.amazon.com/signer/latest/developerguide/revoking.html

QUESTION 98
A company plans to use AWS Key Management Service (AWS KMS) to implement an encryption strategy to protect data at rest. The company requires client-side encryption for company projects. The company is currently conducting multiple projects to test the company's use of AWS KMS. These tests have led to a sudden increase in the company's AWS resource consumption. The test projects include applications that issue multiple requests each second to KMS endpoints for encryption activities.
The company needs to develop a solution that does not throttle the company's ability to use AWS KMS. The solution must improve key usage for client-side encryption and must be cost optimized.
Which solution will meet these requirements?

A. Use keyrings with the AWS Encryption SDK. Use each keyring individually or combine keyrings into a multi-keyring. Decrypt the data by using a keyring that has the primary key in the multi-keyring.
B. Use data key caching. Use the local cache that the AWS Encryption SDK provides with a caching cryptographic materials manager.
C. Use KMS key rotation. Use a local cache in the AWS Encryption SDK with a caching cryptographic materials manager.
D. Use keyrings with the AWS Encryption SDK. Use each keyring individually or combine keyrings into a multi-keyring. Use any of the wrapping keys in the multi-keyring to decrypt the data.

Answer: B
Explanation:
https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/data-key-caching.html

QUESTION 99
A security team is working on a solution that will use Amazon EventBridge to monitor new Amazon S3 objects. The solution will monitor for public access and for changes to any S3 bucket policy or setting that result in public access. The security team configures EventBridge to watch for specific API calls that are logged from AWS CloudTrail. EventBridge has an action to send an email notification through Amazon Simple Notification Service (Amazon SNS) to the security team immediately with details of the API call.
Specifically, the security team wants EventBridge to watch for the s3:PutObjectAcl, s3:DeleteBucketPolicy, and s3:PutBucketPolicy API invocation logs from CloudTrail. While developing the solution in a single account, the security team discovers that the s3:PutObjectAcl API call does not invoke an EventBridge event However, the s3:DeleteBucketPolicy API call and the s3:PutBucketPolicy API call do invoke an event.
The security team has enabled CloudTrail for AWS management events with a basic configuration in the AWS Region in which EventBridge is being tested. Verification of the EventBridge event pattern indicates that the pattern is set up correctly. The security team must implement a solution so that the s3:PutObjectAcl API call will invoke an EventBridge event. The solution must not generate false notifications.
Which solution will meet these requirements?

A. Modify the EventBridge event pattern by selecting Amazon S3. Select All Events as the event type.
B. Modify the EventBridge event pattern by selecting Amazon S3. Select Bucket Level Operations as the event type.
C. Enable CloudTrail Insights to identify unusual API activity.
D. Enable CloudTrail to monitor data events for read and write operations to S3 buckets.

Answer: D
Explanation:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/cloudtrail-logging-s3-info.html#cloudtrail-object-level-tracking

QUESTION 100
A company uses Amazon GuardDuty. The company's security team wants all High severity findings to automatically generate a ticket in a third-party ticketing system through email integration.
Which solution will meet this requirement?

A. Create a verified identity for the third-party ticketing email system in Amazon Simple Email Service (Amazon SES). Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty findings. Specify the SES identity as the target for the EventBridge rule.
B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the third-party ticketing email system to the SNS topic. Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty findings. Specify the SNS topic as the target for the EventBridge rule.
C. Use the GuardDuty CreateFilter API operation to build a filter in GuardDuty to monitor for High severity findings. Export the results of the filter to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the third-party ticketing email system to the SNS topic.
D. Use the GuardDuty CreateFilter API operation to build a filter in GuardDuty to monitor for High severity findings. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the third-party ticketing email system to the SNS topic. Create an Amazon EventBridge rule that includes an event pattern that matches GuardDuty findings that are selected by the filter. Specify the SNS topic as the target for the EventBridge rule.

