You are working for a company which runs a financial investments blog. Your researchers work with a number of different partners to gather insights into the financial markets. You have engaged a company called TopInsights to provide a series of market research reports which they are committed to completing over the next 6 months. You have asked them to provide the completed reports in pdf format and save them to an S3 bucket that you own. TopInsights already use S3 to store all of their internal documentation. What will you need to do to enable TopInsights to deliver their reports to your S3 bucket?

1. Create an IAM user with write permission to the S3 bucket. Provide the username and password of this user to the analyst at TopInsights
2. Create an IAM user with write permission to the S3 bucket. Provide the access key ID and secret access key of this user to the analyst at TopInsights
3. Configure S3 replication to replicate the data from the S3 bucket from the external account to your own S3 bucket
4. Create an IAM role with write permission to the S3 bucket. Configure a trust relationship between your AWS account and the AWS account belonging to TopInsights.

Answer: d

EXPLANATION:

When third parties require access to your organization's AWS resources, you can use roles to delegate access to them. An IAM role provides a mechanism to allow a third party to access your AWS resources without needing to share long-term credentials.

You are working for an investment bank which is designing a new application to analyse historical trading data, and use machine learning to predict stock market performance. The application is running in AWS and needs to access the historical data stored in a proprietary time series database located in your data center. This information is highly confidential and could cause serious repercussions if any data was ever leaked to the public or your competitors. The application itself is extremely sensitive to network inconsistencies and during testing it frequently crashes if the network is not reliable. How should you configure the network connectivity for this application?

1. Use a VPC Gateway Endpoint so that the data never leaves Amazon's network
2. Configure a VPN between your VPC and the data center and access the time series database using a secure port
3. Configure a Direct Connect connection between the VPC and your data center
4. Access the data using a secure port on the times series database so that the data is encrypted in transit
5. Configure a VPN between your VPC and the data center over a Direct Connect connection

Answer: e

EXPLANATION:

With AWS Direct Connect plus VPN, you can combine one or more AWS Direct Connect dedicated network connections with the Amazon VPC VPN. This combination provides an IPsec-encrypted private connection that also reduces network costs, increases bandwidth throughput, and provides a more consistent network experience than internet-based VPN connections.

You are building an application which stores all of its persistent data in an RDS database. This morning, your CEO asked you to avoid embedding database credentials in the application code, so you have now stored the database credentials in Secrets Manager with automatic rotation enabled. However when you test the application, you now find that none of your application servers can access the database. What could the problem be?

1. The EC2 instance role doesn't have permission to rotate the embedded credentials
2. The EC2 instance role doesn't have permission to access the Secret in Secrets Manager
3. The automatic rotation has failed
4. Automatic rotation has not completed yet
5. Your EC2 instances are still using embedded credentials

Answer: b, e

EXPLANATION:

A common Secrets Manager scenario is where an application that's running on an Amazon EC2 instance needs access to a database to perform its required tasks. The application must retrieve the database credentials from Secrets Manager. To make a request to Secrets Manager, like any other AWS service, you must have AWS credentials with permissions to perform the request. The recommended way to achieve this is to create an IAM role that's attached to the EC2 instance profile. When you enable automatic rotation of an RDS password, the password is rotated immediately, so any applications still using embedded credentials will no longer have valid credentials.

You are designing a workflow that will handle very confidential healthcare information. You are designing a loosely coupled system comprised of different services. One service handles a decryption activity using a CMK stored in AWS KMS. To meet very strict audit requirements, you must demonstrate that you are following the Principle of Least Privilege dynamically--meaning that processes should only have the minimal amount of access and only precisely when they need it. Given this requirement and AWS limitations, what method is the most efficient to secure the Decryption service?

1. Use a grant constraint to deny access to the key except for the service account that is running the workflow processes. Enable CloudTrail alerts if any other role attempts to access the CMK.
2. The current AWS platform services are not well suited for implementing Principle of Least Privilege in a dynamic manner. Consider a different design that makes use of a more monolithic architecture rather than services.
3. In the step right before the Decryption step, programmatically apply a grant to the CMK that allows the service access to the CMK key. In the step immediately after the decryption, explicitly revoke the grant.
4. Create a IAM key policy that explicitly allows access to the CMK and assign that to a role. Assign the role to the process that is executing the Decryption service. At the end of the day, programmatically revoke that role until the start of the next day.
5. Create an IAM key policy that explicitly denies access to the Decryption operation of the CMK. Assign that policy to a role that is then assigned to the process executing the Decryption service. Use a Lambda function to programmatically remove and add the IAM policy to the role as needed by the decryption process.

Answer: c

EXPLANATION:

Grants in KMS are useful for dynamically and programmatically allowing a process the ability to use the key then revoking after the need is over. This is more efficient than manipulating IAM roles or policies.

You are using a CMK with imported key material. The key has been in use for one year already and your company policy states that keys must be rotated on an annual basis. What should you do?

1. Create a new CMK, import new key material into the new CMK
2. Generate new key material and import this into the CMK
3. Configure automatic key rotation with a 1 year rotation schedule
4. Create a new CMK, import new key material into the new CMK, delete the original key

Answer: a

EXPLANATION:

Automatic rotation is not supported for a CMK with imported key material. You cannot import different key material into a CMK. Deleting a key must be very carefully thought out. Data can’t be decrypted if the corresponding CMK has been deleted.

You have an application running in AWS which needs to import a large amount of data stored on legacy systems in your on premises data center. Your CEO has requested that you make sure the network connection is private, with reasonably consistent performance to prevent the application timing out. Which of the following approaches do you recommend?

1. Use VPC peering between your VPC and the data center
2. Use Direct Connect
3. Use a site-to-site VPN
4. Transfer the data over the internet using CloudFront and HTTPS

Answer: b

EXPLANATION:

AWS Direct Connect is a dedicated network connection from your premises to AWS. In many cases, Direct Connect can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

You are planning to use KMS to encrypt data in your AWS account. According to company policy, you need to be able to rotate the CMK every three months. Which type of key should you use?

1. Use a CMK managed by you
2. Use an AWS owned CMK
3. Use an AWS managed CMK with automatic rotation enabled
4. Use an AWS managed CMK

Answer: a

EXPLANATION:

You can rotate keys according to your own schedule using a customer managed CMK. An AWS managed or AWS owned CMK does not give you the option to rotate according to your own schedule. AWS managed keys automatically rotate once every three years.

A number of users are trying to access objects in your S3 bucket, however they are receiving the error : HTTP 403: Access Denied. You have already checked the bucket ACLs and bucket policy and they look fine. You checked the IAM permissions of the users and they all have read access to the bucket. What else could be the problem?

1. The S3 lifecycle policy has moved the objects to a different class of storage
2. The users permissions are being restricted by the bucket policy
3. The users permissions are being restricted by a Service Control Policy
4. The objects are encrypted using KMS and the users do not have permission to decrypt them
5. The objects have been compressed and the users do not have permission to extract the files

Answer: c, d

EXPLANATION:

To troubleshoot HTTP 403: Access Denied errors from Amazon S3, check the following: Permissions for bucket and object owners across AWS accounts, Issues in bucket policy or AWS Identity and Access Management (IAM) user policies, User credentials to access Amazon S3, VPC endpoint policy, Missing object, Object encryption by AWS Key Management Service (AWS KMS), Requester Pays enabled on bucket, AWS Organizations service control policy.

