



Vendor: Amazon

Exam Code: AWS-Certified-Security-Specialty

Exam Name: AWS Certified Security - Specialty (SCS-C01)

Version: 22.081

Important Notice

Product

Our Product Manager keeps an eye for Exam updates by Vendors. Free update is available within One year after your purchase.

You can login member center and download the latest product anytime. (Product downloaded from member center is always the latest.)

PS: Ensure you can pass the exam, please check the latest product in 2-3 days before the exam again.

Feedback

We devote to promote the product quality and the grade of service to ensure customers interest.

If you have any questions about our product, please provide Exam Number, Version, Page Number, Question Number, and your Login Account to us, please contact us at support@passleader.com and our technical experts will provide support in 24 hours.

Copyright

The product of each order has its own encryption code, so you should use it independently.

If anyone who share the file we will disable the free update and account access.

Any unauthorized changes will be inflicted legal punishment. We will reserve the right of final explanation for this statement.

Order ID: ****

PayPal Name: ****

PayPal ID: ****

QUESTION 1

An application outputs logs to a text file. The logs must be continuously monitored for security incidents.

Which design will meet the requirements with MINIMUM effort?

- A. Create a scheduled process to copy the component's logs into Amazon S3.
Use S3 events to trigger a Lambda function that updates Amazon CloudWatch metrics with the log data. Set up CloudWatch alerts based on the metrics.
- B. Install and configure the Amazon CloudWatch Logs agent on the application's EC2 instance.
Create a CloudWatch metric filter to monitor the application logs.
Set up CloudWatch alerts based on the metrics.
- C. Create a scheduled process to copy the application log files to AWS CloudTrail.
Use S3 events to trigger Lambda functions that update CloudWatch metrics with the log data.
Set up CloudWatch alerts based on the metrics.
- D. Create a file watcher that copies data to Amazon Kinesis when the application writes to the log file.
Have Kinesis trigger a Lambda function to update Amazon CloudWatch metrics with the log data.
Set up CloudWatch alerts based on the metrics.

Answer: B

Explanation:

Justification: Using scheduled process to monitor continuously is not right and using lambda will more create more process layers and not the best solution.

Better to use CW agent in ec2 instances to monitor continuously -> stream to cw logs, filter and create alerts.

QUESTION 2

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

Which solution is the SIMPLEST way to allow the authentication of users using their social media identities?

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

Answer: A

Explanation:

<https://aws.amazon.com/cn/cognito/>

QUESTION 3

A Security Engineer has been asked to troubleshoot inbound connectivity to a web server. This single web server is not receiving inbound connections from the internet, whereas all other web servers are functioning properly.

The architecture includes network ACLs, security groups, and a virtual security appliance. In addition, the Development team has implemented Application Load Balancers (ALBs) to distribute the load across all web servers. It is a requirement that traffic between the web servers and the internet flow through the virtual security appliance.

The Security Engineer has verified the following:

1. The rule set in the Security Groups is correct
2. The rule set in the network ACLs is correct
3. The rule set in the virtual appliance is correct

Which of the following are other valid items to troubleshoot in this scenario? (Choose two.)

- A. Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to a NAT gateway.
- B. Verify which Security Group is applied to the particular web server's elastic network interface (ENI).
- C. Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to the virtual security appliance.
- D. Verify the registered targets in the ALB.
- E. Verify that the 0.0.0.0/0 route in the public subnet points to a NAT gateway.

Answer: BD

QUESTION 4

Which approach will generate automated security alerts should too many unauthorized AWS API requests be identified?

- A. Create an Amazon CloudWatch metric filter that looks for API call error codes and then implement an alarm based on that metric's rate.
- B. Configure AWS CloudTrail to stream event data to Amazon Kinesis. Configure an AWS Lambda function on the stream to alarm when the threshold has been exceeded.
- C. Run an Amazon Athena SQL query against CloudTrail log files. Use Amazon QuickSight to create an operational dashboard.
- D. Use the Amazon Personal Health Dashboard to monitor the account's use of AWS services, and raise an alert if service error rates increase.

Answer: A

Explanation:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html#cloudwatch-alarms-for-cloudtrail-authorization-failures>

Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>. In the navigation pane, choose Logs. In the list of log groups, select the check box next to the log group that you created for CloudTrail log events. Choose Create Metric Filter. On the Define Logs Metric Filter screen, choose Filter Pattern and then type the following: { (\$.errorCode = "UnauthorizedOperation") || (\$.errorCode = "AccessDenied*") } Choose Assign Metric. For Filter Name, type AuthorizationFailures. For Metric Namespace, type CloudTrailMetrics. For Metric Name, type AuthorizationFailureCount.

QUESTION 5

A company has multiple production AWS accounts. Each account has AWS CloudTrail configured to log to a single Amazon S3 bucket in a central account. Two of the production accounts have trails that are not logging anything to the S3 bucket.

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

- A. Verify that the log file prefix is set to the name of the S3 bucket where the logs should go.
- B. Verify that the S3 bucket policy allows access for CloudTrail from the production AWS account

- IDs.
- C. Create a new CloudTrail configuration in the account, and configure it to log to the account's S3 bucket.
 - D. Confirm in the CloudTrail Console that each trail is active and healthy.
 - E. Open the global CloudTrail configuration in the master account, and verify that the storage location is set to the correct S3 bucket.
 - F. Confirm in the CloudTrail Console that the S3 bucket name is set correctly.

Answer: BDF

Explanation:

E - Can't be right since other accounts are able to log.

QUESTION 6

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

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

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

Answer: AB

Explanation:

https://acloud.guru/forums/aws-certified-security-specialty/discussion/-Lm5A3w6_NybQPhh6tRP/Cloudwatch%20Log%20question

QUESTION 7

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

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

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

Answer: D

Explanation:

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

QUESTION 8

An employee accidentally exposed an AWS access key and secret access key during a public

presentation. The company Security Engineer immediately disabled the key.

How can the Engineer assess the impact of the key exposure and ensure that the credentials were not misused? (Choose two.)

- A. Analyze AWS CloudTrail for activity.
- B. Analyze Amazon CloudWatch Logs for activity.
- C. Download and analyze the IAM Use report from AWS Trusted Advisor.
- D. Analyze the resource inventory in AWS Config for IAM user activity.
- E. Download and analyze a credential report from IAM.

Answer: AE

QUESTION 9

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

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

Answer: A

Explanation:

Network ACL are not stateful. They are stateless.

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

QUESTION 10

A distributed web application is installed across several EC2 instances in public subnets residing in two Availability Zones. Apache logs show several intermittent brute-force attacks from hundreds of IP addresses at the layer 7 level over the past six months.

What would be the BEST way to reduce the potential impact of these attacks in the future?

- A. Use custom route tables to prevent malicious traffic from routing to the instances.
- B. Update security groups to deny traffic from the originating source IP addresses.
- C. Use network ACLs.
- D. Install intrusion prevention software (IPS) on each instance.

Answer: D

Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html>

NACL has limit 20 (can increase to maximum 40 rule), and more rule will make more low-latency.

QUESTION 11

A company plans to move most of its IT infrastructure to AWS. They want to leverage their existing on-premises Active Directory as an identity provider for AWS.

Which combination of steps should a Security Engineer take to federate the company's on-premises Active Directory with AWS? (Choose two.)

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

Answer: AD

Explanation:

AWS cloud directory is its own directory service. To extend existing AD you use an AD connector. Then add AD as a relying trust between AWS.

https://docs.aws.amazon.com/directoryservice/latest/adminguide/directory_ad_connector.html

QUESTION 12

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

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

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

Answer: ADF

QUESTION 13

A financial institution has the following security requirements:

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

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

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

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

E. Establish a two-way trust between the new and existing Active Directory services.

Answer: AD

Explanation:

Deploy a new forest/domain on AWS with one-way trust. If you are planning on leveraging credentials from an on-premises AD on AWS member servers, you must establish at least a one-way trust to the Active Directory running on AWS. In this model, the AWS domain becomes the resource domain where computer objects are located and on-premises domain becomes the account domain.

<https://d1.awsstatic.com/whitepapers/adds-on-aws.pdf>

QUESTION 14

An organization wants to be alerted when an unauthorized Amazon EC2 instance in its VPC performs a network port scan against other instances in the VPC. When the Security team performs its own internal tests in a separate account by using pre-approved third-party scanners from the AWS Marketplace, the Security team also then receives multiple Amazon GuardDuty events from Amazon CloudWatch alerting on its test activities.

How can the Security team suppress alerts about authorized security tests while still receiving alerts about the unauthorized activity?

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

Answer: B

Explanation:

To whitelist an IP address from showing up in GuardDuty, you add it to the trusted IP list.

https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_upload_lists.html

QUESTION 15

The Security team believes that a former employee may have gained unauthorized access to AWS resources sometime in the past 3 months by using an identified access key.

What approach would enable the Security team to find out what the former employee may have done within AWS?

- A. Use the AWS CloudTrail console to search for user activity.
- B. Use the Amazon CloudWatch Logs console to filter CloudTrail data by user.
- C. Use AWS Config to see what actions were taken by the user.
- D. Use Amazon Athena to query CloudTrail logs stored in Amazon S3.

Answer: A

Explanation:

You can use CloudTrail to search event history for the last 90 days. You can use CloudWatch queries to search API history beyond the last 90 days. You can use Athena to query CloudTrail logs over the last 90 days.

<https://aws.amazon.com/premiumsupport/knowledge-center/view-iam-history/>

QUESTION 16

The Security Engineer implemented a new vault lock policy for 10TB of data and called initiate-12 hours ago. The Audit team identified a typo that is allowing incorrect access to the vault. vault-lock

What is the MOST cost-effective way to correct this?

- A. Call the abort-vault-lock operation, fix the typo, and call the initiate-vault-lock again.
- B. Copy the vault data to Amazon S3, delete the vault, and create a new vault with the data.
- C. Update the policy, keeping the vault lock in place.
- D. Update the policy and call initiate-vault-lock again to apply the new policy.

Answer: A

Explanation:

Initiate the lock by attaching a vault lock policy to your vault, which sets the lock to an in-progress state and returns a lock ID. While in the in-progress state, you have 24 hours to validate your vault lock policy before the lock ID expires. Use the lock ID to complete the lock process. If the vault lock policy doesn't work as expected, you can abort the lock and restart from the beginning. For information on how to use the S3 Glacier API to lock a vault, see Locking a Vault by Using the Amazon S3 Glacier API.

<https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-lock-policy.html>

QUESTION 17

A company wants to control access to its AWS resources by using identities and groups that are defined in its existing Microsoft Active Directory.

What must the company create in its AWS account to map permissions for AWS services to Active Directory user attributes?

- A. AWS IAM groups
- B. AWS IAM users
- C. AWS IAM roles
- D. AWS IAM access keys

Answer: C

Explanation:

<https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/>

QUESTION 18

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

Explanation:

Using IAM to grant access to a Third-Party Account
1) Create a role to provide access to the required resources
1.1) Create a role policy that specifies the AWS Account ID to be accessed, "sts:AssumeRole" as action, and "sts:ExternalID" as condition
1.2) Create a role using the role policy just created
1.3) Assign a resource policy to the role. This will provide permission to access resource ARNs to the auditor
2) Repeat steps 1 and 2 on all AWS accounts
3) The auditor connects to the AWS account AWS Security Token Service (STS). The auditor must provide its ExternalID from step 1.2, the ARN of the role he is trying to assume from step 1.3, sts:ExternalID
4) STS provides the auditor with temporary credentials that provide the role access from step 1
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html
<https://aws.amazon.com/blogs/security/how-to-audit-cross-account-roles-using-aws-cloudtrail-and-amazon-cloudwatch-events/>

QUESTION 19

A developer is building a serverless application hosted on AWS that uses Amazon Redshift as a data store. The application has separate modules for read/write and read-only functionality. The modules need their own database users for compliance reasons.

Which combination of steps should a security engineer implement to grant appropriate access?
(Choose two.)

- A. Configure cluster security groups for each application module to control access to database users that are required for read-only and read-write.
- B. Configure a VPC endpoint for Amazon Redshift.
Configure an endpoint policy that maps database users to each application module, and allow access to the tables that are required for read-only and read/write.
- C. Configure an IAM policy for each module.
Specify the ARN of an Amazon Redshift database user that allows the GetClusterCredentials API call.
- D. Create local database users for each module.
- E. Configure an IAM policy for each module.
Specify the ARN of an IAM user that allows the GetClusterCredentials API call.