Answer: B
Explanation:
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings_cloudwatch.html

QUESTION 101
A company is using AWS Organizations to implement a multi-account strategy. The company does not have on-premises infrastructure. All workloads run on AWS. The company currently has eight member accounts. The company anticipates that it will have no more than 20 AWS accounts total at any time.
The company issues a new security policy that contains the following requirements:
- No AWS account should use a VPC within the AWS account for workloads.
- The company should use a centrally managed VPC that all AWS accounts can access to launch workloads in subnets.
- No AWS account should be able to modify another AWS account's application resources within the centrally managed VPC.
- The centrally managed VPC should reside in an existing AWS account that is named Ac-count-A within an organization.
The company uses an AWS CloudFormation template to create a VPC that contains multiple subnets in Account-A. This template exports the subnet IDs through the CloudFormation Outputs section.
Which solution will complete the security setup to meet these requirements?

A. Use a CloudFormation template in the member accounts to launch workloads. Configure the template to use the Fn::ImportValue function to obtain the subnet ID values.
B. Use a transit gateway in the VPC within Account-A. Configure the member accounts to use the transit gateway to access the subnets in Account-A to launch workloads.
C. Use AWS Resource Access Manager (AWS RAM) to share Account-A's VPC subnets with the remaining member accounts. Configure the member accounts to use the shared subnets to launch workloads.
D. Create a peering connection between Account-A and the remaining member accounts. Configure the member accounts to use the subnets in Account-A through the VPC peering connection to launch workloads.

Answer: C
Explanation:
https://aws.amazon.com/blogs/networking-and-content-delivery/vpc-sharing-a-new-approach-to-multiple-accounts-and-vpc-management/

QUESTION 102
A company's security team needs to receive a notification whenever an AWS access key has not been rotated in 90 or more days. A security engineer must develop a solution that provides these notifications automatically.
Which solution will meet these requirements with the LEAST amount of effort?

A. Deploy an AWS Config managed rule to run on a periodic basis of 24 hours. Select the access-keys-rotated managed rule, and set the maxAccessKeyAge parameter to 90 days. Create an Amazon EventBridge rule with an event pattern that matches the compliance type of NON_ COMPLIANT from AWS Config for the managed rule. Configure EventBridge to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
B. Create a script to export a .csv file from the AWS Trusted Advisor check for IAM access key rotation. Load the script into an AWS Lambda function that will upload the .csv file to an Amazon S3 bucket. Create an Amazon Athena table query that runs when the .csv file is uploaded to the S3 bucket. Publish the results for any keys older than 90 days by using an invocation of an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
C. Create a script to download the IAM credentials report on a periodic basis. Load the script into an AWS Lambda function that will run on a schedule through Amazon EventBridge. Configure the Lambda script to load the report into memory and to filter the report for records in which the key was last rotated at least 90 days ago. If any records are detected, send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
D. Create an AWS Lambda function that queries the IAM API to list all the users. Iterate through the users by using the ListAccessKeys operation. Verify that the value in the CreateDate field is not at least 90 days old. Send an Amazon Simple Notification Service (Amazon SNS) notification to the security team if the value is at least 90 days old. Create an Amazon EventBridge rule to schedule the Lambda function to run each day.

Answer: A

QUESTION 103
A company maintains an open-source application that is hosted on a public GitHub repository. While creating a new commit to the repository, an engineer uploaded their AWS access key and secret access key. The engineer reported the mistake to a manager, and the manager immediately disabled the access key.
The company needs to assess the impact of the exposed access key. A security engineer must recommend a solution that requires the least possible managerial overhead.
Which solution meets these requirements?

A. Analyze an AWS Identity and Access Management (IAM) use report from AWS Trusted Advisor to see when the access key was last used.
B. Analyze Amazon CloudWatch Logs for activity by searching for the access key.
C. Analyze VPC flow logs for activity by searching for the access key.
D. Analyze a credential report in AWS Identity and Access Management (IAM) to see when the access key was last used.