You are using a CMK with imported key material. You have been asked by the head of Security to start rotating your key on an annual basis. The key has already been in use for over a year and you have been asked to perform the first rotation this week. How should you do this?

1. Create a new key with new key material and delete the old key
2. Configure automatic key rotation
3. Manually rotate the key
4. Manually import new key material into the CMK

Answer: c

EXPLANATION:

Automatic key rotation is not available for CMKs that have imported key material, you will need to do this manually

You are using a CMK with imported key material. One of your administrators accidentally deleted the key material and you can now no longer access any of your encrypted files. What can you do to fix this?

1. Create a new CMK, import the original key material into the new CMK
2. Re-import the same key material to your CMK
3. Create a new CMK with new key material
4. Import new key material into the CMK

Answer: b

EXPLANATION:

If you delete the key material, the CMK's key state changes to pending import, and the CMK becomes unusable. To use the CMK again, you must reimport the same key material. You cannot import the key material into a different key or import different key material, this will not work.

An external auditor is reviewing your process documentation for a Payment Card Industry (PCI) audit. The scope of this audit will extend to your immediate vendors where you store, transmit or process cardholder data. Because you do store cardholder data in the AWS Cloud, the auditor would like to review AWS's PCI DSS Attestation of Compliance and Responsibility. How would you go about getting this document?

1. AWS IAM Console
2. AWS Macie
3. Submit a Support Case requesting the document
4. AWS Artifact
5. AWS WorkDocs
6. AWS Legal Services website

Answer: d

EXPLANATION:

AWS Artifact provides on-demand downloads of AWS security and compliance documents, such as AWS ISO certifications, Payment Card Industry (PCI), and Service Organization Control (SOC) reports. You can submit the security and compliance documents (also known as audit artifacts) to your auditors or regulators to demonstrate the security and compliance of the AWS infrastructure and services that you use. You can also use these documents as guidelines to evaluate your own cloud architecture and assess the effectiveness of your company's internal controls.

You need to temporarily delegate access to your internal auditor to decrypt encrypted files stored in S3. How can you do this in AWS?

1. Update the user's IAM permissions to add permission to use the CMK
2. Update the Key policy permissions to add permission to use the CMK
3. Use a KMS Grant to grant access to use the CMK
4. Update the S3 bucket policy to add permission for to decrypt the files

Answer: c

EXPLANATION:

With grants you can programmatically delegate the use of KMS CMK to other AWS principals. You can use them to allow access, but not deny it. Grants are typically used to provide temporary permissions or more granular permissions.

You have been asked to create a WORM - Write Once Read Many - archive using AWS. Which of the following services can you use to configure this?

1. Use S3 bucket policies and lifecycle rules
2. Use Glacier lifecycle rules
3. Configure a Vault Lock policy
4. Use Glacier resource policies and lifecycle rules

Answer: c

EXPLANATION:

Glacier Vault Lock allows you to easily deploy and enforce compliance controls for individual Glacier vaults with a vault lock policy. You can specify controls such as Write Once Read Many in a vault lock policy and lock the policy from future edits.

Which statements about Amazon Macie are true?

1. It can prevent user from accessing PII they shouldn't have access to
2. It automatically prevents data from leaving protected zones
3. It can identify PII in S3 buckets
4. It can detect when large quantities of business-critical documents are shared - both internally and externally.
5. It uses NLP methods to understand data.

Answer: c, d, e

EXPLANATION:

Macie doesn't automatically prevent data from leaving protected zones but you can receive notifications when that happens.

A client has asked you to review their system architecture in advance of a compliance audit. Their production environment is setup in a single AWS account that can only be accessed through a monitored and audited bastion host. Their EC2 Linux instances currently use AWS-encrypted EBS volumes and the web server instances sit in a private subnet behind an ALB that terminates TLS using a certificate from ACM. All their web servers share a single Security Group, and their application and data layer servers similarly share one Security Group each. Their S3 objects are stored with SSE-S3. The auditors will require all data to be encrypted at rest and will expect the system to secure against the possibility that TLS certificates might be stolen by would-be spoofers. How would you help this client pass their audit in a cost effective way?

1. Encrypt the S3 objects with OpenPGP locally before re-uploading them to S3.
2. Reconfigure the EC2 EBS volumes to use LUKS OS-Level encryption.
3. Leave the S3 objects alone.
4. Continue to use the ACM for the TLS certificate.
5. Make no changes to the EBS volumes.
6. Deploy CloudHSM and migrate the TLS keys to that service.

Answer: c, d, e

EXPLANATION:

All the measures they have taken with Certificate Manager, S3 encryption and the EBS volumes meet the audit requirements. There is no need for LUKS, CloudHSM or client-side encryption.

Per the requirements of a government contract which your company recently won, you must encrypt all data at rest. Additionally, the material used to generate the encryption key cannot be produced by a third-party because that could result in a vulnerability. You are making use of S3, EBS and RDS as data stores, so these must be encrypted. Which of the following will meet the requirements at the least cost?

1. Initialize a CloudHSM instance. Use it to generate custom encryption keys for each service you will use. When creating an S3 bucket, EBS volume or RDS instance, select the custom CloudHSM key from the dropdown in the setup wizard.
2. Use AMS KMS to create a customer-managed CMK. Create a random 256-bit key and encrypt it with the wrapping key. Import the encrypted key with the import token. When creating S3 buckets, EBS volumes or RDS instances, select the CMK from the dropdown list.
3. Generate a public and private key pair. Upload the public key via the EC2 dashboard. When creating EBS volumes, select encryption and select this public key. When creating S3 buckets, implement a bucket policy which requires encryption at rest only, rejecting other files. Create an RDS instance and select the public key from the dropdown in the setup wizard.
4. Use AMS KMS to create a 256-bit encryption key. Use a grant to only allow access by S3, RDS and EBS. When creating an S3 bucket, select the SSE-KMS option and pick the key from the dropdown. For EBS and RDS, use the CLI to assign the KMS key when creating those instances.

Answer: b

EXPLANATION:

When possible, making use of KMS is much more cost-effective than CloudHSM. We can import our own key material into KMS for creating Customer Master Keys. Because KMS works natively with the services we will be using, we save on any sort of custom integration that CloudHSM would have required.

Your CTO has asked you to design an automated incident response system which will detect and proactively remediate security weaknesses in your AWS account. Which of the following approaches meets the requirement?

1. Use AWS Config rules to monitor for deviations against your desired configurations, send alerts to CloudWatch events and use CloudFormation to automatically remediate security weaknesses
2. Use AWS Config rules to monitor for deviations against your desired configurations, send alerts to CloudWatch events and use Lambda to automatically remediate security weaknesses
3. Install Chaos Monkey to find weaknesses in your environment, log all findings to CloudWatch Logs and use Elastic Beanstalk to proactively remediate security weaknesses
4. Use CloudTrail and GuardDuty to monitor for deviations against your desired configurations, send alerts to CloudWatch Logs and use Lambda to automatically remediate security weaknesses

Answer: b

EXPLANATION:

Through tools such as AWS CloudTrail, Amazon CloudWatch, AWS Config, and AWS Config Rules, it is possible to track, monitor, analyze, and audit events. If these tools identify an event, which is analyzed and qualified as an incident, that may trigger an incident management process and any appropriate response actions necessary to mitigate the incident.