Answer: AD

QUESTION 20

An application is currently secured using network access control lists and security groups. Web servers are located in public subnets behind an Application Load Balancer (ALB); application servers are located in private subnets.

How can edge security be enhanced to safeguard the Amazon EC2 instances against attack?
(Choose two.)

- A. Configure the application's EC2 instances to use NAT gateways for all inbound traffic.
- B. Move the web servers to private subnets without public IP addresses.
- C. Configure AWS WAF to provide DDoS attack protection for the ALB.
- D. Require all inbound network traffic to route through a bastion host in the private subnet.
- E. Require all inbound and outbound network traffic to route through an AWS Direct Connect connection.

Answer: BC

Explanation:

A is incorrect. Nat gateways is for outbound only traffic.

D is incorrect. Bastion host is mostly for incoming SSH/FTP connections and it must be placed on a public subnet

E is incorrect. AWS Direct connect is used to connect your on-premises datacenter to AWS

QUESTION 21

A Security Administrator is restricting the capabilities of company root user accounts. The company uses AWS Organizations and has enabled it for all feature sets, including consolidates billing. The top-level account is used for billing and administrative purposes, not for operational AWS resource purposes.

How can the Administrator restrict usage of member root user accounts across the organization?

- A. Disable the use of the root user account at the organizational root. Enable multi-factor authentication of the root user account for each organizational member account.
- B. Configure IAM user policies to restrict root account capabilities for each Organizations member account.
- C. Create an organizational unit (OU) in Organizations with a service control policy that controls usage of the root user. Add all operational accounts to the new OU.
- D. Configure AWS CloudTrail to integrate with Amazon CloudWatch Logs and then create a metric filter for RootAccountUsage.

Answer: C

Explanation:

To limit root user, you use SCP within organizations.

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html

QUESTION 22

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

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

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

Answer: B

QUESTION 23

A company requires that IP packet data be inspected for invalid or malicious content.

Which of the following approaches achieve this requirement? (Choose two.)

- A. Configure a proxy solution on Amazon EC2 and route all outbound VPC traffic through it. Perform inspection within proxy software on the EC2 instance.
- B. Configure the host-based agent on each EC2 instance within the VPC. Perform inspection within the host-based agent.
- C. Enable VPC Flow Logs for all subnets in the VPC. Perform inspection from the Flow Log data within Amazon CloudWatch Logs.
- D. Configure Elastic Load Balancing (ELB) access logs. Perform inspection from the log data within the ELB access log files.
- E. Configure the CloudWatch Logs agent on each EC2 instance within the VPC. Perform inspection from the log data within CloudWatch Logs.

Answer: AB

Explanation:

AWS native services do not offer packet inspection. Third party tools needed.

<https://aws.amazon.com/answers/networking/vpc-security-capabilities/>

QUESTION 24

A Security Engineer launches two Amazon EC2 instances in the same Amazon VPC but in separate Availability Zones. Each instance has a public IP address and is able to connect to external hosts on the internet. The two instances are able to communicate with each other by using their private IP addresses, but they are not able to communicate with each other when using their public IP addresses.

Which action should the Security Engineer take to allow communication over the public IP addresses?

- A. Associate the instances to the same security groups.
- B. Add 0.0.0.0/0 to the egress rules of the instance security groups.
- C. Add the instance IDs to the ingress rules of the instance security groups.
- D. Add the public IP addresses to the ingress rules of the instance security groups.

Answer: D

QUESTION 25

The Security Engineer is managing a web application that processes highly sensitive personal information. The application runs on Amazon EC2. The application has strict compliance requirements, which instruct that all incoming traffic to the application is protected from common web exploits and that all outgoing traffic from the EC2 instances is restricted to specific whitelisted URLs.

Which architecture should the Security Engineer use to meet these requirements?

- A. Use AWS Shield to scan inbound traffic for web exploits. Use VPC Flow Logs and AWS Lambda to restrict egress traffic to specific whitelisted URLs.
- B. Use AWS Shield to scan inbound traffic for web exploits. Use a third-party AWS Marketplace solution to restrict egress traffic to specific whitelisted URLs.
- C. Use AWS WAF to scan inbound traffic for web exploits. Use VPC Flow Logs and AWS Lambda to restrict egress traffic to specific whitelisted URLs.
- D. Use AWS WAF to scan inbound traffic for web exploits. Use a third-party AWS Marketplace solution to restrict egress traffic to specific whitelisted URLs.

Answer: D

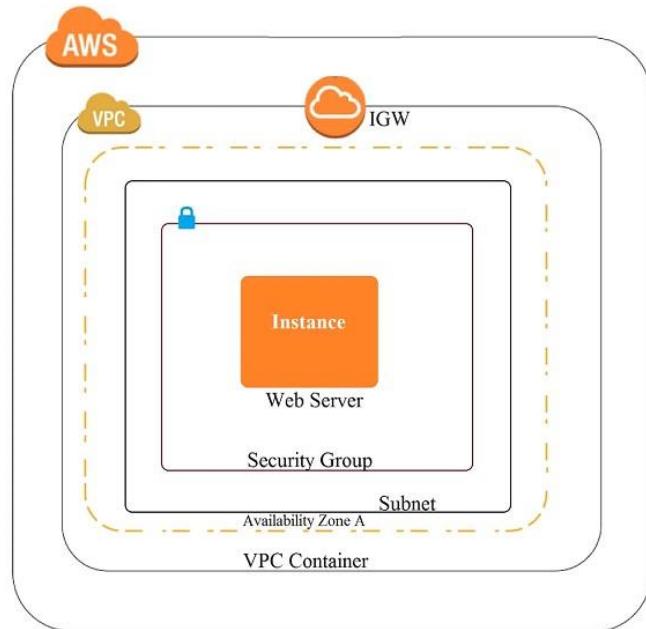
Explanation:

We can use shield for CWE, whereas WAF is better for this case. We can use available templates to scan and filter.

QUESTION 26

A company recently experienced a DDoS attack that prevented its web server from serving content. The website is static and hosts only HTML, CSS, and PDF files that users download.

Based on the architecture shown in the image, what is the BEST way to protect the site against future attacks while minimizing the ongoing operational overhead?



- A. Move all the files to an Amazon S3 bucket. Have the web server serve the files from the S3 bucket.
- B. Launch a second Amazon EC2 instance in a new subnet. Launch an Application Load Balancer in front of both instances.
- C. Launch an Application Load Balancer in front of the EC2 instance. Create an Amazon CloudFront distribution in front of the Application Load Balancer.
- D. Move all the files to an Amazon S3 bucket. Create a CloudFront distribution in front of the bucket and terminate the web server.

Answer: D**Explanation:**

S3 - S3 is object storage with a simple web service interface to store and retrieve any amount of data from anywhere on the web.

CloudFront - When architecting your application for DDoS resiliency, it is important to protect origin resources, such as S3 buckets, from discovery by a malicious actor.

QUESTION 27

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

What is causing this situation?

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

Answer: D

Explanation:

Classic load balancers support some of the legacy cipher suites. Given that some of the users are having problems could mean that legacy cipher suites have been deprecated in ALBs.

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

QUESTION 28

A security team is responsible for reviewing AWS API call activity in the cloud environment for security violations. These events must be recorded and retained in a centralized location for both current and future AWS regions.

What is the SIMPLEST way to meet these requirements?

- A. Enable AWS Trusted Advisor security checks in the AWS Console, and report all security incidents for all regions.
- B. Enable AWS CloudTrail by creating individual trails for each region, and specify a single Amazon S3 bucket to receive log files for later analysis.
- C. Enable AWS CloudTrail by creating a new trail and applying the trail to all regions. Specify a single Amazon S3 bucket as the storage location.
- D. Enable Amazon CloudWatch logging for all AWS services across all regions, and aggregate them to a single Amazon S3 bucket for later analysis.

Answer: C

Explanation:

The simplest answer would be to setup one trail for all regions and global events. So new regions would automatically be added.

<https://aws.amazon.com/blogs/aws/aws-cloudtrail-update-turn-on-in-all-regions-use-multipletrails/>

QUESTION 29

A Security Administrator is performing a log analysis as a result of a suspected AWS account compromise. The Administrator wants to analyze suspicious AWS CloudTrail log files but is overwhelmed by the volume of audit logs being generated.

What approach enables the Administrator to search through the logs MOST efficiently?

- A. Implement a "write-only" CloudTrail event filter to detect any modifications to the AWS account resources.
- B. Configure Amazon Macie to classify and discover sensitive data in the Amazon S3 bucket that contains the CloudTrail audit logs.
- C. Configure Amazon Athena to read from the CloudTrail S3 bucket and query the logs to examine account activities.
- D. Enable Amazon S3 event notifications to trigger an AWS Lambda function that sends an email alarm when there are new CloudTrail API entries.

Answer: C

Explanation:

Athena is best fit for the case. Use Athena to query trail logs in s3 and use quicksight for further intelligence.

QUESTION 30

A Systems Engineer has been tasked with configuring outbound mail through Simple Email Service (SES) and requires compliance with current TLS standards.

The mail application should be configured to connect to which of the following endpoints and corresponding ports?

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

Answer: C

Explanation:

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

QUESTION 31

A water utility company uses a number of Amazon EC2 instances to manage updates to a fleet of 2,000 Internet of Things (IoT) field devices that monitor water quality. These devices each have unique access credentials.

An operational safety policy requires that access to specific credentials is independently auditable.

What is the MOST cost-effective way to manage the storage of credentials?

- A. Use AWS Systems Manager to store the credentials as Secure Strings Parameters. Secure by using an AWS KMS key.
- B. Use AWS Key Management System to store a master key, which is used to encrypt the credentials. The encrypted credentials are stored in an Amazon RDS instance.
- C. Use AWS Secrets Manager to store the credentials.
- D. Store the credentials in a JSON file on Amazon S3 with server-side encryption.

Answer: A

Explanation:

AWS System Manager allow you to separate your secrets and configuration data from your code by using parameters, with or without encryption, and then reference those parameters from a number of other AWS services.

<https://docs.aws.amazon.com/systems-manager/latest/userguide/what-is-systems-manager.html>

QUESTION 32

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

An inspection revealed that the instance has attached Amazon EBS volumes that were encrypted

by using a Customer Master Key (CMK). When these encrypted volumes were detached, the IAM user was able to start the EC2 instances.

The IAM user policy is as follows:

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

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

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

Answer: CE

Explanation:

The EBS which is AWS resource service is encrypted with CMK and to allow EC2 to decrypt , the IAM user should create a grant (action) and a boolean condition for the AWs resource . This link explains how AWS keys works.

<https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html>

QUESTION 33

A Security Administrator has a website hosted in Amazon S3. The Administrator has been given the following requirements:

Users may access the website by using an Amazon CloudFront distribution. Users may not access the website directly by using an Amazon S3 URL.

Which configurations will support these requirements? (Choose two.)

- A. Associate an origin access identity with the CloudFront distribution.
- B. Implement a "Principal": "cloudfront.amazonaws.com" condition in the S3 bucket policy.

- C. Modify the S3 bucket permissions so that only the origin access identity can access the bucket contents.
- D. Implement security groups so that the S3 bucket can be accessed only by using the intended CloudFront distribution.
- E. Configure the S3 bucket policy so that it is accessible only through VPC endpoints, and place the CloudFront distribution into the specified VPC.

Answer: AC

Explanation:

A is needed. OAI needs to be setup with cloudfront. D is invalid. S3 restrictions are not done with security groups. There are global resources and are not within VPC.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

QUESTION 34

A Security Engineer has created an Amazon CloudWatch event that invokes an AWS Lambda function daily. The Lambda function runs an Amazon Athena query that checks AWS CloudTrail logs in Amazon S3 to detect whether any IAM user accounts or credentials have been created in the past 30 days. The results of the Athena query are created in the same S3 bucket. The Engineer runs a test execution of the Lambda function via the AWS Console, and the function runs successfully.

After several minutes, the Engineer finds that his Athena query has failed with the error message: "Insufficient Permissions". The IAM permissions of the Security Engineer and the Lambda function are shown below:

Security Engineer

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "s3:*",  
                "iam:*",  
                "lambda:*",  
                "athena:Get*",  
                "athena>List*",  
                "cloudwatch:*"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Lambda function execution role

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "athena:*",  
                "cloudwatch:*"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

What is causing the error?

- A. The Lambda function does not have permissions to start the Athena query execution.
- B. The Security Engineer does not have permissions to start the Athena query execution.
- C. The Athena service does not support invocation through Lambda.
- D. The Lambda function does not have permissions to access the CloudTrail S3 bucket.