Answer: D
Explanation:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

QUESTION 104
A company plans to create individual child accounts within an existing organization in AWS Organizations for each of its DevOps teams. AWS CloudTrail has been enabled and configured on all accounts to write audit logs to an Amazon S3 bucket in a centralized AWS account. A security engineer needs to ensure that DevOps team members are unable to modify or disable this configuration.
How can the security engineer meet these requirements?

A. Create an IAM policy that prohibits changes to the specific CloudTrail trail and apply the policy to the AWS account root user.
B. Create an S3 bucket policy in the specified destination account for the CloudTrail trail that prohibits configuration changes from the AWS account root user in the source account.
C. Create an SCP that prohibits changes to the specific CloudTrail trail and apply the SCP to the appropriate organizational unit or account in Organizations.

D. Create an IAM policy that prohibits changes to the specific CloudTrail trail and apply the policy to a new IAM group. Have team members use individual IAM accounts that are members of the new IAM group.

Answer: C

QUESTION 105
A company's policy requires that all API keys be encrypted and stored separately from source code in a centralized security account. This security account is managed by the company's security team. However, an audit revealed that an API key is stored with the source code of an AWS Lambda function in an AWS CodeCommit repository in the DevOps account.
How should the security team securely store the API key?

A. Create a CodeCommit repository in the security account using AWS Key Management Service (AWS KMS) for encryption. Require the development team to migrate the Lambda source code to this repository.
B. Store the API key in an Amazon S3 bucket in the security account using server-side encryption with Amazon S3 managed encryption keys (SSE-S3) to encrypt the key. Create a presigned URL for the S3 key, and specify the URL in a Lambda environmental variable in the AWS CloudFormation template. Update the Lambda function code to retrieve the key using the URL and call the API.
C. Create a secret in AWS Secrets Manager in the security account to store the API key using AWS Key Management Service (AWS KMS) for encryption. Grant access to the IAM role used by the Lambda function so that the function can retrieve the key from Secrets Manager and call the API.
D. Create an encrypted environment variable for the Lambda function to store the API key using AWS Key Management Service (AWS KMS) for encryption. Grant access to the IAM role used by the Lambda function so that the function can decrypt the key at runtime.

Answer: C

QUESTION 106
A security engineer is asked to update an AWS CloudTrail log file prefix for an existing trail. When attempting to save the change in the CloudTrail console, the security engineer receives the following error message: "There is a problem with the bucket policy."
What will enable the security engineer to save the change?

A. Create a new trail with the updated log file prefix, and then delete the original trail. Update the existing bucket policy in the Amazon S3 console with the new log file prefix, and then update the log file prefix in the CloudTrail console.
B. Update the existing bucket policy in the Amazon S3 console to allow the security engineer's principal to perform PutBucketPolicy, and then update the log file prefix in the CloudTrail console.
C. Update the existing bucket policy in the Amazon S3 console with the new log file prefix, and then update the log file prefix in the CloudTrail console.
D. Update the existing bucket policy in the Amazon S3 console to allow the security engineer's principal to perform GetBucketPolicy, and then update the log file prefix in the CloudTrail console.

Answer: C
Explanation:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/create-s3-bucket-policy-for-cloudtrail.html#cloudtrail-add-change-or-remove-a-bucket-prefix

QUESTION 107
A company uses AWS Organizations. The company wants to implement short-term credentials for third-party AWS accounts to use to access accounts within the company's organization. Access is for the AWS Management Console and third-party software-as-a-service (SaaS) applications. Trust must be enhanced to prevent two external accounts from using the same credentials. The solution must require the least possible operational effort.
Which solution will meet these requirements?

A. Use a bearer token authentication with OAuth or SAML to manage and share a central Amazon Cognito user pool across multiple Amazon API Gateway APIs.
B. Implement AWS IAM Identity Center (AWS Single Sign-On), and use an identity source of choice. Grant access to users and groups from other accounts by using permission sets that are assigned by account.
C. Create a unique IAM role for each external account. Create a trust policy Use AWS Secrets Manager to create a random external key.
D. Create a unique IAM role for each external account. Create a trust policy that includes a condition that uses the sts:ExternalId condition key.