One of your team has mistakenly leaked their access key and secret access key on GitHub. What should you do immediately to secure your account?

1. Isolate all EC2 instances associated with the account
2. Create a new access key
3. Make the access key inactive or delete it
4. Quarantine the account

Answer: b, c

EXPLANATION:

If you suspect that your account is compromised, do the following: Change your AWS account root user password. Delete or rotate all root and AWS Identity and Access Management (IAM) access keys. Delete any potentially compromised IAM users, and change the password for all other IAM users. Delete any resources on your account you didn't create, such as EC2 instances and AMIs, EBS volumes and snapshots, and IAM users. Respond to any notifications you received from AWS Support through the AWS Support Center.

You have recently fallen victim to a malicious attack which resulted in some of your EC2 instances being compromised. As part of your Incident Response Plan, one of the critical steps is to isolate any compromised instances so that they cannot communicate with any other instances in your VPC or with any third party command and control server. Your Head of Security has asked you to recommend a way to do this automatically. What do you recommend?

1. Use Lambda to create a restrictive Security Group which only allows SSH from a single forensic workstation. Use AWS Config to replace the Security Group to the instance as soon as it is detected as being compromised
2. Create a restrictive Security Group which only allows SSH from a single forensic workstation. Use Lambda to replace the Security Group to the instance as soon as it is detected as being compromised
3. Create a restrictive Network ACL which only allows SSH from a single forensic workstation. Use Lambda to replace the ACL to the instance as soon as it is detected as being compromised
4. Create a restrictive Security Group which only allows SSH from a single forensic workstation. Use CloudFormation to apply the Security Group to the instance as soon as it is detected as being compromised
5. Create a restrictive Network ACL which only allows SSH from a single forensic workstation. Use AWS Config to apply the ACL to the instance as soon as it is detected as being compromised

Answer: b

EXPLANATION:

Create a restrictive Security Group which only allows SSH from a single forensic workstation. Use Lambda to replace the existing Security Group with the newly created restrictive Security Group as soon as the instance is detected as being compromised. You cannot apply a Network ACL to an instance because ACLs apply to the whole subnet.

You have been asked to help develop a process for monitoring and alerting staff when malicious or unauthorized activity occurs. Your Chief Security Officer is asking for a solution that is both fast to implement but also very low maintenance. Which option best fits these requirements?

1. Enable AWS GuardDuty to monitor for malicious and unauthorized behavior. Configure a custom blocklist for the IPs which you have seen suspect activity in the past. Setup a Lambda function triggered from a CloudWatch event when anomalies are detected.
2. Use Lambda to periodically reviews CloudFront logs for malicious and unauthorized behavior. Trigger an SES email to the Security Officer.
3. Configure VPC Flow Logs to capture all traffic going in and out of the VPC. Use ElastiSearch to process the logs and trigger a Lambda function whenever malicious or unauthorized behavior is found.
4. Configure CloudWatch to create an event whenever malicious or unauthorized behavior is observed. Trigger an SMS message via SNS to the Security Officer whenever the event happens.
5. Enable AWS Macie to monitor for malicious and unauthorized behavior. Configure a custom allow list for the IPs that were wrongly flagged. Setup a Lambda function triggered from a CloudWatch event when anomalies are detected.

Answer: a

EXPLANATION:

AWS GuardDuty is a managed service that can watch CloudTrail, VPC Flow Logs and DNS Logs, watching for malicious activity. It has a build-in list of suspect IP addresses and you can also upload your own lists of IPs. GuardDuty can trigger CloudWatch events which can then be used for a variety of activities like notifications or automatically responding to a threat. AWS Macie is a service to discovery and classify potentially sensitive information. CloudWatch alone lacks the business rules that are provided with GuardDuty.

You have discovered that your AWS account may have been compromised. What steps should you carry out immediately in order to secure your account?

1. Delete any resources in your account that you didn't create yourself
2. Rotate all CMKs
3. Delete all IAM user accounts
4. Rotate all passwords and IAM access Keys

Answer: a, d

EXPLANATION:

If you suspect that your account is compromised, do the following: Change your AWS account root user password. Delete or rotate all root and AWS Identity and Access Management (IAM) access keys. Delete any potentially compromised IAM users, and change the password for all other IAM users. Delete any resources on your account which you didn't create.

You are running a third party IDS/IPS on EC2. Your application contains extremely sensitive data and it would be a national security disaster if the any of the information was ever leaked. You would like to configure your IDS system to trigger an automated response to contain an attack by immediately shutting down affected systems if an intrusion is detected. Which of the following options would you recommend?

1. Send the IDS application logs to CloudTrail, use CloudWatch to send an SNS notification alerting you of any incidents. Use Lambda to shut down affected systems.
2. Send the application server logs to CloudWatch Logs, use CloudWatch to send an SNS notification alerting you of any incidents. Use Lambda to shut down affected systems.
3. Send the IDS application logs to CloudWatch Logs, use CloudWatch to send an SNS notification alerting you of any incidents. Use Lambda to shut down affected systems.
4. Send the CloudTrail logs to CloudWatch Logs, use CloudWatch to send an SNS notification alerting you of any incidents. Use Lambda to shut down affected systems.

Answer: c

EXPLANATION:

The alerting and remediation should be triggered by the IDS IPS application logs, which can be sent to CloudWatch which will trigger Lambda to shut down the affected systems.

You work for a large organization and many of your departments have access to the AWS console. The company has been using AWS for a number of years, and user permissions have been managed with different designs during that time. You have already reviewed the IAM accounts and policies and deleted any accounts that are no longer required, but your CTO still suspects that many of the users have greater access than they need for their role, with many users having the ability to launch EC2 instances and change Security Group settings at any time, which is against the company Security Policy. What measures can you suggest?

1. Implement event based security using GuardDuty and CloudWatch Events which alerts when a user performs an action which is against company policy and sends an SNS notification
2. Implement event based security using CloudTrail and CloudWatch Events which alerts when a user performs an action which is against company policy and sends an SNS notification
3. Implement event based security using CloudWatch Logs and CloudWatch Events which alerts when a user performs an action which is against company policy and sends an SNS notification
4. Implement event based security using Lambda and CloudWatch Events to alert when a user performs an action which is against company policy and sends an SNS notification

Answer: b

EXPLANATION:

Through tools such as AWS CloudTrail, Amazon CloudWatch, AWS Config, and AWS Config Rules, it is possible to track, monitor, analyze, and audit events. If these tools identify an event, which is analyzed and qualified as an incident, that may trigger an incident management process and any appropriate response actions necessary to mitigate the incident.

What does the following snippet from an IAM policy Statement do ?: { "Effect":"Allow", "Action": "s3:\*", "Resource":["arn:s3:::mybucket/\*" }

1. It allows this user or group no access to all S3 actions to mybucket
2. It allows this user or group full access to certain S3 actions to mybucket
3. It allows this user or group full access to all AWS actions
4. It allows this user or group full access to all S3 actions to mybucket

Answer: d

EXPLANATION:

This snippet from an IAM policy allows this user or group full access to all S3 actions for all buckets.

What is the recommended approach to configuring a mobile application to allow users to sign-in and sign-up to your application via Facebook?