Answer: D

QUESTION 35

Your company has multiple accounts in various regions which contains resources such as EC2, CloudWatch, DynamoDB, EBS, Redshift, RDS , S3, Elasticbeanstalk, IAM , Autoscaling and ElasticloadBalancer. The IT Audit department requires a compliance report of all the resources that are used by your company.

Which of the following will help you to provide a report in the easiest way?

- A. Create a powershell script using the AWS CLI. Query for all resources with the tag of production.
- B. Create a bash shell script with the AWS CLI. Query for all resources in all regions. Store the results in an S3 bucket.
- C. Use Cloud Trail to get the list of all resources
- D. Use AWS Config to get the list of all resources

Answer: D

Explanation:

<https://stackoverflow.com/questions/54172923/run-aws-athena-s-queries-with-lambda-function>

QUESTION 36

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

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

- A. Create a VPC endpoint for DynamoDB within a VPC.
Configure the Lambda function to access resources in the VPC.

- B. Create a resource policy that grants the Lambda function permissions to write to the DynamoDB table.
Attach the policy to the DynamoDB table.
- C. Create an IAM user with permissions to write to the DynamoDB table.
Store an access key for that user in the Lambda environment variables.
- D. Create an IAM service role with permissions to write to the DynamoDB table.
Associate that role with the Lambda function.

Answer: D

Explanation:

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

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

If your Lambda function code accesses other AWS resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role. If the event source is stream-based (Amazon Kinesis Data Streams and DynamoDB streams), AWS Lambda polls these streams on your behalf. AWS Lambda needs permissions to poll the stream and read new records on the stream so you need to grant the relevant permissions to this role.

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

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

Option C is invalid because AWS Roles should be used and not IAM Users For more information on the Lambda permission model,

<https://docs.aws.amazon.com/lambda/latest/dg/intro-permission-model.html>

QUESTION 37

Your company has defined privileged users for their AWS Account. These users are administrators for key resources defined in the company. There is now a mandate to enhance the security authentication for these users. How can this be accomplished?

- A. Enable MFA for these user accounts
- B. Enable versioning for these user accounts
- C. Enable accidental deletion for these user accounts
- D. Disable root access for the users

Answer: A

Explanation:

The AWS Documentation mentions the following as a best practices for IAM users. For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).

Option B,C and D are invalid because no such security options are available in AWS For more information on IAM best practices, please visit the below URL

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

QUESTION 38

An application running on EC2 instances must use a username and password to access a database. The developer has stored those secrets in the SSM Parameter Store with type SecureString using the default KMS CMK.

Which combination of configuration steps will allow the application to access the secrets via the API? Select 2 answers from the options below

- A. Add the EC2 instance role as a trusted service to the SSM service role.
- B. Add permission to use the KMS key to decrypt to the SSM service role.
- C. Add permission to read the SSM parameter to the EC2 instance role.
- D. Add permission to use the KMS key to decrypt to the EC2 instance role.
- E. Add the SSM service role as a trusted service to the EC2 instance role.

Answer: CD

Explanation:

The below example policy from the AWS Documentation is required to be given to the EC2 Instance in order to read a secure string from AWS KMS. Permissions need to be given to the Get Parameter API and the KMS API call to decrypt the secret.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ssm:GetParameter*",  
                "kms:Decrypt"  
            ],  
            "Resource": "arn:aws:ssm:us-west-2:111122223333:parameter/ReadableParameters/*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "kms:Decrypt"  
            ],  
            "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"  
        }  
    ]  
}
```

Option A is invalid because roles can be attached to EC2 and not EC2 roles to SSM

Option B is invalid because the KMS key does not need to decrypt the SSM service role.

Option E is invalid because this configuration is valid For more information on the parameter store, please visit the below URL:

<https://docs.aws.amazon.com/kms/latest/developerguide/services-parameter-store.html>

QUESTION 39

Your application currently uses customer keys which are generated via AWS KMS in the US east region. You now want to use the same set of keys from the EU-Central region.

How can this be accomplished?

- A. Export the key from the US east region and import them into the EU-Central region
- B. Use key rotation and rotate the existing keys to the EU-Central region
- C. Use the backing key from the US east region and use it in the EU-Central region
- D. This is not possible since keys from KMS are region specific

Answer: D

Explanation:

Option A is invalid because keys cannot be exported and imported across regions.

Option B is invalid because key rotation cannot be used to export keys Option C is invalid because the backing key cannot be used to export keys This is mentioned in the AWS documentation

What geographic region are my keys stored in?

Keys are only stored and used in the region in which they are created. They cannot be transferred to another region. For example; keys created in the EU-Central (Frankfurt) region are only stored and used within the EU-Central (Frankfurt) region For more information on KMS please visit the following URL:

<https://aws.amazon.com/kms/faqs/>

QUESTION 40

You have a set of Customer keys created using the AWS KMS service. These keys have been used for around 6 months.

You are now trying to use the new KMS features for the existing set of key's but are not able to do so.

What could be the reason for this?

- A. You have not explicitly given access via the key policy
- B. You have not explicitly given access via the bucket policy
- C. You have not given access via the I AM roles X
- D. You have not explicitly given access via I AM users

Answer: A

QUESTION 41

A security team must present a daily briefing to the CISO that includes a report of which of the company's thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day's report.

How can the security team fulfill these requirements?

- A. Use Amazon QuickSight and Cloud Trail to generate the report of out of compliance instances/servers. Redeploy all out of compliance instances/servers using an AMI with the latest patches.
- B. Use Systems Manager Patch Manager to generate the report of out of compliance instances/servers. Use Systems Manager Patch Manager to install the missing patches.
- C. Use Systems Manager Patch Manager to generate the report of out of compliance instances/

- servers. Redeploy all out of compliance instances/servers using an AMI with the latest patches.
- D. Use Trusted Advisor to generate the report of out of compliance instances/ servers. Use Systems Manager Patch Manager to install the missing patches.

Answer: B

QUESTION 42

A company's database developer has just migrated an Amazon RDS database credential to be stored and managed by AWS Secrets Manager. The developer has also enabled rotation of the credential within the Secrets Manager console and set the rotation to change every 30 days.

After a short period of time, a number of existing applications have failed with authentication errors.

What is the MOST likely cause of the authentication errors?

- A. Migrating the credential to RDS requires that all access come through requests to the Secrets Manager.
- B. Enabling rotation in Secrets Manager causes the secret to rotate immediately and the applications are using the earlier credential.
- C. The Secrets Manager IAM policy does not allow access to the RDS database.
- D. The Secrets Manager IAM policy does not allow access for the applications.

Answer: B

Explanation:

Enabling rotation causes the secret to rotate once immediately when you save the secret. Before you enable rotation, be sure you update all of your applications using this secret credentials to retrieve the secret from Secrets Manager. The original credentials might not be usable after the initial rotation. Any applications you fail to update break as soon as the old credentials become invalid.

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/enable-rotation-rds.html>

QUESTION 43

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

- A. Enable AWS Guard Duty for the Instance
- B. Use AWS Trusted Advisor
- C. Use AWS Inspector
- D. Use AWS Made

Answer: C

Explanation:

The AWS Inspector service can inspect EC2 Instances based on specific Rules. One of the rules packages is based on the guidelines set by the Center of Internet Security Option A is invalid because this can be used to protect an instance but not give the list of vulnerabilities Option B and D are invalid because these services cannot give a list of vulnerabilities For more information on the guidelines, please visit the below URL

https://docs.aws.amazon.com/inspector/latest/userguide/inspector_cis.html

QUESTION 44

You have an instance setup in a test environment in AWS. You installed the required application and the promoted the server to a production environment. Your IT Security team has advised that there maybe traffic flowing in from an unknown IP address to port 22.
How can this be mitigated immediately?

- A. Shutdown the instance
- B. Remove the rule for incoming traffic on port 22 for the Security Group
- C. Change the AMI for the instance
- D. Change the Instance type for the Instance

Answer: B

Explanation:

In the test environment, the security groups might have been opened to all IP addresses for testing purpose. Always to ensure to remove this rule once all testing is completed.
Option A , C and D are all invalid because this would affect the application running on the server.
The easiest way is just to remove the rule for access on port 22. For more information on authorizing access to an instance, please visit the below URL
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html>

QUESTION 45

Your company has defined a number of EC2 Instances. They want to know if any of the security groups allow unrestricted access to a resource.

Which of the following provides the SIMPLEST solution to accomplish the requirement?

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

Answer: B

Explanation:

The AWS Trusted Advisor can check security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data). If you go to AWS Trusted Advisor , you can see the details Option A is invalid because AWS Inspector is used to detect security vulnerabilities in instances and not for security groups. Option C is invalid because this can be used to detect changes in security groups but not show you security groups that have compromised access. Option D is partially valid but would just be a maintenance over head For more information on the AWS Trusted Advisor, please visit the below URL
<https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices/>

QUESTION 46

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

What combination of steps will protect the log files from intentional or unintentional alteration?

Choose 2 answers from the options given below

- A. Create an S3 bucket in a dedicated log account and grant the other accounts write only access. Deliver all log files from every account to this S3 bucket.
- B. Write a Lambda function that queries the Trusted Advisor Cloud Trail checks. Run the function every 10 minutes.

- C. Enable Cloud Trail log file integrity validation
- D. Use Systems Manager Configuration Compliance to continually monitor the access policies of S3 buckets containing Cloud Trail logs.
- E. Create a Security Group that blocks all traffic except calls from the CloudTrail service. Associate the security group with all the Cloud Trail destination S3 buckets.

Answer: AC

Explanation:

The AWS Documentation mentions the following To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it, you can use CloudTrail log file integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. Option B is invalid because there is no such thing as Trusted Advisor Cloud Trail checks Option D is invalid because Systems Manager cannot be used for this purpose. Option E is invalid because Security Groups cannot be used to block calls from other services For more information on Cloudtrail log file validation, please visit the below URL <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html> For more information on delivering Cloudtrail logs from multiple accounts, please visit the below URL <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-receive-logs-from-multiple-accounts.html>

QUESTION 47

A security team is creating a response plan in the event an employee executes unauthorized actions on AWS infrastructure.

They want to include steps to determine if the employee's IAM permissions changed as part of the incident.

What steps should the team document in the plan?

- A. Use AWS Config to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.
- B. Use Made to examine the employee's 1AM permissions prior to the incident and compare them to the employee's current 1AM permissions.
- C. Use CloudTrail to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.
- D. Use Trusted Advisor to examine the employee's 1AM permissions prior to the incident and compare them to the employee's current 1AM permissions.

Answer: A

Explanation:

You can use the AWS Config history to see the history of a particular item. The below snapshot shows an example configuration for a user in AWS Config Option B,C and D are all invalid because these services cannot be used to see the history of a particular configuration item. This can only be accomplished by AWS Config. For more information on tracking changes in AWS Config, please visit the below URL

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/TrackingChanges.html>

QUESTION 48

During a recent internal investigation, it was discovered that all API logging was disabled in a production account, and the root user had created new API keys that appear to have been used several times.

What could have been done to detect and automatically remediate the incident?

- A. Using Amazon Inspector, review all of the API calls and configure the inspector agent to leverage SNS topics to notify security of the change to AWS CloudTrail, and revoke the new API keys for the root user.
- B. Using AWS Config, create a config rule that detects when AWS CloudTrail is disabled, as well as any calls to the root user create-api-key. Then use a Lambda function to re-enable CloudTrail logs and deactivate the root API keys.
- C. Using Amazon CloudWatch, create a CloudWatch event that detects AWS CloudTrail deactivation and a separate Amazon Trusted Advisor check to automatically detect the creation of root API keys. Then use a Lambda function to enable AWS CloudTrail and deactivate the root API keys.
- D. Using Amazon CloudTrail, create a new CloudTrail event that detects the deactivation of CloudTrail logs, and a separate CloudTrail event that detects the creation of root API keys. Then use a Lambda function to enable CloudTrail and deactivate the root API keys.

Answer: B

Explanation:

You can develop custom rules and add them to AWS Config. You associate each custom rule with an AWS Lambda function, which contains the logic that evaluates whether your AWS resources comply with the rule.

https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules.html - Check AWS config custom rule

QUESTION 49

An application has a requirement to be resilient across not only Availability Zones within the application's primary region but also be available within another region altogether.

Which of the following supports this requirement for AWS resources that are encrypted by AWS KMS?

- A. Copy the application's AWS KMS CMK from the source region to the target region so that it can be used to decrypt the resource after it is copied to the target region.
- B. Configure AWS KMS to automatically synchronize the CMK between regions so that it can be used to decrypt the resource in the target region.
- C. Use AWS services that replicate data across regions, and re-wrap the data encryption key created in the source region by using the CMK in the target region so that the target region's CMK can decrypt the database encryption key.
- D. Configure the target region's AWS service to communicate with the source region's AWS KMS so that it can decrypt the resource in the target region.

Answer: C

QUESTION 50

An organization policy states that all encryption keys must be automatically rotated every 12 months.

Which AWS Key Management Service (KMS) key type should be used to meet this requirement?

- A. AWS managed Customer Master Key (CMK)
- B. Customer managed CMK with AWS generated key material
- C. Customer managed CMK with imported key material
- D. AWS managed data key

Answer: B

Explanation:

AWS KMS automatically rotates the key material for an AWS managed CMK or customer managed CMK.

QUESTION 51

A Security Engineer received an AWS Abuse Notice listing EC2 instance IDs that are reportedly abusing other hosts.

Which action should the Engineer take based on this situation? (Choose three.)

- A. Use AWS Artifact to capture an exact image of the state of each instance.
- B. Create EBS Snapshots of each of the volumes attached to the compromised instances.
- C. Capture a memory dump.
- D. Log in to each instance with administrative credentials to restart the instance.
- E. Revoke all network ingress and egress except for to/from a forensics.
- F. Run Auto Recovery for Amazon EC2.

Answer: BCE

QUESTION 52

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

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

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

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

Answer: ACE

QUESTION 53

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

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

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

Answer: C

Explanation:

kms:ViaService - Condition key limits use of an AWS KMS customer master key (CMK) to requests from specified AWS services.

The kms:ViaService condition key is valid for all AWS KMS operations except: CreateKey, GenerateRandom, ListAliases, ListKeys, ListRetirableGrants, RetireGrant.

QUESTION 54

A Security Engineer who was reviewing AWS Key Management Service (AWS KMS) key policies found this statement in each key policy in the company AWS account.