Answer: D
Explanation:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html

QUESTION 108
A company is evaluating its security posture. In the past, the company has observed issues with specific hosts and host header combinations that affected the company's business. The company has configured AWS WAF web ACLs as an initial step to mitigate these issues.
The company must create a log analysis solution for the AWS WAF web ACLs to monitor problematic activity. The company wants to process all the AWS WAF logs in a central location. The company must have the ability to filter out requests based on specific hosts.
A security engineer starts to enable access logging for the AWS WAF web ACLs.
What should the security engineer do next to meet these requirements with the MOST operational efficiency?

A. Specify Amazon Redshift as the destination for the access logs. Deploy the Amazon Athena Redshift connector. Use Athena to query the data from Amazon Redshift and to filter the logs by host.
B. Specify Amazon CloudWatch as the destination for the access logs. Use Amazon CloudWatch Logs Insights to design a query to filter the logs by host.
C. Specify Amazon CloudWatch as the destination for the access logs. Export the CloudWatch logs to an Amazon S3 bucket. Use Amazon Athena to query the logs and to filter the logs by host.
D. Specify Amazon CloudWatch as the destination for the access logs. Use Amazon Redshift Spectrum to query the logs and to filter the logs by host.

Answer: B
Explanation:
https://aws.amazon.com/blogs/mt/analyzing-aws-waf-logs-in-amazon-cloudwatch-logs/

QUESTION 109
A security engineer is trying to use Amazon EC2 Image Builder to create an image of an EC2 instance. The security engineer has configured the pipeline to send logs to an Amazon S3 bucket. When the security engineer runs the pipeline, the build fails with the following error: "AccessDenied: Access Denied status code: 403".
The security engineer must resolve the error by implementing a solution that complies with best practices for least privilege access.
Which combination of steps will meet these requirements? (Choose two.)

A. Ensure that the following policies are attached to the IAM role that the security engineer is using 香C2InstanceProfileForImageBuilder, EC2InstanceProfileForImageBuilderECRContainerBuilds, and AmazonSSMManagedInstanceCore.
B. Ensure that the following policies are attached to the instance profile for the EC2 instance: EC2InstanceProfileForImageBuilder, EC2InstanceProfileForImageBuilderECRContainerBuilds, and AmazonSSMManagedInstanceCore.
C. Ensure that the AWSImageBuilderFullAccess policy is attached to the instance profile for the EC2 instance.
D. Ensure that the security engineer's IAM role has the s3:PutObject permission for the S3 bucket.

E. Ensure that the instance profile for the EC2 instance has the s3:PutObject permission for the S3 bucket.

Answer: BE
Explanation:
https://docs.aws.amazon.com/imagebuilder/latest/userguide/troubleshooting.html#ts-access-denied

QUESTION 110
A security engineer must use AWS Key Management Service (AWS KMS) to design a key management solution for a set of Amazon Elastic Block Store (Amazon EBS) volumes that contain sensitive data. The solution needs to ensure that the key material automatically expires in 90 days.
Which solution meets these criteria?

A. A customer managed key that uses customer provided key material
B. A customer managed key that uses AWS provided key material
C. An AWS managed key
D. Operating system encryption that uses GnuPG

Answer: A
Explanation:
https://awscli.amazonaws.com/v2/documentation/api/latest/reference/kms/import-key-material.html

QUESTION 111
A security engineer is building a Java application that is running on Amazon EC2. The application communicates with an Amazon RDS instance and authenticates with a user name and password.
Which combination of steps can the engineer take to protect the credentials and minimize downtime when the credentials are rotated? (Choose two.)

A. Have a database administrator encrypt the credentials and store the ciphertext in Amazon S3. Grant permission to the instance role associated with the EC2 instance to read the object and decrypt the ciphertext.
B. Configure a scheduled job that updates the credential in AWS Systems Manager Parameter Store and notifies the engineer that the application needs to be restarted.
C. Configure automatic rotation of credentials in AWS Secrets Manager.
D. Store the credential in an encrypted string parameter in AWS Systems Manager Parameter Store. Grant permission to the instance role associated with the EC2 instance to access the parameter and the AWS KMS key that is used to encrypt it.
E. Configure the Java application to catch a connection failure and make a call to AWS Secrets Manager to retrieve updated credentials when the password is rotated. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.