1. Use Cognito as an Identity Broker between your application and the Web Identity Provider
2. Use IAM as an Identity Broker between your application and the Web Identity Provider
3. Use encrypted AWS credentials within your application code and store them locally on the device
4. Use a custom Lambda function to act as an Identity Broker between your application and the Web Identity Provider

Answer: a

EXPLANATION:

Cognito is the preferred Web ID Federation mechanism in AWS

You are working as the lead Security Architect for a large retail bank and you have an external auditor visiting from your regulating body. The auditor will be spending the next two weeks with your team and needs access to read your CloudTrail logs in order to complete their assessment and they already have their own AWS account. How can you configure access for the Auditor to complete their assessment?

1. Create a trust policy enabling read-only access to the log files for the external account. Configure an IAM role in your account allowing the Auditor's AWS account to assume the role.
2. Create an IAM role in your account with an access policy allowing read-only access to the log files. Configure a trust policy in your account allowing the Auditor's AWS account to assume the role.
3. Create an IAM role in your account with an access policy allowing read-only access to the log files. Configure a trust policy in the external account allowing the Auditor's AWS account to assume the role in your account.
4. Create an new guest user account with administrator level access and supply the login credentials to the auditor. When the auditor has completed her work, delete the account.

Answer: b

EXPLANATION:

You need to configure cross account access for the Auditor to enable them to have read only access to the relevant resources in your account - i.e. CloudTrail and the relevant S3 bucket. A trust policy is also required to enable the external account to assume the role.

You are the Head of Security for the Gaming division of a large software company responsible for developing augmented reality games that users can play on their smartphones. Due to the popularity of your latest release, your organization is growing rapidly and as the infrastructure grows, you want to ensure that all new projects have complete segregation between Development, Testing and Production environments, to avoid sharing resources across different environments. Which of the following is the best option to achieve this?

1. Create one AWS account for production services, one for development, and one for testing.
2. Use a single account to centralize information security management and minimize overhead, then use IAM Users, Groups and Roles to control access to each environment.
3. Use a single account to centralize information security management and minimize overhead, then use separate VPCs to segregate each different environment.
4. Create a single AWS account for common project resources. Then create separate AWS accounts on a per project basis.

Answer: a

EXPLANATION:

The Security Best Practices Whitepaper recommends creating separate accounts if you have a requirement to separate your Development, Test and Production environments. Please make sure you read and understand this whitepaper before taking the exam!

Your application consists of a Lambda function which reads and writes items to a DynamoDB table and writes logs to CloudWatch Logs. During testing, you discover that no logs are appearing in CloudWatch even though the function seems to be running successfully. What might be the problem?

1. CloudWatch does not have permission to trigger the function
2. CloudWatch is not enabled
3. DynamoDB does not have permission to trigger the function
4. The function does not have permission to write to DynamoDB
5. The function role does not include permission to write to CloudWatch Logs

Answer: e

EXPLANATION:

The Lambda function will need permissions to read and write to the DynamoDB table and to write logs to CloudWatch Logs. This should be done using an IAM role. The function will assume the role to gain the required access to DynamoDB and CloudWatch Logs

You are working on a project to build an online fashion retail website. The application is running on an auto-scaling group of EC2 instances behind an Elastic Load Balancer. The application needs to access a DynamoDB table to find product information, including sizing measurements, fabric content and care instructions. Promotional images and videos of models wearing the products are stored in S3. How can you give the EC2 instances access to the product data, promotional images and videos?

1. Create an IAM role and assign read only permission to the DynamoDB table and the S3 bucket. Then distribute the IAM credentials to each instance so that the application can access the resources.
2. Create an IAM user and assign read only permission to the DynamoDB table and the S3 bucket. Then distribute the IAM credentials to each instance so that the application can access the resources.
3. Create an IAM role and assign read only permission to the DynamoDB table and the S3 bucket. Attach the role to the EC2 instance.
4. Create an IAM user and assign read only permission to the DynamoDB table and the S3 bucket. Then distribute the Secret Access Key to each instance so that the application can access the resources.

Answer: c

EXPLANATION:

Applications that run on an Amazon EC2 instance and that need access to AWS resources such as Amazon S3 buckets or an Amazon DynamoDB table must have security credentials in order to make programmatic requests to AWS. An IAM role lets you define a set of permissions to access the resources that a user or service needs, but the permissions are not attached to a specific IAM user or group. Instead, IAM users, mobile and EC2-based applications, or AWS services like EC2 can programmatically assume the role. Distributing long-term IAM credentials to each instance is challenging to manage and a potential security risk.

You are reviewing the Key policy attached to one of your CMKs and you notice the following statement: { "Effect": "Deny", "Principal": { "AWS": "arn:aws:iam::111122223333:user/betty" }, "Action": [ "kms:Encrypt" ], "Resource": "\*", "Condition": { "StringEquals": { "kms:ViaService": [ "lambda.us-west-2.amazonaws.com" ] What does this mean?

1. The policy prevents the CMK from being used when the request comes from AWS Lambda on behalf of the user betty
2. The policy prevents the CMK from being used for encrypt operations when the request comes from AWS Lambda on behalf of the user betty
3. The policy prevents the CMK from being used for encrypt operations if the request comes from the user betty
4. The policy allows the CMK from being used for encrypt operations unless the request comes from Lambda in us-west-2
5. The policy prevents the CMK from being used for any encrypt operations unless the request comes from Lambda in us-west-2
6. The policy prevents the CMK from being used for encrypt operations unless the request comes from the user betty

Answer: b

EXPLANATION:

The first part of the statement denies Betty access to use the CMK to perform encrypt operations. The second part of the statement adds the condition that in order for the policy to take effect, the request must come from Lambda. Therefore the policy prevents the CMK from being used by betty for encrypt operations when the request comes from AWS Lambda.

You are designing a pet supplies website, which allows customers to purchase treats and toys for their pets as well as book them in for routine events like grooming, puppy training and health checks. Your application code runs as a number of different Lambda functions, with static web content stored in S3 and persistent customer and product data in DynamoDB tables. During testing, you notice that customers are not able to update their contact details in your application, what could be the reason for this?

1. The Lambda execution role does not have permission to write to S3
2. The customer's IAM role does not have permission to write to DynamoDB
3. The Lambda function is not being triggered when it should
4. The instance role does not have permission to write to DynamoDB
5. The function policy does not have permission to write to DynamoDB
6. The Lambda execution role does not have permission to write to the DynamoDB table

Answer: f

EXPLANATION:

The Lambda function will need permissions to read and write to the DynamoDB table. This should be done using an IAM role.

Your company is responsible for providing market research data to a range of customers in the retail industry. Your application generates monthly reports which are stored in S3 and accessed by your clients who are based all around the world. You have configured a CloudFront distribution and would like to make sure that your customers use CloudFront to access the files rather than accessing them directly using S3. How can you do this?

1. Create an origin access identity
2. Change the permissions on your S3 bucket so that only the origin access identity has read permission
3. Select the Restrict Access To CloudFront Only checkbox in the S3 console
4. Configure Cross Origin Resource Sharing

Answer: a, b

EXPLANATION:

Create an origin access identity, which is a special CloudFront user, and associate the origin access identity with your distribution. Change the permissions either on your Amazon S3 bucket or on the files in your bucket so that only the origin access identity has read permission (or read and download permission). When your users access your Amazon S3 files through CloudFront, the CloudFront origin access identity gets the files on behalf of your users. If your users request files directly by using Amazon S3 URLs, they're denied access.