```
{  
    "Sid": "Enable IAM User Permissions",  
    "Effect": "Allow",  
    "Principal": {  
        "AWS": "arn:aws:iam::111122223333:root"  
    },  
    "Action": "kms:*",  
    "Resource": "*"  
}
```

What does the statement allow?

- A. All principals from all AWS accounts to use the key.
- B. Only the root user from account 111122223333 to use the key.
- C. All principals from account 111122223333 to use the key but only on Amazon S3.
- D. Only principals from account 111122223333 that have an IAM policy applied that grants access to this key to use the key.

Answer: D

Explanation:

Enables IAM policies to allow access to the CMK.

IAM policies by themselves are not sufficient to allow access to a CMK. However, you can use them in combination with a CMK's key policy if the key policy enables it. Giving the AWS account (root) full access to the CMK does this; it enables you to use IAM policies to give IAM users and roles in the account access to the CMK. It does not by itself give any IAM users or roles access to the CMK, but it enables you to use IAM policies to do so. For more information, see Managing Access to AWS KMS CMKs.

The following example shows the policy statement that allows access to the AWS account and thereby enables IAM policies.

```
{  
"Sid": "Enable IAM User Permissions",  
"Effect": "Allow",  
"Principal": {"AWS": "arn:aws:iam::111122223333:root"},  
"Action": "kms:*",  
"Resource": "*"  
}
```

<https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html>

QUESTION 55

A threat assessment has identified a risk whereby an internal employee could exfiltrate sensitive data from production host running inside AWS (Account 1). The threat was documented as follows:

Threat description: A malicious actor could upload sensitive data from Server X by configuring credentials for an AWS account (Account 2) they control and uploading data to an Amazon S3 bucket within their control.

Server X has outbound internet access configured via a proxy server. Legitimate access to S3 is required so that the application can upload encrypted files to an S3 bucket. Server X is currently using an IAM instance role. The proxy server is not able to inspect any of the server

communication due to TLS encryption.

Which of the following options will mitigate the threat? (Choose two.)

- A. Bypass the proxy and use an S3 VPC endpoint with a policy that whitelists only certain S3 buckets within Account 1.
- B. Block outbound access to public S3 endpoints on the proxy server.
- C. Configure Network ACLs on Server X to deny access to S3 endpoints.
- D. Modify the S3 bucket policy for the legitimate bucket to allow access only from the public IP addresses associated with the application server.
- E. Remove the IAM instance role from the application server and save API access keys in a trusted and encrypted application config file.

Answer: AB

Explanation:

C is sure wrong since security groups and not NACL are used for hosts. D is incorrect because the legitimate S3 bucket has nothing to do with exfiltrating data from Server X and upload to another bucket which they control, so working on the legitimate bucket has nothing to do with it, they are uploading data to their own S3 bucket and we need to stop them.

QUESTION 56

A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of "Sensitive," "Confidential," and "Restricted." The security solution must meet all of the following requirements:

Each object must be encrypted using a unique key.

Items that are stored in the "Restricted" bucket require two-factor authentication for decryption. AWS KMS must automatically rotate encryption keys annually.

Which of the following meets these requirements?

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

Answer: A

Explanation:

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

QUESTION 57

An organization wants to deploy a three-tier web application whereby the application servers run on Amazon EC2 instances. These EC2 instances need access to credentials that they will use to authenticate their SQL connections to an Amazon RDS DB instance. Also, AWS Lambda

functions must issue queries to the RDS database by using the same database credentials.

The credentials must be stored so that the EC2 instances and the Lambda functions can access them. No other access is allowed. The access logs must record when the credentials were accessed and by whom.

What should the Security Engineer do to meet these requirements?

- A. Store the database credentials in AWS Key Management Service (AWS KMS). Create an IAM role with access to AWS KMS by using the EC2 and Lambda service principals in the role's trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances. Set up Lambda to use the new role for execution.
- B. Store the database credentials in AWS KMS. Create an IAM role with access to KMS by using the EC2 and Lambda service principals in the role's trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances and the Lambda function.
- C. Store the database credentials in AWS Secrets Manager. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role's trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances and the Lambda function.
- D. Store the database credentials in AWS Secrets Manager. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role's trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances. Set up Lambda to use the new role for execution.

Answer: D

Explanation:

A & B are wrong because you do not store credentials in AWS-KMS . C is wrong because you do not attach EC2 instance profile to lamda function, you attach only to EC2 instance.

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-intro-execution-role.html>

QUESTION 58

An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing.

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

- A. Use an EC2 run command to confirm that the "awslogs" service is running on all instances.
- B. Verify that the permissions used by the agent allow creation of log groupsstreams and to put log events.
- C. Check whether any application log entries were rejected because of invalid time stamps by reviewing / var/cwlogs/rejects.log.
- D. Check that the trust relationship grants the service "cwlogs.amazonaws.com" permission to write objects to the Amazon S3 staging bucket.
- E. Verify that the time zone on the application servers is in UTC.

Answer: AB

Explanation:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/troubleshooting-CloudWatch-Agent.html>

https://docs.aws.amazon.com/AmazonCloudWatchLogs/latest/APIReference/API_CreateLogStream.html

QUESTION 59

An employee accidentally exposed an AWS access key and secret access key during a public presentation. The company Security Engineer immediately disabled the key.

How can the Engineer assess the impact of the key exposure and ensure that the credentials were not misused? (Choose two.)

- A. Analyze AWS CloudTrail for activity.
- B. Analyze Amazon CloudWatch Logs for activity.
- C. Download and analyze the IAM Use report from AWS Trusted Advisor.
- D. Analyze the resource inventory in AWS Config for IAM user activity.
- E. Download and analyze a credential report from IAM.

Answer: AE

QUESTION 60

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

What is the MOST efficient way to meet these requirements?

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

Answer: D

Explanation:

You can set your application to send logs and cloudwatch to receive them using the cloudwatch agent. A Lambda is not necessary.

<https://aws.amazon.com/blogs/devops/new-how-to-better-monitor-your-custom-application-metrics-using-amazon-cloudwatch-agent/>

QUESTION 61

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

What can be done to implement the above policy?

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

Answer: D

Explanation:

You might prefer to rotate keys manually so you can control the rotation frequency. It's also a good solution for CMKs that are not eligible for automatic key rotation, such as asymmetric CMKs, CMKs in custom key stores and CMKs with imported key material.

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

To update the target CMK of an alias, use `UpdateAlias` operation in the AWS KMS API.

<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html#rotate-keys-manually>

QUESTION 62

During a recent security audit, it was discovered that multiple teams in a large organization have placed restricted data in multiple Amazon S3 buckets, and the data may have been exposed. The auditor has requested that the organization identify all possible objects that contain personally identifiable information (PII) and then determine whether this information has been accessed.

What solution will allow the Security team to complete this request?

- A. Using Amazon Athena, query the impacted S3 buckets by using the PII query identifier function. Then, create a new Amazon CloudWatch metric for Amazon S3 object access to alert when the objects are accessed.
- B. Enable Amazon Macie on the S3 buckets that were impacted, then perform data classification. For identified objects that contain PII, use the research function for auditing AWS CloudTrail logs and S3 bucket logs for GET operations.
- C. Enable Amazon GuardDuty and enable the PII rule set on the S3 buckets that were impacted, then perform data classification. Using the PII findings report from GuardDuty, query the S3 bucket logs by using Athena for GET operations.
- D. Enable Amazon Inspector on the S3 buckets that were impacted, then perform data classification. For identified objects that contain PII, query the S3 bucket logs by using Athena for GET operations.

Answer: B

QUESTION 63

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

What is the MOST efficient way to meet these requirements?

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

Answer: D

Explanation:

You can set your application to send logs and cloudwatch to receive them using the cloudwatch agent. A Lambda is not necessary.

<https://aws.amazon.com/blogs/devops/new-how-to-better-monitor-your-custom-application-metrics-using-amazon-cloudwatch-agent/>

QUESTION 64

A Security Engineer is trying to determine whether the encryption keys used in an AWS service are in compliance with certain regulatory standards.

Which of the following actions should the Engineer perform to get further guidance?

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

Answer: B

QUESTION 65

The Development team receives an error message each time the team members attempt to encrypt or decrypt a Secure String parameter from the SSM Parameter Store by using an AWS KMS customer managed key (CMK).

Which CMK-related issues could be responsible? (Choose two.)

- A. The CMK specified in the application does not exist.
- B. The CMK specified in the application is currently in use.
- C. The CMK specified in the application is using the CMK KeyID instead of CMK Amazon Resource Name.
- D. The CMK specified in the application is not enabled.
- E. The CMK specified in the application is using an alias.

Answer: AD

Explanation:

<https://docs.aws.amazon.com/kms/latest/developerguide/services-parameter-store.html#parameter-store-cmk-fail>

QUESTION 66

An application has been written that publishes custom metrics to Amazon CloudWatch. Recently, IAM changes have been made on the account and the metrics are no longer being reported.

Which of the following is the LEAST permissive solution that will allow the metrics to be delivered?

- A. Add a statement to the IAM policy used by the application to allow logs:putLogEvents and logs:createLogStream
- B. Modify the IAM role used by the application by adding the CloudWatchFullAccess managed policy.
- C. Add a statement to the IAM policy used by the application to allow cloudwatch:putMetricData.
- D. Add a trust relationship to the IAM role used by the application for cloudwatch.amazonaws.com.

Answer: C

Explanation:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/permissions-reference-cw.html>

QUESTION 67

A Developer's laptop was stolen. The laptop was not encrypted, and it contained the SSH key used to access multiple Amazon EC2 instances. A Security Engineer has verified that the key has not been used, and has blocked port 22 to all EC2 instances while developing a response plan.

How can the Security Engineer further protect currently running instances?

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

Answer: C

Explanation:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html#delete-key-pair>

QUESTION 68

An organization has tens of applications deployed on thousands of Amazon EC2 instances. During testing, the Application team needs information to let them know whether the network access control lists (network ACLs) and security groups are working as expected.

How can the Application team's requirements be met?

- A. Turn on VPC Flow Logs, send the logs to Amazon S3, and use Amazon Athena to query the logs.
- B. Install an Amazon Inspector agent on each EC2 instance, send the logs to Amazon S3, and use Amazon EMR to query the logs.
- C. Create an AWS Config rule for each network ACL and security group configuration, send the logs to Amazon S3, and use Amazon Athena to query the logs.
- D. Turn on AWS CloudTrail, send the trails to Amazon S3, and use AWS Lambda to query the trails.

Answer: A

Explanation:

<https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/>

QUESTION 69

Your development team has started using AWS resources for development purposes. The AWS account has just been created. Your IT Security team is worried about possible leakage of AWS keys. What is the first level of measure that should be taken to protect the AWS account.

- A. Delete the AWS keys for the root account
- B. Create IAM Groups
- C. Create IAM Roles
- D. Restrict access using IAM policies

Answer: A**Explanation:**

The first level or measure that should be taken is to delete the keys for the IAM root user. When you log into your account and go to your Security Access dashboard, this is the first step that can be seen. Option B and C are wrong because creation of IAM groups and roles will not change the impact of leakage of AWS root access keys. Option D is wrong because the first key aspect is to protect the access keys for the root account. For more information on best practises for Security Access keys, please visit the below URL: <https://docs.aws.amazon.com/general/latest/gr/aws-access-keys-best-practices.html>

QUESTION 70

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

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

Answer: A**Explanation:**

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

You should audit your security configuration in the following situations:

On a periodic basis.

If there are changes in your organization, such as people leaving. If you have stopped using one or more individual AWS services. This is important for removing permissions that users in your account no longer need. If you've added or removed software in your accounts, such as applications on Amazon EC2 instances, AWS OpsWor stacks, AWS CloudFormation templates, etc. If you ever suspect that an unauthorized person might have accessed your account.

Option B, C and D are all the right ways and recommended best practices when it comes to conducting audits.

For more information on Security Audit guideline, please visit the below URL:

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

QUESTION 71

Your company hosts critical data in an S3 bucket. There is a requirement to ensure that all data is encrypted. There is also metadata about the information stored in the bucket that needs to be encrypted as well. Which of the below measures would you take to ensure that the metadata is encrypted?

- A. Put the metadata as metadata for each object in the S3 bucket and then enable S3 Server side encryption.
- B. Put the metadata as metadata for each object in the S3 bucket and then enable S3 Server KMS encryption.
- C. Put the metadata in a DynamoDB table and ensure the table is encrypted during creation time.
- D. Put the metadata in the S3 bucket itself.

Answer: C**Explanation:**

Option A, B and D are all invalid because the metadata will not be encrypted in any case and this is a key requirement from the question. One key thing to note is that when the S3 bucket objects

are encrypted, the meta data is not encrypted. So the best option is to use an encrypted DynamoDB table Important

All GET and PUT requests for an object protected by AWS KMS will fail if they are not made via SSL or by using SigV4. SSE-KMS encrypts only the object data. Any object metadata is not encrypted.

For more information on using KMS encryption for S3, please refer to below URL:
<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html>

QUESTION 72

An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing.

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

- A. Use an EC2 run command to confirm that the "awslogs" service is running on all instances.
- B. Verify that the permissions used by the agent allow creation of log groupsstreams and to PutLogEvents.
- C. Check whether any application log entries were rejected because of invalid time stamps by reviewing / var/cwlogs/rejects.log.
- D. Check that the trust relationship grants the service "cwlogs.amazonaws.com" permission to write objects to the Amazon S3 staging bucket.
- E. Verify that the time zone on the application servers is in UTC.

Answer: AB

Explanation:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/troubleshooting-CloudWatch-Agent.html>

https://docs.aws.amazon.com/AmazonCloudWatchLogs/latest/APIReference/API_CreateLogStream.html

QUESTION 73

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

How can this be accomplished?

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

Answer: A

QUESTION 74

An organization has a system in AWS that allows a large number of remote workers to submit data files. File sizes vary from a few kilobytes to several megabytes. A recent audit highlighted a concern that data files are not encrypted while in transit over untrusted networks.

Which solution would remediate the audit finding while minimizing the effort required?

- A. Upload an SSL certificate to IAM, and configure Amazon CloudFront with the passphrase for the private key.
- B. Call KMS.Encrypt() in the client, passing in the data file contents, and call KMS.Decrypt() server-side.
- C. Use AWS Certificate Manager to provision a certificate on an Elastic Load Balancing in front of the web service's servers.
- D. Create a new VPC with an Amazon VPC VPN endpoint, and update the web service's DNS record.

Answer: C

QUESTION 75

Which option for the use of the AWS Key Management Service (KMS) supports key management best practices that focus on minimizing the potential scope of data exposed by a possible future key compromise?

- A. Use KMS automatic key rotation to replace the master key, and use this new master key for future encryption operations without re-encrypting previously encrypted data.
- B. Generate a new Customer Master Key (CMK), re-encrypt all existing data with the new CMK, and use it for all future encryption operations.
- C. Change the CMK alias every 90 days, and update key-calling applications with the new key alias.
- D. Change the CMK permissions to ensure that individuals who can provision keys are not the same individuals who can use the keys.

Answer: B

Explanation:

"automatic key rotation has no effect on the data that the CMK protects. It does not rotate the data keys that the CMK generated or re-encrypt any data protected by the CMK, and it will not mitigate the effect of a compromised data key. You might decide to create a new CMK and use it in place of the original CMK. This has the same effect as rotating the key material in an existing CMK, so it's often thought of as manually rotating the key."

<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>

QUESTION 76

A Security Engineer must enforce the use of only Amazon EC2, Amazon S3, Amazon RDS, Amazon DynamoDB, and AWS STS in specific accounts.

What is a scalable and efficient approach to meet this requirement?

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "dynamodb:*", "rds:*", "ec2:*",
                "s3:*", "sts:*
```