Answer: CE

QUESTION 112
A company uses SAML federation to grant users access to AWS accounts. A company workload that is in an isolated AWS account runs on immutable infrastructure with no human access to Amazon EC2. The company requires a specialized user known as a break glass user to have access to the workload AWS account and instances in the case of SAML errors. A recent audit discovered that the company did not create the break glass user for the AWS account that contains the workload.
The company must create the break glass user. The company must log any activities of the break glass user and send the logs to a security team.
Which combination of solutions will meet these requirements? (Choose two.)

A. Create a local individual break glass IAM user for the security team. Create a trail in AWS CloudTrail that has Amazon CloudWatch Logs turned on. Use Amazon EventBridge to monitor local user activities.

B. Create a break glass EC2 key pair for the AWS account. Provide the key pair to the security team. Use AWS CloudTrail to monitor key pair activity. Send notifications to the security team by using Amazon Simple Notification Service (Amazon SNS).
C. Create a break glass IAM role for the account. Allow security team members to perform the AssumeRoleWithSAML operation. Create an AWS CloudTrail trail that has Amazon CloudWatch Logs turned on. Use Amazon EventBridge to monitor security team activities.
D. Create a local individual break glass IAM user on the operating system level of each workload instance. Configure unrestricted security groups on the instances to grant access to the break glass IAM users.
E. Configure AWS Systems Manager Session Manager for Amazon EC2. Configure an AWS CloudTrail filter based on Session Manager. Send the results to an Amazon Simple Notification Service (Amazon SNS) topic.

Answer: CE
Explanation:
https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/break-glass-access.html

QUESTION 113
A security engineer is working with a product team building a web application on AWS. 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 allow users to be authenticated into the web application and call APIs? (Choose three.)

A. Create a custom authorization service using AWS 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: BCF

QUESTION 114
A company needs to improve its ability to identify and prevent IAM policies that grant public access or cross-account access to resources. The company has implemented AWS Organizations and has started using AWS Identity and Access Management Access Analyzer to refine overly broad access to accounts in the organization.
A security engineer must automate a response in the company's organization for any newly created policies that are overly permissive. The automation must remediate external access and must notify the company's security team.
Which combination of steps should the security engineer take to meet these requirements? (Choose three.)

A. Create an AWS Step Functions state machine that checks the resource type in the finding and adds an explicit Deny statement in the trust policy for the IAM role. Configure the state machine to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic.
B. Create an AWS Batch job that forwards any resource type findings to an AWS Lambda function. Configure the Lambda function to add an explicit Deny statement in the trust policy for the IAM role. Configure the AWS Batch job to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic.
C. In Amazon EventBridge, create an event rule that matches active IAM Access Analyzer findings and invokes AWS Step Functions for resolution.
D. In Amazon CloudWatch, create a metric filter that matches active IAM Access Analyzer findings and invokes AWS Batch for resolution.
E. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the queue to forward a notification to the security team that an external principal has been granted access to the specific IAM role and has been blocked.

F. Create an Amazon Simple Notification Service (Amazon SNS) topic for external or cross-account access notices. Subscribe the security team's email addresses to the topic.

Answer: ACF
Explanation:
https://aws.amazon.com/blogs/compute/orchestrating-a-security-incident-response-with-aws-step-functions/

QUESTION 115
A security engineer is configuring a mechanism to send an alert when three or more failed sign-in attempts to the AWS Management Console occur during a 5-minute period. The security engineer creates a trail in AWS CloudTrail to assist in this work.
Which solution will meet these requirements?