Your Lambda function needs to write to the ev\_charge\_stations, ev\_networks and ev\_plugs DynamoDB tables. From a security perspective, select the best answer that describes the most suitable policy.

1. Configure the resource and action values as 'arn:aws:dynamodb:region:account-id:table/\*' and 'dynamodb:\*'
2. For the resource value, specify all 3 tables individually, e.g. 'arn:aws:dynamodb:region:account-ID:table/ev\_charge\_stations' and use 'dynamodb:PutItem' as the policy's action value.
3. Use '\*' as the resource value and specify 'dynamodb:PutItem' as the policy's action value.
4. Specify 'dynamodb:PutItem' as the policy's action value and use 'arn:aws:dynamodb:region:account-id:table/ev\_\*' as the value for the resource.

Answer: b

EXPLANATION:

Serverless applications should always follow the principle of 'least privilege'. In this case, this can be achieved by spelling out the exact actions on the specific resources.

You are providing a security administrator with some on-the-job training regarding IAM, roles and policies. The security administrator asks just what the policy evaluation logic is when a request is made? For example, when a user tries to use the AWS Management Console, what is the process that AWS goes through to determine if that request is allowed?

1. First AWS evaluates organizational boundaries of the request in context of the principal. Next, any STS assumed role policies are evaluated. Then, permission boundaries are evaluated against the principals request. Finally, AWS then issues a decision of allow if there were no explicit deny.
2. The AWS service receives the request from the principal. AWS first evaluates the authority of the principal in context of the service. Next, any identity-based or resource-based policies are evaluated. Then, explicit Action statements are evaluated in context of the request. Finally, AWS issues a decision on whether to allow or deny the request.
3. The AWS service receives the request. AWS first authenticates the principal. Next, AWS determines which policy to apply to the request. Then, AWS evaluates the policy types and arranges an order of evaluation. Finally, AWS then processes the policies against the request context to determine if it is allowed.
4. Upon receiving the request, AWS will first evaluate the permissions of the principal and the request. Next, any STS assumed role policies are evaluate. Then, specific user or role permission boundaries are evaluated against the request and the principal. Finally, any Organizational boundaries (SCPs) are evaluated against the request. If there are no explicit deny actions, the request is allowed.

Answer: c

EXPLANATION:

Knowing this logic flow can help troubleshoot security issues.

You have configured your AWS account to enable federation with your corporate Active Directory environment located in your own data center. Which of the following best describes the user authentication process?

1. The user authenticates using the Security Token Service, STS authenticates the user against Active Directory and returns temporary credentials to allow the user to access the console.
2. The user authenticates against Active Directory and provides a SAML token which is passed to AWS STS, STS returns temporary credentials to allow the user to access the console.
3. The user authenticates using the ADFS portal, ADFS authenticates the user against Active Directory and provides a SAML token which is passed to AWS STS, STS returns temporary credentials to allow the user to access the console.
4. The user authenticates using the AWS console, ADFS authenticates the user against Active Directory and provides a SAML token which is passed to AWS STS, STS returns temporary credentials to allow the user to access the console.

Answer: c

EXPLANATION:

Corporate user accesses the corporate Active Directory Federation Services portal sign-in page and provides Active Directory authentication credentials. AD FS authenticates the user against Active Directory. Active Directory returns the user’s information, including AD group membership information. Temporary credentials are returned using STS AssumeRoleWithSAML. The user is authenticated and provided access to the AWS management console.

You have added the following statement to your S3 bucket policy, to give a user access to all items in the bucket called mys3bucket: { "Effect": "Allow", "Action": "\*", "Resource":"arn:aws:s3:::myS3bucket" } However when you try to add the policy, you get the following error: Action does not apply to any resource(s) in statement. What do you need to do resolve this?

1. Change the resource section to: "Resource":"arn:aws:s3:::myS3bucket/"
2. Change the resource section to: "Resource":"arn:aws:s3:::myS3bucket/\*"
3. Change the resource section to: "Resource":"arn:aws:s3:::myS3/bucket/"
4. Change the resource section to: "Resource":"arn:aws:s3:::/S3/myS3bucket"

Answer: b

EXPLANATION:

You need to use a wildcard to refer to all the items in the S3 bucket otherwise the policy will not work

Your web application is running on an auto-scaling group of EC2 instances behind an Elastic Load Balancer. You are receiving reports of multiple malicious requests which are attempting to perform a SQL injection attack. The requests are coming from a group of IP addresses in the same range. Which of the following could you do to block these requests to prevent them from impacting your application?

1. Use AWS GuardDuty to block traffic from this IP address range
2. Use a NACL to block traffic from this IP range
3. Use AWS WAF to block SQL traffic from this IP address range
4. Use AWS Inspector to block traffic from this IP address range

Answer: b, c

EXPLANATION:

AWS WAF is a web application firewall that helps protect web applications from attacks by allowing you to configure rules that allow, block, or monitor web requests based on conditions that you define. These conditions include IP addresses, HTTP headers, HTTP body, URI strings, SQL injection and cross-site scripting. Security Groups cannot be configured to deny access to a group of servers. GuardDuty is a Threat Detection service and cannot be used to block traffic. Inspector assesses applications for exposure, vulnerabilities, and deviations from best practices, it cannot be used to block traffic.

You have been asked to design an IPS/IDS solution to protect your AWS infrastructure from possible incidents, violations and threats. Which of the following do you recommend?

1. Use iptables
2. Use VPC Flow logs
3. Use Windows firewall
4. Use a third party solution
5. Search the AWS Marketplace for a suitable solution
6. Use AWS Shield
7. Use GuardDuty

Answer: d, e

EXPLANATION:

Intrusion Detection is the process of monitoring the events occurring in your network, analyzing for signs of possible incidents, violations, or threats. Intrusion Prevention is the process of performing Intrusion Detection and then stopping the detected incidents. AWS acknowledge that they do not provide IPS/IDS. Instead they suggest that third-party software can be used to provide additional functionality such as deep packet inspection, IPS/IDS, or network threat protection. Search for IPS on AWS Marketplace and you will find a range of suitable products!

On your last Security Penetration Test Audit, the auditors noticed that you were not effectively protecting against SQL injection attacks. Even though you don't have any resources that are vulnerable to that type of attack, your Chief Information Security Officer insists you do something. Which steps will allow you to most efficiently protect against SQL injection attacks?

1. Ensure all accounts are members of an organization in the AWS Organizations. Use CloudFormation to implement request restrictions for SQL code on the CloudFront distributions across all accounts. Setup a CloudWatch event to notify administrators if requests with SQL code are seen.
2. Create a custom NACL filter to check requests for SQL code. Use Lambda to apply the NACL across all public subnets.
3. Ensure all accounts are members of an organization in the AWS Organizations service and use Consolidated Billing. Subscribe to AWS Shield to automatically enable SQL injection protection across all sub-accounts.
4. Use AWS WAF to deny requests that contain SQL code

Answer: d

EXPLANATION:

Firewall Manager is a very effective way of managing WAF rules across many WAF instances and accounts. It does require that the accounts be linked as an AWS Organization.

You would like to use AWS WAF to protect your website. How must your website receive incoming traffic if you are to protect it using AWS WAF?