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

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

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "dynamodb:*", "rds:*", "ec2:*",
                "s3:*", "sts:*
```

```
                ],
                "Effect": "Allow",
                "Resource": "*"
            }
        ]
    }
}
```

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

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

```
                ],
                "Effect": "Deny",
                "Resource": "*"
            }
        ]
    }
}
```

Answer: A

Explanation:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_reference_scp-syntax.html
 It says specific accounts which mean specific governed OUs under your organization and you apply specific service control policy to these OUs.

QUESTION 77

A Software Engineer is trying to figure out why network connectivity to an Amazon EC2 instance does not appear to be working correctly. Its security group allows inbound HTTP traffic from 0.0.0.0/0, and the outbound rules have not been modified from the default.

A custom network ACL associated with its subnet allows inbound HTTP traffic from 0.0.0.0/0 and has no outbound rules.

What would resolve the connectivity issue?

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

Answer: C

Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-recommended-nacl-rules.html>

QUESTION 78

A Security Engineer has been asked to create an automated process to disable IAM user access keys that are more than three months old.

Which of the following options should the Security Engineer use?

- A. In the AWS Console, choose the IAM service and select "Users". Review the "Access Key Age" column.
- B. Define an IAM policy that denies access if the key age is more than three months and apply to all users.
- C. Write a script that uses the GenerateCredentialReport, GetCredentialReport, and UpdateAccessKey APIs.
- D. Create an Amazon CloudWatch alarm to detect aged access keys and use an AWS Lambda function to disable the keys older than 90 days.

Answer: D

Explanation:

When you set a password expiration period, the expiration period is enforced immediately.

QUESTION 79

The InfoSec team has mandated that in the future only approved Amazon Machine Images (AMIs) can be used.

How can the InfoSec team ensure compliance with this mandate?

- A. Terminate all Amazon EC2 instances and relaunch them with approved AMIs.
- B. Patch all running instances by using AWS Systems Manager.
- C. Deploy AWS Config rules and check all running instances for compliance.
- D. Define a metric filter in Amazon CloudWatch Logs to verify compliance.

Answer: C

Explanation:

<https://docs.aws.amazon.com/config/latest/developerguide/approved-amis-by-id.html>

QUESTION 80

A pharmaceutical company has digitized versions of historical prescriptions stored on premises. The company would like to move these prescriptions to AWS and perform analytics on the data in them. Any operation with this data requires that the data be encrypted in transit and at rest.

Which application flow would meet the data protection requirements on AWS?

- A. Digitized files -> Amazon Kinesis Data Analytics
- B. Digitized files -> Amazon Kinesis Data Firehose -> Amazon S3 -> Amazon Athena
- C. Digitized files -> Amazon Kinesis Data Streams -> Kinesis Client Library consumer -> Amazon S3 -> Athena
- D. Digitized files -> Amazon Kinesis Data Firehose -> Amazon Elasticsearch

Answer: B

Explanation:

A is not right, since you can't ingest directly to kinesis analytics. Source has to be from data stream or firehose delivery stream.

C not efficient. D can't do any analysis. U need kibana or other analytics tool on top of ES

QUESTION 81

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

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

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

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

Answer: AC

Explanation:

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

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

QUESTION 82

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

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

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

Answer: D

Explanation:

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

[https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and- https- requirements.html](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html)

QUESTION 83

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

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

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

Answer: A

QUESTION 84

An organization is moving non-business-critical applications to AWS while maintaining a mission-critical application in an on-premises data center. An on-premises application must share limited confidential information with the applications in AWS. The internet performance is unpredictable. Which configuration will ensure continued connectivity between sites MOST securely?

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

Answer: C

Explanation:

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-plus-vpn-network-to-amazon.html>

QUESTION 85

An application has been built with Amazon EC2 instances that retrieve messages from Amazon SQS. Recently, IAM changes were made and the instances can no longer retrieve messages. What actions should be taken to troubleshoot the issue while maintaining least privilege. (Select two.)

- A. Configure and assign an MFA device to the role used by the instances.
- B. Verify that the SQS resource policy does not explicitly deny access to the role used by the instances.
- C. Verify that the access key attached to the role used by the instances is active.
- D. Attach the AmazonSQSFullAccess managed policy to the role used by the instances.
- E. Verify that the role attached to the instances contains policies that allow access to the queue.

Answer: BE

Explanation:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-using-identity-based-policies.html>

QUESTION 86

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

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

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

Answer: AB

Explanation:

Amazon Elasticsearch Service is a managed service that makes it easy to deploy, operate, and scale Elasticsearch clusters in the AWS Cloud. Elasticsearch is a popular open-source search and analytics engine for use cases such as log analytics, real-time application monitoring, and click stream analytics.

Amazon Kinesis is an Amazon Web Service (AWS) for processing big data in real time. Kinesis is capable of processing hundreds of terabytes per hour from high volumes of streaming data from sources such as operating logs, financial transactions and social media feeds.

QUESTION 87

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

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

Answer: C

Explanation:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-aws-kms.html>

QUESTION 88

An organization is using AWS CloudTrail, Amazon CloudWatch Logs, and Amazon CloudWatch to send alerts when new access keys are created. However, the alerts are no longer appearing in the Security Operations mail box.

Which of the following actions would resolve this issue?

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

Answer: C

Explanation:

<https://docs.aws.amazon.com/sns/latest/dg/sns-tutorial-create-subscribe-endpoint-to-topic.html>

To receive messages published to a topic, you must **subscribe** an endpoint (such as AWS Lambda, Amazon SQS, HTTP/S, or an email address) to the topic. When you subscribe an endpoint to a topic and confirm the subscription, the endpoint begins to receive messages published to the associated topic.

QUESTION 89

A Security Engineer must add additional protection to a legacy web application by adding the following HTTP security headers:

-Content Security-Policy
-X-Frame-Options
-X-XSS-Protection

The Engineer does not have access to the source code of the legacy web application.

Which of the following approaches would meet this requirement?

- A. Configure an Amazon Route 53 routing policy to send all web traffic that does not include the required headers to a black hole.
- B. Implement an AWS Lambda@Edge origin response function that inserts the required headers.
- C. Migrate the legacy application to an Amazon S3 static website and front it with an Amazon

- CloudFront distribution.
- D. Construct an AWS WAF rule to replace existing HTTP headers with the required security headers by using regular expressions.

Answer: B

Explanation:

- B - We can use lambda@edge to add security headers.
- D - WAF can't be used to add headers.
- A - Not viable.
- C - We can do this + use lambda@edge

QUESTION 90

During a security event, it is discovered that some Amazon EC2 instances have not been sending Amazon CloudWatch logs.

Which steps can the Security Engineer take to troubleshoot this issue? (Select two.)

- A. Connect to the EC2 instances that are not sending the appropriate logs and verify that the CloudWatch Logs agent is running.
- B. Log in to the AWS account and select CloudWatch Logs. Check for any monitored EC2 instances that are in the "Alerting" state and restart them using the EC2 console.
- C. Verify that the EC2 instances have a route to the public AWS API endpoints.
- D. Connect to the EC2 instances that are not sending logs. Use the command prompt to verify that the right permission have been set for the Amazon SNS topic.
- E. Verify that the network access control lists and security groups of the EC2 instances have the access to send logs over SNMP.

Answer: AC

Explanation:

A: CORRECT nailed on.

B: INCORRECT : Is restarting which is fixing NOT troubleshooting.

C: CORRECT. Dubious A as EC2 does not have an RT AND IF all instances in the same VPC will use the VPC RT .. but there you go maybe the instances are in a different vpc.

RE public AWS API endpoints assumption is this is public as AWS has documented the use of vpc private links as an option to connect to CW :

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/cloudwatch-logs-and-interface-VPC.html>

D: INCORRECT : SNS is for alarming not logging.

E: INCORRECT CloudWatch works apparently at the hypervisor level does not use SNMP

<https://stackoverflow.com/questions/53872529/does-cloudwatch-perform-snmp-monitoring>

See also the below for overall interest

<https://aws.amazon.com/premiumsupport/knowledge-center/push-log-data-cloudwatch-awslogs/>

QUESTION 91

A Security Engineer discovers that developers have been adding rules to security groups that allow SSH and RDP traffic from 0.0.0.0/0 instead of the organization firewall IP. What is the most efficient way to remediate the risk of this activity?

- A. Delete the internet gateway associated with the VPC.
- B. Use network access control lists to block source IP addresses matching 0.0.0.0/0.
- C. Use a host-based firewall to prevent access from all but the organization's firewall IP.
- D. Use AWS Config rules to detect 0.0.0.0/0 and invoke an AWS Lambda function to update the security group with the organization's firewall IP.

Answer: D

Explanation:

<https://medium.com/@grigggeo/modifying-ec2-security-groups-via-aws-lambda-functions-115a1828cdb6>

QUESTION 92

In response to the past DDoS attack experiences, a Security Engineer has set up an Amazon CloudFront distribution for an Amazon S3 bucket. There is concern that some users may bypass the CloudFront distribution and access the S3 bucket directly.

What must be done to prevent users from accessing the S3 objects directly by using URLs?

- A. Change the S3 bucket/object permission so that only the bucket owner has access.
- B. Set up a CloudFront origin access identity (OAI), and change the S3 bucket/object permission so that only the OAI has access.
- C. Create IAM roles for CloudFront, and change the S3 bucket/object permission so that only the IAM role has access.
- D. Redirect S3 bucket access to the corresponding CloudFront distribution.

Answer: B

Explanation:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

QUESTION 93