A. In CloudTrail, turn on Insights events on the trail. Configure an alarm on the insight with eventName matching ConsoleLogin and errorMessage matching "Failed authentication". Configure a threshold of 3 and a period of 5 minutes.
B. Configure CloudTrail to send events to Amazon CloudWatch Logs. Create a metric filter for the relevant log group. Create a filter pattern with eventName matching ConsoleLogin and errorMessage matching "Failed authentication". Create a CloudWatch alarm with a threshold of 3 and a period of 5 minutes.
C. Create an Amazon Athena table from the CloudTrail events. Run a query for eventName matching ConsoleLogin and for errorMessage matching "Failed authentication". Create a notification action from the query to send an Amazon Simple Notification Service (Amazon SNS) notification when the count equals 3 within a period of 5 minutes.
D. In AWS Identity and Access Management Access Analyzer, create a new analyzer. Configure the analyzer to send an Amazon Simple Notification Service (Amazon SNS) notification when a failed sign-in event occurs 3 times for any IAM user within a period of 5 minutes.

Answer: B

QUESTION 116
A company's security engineer is developing an incident response plan to detect suspicious activity in an AWS account for VPC hosted resources. The security engineer needs to provide visibility for as many AWS Regions as possible.
Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

A. Turn on VPC Flow Logs for all VPCs in the account.
B. Activate Amazon GuardDuty across all AWS Regions.
C. Activate Amazon Detective across all AWS Regions.
D. Create an Amazon Simple Notification Service (Amazon SNS) topic. Create an Amazon EventBridge rule that responds to findings and publishes the findings to the SNS topic.
E. Create an AWS Lambda function. Create an Amazon EventBridge rule that invokes the Lambda function to publish findings to Amazon Simple Email Service (Amazon SES).

Answer: BD

QUESTION 117
A company stores images for a website in an Amazon S3 bucket. The company is using Amazon CloudFront to serve the images to end users. The company recently discovered that the images are being accessed from countries where the company does not have a distribution license.
Which actions should the company take to secure the images to limit their distribution? (Choose two.)

A. Update the S3 bucket policy to restrict access to a CloudFront origin access control (OAC).
B. Update the website DNS record to use an Amazon Route 53 geolocation record deny list of countries where the company lacks a license.
C. Add a CloudFront geo restriction deny list of countries where the company lacks a license.
D. Update the S3 bucket policy with a deny list of countries where the company lacks a license.

E. Enable the Restrict Viewer Access option in CloudFront to create a deny list of countries where the company lacks a license.

Answer: AC
Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html

QUESTION 118
A company has deployed servers on Amazon EC2 instances in a VPC. External vendors access these servers over the internet. Recently, the company deployed a new application on EC2 instances in a new CIDR range. The company needs to make the application available to the vendors.
A security engineer verified that the associated security groups and network ACLs are allowing the required ports in the inbound direction. However, the vendors cannot connect to the application.
Which solution will provide the vendors access to the application?

A. Modify the security group that is associated with the EC2 instances to have the same outbound rules as inbound rules.
B. Modify the network ACL that is associated with the CIDR range to allow outbound traffic to ephemeral ports.
C. Modify the inbound rules on the internet gateway to allow the required ports.
D. Modify the network ACL that is associated with the CIDR range to have the same outbound rules as inbound rules.

Answer: B
Explanation:
You must allow the ephemeral ports in the outbound NACL for the CIDR range.

QUESTION 119
A company uses infrastructure as code (IaC) to create AWS infrastructure. The company writes the code as AWS CloudFormation templates to deploy the infrastructure. The company has an existing CI/CD pipeline that the company can use to deploy these templates.
After a recent security audit, the company decides to adopt a policy-as-code approach to improve the company's security posture on AWS. The company must prevent the deployment of any infrastructure that would violate a security policy, such as an unencrypted Amazon Elastic Block Store (Amazon EBS) volume.
Which solution will meet these requirements?