1. Using a direct HTTPS connection to the EC2 instance
2. Using a Classic Load Balancer
3. Using an Application Load Balancer
4. Using a Network Load Balancer
5. Using S3 website endpoint
6. Using a CloudFront CDN

Answer: c, f

EXPLANATION:

AWS WAF protects websites against SQL injection and cross-site scripting attacks. WAF is closely integrated with CloudFront and Application Load Balancer as well and can be used to protect websites which are accessed using these services. You can deploy AWS WAF on either Amazon CloudFront as part of your CDN solution, the Application Load Balancer that fronts your web servers or origin servers running on EC2, or Amazon API Gateway for your APIs.

You have configured a bastion host to enable your systems administrators to log in to their Linux systems from their corporate workstations. Which of the following security group rules will you need to configure to allow the team to securely access the bastion?

1. Create an inbound rule allowing access on port 22 for the corporate workstations. Create a corresponding outbound rule allowing access to the corporate workstations on ephemeral ports
2. Create an inbound rule allowing access on port 22 for the corporate workstations
3. Create an inbound rule allowing access on port 22 for the corporate workstations. Create a corresponding outbound rule allowing access to the corporate workstations on port 22
4. Create an inbound rule allowing access on port 22 for 10.0.0.0/0

Answer: b

EXPLANATION:

Security Groups are stateless, so no corresponding outbound rule is required. You should only enable access to the corporate workstations that need it, not to the whole world.

You have been asked to investigate whether unrestricted SSH access is enabled to any of your EC2 instances. How should you approach this?

1. Run a manual check on each EC2 instance
2. Use Trusted Advisor to report Security Groups configured with unrestricted access
3. Use Kali Linux to run a penetration test
4. Use AWS Config to check which Security Groups are configured with unrestricted access

Answer: b

EXPLANATION:

Trusted Advisor checks security groups for rules that allow unrestricted access to specific ports. AWS Config can alert you to any modifications to a security group but will not perform a check for unrestricted access. Running a manual check or a full penetration test is not an efficient way to get this information.

You are designing a secure website which will deliver content over HTTPS, users will only be able to access the website using CloudFront. You have already purchased a registered domain name for your company and you are planning to use ACM to manage your SSL/TLS X.509 certificate. In which region should you request the certificate?

1. Use the same region that the CloudFront edge location is in
2. us-east-1
3. Use the same region that your website is located in
4. Use the region where the majority of your users are located
5. us-east-2

Answer: b

EXPLANATION:

If you want to require HTTPS between viewers and CloudFront, you must change the AWS region to US East 1 (N. Virginia) in the AWS Certificate Manager console before you request or import a certificate.

Which of the following services can AWS WAF be deployed with?

1. Application Load Balancer
2. Elasticache
3. S3 Endpoint
4. Lambda
5. CloudFront

Answer: a, e

EXPLANATION:

AWS WAF can be deployed on Amazon CloudFront, the Application Load Balancer, and Amazon API Gateway. As part of Amazon CloudFront it can be part of your Content Distribution Network protecting your resources and content at the Edge locations. As part of the Application Load Balancer it can protect your origin web servers running behind the ALBs. As part of Amazon API Gateway, it can help secure and protect your REST APIs.

You are working as a Security Architect at a large retail bank, designing a new secure website which will enable customers to apply for a personal loan online. You would like to protect your application from attacks such as SQL injection and cross-site scripting. Which of the following AWS services would you consider using when planning this website?

1. CloudWatch
2. AWS Shield
3. AWS WAF
4. Application Load Balancer
5. CloudFront
6. Network Load Balancer

Answer: c, d, e

EXPLANATION:

AWS WAF protects websites against SQL injection and cross-site scripting attacks. WAF is closely integrated with CloudFront and Application Load Balancer.

You are designing an e-commerce application which will run on a number of EC2 instances behind and Application Load Balancer, storing product and customer data in DynamoDB and product images in S3. In your previous role at another company, your systems were frequently targeted by SQL injection and cross-site scripting attacks. Which of the following can be used to protect against this type of attack?

1. AWS Trusted Advisor
2. AWS WAF
3. AWS Shield
4. Amazon Inspector

Answer: b

EXPLANATION:

AWS WAF is a web application firewall that helps protect web applications from attacks by allowing you to configure rules that allow, block, or monitor web requests based on conditions that you define. These conditions include IP addresses, HTTP headers, HTTP body, URI strings, SQL injection and cross-site scripting.

You are troubleshooting a CloudFront setup for a client. The client has an Apache web server that is configured for both HTTP and HTTPS. It has a valid TLS certificate acquired from LetsEncrypt.org. They have also configured the Apache server to redirect HTTP to HTTPS to ensure a safe connection. In front of that web server, they have created a CloudFront distribution with the web server as the origin. The distribution is set for GET and HEAD HTTP methods using an Origin Protocol Policy of HTTP only. When a web browser tries to connect to the CloudFront URL, the browser just spins and never reaches the web server. However, when a web browser points to the web server itself, we get the page properly. Which of the following if done by themselves would most likely fix the problem?

1. Add the OPTION HTTP methods on the CloudFront distribution.
2. Enable CloudFront to forward cookies and enable query string forwarding.
3. Remove the redirection policy on the origin server and allow it to accept HTTP.
4. Use an ALB instead of CloudFront to provide content caching.
5. Add POST and PUT HTTP methods on the CloudFront distribution.
6. Change the CloudFront distribution origin protocol policy to use only HTTPS.

Answer: c, f

EXPLANATION:

With CloudFront only configured for HTTP Only, we have a loop when the web server redirects HTTP to HTTPS. We can either enable HTTPS on CloudFront or disable the redirection policy on the Apache server.

Your company website uses a combination of EC2 instances and S3. Your Head Of Security has asked you to implement a solution to help protect the website from DDoS attacks. Which of the following AWS Services would you recommend?

1. Amazon GuardDuty
2. AWS Trusted Advisor
3. AWS WAF
4. CloudFront
5. Amazon Inspector
6. AWS Shield

Answer: c, d, f

EXPLANATION:

When attempting to protect your application against DDoS attacks, services such as Route 53, Amazon CloudFront, Elastic Load Balancing, and AWS WAF can all be used to control and absorb traffic, and deflect unwanted requests. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS.

You would like to use your own DNS server rather than using the Amazon DNS server. Which of the following are valid steps to configuring this?

1. Create a new DHCP option set for your VPC, specifying the name of your own DNS server
2. Update your Security Groups and Network ACLs to prevent applications from querying the Amazon DNS Server
3. Update the DHCP option set for your VPC, specifying the IP address your own DNS server
4. Create a new DHCP option set for your VPC, specifying the IP address your own DNS server

Answer: d

EXPLANATION:

By default, AWS provides the Amazon DNS server. To use your own DNS server you can create a new set of DHCP options for your VPC. The default DHCP option set specifies AmazonProvidedDNS but you can provide the IP address of up to 4 of your own DNS servers. You cannot update the existing option set, you must delete it and create a new one.

You are working for a charity which is working to monitor global climate change. You have created a VPC which has a private subnet and a public subnet with a NAT Gateway. You have been asked to provision a number of EC2 instances which will run an application which needs to download publicly available climate statistics from a government website. Which of the following options is the most secure way to configure this?