A company plans to move most of its IT infrastructure to AWS. The company wants to leverage its existing on-premises Active Directory as an identity provider for AWS. Which steps should be taken to authenticate to AWS services using the company's on-premises Active Directory? (Choose three).

- A. Create IAM roles with permissions corresponding to each Active Directory group.
- B. Create IAM groups with permissions corresponding to each Active Directory group.
- C. Create a SAML provider with IAM.
- D. Create a SAML provider with Amazon Cloud Directory.
- E. Configure AWS as a trusted relying party for the Active Directory.
- F. Configure IAM as a trusted relying party for Amazon Cloud Directory.

Answer: ACE

Explanation:

<https://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directory-federation-services-ad-fs/>

QUESTION 94

A Security Analyst attempted to troubleshoot the monitoring of suspicious security group changes. The Analyst was told that there is an Amazon CloudWatch alarm in place for these AWS CloudTrail log events. The Analyst tested the monitoring setup by making a configuration change to the security group but did not receive any alerts.

Which of the following troubleshooting steps should the Analyst perform?

- A. Ensure that CloudTrail and S3 bucket access logging is enabled for the Analyst's AWS account.
- B. Verify that a metric filter was created and then mapped to an alarm. Check the alarm notification.

- action.
- C. Check the CloudWatch dashboards to ensure that there is a metric configured with an appropriate dimension for security group changes.
 - D. Verify that the Analyst's account is mapped to an IAM policy that includes permissions for cloudwatch:
GetMetricStatistics and Cloudwatch: ListMetrics.

Answer: B

Explanation:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html>

QUESTION 95

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

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

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

Answer: D

Explanation:

Amazon EBS volumes are presented to you as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs immediately before reuse so that you can be assured that the wipe process completed. If you have procedures requiring that all data be wiped via a specific method, such as those detailed in NIST 800- 88 ("Guidelines for Media Sanitization"), you have the ability to do so on Amazon EBS. You should conduct a specialized wipe procedure prior to deleting the volume for compliance with your established requirements.
<https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf>

QUESTION 96

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

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

When trying to download an object from the S3 bucket from 10.10.10.40, the IAM user receives an access denied message.

What does the Administrator need to change to grant access to the user?

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

Answer: A

QUESTION 97

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

Pattern:

"randomID_datestamp_PII.csv"

Example:

"1234567_12302017_000-00-0000 csv"

The bucket where these objects are being stored is using server-side encryption (SSE).

Which solution is the most secure and cost-effective option to protect the sensitive data?

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

Answer: C

Explanation:

https://docs.aws.amazon.com/AmazonS3/latest/API/API_GetObject.html

Permissions

You need the s3:GetObject permission for this operation. For more information, see Specifying Permissions in a Policy. If the object you request does not exist, the error Amazon S3 returns depends on whether you also have the s3>ListBucket permission.

QUESTION 98

AWS CloudTrail is being used to monitor API calls in an organization. An audit revealed that CloudTrail is failing to deliver events to Amazon S3 as expected.

What initial actions should be taken to allow delivery of CloudTrail events to S3? (Select two)

- A. Verify that the S3 bucket policy allow CloudTrail to write objects.
- B. Verify that the IAM role used by CloudTrail has access to write to Amazon CloudWatch Logs.
- C. Remove any lifecycle policies on the S3 bucket that are archiving objects to Amazon Glacier.
- D. Verify that the S3 bucket defined in CloudTrail exists.
- E. Verify that the log file prefix defined in CloudTrail exists in the S3 bucket.

Answer: AD

Explanation:

Cloudguy365, yes that a possibility that i did not see.

That the bucket already existed when the cloudtrail was created. That's makes A as correct. And the folder prefix is optional on the bucket policy.

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/create-s3-bucket-policy-for-cloudtrail.html>

QUESTION 99

Due to new compliance requirements, a Security Engineer must enable encryption with customer-provided keys on corporate data that is stored in DynamoDB. The company wants to retain full control of the encryption keys.

Which DynamoDB feature should the Engineer use to achieve compliance'?

- A. Use AWS Certificate Manager to request a certificate. Use that certificate to encrypt data prior to uploading it to DynamoDB.
- B. Enable S3 server-side encryption with the customer-provided keys. Upload the data to Amazon S3, and then use S3Copy to move all data to DynamoDB
- C. Create a KMS master key. Generate per-record data keys and use them to encrypt data prior to

uploading it to DynamoDB. Dispose of the cleartext and encrypted data keys after encryption without storing.

- D. Use the DynamoDB Java encryption client to encrypt data prior to uploading it to DynamoDB.

Answer: D

Explanation:

We can use dynamodb java or python client for encryption for this scenario.

QUESTION 100

A Security Engineer must design a system that can detect whether a file on an Amazon EC2 host has been modified. The system must then alert the Security Engineer of the modification. What is the most efficient way to meet these requirements?

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

Answer: B

Explanation:

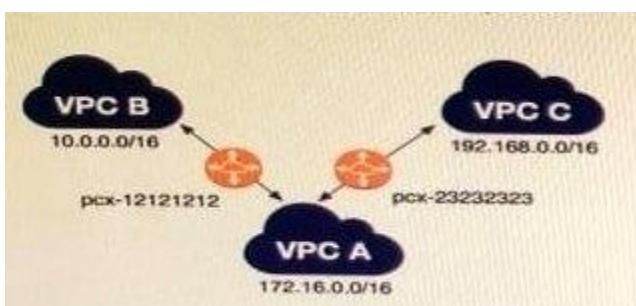
We can use cw for file integrity check. We are using script to achieve the same. Now IDS like trend have this feature. I think, better to use ids to achieve above use case.

QUESTION 101

A company has multiple VPCs in their account that are peered, as shown in the diagram.

A Security Engineer wants to perform penetration tests of the Amazon EC2 instances in all three VPCs.

How can this be accomplished? (Choose two.)



- A. Deploy a pre-authorized scanning engine from the AWS Marketplace into VPC B, and use it to scan instances in all three VPCs. Do not complete the penetration test request form.
- B. Deploy a pre-authorized scanning engine from the Marketplace into each VPC, and scan instances in each VPC from the scanning engine in that VPC. Do not complete the penetration test request form.
- C. Create a VPN connection from the data center to VPC A. Use an on-premises scanning engine to scan the instances in all three VPCs. Complete the penetration test request form for all three VPCs.

- D. Create a VPN connection from the data center to each of the three VPCs. Use an on-premises scanning engine to scan the instances in each VPC. Do not complete the penetration test request form.
- E. Create a VPN connection from the data center to each of the three VPCs. Use an on-premises scanning engine to scan the instances in each VPC. Complete the penetration test request form for all three VPCs.

Answer: BD

Explanation:

No Penetration Testing approval required now.

<https://aws.amazon.com/premiumsupport/knowledge-center/penetration-testing/>

QUESTION 102

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 Services to encrypt all the traffic between the client and application servers.

Answer: BD

Explanation:

The answer is in the question: check for known vulnerabilities (inspector) limit the attack surface (close unnecessary ports) terminating SSL alone in an ELB is only part of a solution, you have to take additional steps with security groups, moving EC2 to private subnets, etc.

QUESTION 103

For compliance reasons, an organization limits the use of resources to three specific AWS regions. It wants to be alerted when any resources are launched in unapproved regions.

Which of the following approaches will provide alerts on any resources launched in an unapproved region?

- A. Develop an alerting mechanism based on processing AWS Cloud Trail logs.
- B. Monitor Amazon S3 Event Notifications for objects stored in buckets in unapproved regions.
- C. Analyze Amazon CloudWatch Logs for activities in unapproved regions.
- D. Use AWS Trusted Advisor to alert on all resources being created.

Answer: A

Explanation:

You can now turn on a trail across all regions for your AWS account. CloudTrail will deliver log files from all regions to the Amazon S3 bucket and an optional CloudWatch Logs log group you specified. Additionally, when AWS launches a new region, CloudTrail will create the same trail in the new region. As a result, you will receive log files containing API activity for the new region without taking any action.

<https://aws.amazon.com/about-aws/whats-new/2015/12/turn-on-cloudtrail-across-all-regions-and-support-for-multiple-trails/>

QUESTION 104

A company runs an application on AWS that needs to be accessed only by employees. Most employees work from the office, but others work remotely or travel.

How can the Security Engineer protect this workload so that only employees can access it?

- A. Add each employee's home IP address to the security group for the application so that only those users can access the workload.
- B. Create a virtual gateway for VPN connectivity for each employee, and restrict access to the workload from within the VPC.
- C. Use a VPN appliance from the AWS Marketplace for users to connect to, and restrict workload access to traffic from that appliance.
- D. Route all traffic to the workload through AWS WAF. Add each employee's home IP address into an AWS WAF rule, and block all other traffic.

Answer: B

Explanation:

AWS VPN CloudHub If you have more than one remote network (for example, multiple branch offices), you can create multiple AWS Site-to-Site VPN connections via your virtual private gateway to enable communication between these networks. For more information, see Providing Secure Communication Between Sites Using VPN CloudHub in the AWS Site-to-Site VPN User Guide.

<https://aws.amazon.com/about-aws/whats-new/2018/12/introducing-aws-client-vpn-to-securely-access-aws-and-on-premises-resources/>

QUESTION 105

A Systems Engineer is troubleshooting the connectivity of a test environment that includes a virtual security appliance deployed inline. In addition to using the virtual security appliance, the Development team wants to use security groups and network ACLs to accomplish various security requirements in the environment.

What configuration is necessary to allow the virtual security appliance to route the traffic?

- A. Disable network ACLs.
- B. Configure the security appliance's elastic network interface for promiscuous mode.
- C. Disable the Network Source/Destination check on the security appliance's elastic network interface
- D. Place the security appliance in the public subnet with the internet gateway

Answer: C

Explanation:

Customers who need EC2 network appliances to run network address translation, routing, or firewall services can change this default behavior by disabling the Source/Destination Check attribute and configuring VPC route tables to send outbound traffic through the network appliance.

QUESTION 106

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

- Storage is accessible by using only VPCs.
- Service has tamper-evident controls.
- Access logging is enabled.

-Storage has high availability.

Which of the following services meets these requirements?

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

Answer: B

Explanation:

<https://aws.amazon.com/blogs/aws/aws-cloud-hsm-secure-key-storage-and-cryptographic-operations/>

QUESTION 107

An AWS account includes two S3 buckets: bucket1 and bucket2. The bucket2 does not have a policy defined, but bucket1 has the following bucket policy:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {"AWS": "arn:aws:iam::123456789012:user/alice"},  
            "Action": "s3:*",  
            "Resource": ["arn:aws:s3:::bucket1", "arn:aws:s3:::bucket1/*"]  
        }  
    ]  
}
```