A. Turn on AWS Trusted Advisor. Configure security notifications as webhooks in the preferences section of the CI/CD pipeline.
B. Turn on AWS Config. Use the prebuilt rules or customized rules. Subscribe tile CI/CD pipeline to an Amazon Simple Notification Service (Amazon SNS) topic that receives notifications from AWS Config.
C. Create rule sets in AWS CloudFormation Guard. Run validation checks for CloudFormation templates as a phase of the CI/CD process.
D. Create rule sets as SCPs. Integrate the SCPs as a part of validation control in a phase of the CI/CD process.

Answer: C

QUESTION 120
A company is running an Amazon RDS for MySQL DB instance in a VPC. The VPC must not send or receive network traffic through the internet.
A security engineer wants to use AWS Secrets Manager to rotate the DB instance credentials automatically. Because of a security policy, the security engineer cannot use the standard AWS Lambda function that Secrets Manager provides to rotate the credentials.
The security engineer deploys a custom Lambda function in the VPC. The custom Lambda function will be responsible for rotating the secret in Secrets Manager. The security engineer edits the DB instance's security group to allow connections from this function. When the function is invoked, the function cannot communicate with Secrets Manager to

rotate the secret properly.
What should the security engineer do so that the function can rotate the secret?

A. Add an egress-only internet gateway to the VPC. Allow only the Lambda function's subnet to route traffic through the egress-only internet gateway.
B. Add a NAT gateway to the VPC. Configure only the Lambda function's subnet with a default route through the NAT gateway.
C. Configure a VPC peering connection to the default VPC for Secrets Manager. Configure the Lambda function's subnet to use the peering connection for routes.
D. Configure a Secrets Manager interface VPC endpoint. Include the Lambda function's private subnet during the configuration process.

Answer: D

QUESTION 121
The security engineer is managing a traditional three-tier web application that is running on Amazon EC2 instances. The application has become the target of increasing numbers of malicious attacks from the internet.
What steps should the security engineer take to check for known vulnerabilities and limit the attack surface? (Choose two.)

A. Use AWS Certificate Manager to encrypt all traffic between the client and application servers.
B. Review the application security groups to ensure that only the necessary ports are open.
C. Use Elastic Load Balancing to offload Secure Sockets Layer encryption.
D. Use Amazon Inspector to periodically scan the backend instances.
E. Use AWS Key Management Service (AWS KMS) to encrypt all the traffic between the client and application servers.

Answer: BD

QUESTION 122
A company is using Amazon Elastic Container Service (Amazon ECS) to run its container-based application on AWS. The company needs to ensure that the container images contain no severe vulnerabilities. The company also must ensure that only specific IAM roles and specific AWS accounts can access the container images.
Which solution will meet these requirements with the LEAST management overhead?

A. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use identity-based policies to restrict access to which IAM principals can access the images.
B. Pull images from the public container registry. Publish the images to a private container registry that is hosted on Amazon EC2 instances in a centralized AWS account. Deploy host-based container scanning tools to EC2 instances that run Amazon ECS. Restrict access to the container images by using basic authentication over HTTPS.
C. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.
D. Pull images from the public container registry. Publish the images to AWS CodeArtifact repositories in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.

Answer: C
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/secondary-account-access-ecr/

QUESTION 123
A company's data scientists want to create artificial intelligence and machine learning (AI/ML) training models by using Amazon SageMaker. The training models will use large datasets in an Amazon S3 bucket. The datasets contain sensitive information.
On average, the data scientists need 30 days to train models. The S3 bucket has been secured appropriately. The company's data retention policy states that all data that is older than 45 days must be removed from the S3 bucket.
Which action should a security engineer take to enforce this data retention policy?

A. Configure an S3 Lifecycle rule on the S3 bucket to delete objects after 45 days.
B. Create an AWS Lambda function to check the last-modified date of the S3 objects and delete objects that are older than 45 days. Create an S3 event notification to invoke the Lambda function for each PutObject operation.
C. Create an AWS Lambda function to check the last-modified date of the S3 objects and delete objects that are older than 45 days. Create an Amazon EventBridge rule to invoke the Lambda function each month.
D. Configure S3 Intelligent-Tiering on the S3 bucket to automatically transition objects to another storage class.

Answer: A