1. Launch the EC2 instances in the private subnet, route internet-bound traffic to the NAT Gateway in the public subnet to access the government website
2. Launch the EC2 instances and a NAT Gateway in the public subnet, route internet-bound traffic to the NAT gateway to access the government website
3. Launch the EC2 instances in the public subnet, route internet-bound traffic to the NAT Gateway to access the government website
4. Launch the EC2 instances in the private subnet, launch a NAT Gateway in the private subnet, route internet-bound traffic to the NAT gateway to access the government website
5. Launch the EC2 instances in the public subnet, launch a NAT Gateway in the private subnet, route internet-bound traffic to the NAT gateway to access the government website

Answer: a

EXPLANATION:

EC2 instances in the private subnet can access the Internet by using a NAT Gateway that resides in the public subnet due to normal routing.

You are helping a client migrate over an internal application from on-prem to AWS. The application landscape on AWS will consist of a fleet of EC2 instances behind an Application Load Balancer. The application client is an in-house custom application that communicates to the server via HTTPS and is used by around 40,000 users globally across several business units. The same exact application and landscape will be deployed in US-WEST-2 as well as EU-CENTRAL-1. Route 53 will then be used to redirect users to the closest region. When the application was originally built, they chose to use a self-signed 2048-bit RSA X.509 certificate (SSL/TLS server certificate) and embedded the self-signed certificate information into the in-house custom client application. Regarding the SSL certificate, which activities are both feasible and minimize extra administrative work?

1. Use Service Catalog to push an update of the in-house app which includes an updated certificate and CA chain. Generate a new private certificate using OpenSSL. Import the new certificate to Certificate Manager in US-EAST-1. Assign the new certificate to the Application Load Balancers in all regions.
2. Create a new Certificate Authority within Certificate Manager and import the existing certificate. Generate a new certificate, CA chain and private key and push an update for the application. Assign the new certificate to the Application Load Balancers in all regions.
3. Import the existing certificate and private key into Certificate Manager in both regions. Assign that imported certificate to the Application Load Balancers using their respective regionally imported certificate.
4. Create a new public SSL/TLS certificate using Certificate Manager and configure the common name and OU to match the existing certificate. Assign the new certificate to the Application Load Balancers in all regions.
5. Purchase a new public SSL/TLS certificate from a third-party CA. Upload the certificate to Certificate Manager and assign that certificate to the Application Load Balancers.

Answer: c

EXPLANATION:

You can import private certificates into Certificate Manager and assign them to all the same resources you can with generated certificates, including an ALB. Also note that Certificate Manager is a regional service so certificates must be imported in each region where they will be used. The other options in this question would either require you to update the certificate on the client or requires unnecessary steps to resolve the challenge.

You are designing a bastion host to enable your systems administrators to securely access your Linux EC2 instances. You need to explain to the provisioning team how you want them to configure the system. Which of the following options will you recommend?

1. Deploy the bastion host in the public subnet of your VPC
2. Deploy the bastion host in the private subnet of your VPC
3. Limit inbound connections to the bastion host to the CIDR range that will be used by your administrators
4. Configure your Security Group to allow inbound connections on port 25
5. Configure your Security Group to allow inbound connections on port 22
6. Limit access to the bastion hosts to a CIDR range of 10.0.0.0/0

Answer: a, c, e

EXPLANATION:

Access to bastion hosts should be locked down to known CIDR ranges for ingress. Ports should be limited to allow only the necessary access to the bastion hosts. For Linux bastion hosts, TCP port 22 for SSH connections is typically the only port allowed. Bastion hosts are deployed in the public subnets of the VPC.

An external auditor has been commissioned to review activity in your AWS account. She has asked to review all the API events in your account over the next two weeks. Your department currently has 7 AWS accounts and the auditor will need to assess each one. Which of the following options is the best way to configure this?

1. Configure CloudTrail in each account and send the logs to an S3 bucket in each account. Grant the auditor read only access to each S3 bucket to read the logs
2. Configure CloudTrail in each account and send the logs to a single S3 bucket. Grant the auditor read only access to the S3 bucket to read the logs
3. Configure CloudWatch in each account and send the logs to an S3 bucket in each account. Grant the auditor read only access to each S3 bucket to read the logs
4. Configure a new AWS Organization and add all the accounts to the organization, then configure CloudTrail for the primary account and grant the auditor access to read the logs

Answer: b

EXPLANATION:

You can have CloudTrail deliver log files from multiple AWS accounts into a single Amazon S3 bucket. Turn on CloudTrail in the account where the destination bucket will belong, Update the bucket policy on your destination bucket to grant cross-account permissions to CloudTrail, turn on CloudTrail in the other accounts you want, configure CloudTrail in these accounts to use the same bucket belonging to the account that you specified in step 1.

You are running your web application on a number of EC2 instances behind an Application Load Balancer. You have configured the application to send error logs and security logs to CloudWatch logs. Persistent data generated by the application is stored in DynamoDB and website images and static content is stored in S3. Over the weekend the application crashed a number of times, causing a serious system outage. The application support team managed to get the system back online, but on Monday morning when they tried to access the logs to analyze what went wrong, they discover that no logs exist for this application. What might be the problem?

1. The Instance role does not have permission to write to CloudWatch Logs
2. The CloudWatch Logs agent is not running
3. The CloudWatch Logs agent does not have permission to read DynamoDB tables
4. The IAM user does not have permission to write to CloudWatch Logs
5. DynamoDB does not have permission to write to CloudWatch Logs
6. The CloudWatch Logs agent is not installed

Answer: a, b, f

EXPLANATION:

Access to AWS resources requires permissions. You need to create an IAM role that includes the permissions you need for the CloudWatch agent to write logs to CloudWatch. The CloudWatch agent must be installed and running in order for the EC2 instance to send application logs to CloudWatch Logs.

You would like to analyse the API activity in your AWS account and have the ability to isolate activity by attributes, such as source IP address and user. Which of the following AWS services can you use to do this?

1. GuardDuty
2. Network ACLs
3. VPC Flow Logs
4. CloudTrail
5. Athena
6. CloudWatch Logs

Answer: d, e

EXPLANATION:

CloudTrail is used to record all API activity in your account. Using Athena with CloudTrail logs is a powerful way to enhance your analysis of AWS service activity. For example, you can use standard SQL queries to identify trends and further query activity by attributes, such as source IP address or user.

You are trying to debug your Lambda function, however you notice that you are not receiving data level events from either Lambda or S3. What could be the reason for this?

1. You need to enable data events in Lambda and S3
2. You need to enable data events in CloudWatch
3. Your function does not have permission to write data events and you need to enable cross origin resource sharing to allow S3 to send data events to CloudTrail
4. Data events are disabled by default
5. Your function does not have permission to write data events to CloudWatch, or your S3 bucket is not authorized to log data events to CloudWatch

Answer: d, e

EXPLANATION:

Data events provide insight into the resource operations performed on or within a resource, these events are often high-volume activities. Example data events include S3 object-level API activity and Lambda function execution activity , the Invoke API. Data events are disabled by default when you create a trail. To record CloudTrail data events, you must explicitly add the supported resources or resource types for which you want to collect activity to a trail.

You are supporting an in-house developed online credit checking application which generates a large amount of logging data, including security alerts and critical warnings. The application is mission critical for your company and your CEO wants to be informed immediately if the logs generate any security related messages. How can you configure this?

1. Configure the application to deliver the logs to an S3 bucket, create a Lambda function to scan the files and generate an SNS notification for any security related events
2. Configure the application to deliver the logs to CloudWatch Logs, then use a custom metric filter to trigger alarms and notifications
3. Configure the application to deliver the logs to CloudTrail, then use a custom metric filter to trigger alarms and notifications
4. Use Amazon Inspector to review the log files and launch a Lambda function to generate an SNS notification for any security related events

Answer: b

EXPLANATION:

You can use CloudWatch Logs to monitor applications and systems using log data. For example, you can monitor application logs for specific literal terms, or count the number of occurrences of a literal term at a particular position in log data. When the term you are searching for is found, CloudWatch Logs reports the data to a CloudWatch metric that you specify.

You have been asked to make sure that insecure protocols like Telnet and FTP are disabled on all of your EC2 instances. You would like to perform a regular automated review of your environment. Which of the following solutions will meet this requirement?

1. Use a CloudWatch Event to trigger AWS Config to evaluate the restricted-common-ports rule for every EC2 instance.
2. Use CloudWatch Events to schedule Amazon Inspector to complete a Runtime Behaviour Analysis check on every EC2 instance.
3. Use a Lambda scheduled event to launch Trusted Advisor to run a check on security best practices
4. Use a scheduled Lambda event to trigger AWS Config to evaluate the restricted-common-ports rule for every EC2 instance.

Answer: b

EXPLANATION:

You can configure Amazon Inspector as a target for CloudWatch Events. The runtime behaviour package checks for insecure protocols like Telnet, FTP, HTTP, IMAP, rlogin etc. Neither the AWS Config restricted-common-ports check or Trusted Advisor will give you this information.

You are responsible for the security profile of a number of mission critical applications at a large global telecommunications company. Your team lead asks you to propose a solution to trace all changes made to the AWS infrastructure. You must also prevent any evidence from tampering or deletion by malicious actors attempting to conceal unauthorized activities. Which of the following approaches do you propose?

1. Only allow the Security Team permission to make changes in CloudTrail.
2. Verify the MD5 checksum value of the log files to check if they have been tampered with
3. Enable CloudTrail in all AWS regions and send logs to a dedicated S3 bucket. Grant read only access to the Security Team members who need to review the logs.
4. Use AWS Config to notify you of any changes made to your AWS infrastructure. Send logs to a dedicated S3 bucket. Grant read only access to the Security Team members who need to review the logs.
5. Use CloudWatch Logs to log any changes made to your AWS infrastructure. Send logs to a dedicated S3 bucket. Grant read only access to the Security Team members who need to review the logs.

Answer: a, c

EXPLANATION:

AWS CloudTrail is a web service that records activity made on your account and delivers log files to your Amazon S3 bucket. It is recommended to use a dedicated S3 bucket for CloudTrail logs. When you apply a trail to all regions, CloudTrail uses the trail that you create in a particular region to create trails with identical configurations in all other regions in your account. To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it, you can use CloudTrail log file integrity validation.

Your CTO has asked you to make sure all EC2 instances are using encryption at rest for their data volumes. You have been tasked with configuring an automated notification system to send a notification if there are any EC2 instances with EBS volumes that are not protected by encryption. Which of the following is the best approach?

1. Use GuardDuty to check for unencrypted volumes and send an SNS notification
2. Create a Lambda function to check for unencrypted volumes and send an SNS notification
3. Use an AWS Config rule to check for unencrypted volumes and send an SNS notification
4. Use Trusted Advisor to check for unencrypted volumes and send an SNS notification

Answer: c

EXPLANATION:

AWS Config includes a managed rule which can check whether the EBS volumes that are in an attached state are encrypted.

You suspect that someone in your organization has recently been making unauthorized changes to EC2 instances in your account. Which of the following can you use to investigate what has happened and who is responsible?

1. Write a Lambda function to query the CloudTrail data and cross reference against the current configuration of your EC2 instances
2. Generate a Credential Report to find out who has been running EC2 commands and use AWS Config to compare the current configuration to the previous configuration
3. Use Athena to query your CloudWatch data and use Trusted Advisor to compare the current configuration to the previous configuration
4. Use Athena to query your CloudTrail data and use AWS Config to compare the current configuration to the previous configuration

Answer: d

EXPLANATION:

AWS Config maintains historical records of the configuration items of your resources from the time you start the configuration recorder. Athena can be used to run SQL queries on CloudTrail logs stored in S3.

You have multiple separate AWS accounts for each department in your company. You have enabled CloudTrail logging for each of these accounts and configured each one to send logs to the same S3 bucket. However some of your accounts have not been sending any logs. What do you think the problem is?

1. For security reasons, is not possible to send CloudTrail logs to a bucket that is not owned by the same AWS account generating the logs
2. The accounts do not have permission to write to the S3 bucket
3. You need to configure an origin access identity with permission to write to the S3 bucket
4. You need to configure cross origin resource sharing to enable CloudTrail to write to an S3 bucket in another account

Answer: b

EXPLANATION:

You can have CloudTrail deliver log files from multiple AWS accounts into a single Amazon S3 bucket. To accomplish this, turn on CloudTrail in the account where the destination bucket will belong, configure the bucket policy to allow cross-account permission. Turn on CloudTrail in the other accounts, configure all accounts to log to the destination bucket.

Your team suspects that one of your instances has been compromised and is attempting to communicate with a command and control server. Which services can you use to investigate this?

1. Amazon Inspector
2. Trusted Advisor
3. VPC Flow Logs
4. GuardDuty

Answer: c, d

EXPLANATION:

This kind of activity can be detected using GuardDuty. You can also investigate network flow in and out of your VPC by reviewing the VPC flow logs. Trusted Advisor can make security recommendations based on best practices. Amazon Inspector is an automated security assessment service that helps you test the network accessibility of your Amazon EC2 instances and the security state of your applications running on the instances.

You are attempting to access the CloudTrail logs to investigate a suspected security breach. However you are unable to access the logs. You have checked your IAM permissions and your user account definitely has permission to describe CloudTrail logs and look up events. What could be the problem?

1. You do not have permission to use the CloudTrail APIs
2. You do not have permission to use the CMK to decrypt the logs
3. You do not have permission to turn on CloudTrail
4. You do not have read permission for the S3 bucket

Answer: b, d

EXPLANATION:

You must have S3 read permission on the bucket. If you are using KMS to encrypt the logs, any user who accesses the must be granted decrypt permission by the CMK policy.

You have noticed some strange activity in your AWS accounts and have engaged an external consultancy to review your accounts and try to understand what is going on. The consultant has asked to review all the API events in your account over the next two weeks. Your department currently has a number of different accounts, and you are struggling to keep track of everything. The consultant needs to check what is going on in each of these accounts. Which of the following options is the best way to enable this?

1. Configure CloudTrail in each account and send the logs to a separate S3 bucket. Grant read only access to CloudTrail and the S3 bucket for the consultant.
2. Create a new AWS Organization, add each account to the Organization, then enable CloudTrail in each account. Grant the consultant read only access to CloudWatch and the S3 bucket.
3. Create a new AWS Organization, add each account to the Organization, then create a single CloudTrail which covers all accounts. Grant read only access to CloudTrail and the S3 bucket for the consultant.
4. Configure CloudWatch Logs in each account and send the logs to a single S3 bucket. Grant read only access to the S3 bucket for the consultant.

Answer: c

EXPLANATION:

With the accounts in an AWS Organization, you can create a single trail that covers all accounts.