In addition, the same account has an IAM User named "alice", with the following IAM policy.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {"Effect": "Allow",  
         "Action": "s3:*",  
         "Resource": ["arn:aws:s3:::bucket2", "arn:aws:s3:::bucket2/*"]  
    }  
]  
}
```

Which buckets can user "alice" access?

- A. Bucket1 only
- B. Bucket2 only
- C. Both bucket1 and bucket2
- D. Neither bucket1 nor bucket2

Answer: C

Explanation:

Both S3 policies and IAM policies can be used to grant access to buckets. IAM policies specify what actions are allowed or denied on what AWS resources (e.g. allow ec2:TerminateInstance on the EC2 instance with instance_id=i-8b3620ec). You attach IAM policies to IAM users, groups, or roles, which are then subject to the permissions you've defined. In other words, IAM policies define what a principal can do in your AWS environment. S3 bucket policies, on the other hand, are attached only to S3 buckets. S3 bucket policies specify what actions are allowed or denied for which principals on the bucket that the bucket policy is attached to (e.g. allow user Alice to PUT but not DELETE objects in the bucket).

<https://aws.amazon.com/blogs/security/iam-policies-and-bucket-policies-and-acls-oh-my-controlling-access-to-s3-resources/>

QUESTION 108

An organization has three applications running on AWS, each accessing the same data on Amazon S3. The data on Amazon S3 is server-side encrypted by using an AWS KMS Customer Master Key (CMK).

What is the recommended method to ensure that each application has its own programmatic access control permissions on the KMS CMK?

- A. Change the key policy permissions associated with the KMS CMK for each application when it must access the data in Amazon S3.
- B. Have each application assume an IAM role that provides permissions to use the AWS Certificate Manager CMK.
- C. Have each application use a grant on the KMS CMK to add or remove specific access controls on the KMS CMK.
- D. Have each application use an IAM policy in a user context to have specific access permissions on the KMS CMK.

Answer: C

Explanation:

<https://docs.aws.amazon.com/kms/latest/developerguide/grants.html>

QUESTION 109

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

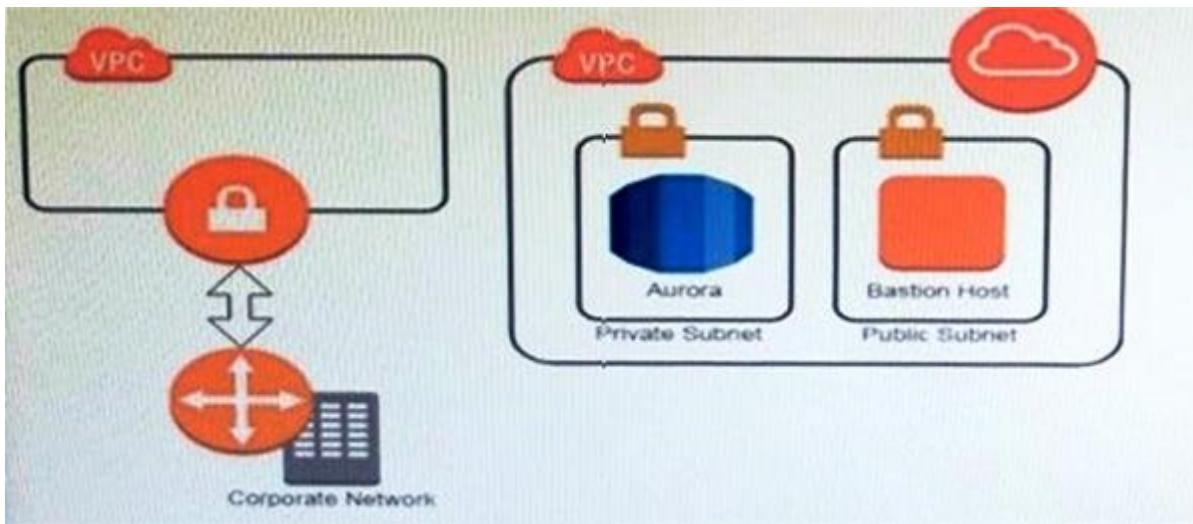
What would resolve the connectivity issue?

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

Answer: C

QUESTION 110

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



A security review has flagged this architecture as vulnerable, and a Security Engineer has been asked to make this design more secure. The company has a short deadline and a second VPN connection to the Aurora account is not possible.

How can a Security Engineer securely set up the bastion host?

- A. Move the bastion host to the VPC and VPN connectivity. Create a VPC peering relationship

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

Answer: A

QUESTION 111

An organization operates a web application that serves users globally. The application runs on Amazon EC2 instances behind an Application Load Balancer. There is an Amazon CloudFront distribution in front of the load balancer, and the organization uses AWS WAF. The application is currently experiencing a volumetric attack whereby the attacker is exploiting a bug in a popular mobile game. The application is being flooded with HTTP requests from all over the world with the User-Agent set to the following string: Mozilla/5.0 (compatible; ExampleCorp; ExampleGame/1.22; Mobile/1.0) What mitigation can be applied to block attacks resulting from this bug while continuing to service legitimate requests?

- A. Create a rule in AWS WAF rules with conditions that block requests based on the presence of ExampleGame/1.22 in the User-Agent header
- B. Create a geographic restriction on the CloudFront distribution to prevent access to the application from most geographic regions
- C. Create a rate-based rule in AWS WAF to limit the total number of requests that the web application services.
- D. Create an IP-based blacklist in AWS WAF to block the IP addresses that are originating from requests that contain ExampleGame/1.22 in the User-Agent header.

Answer: A

Explanation:

Rate based will still allow requests. Better to block completely based on headers using WAF.

QUESTION 112

Some highly sensitive analytics workloads are to be moved to Amazon EC2 hosts. Threat modeling has found that a risk exists where a subnet could be maliciously or accidentally exposed to the internet.

Which of the following mitigations should be recommended?

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

Answer: A

Explanation:

By default, Private instance has a private IP address, but no public IP address. These instances can communicate with each other, but can't access the Internet. You can enable Internet access for an instance launched into a nondefault subnet by attaching an Internet gateway to its VPC (if its VPC is not a default VPC) and associating an Elastic IP address with the instance.

Alternatively, to allow an instance in your VPC to initiate outbound connections to the Internet but prevent unsolicited inbound connections from the Internet, you can use a network address translation (NAT) instance. NAT maps multiple private IP addresses to a single public IP address. A NAT instance has an Elastic IP address and is connected to the Internet through an Internet gateway. You can connect an instance in a private subnet to the Internet through the NAT instance, which routes traffic from the instance to the Internet gateway, and routes any responses to the instance.

QUESTION 113

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

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

Answer: D

QUESTION 114

A Security Administrator at a university is configuring a fleet of Amazon EC2 instances. The EC2 instances are shared among students, and non-root SSH access is allowed. The Administrator is concerned about students attacking other AWS account resources by using the EC2 instance metadata service. What can the Administrator do to protect against this potential attack?

- A. Disable the EC2 instance metadata service.
- B. Log all student SSH interactive session activity.
- C. Implement ip tables-based restrictions on the instances.
- D. Install the Amazon Inspector agent on the instances.

Answer: A

Explanation:

<https://aws.amazon.com/about-aws/whats-new/2019/11/announcing-updates-amazon-ec2-instance-metadata-service/>

QUESTION 115

An organization receives an alert that indicates that an EC2 instance behind an ELB Classic Load Balancer has been compromised.

What techniques will limit lateral movement and allow evidence gathering?

- A. Remove the instance from the load balancer and terminate it.

- B. Remove the instance from the load balancer, and shut down access to the instance by tightening the security group.
- C. Reboot the instance and check for any Amazon CloudWatch alarms.
- D. Stop the instance and make a snapshot of the root EBS volume.

Answer: B

Explanation:

B - isolate the compromised instance and lockdown with Security group is the first step we do, followed by cpu and memory dump and further investigation.

C - Reboot will destroy evidence

D - this also we can consider. This is usually done after step B.

QUESTION 116

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

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

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

Answer: B

Explanation:

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

QUESTION 117

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

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

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

Answer: BDE

Explanation:

A: wrong. No need to remove ENI as best practice is to restrict Security Group.

C: No benefit of DNS health check.

F: No benefit as EC2 already compromised.

QUESTION 118

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

enable detection of any modification to the logs.

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

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

Answer: ACE

Explanation:

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

If you have created an organization in AWS Organizations, you can create a trail that will log all events for all AWS accounts in that organization. This is sometimes referred to as an organization trail. You can also choose to edit an existing trail in the master account and apply it to an organization, making it an organization trail. Organization trails log events for the master account and all member accounts in the organization. For more information about AWS Organizations, see Organizations Terminology and Concepts. Note Reference:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html> You must be logged in with the master account for the organization in order to create an organization trail. You must also have sufficient permissions for the IAM user or role in the master account in order to successfully create an organization trail. If you do not have sufficient permissions, you will not see the option to apply a trail to an organization.

QUESTION 119

A Security Engineer is implementing a solution to allow users to seamlessly encrypt Amazon S3 objects without having to touch the keys directly. The solution must be highly scalable without requiring continual management. Additionally, the organization must be able to immediately delete the encryption keys.

Which solution meets these requirements?

- A. Use AWS KMS with AWS managed keys and the ScheduleKeyDeletion API with a PendingWindowInDays set to 0 to remove the keys if necessary.
- B. Use KMS with AWS imported key material and then use the DeleteImportedKeyMaterial API to remove the key material if necessary.
- C. Use AWS CloudHSM to store the keys and then use the CloudHSM API or the PKCS11 library to delete the keys if necessary.
- D. Use the Systems Manager Parameter Store to store the keys and then use the service API operations to delete the key if necessary.

Answer: B

QUESTION 120

An application uses Amazon Cognito to manage end users' permissions when directly accessing AWS resources, including Amazon DynamoDB. A new feature request reads as follows:

Provide a mechanism to mark customers as suspended pending investigation or suspended permanently. Customers should still be able to log in when suspended, but should not be able to make changes. The priorities are to reduce complexity and avoid potential for future security issues. Which approach will meet these requirements and priorities?

- A. Create a new database field "suspended_status" and modify the application logic to validate that field when processing requests.
- B. Add suspended customers to second Cognito user pool and update the application login flow to check both user pools.
- C. Use Amazon Cognito Sync to push out a "suspension_status" parameter and split the IAM policy into normal users and suspended users.
- D. Move suspended customers to a second Cognito group and define an appropriate IAM access policy for the group.

Answer: D

Explanation:

As A and B increase the complexity. Simple solution is to make another group with less permission.

QUESTION 121

A company stores data on an Amazon EBS volume attached to an Amazon EC2 instance. The data is asynchronously replicated to an Amazon S3 bucket. Both the EBS volume and the S3 bucket are encrypted with the same AWS KMS Customer Master Key (CMK). A former employee scheduled a deletion of that CMK before leaving the company.

The company's Developer Operations department learns about this only after the CMK has been deleted.

Which steps must be taken to address this situation?

- A. Copy the data directly from the EBS encrypted volume before the volume is detached from the EC2 instance.
- B. Recover the data from the EBS encrypted volume using an earlier version of the KMS backing key.
- C. Make a request to AWS Support to recover the S3 encrypted data.
- D. Make a request to AWS Support to restore the deleted CMK, and use it to recover the data.

Answer: A

Explanation:

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

QUESTION 122

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

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

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

- D. The version of the Lambda function that was executed was not current.

Answer: A

Explanation:

<https://docs.aws.amazon.com/lambda/latest/dg/troubleshooting.html>

QUESTION 123

A company has Windows Amazon EC2 instances in a VPC that are joined to on-premises Active Directory servers for domain services. The security team has enabled Amazon GuardDuty on the AWS account to alert on issues with the instances.

During a weekly audit of network traffic, the Security Engineer notices that one of the EC2 instances is attempting to communicate with a known command-and-control server but failing.

This alert does not show up in GuardDuty.

Why did GuardDuty fail to alert to this behavior?

- A. GuardDuty did not have the appropriate alerts activated.
- B. GuardDuty does not see these DNS requests.
- C. GuardDuty only monitors active network traffic flow for command-and-control activity.
- D. GuardDuty does not report on command-and-control activity.

Answer: B

Explanation:

As per AWS DNS logs If you use AWS DNS resolvers for your EC2 instances (the default setting), then GuardDuty can access and process your request and response DNS logs through the internal AWS DNS resolvers. If you are using a 3rd party DNS resolver, for example, OpenDNS or GoogleDNS, or if you set up your own DNS resolvers, then GuardDuty cannot access and process data from this data source.

https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_data-sources.html

QUESTION 124

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

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

Answer: C

Explanation:

Both encrypted and plaintext parameter values are stored with only the Lambda function having permissions to decrypt the secrets.

<https://aws.amazon.com/blogs/compute/sharing-secrets-with-aws-lambda-using-aws-systems-manager-parameter-store/>

QUESTION 125

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

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

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

Answer: AE

Explanation:

You can develop custom rules and add them to AWS Config. You associate each custom rule with an AWS Lambda function, which contains the logic that evaluates whether your AWS resources comply with the rule.

https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules.html
<https://aws.amazon.com/blogs/security/how-to-audit-your-aws-resources-for-security-compliance-by-using-custom-aws-config-rules/>

QUESTION 126

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

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

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

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

Answer: B

QUESTION 127

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

Which action would provide the required functionality?

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

- D. Use key policies to restrict access to the appropriate IAM groups.

Answer: C

Explanation:

<https://aws.amazon.com/blogs/security/how-to-protect-the-integrity-of-your-encrypted-data-by-using-aws-key-management-service-and-encryptioncontext/>

QUESTION 128

An application makes calls to AWS services using the AWS SDK. The application runs on Amazon EC2 instances with an associated IAM role. When the application attempts to access an object within an Amazon S3 bucket; the Administrator receives the following error message:
HTTP 403: Access Denied.

Which combination of steps should the Administrator take to troubleshoot this issue? (Select three.)

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

Answer: BCE

Explanation:

You do not need SG to access S3 from Ec2 you need bucket policy as S3 uses multiple dynamic Ips.

<https://docs.aws.amazon.com/config/latest/developerguide/s3-bucket-policy.html>

QUESTION 129

A Security Engineer must implement mutually authenticated TLS connections between containers that communicate inside a VPC.

Which solution would be MOST secure and easy to maintain?

- A. Use AWS Certificate Manager to generate certificates from a public certificate authority and deploy them to all the containers.
- B. Create a self-signed certificate in one container and use AWS Secrets Manager to distribute the certificate to the other containers to establish trust.
- C. Use AWS Certificate Manager Private Certificate Authority (ACM PCA) to create a subordinate certificate authority, then create the private keys in the containers and sign them using the ACM PCA API.
- D. Use AWS Certificate Manager Private Certificate Authority (ACM PCA) to create a subordinate certificate authority, then use AWS Certificate Manager to generate the private certificates and deploy them to all the containers.

Answer: C

Explanation:

<https://aws.amazon.com/blogs/compute/maintaining-transport-layer-security-all-the-way-to-your-container-part-2-using-aws-certificate-manager-private-certificate-authority/>

QUESTION 130

The Accounting department at Example Corp. has made a decision to hire a third-party firm,

AnyCompany, to monitor Example Corp.'s AWS account to help optimize costs. The Security Engineer for Example Corp. has been tasked with providing AnyCompany with access to the required Example Corp. AWS resources. The Engineer has created an IAM role and granted permission to AnyCompany's AWS account to assume this role.

When customers contact AnyCompany, they provide their role ARN for validation. The Engineer is concerned that one of AnyCompany's other customers might deduce Example Corp.'s role ARN and potentially compromise the company's account.

What steps should the Engineer perform to prevent this outcome?

- A. Create an IAM user and generate a set of long-term credentials. Provide the credentials to AnyCompany. Monitor access in IAM access advisor and plan to rotate credentials on a recurring basis.
- B. Request an external ID from AnyCompany and add a condition with sts:ExternalId to the role's trust policy.
- C. Require two-factor authentication by adding a condition to the role's trust policy with aws:MultiFactorAuthPresent.
- D. Request an IP range from AnyCompany and add a condition with aws:SourceIp to the role's trust policy.

Answer: B

QUESTION 131

A company maintains sensitive data in an Amazon S3 bucket that must be protected using an AWS KMS CMK. The company requires that keys be rotated automatically every year.

How should the bucket be configured?

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

Answer: B

QUESTION 132

An Amazon S3 bucket is encrypted using an AWS KMS CMK. An IAM user is unable to download objects from the S3 bucket using the AWS Management Console; however, other users can download objects from the S3 bucket.

Which policies should the Security Engineer review and modify to resolve this issue? (Select three.)

- A. The CMK policy
- B. The VPC endpoint policy
- C. The S3 bucket policy
- D. The S3 ACL
- E. The IAM policy

Answer: ACE

QUESTION 133

While analyzing a company's security solution, a Security Engineer wants to secure the AWS account root user.

What should the Security Engineer do to provide the highest level of security for the account?

- A. Create a new IAM user that has administrator permissions in the AWS account. Delete the password for the AWS account root user.
- B. Create a new IAM user that has administrator permissions in the AWS account. Modify the permissions for the existing IAM users.
- C. Replace the access key for the AWS account root user. Delete the password for the AWS account root user.
- D. Create a new IAM user that has administrator permissions in the AWS account. Enable multi-factor authentication for the AWS account root user.

Answer: D

Explanation:

If you continue to use the root user credentials, we recommend that you follow the security best practice to enable multi-factor authentication (MFA) for your account. Because your root user can perform sensitive operations in your account, adding an additional layer of authentication helps you to better secure your account. Multiple types of MFA are available.

QUESTION 134

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 enable 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 135

While securing the connection between a company's VPC and its on-premises data center, a Security Engineer sent a ping command from an on-premises host (IP address 203.0.113.12) to an Amazon EC2 instance (IP address 172.31.16.139). The ping command did not return a response. The flow log in the VPC showed the following:

```
2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027  
1432917142 ACCEPT OK  
2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094  
1432917142 REJECT OK
```

What action should be performed to allow the ping to work?

- A. In the security group of the EC2 instance, allow inbound ICMP traffic.
- B. In the security group of the EC2 instance, allow outbound ICMP traffic.
- C. In the VPC's NACL, allow inbound ICMP traffic.
- D. In the VPC's NACL, allow outbound ICMP traffic.

Answer: C

Explanation:

All subnets in the same VPC can be connected to each other by default.

QUESTION 136

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 137

A company has several production AWS accounts and a central security AWS account. The security account is used for centralized monitoring and has IAM privileges to all resources in every corporate account. All of the company's Amazon S3 buckets are tagged with a value denoting the data classification of their contents.

A Security Engineer is deploying a monitoring solution in the security account that will enforce bucket policy compliance. The system must monitor S3 buckets in all production accounts and confirm that any policy change is in accordance with the bucket's data classification. If any change is out of compliance; the Security team must be notified quickly.

Which combination of actions would build the required solution? (Choose three.)

- A. Configure Amazon CloudWatch Events in the production accounts to send all S3 events to the security account event bus.
- B. Enable Amazon GuardDuty in the security account. and join the production accounts as members.
- C. Configure an Amazon CloudWatch Events rule in the security account to detect S3 bucket creation or modification events.
- D. Enable AWS Trusted Advisor and activate email notifications for an email address assigned to the security contact.
- E. Invoke an AWS Lambda function in the security account to analyze S3 bucket settings in response to S3 events, and send non-compliance notifications to the Security team.

- F. Configure event notifications on S3 buckets for PUT; POST, and DELETE events.

Answer: ACE

Explanation:

<https://docs.aws.amazon.com/config/latest/developerguide/monitor-config-with-cloudwatchevents.html>

B: GuardDuty is advance threat protection. <https://aws.amazon.com/guardduty/>

D: Trusted Advisor cannot do this kind of monitoring. It's more on advisory.

F: This is for S3 object modifications and not bucket changes.

QUESTION 138

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

- A. Server-side encryption with Amazon S3-managed keys (SSE-S3)
- B. Server-side encryption with AWS KMS-managed keys (SSE-KMS)
- C. Server-side encryption with customer-provided keys (SSE-C)
- D. Client-side encryption with an AWS KMS-managed CMK

Answer: B

QUESTION 139

A Security Engineer is defining the logging solution for a newly developed product. Systems Administrators and Developers need to have appropriate access to event log files in AWS CloudTrail to support and troubleshoot the product.

Which combination of controls should be used to protect against tampering with and unauthorized access to log files? (Choose two.)

- A. Ensure that the log file integrity validation mechanism is enabled.
- B. Ensure that all log files are written to at least two separate Amazon S3 buckets in the same account.
- C. Ensure that Systems Administrators and Developers can edit log files, but prevent any other access.
- D. Ensure that Systems Administrators and Developers with job-related need-to-know requirements only are capable of viewing--but not modifying--the log files.
- E. Ensure that all log files are stored on Amazon EC2 instances that allow SSH access from the internal corporate network only.

Answer: AD

QUESTION 140

A company has a few dozen application servers in private subnets behind an Elastic Load Balancer (ELB) in an AWS Auto Scaling group. The application is accessed from the web over HTTPS. The data must always be encrypted in transit. The Security Engineer is worried about potential key exposure due to vulnerabilities in the application software.

Which approach will meet these requirements while protecting the external certificate during a breach?

- A. Use a Network Load Balancer (NLB) to pass through traffic on port 443 from the internet to port

- 443 on the instances.
- B. Purchase an external certificate, and upload it to the AWS Certificate Manager (for use with the ELB) and to the instances. Have the ELB decrypt traffic, and route and re-encrypt with the same certificate.
 - C. Generate an internal self-signed certificate and apply it to the instances. Use AWS Certificate Manager to generate a new external certificate for the ELB. Have the ELB decrypt traffic, and route and re- encrypt with the internal certificate.
 - D. Upload a new external certificate to the load balancer. Have the ELB decrypt the traffic and forward it on port 80 to the instances.

Answer: C

QUESTION 141

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

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

Answer: BC

Explanation:

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

QUESTION 142

A company uses identity federation to authenticate users into an identity account (987654321987) where the users assume an IAM role named IdentityRole. The users then assume an IAM role named JobFunctionRole in the target AWS account (123456789123) to perform their job functions. A user is unable to assume the IAM role in the target account. The policy attached to the role in the identity account is:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "sts:AssumeRole"  
            ],  
            "Resource": [  
                "arn:aws:iam::*:role/JobFunctionRole"  
            ],  
            "Effect": "Allow"  
        }  
    ]  
}
```

What should be done to enable the user to assume the appropriate role in the target account?

- A. Update the IAM policy attached to the role in the identity account to be:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "sts:AssumeRole"  
            ],  
            "Resource": [  
                "arn:aws:iam::123456789123:role/JobFunctionRole"  
            ],  
            "Effect": "Allow"  
        }  
    ]  
}
```

- B. Update the trust policy on the role in the target account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::987654321987:role/IdentityRole"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

- C. Update the trust policy on the role in the identity account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": { "AWS": "arn:aws:iam::987654321987:root" },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

- D. Update the IAM policy attached to the role in the target account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1502946463000",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::123456789123:role/JobFunctionRole"
        }
    ]
}
```

Answer: A

QUESTION 143

A Security Engineer is working with the development team to design a supply chain application that stores sensitive inventory data in an Amazon S3 bucket. The application will use an AWS KMS customer master key (CMK) to encrypt the data on Amazon S3. The inventory data on Amazon S3 will be shared of vendors. All vendors will use AWS principals from their own AWS

accounts to access the data on Amazon S3. The vendor list may change weekly, and the solution must support cross-account access. What is the MOST efficient way to manage access control for the KMS CMK?

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

Answer: A

QUESTION 144

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

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

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

Answer: B

QUESTION 145

A corporate cloud security policy states that communications between the company's VPC and KMS must travel entirely within the AWS network and not use public service endpoints. Which combination of the following actions MOST satisfies this requirement? (Choose two.)

- A. Add the aws:sourceVpce condition to the AWS KMS key policy referencing the company's VPC endpoint ID.
- B. Remove the VPC internet gateway from the VPC and add a virtual private gateway to the VPC to prevent direct, public internet connectivity.
- C. Create a VPC endpoint for AWS KMS with private DNS enabled.
- D. Use the KMS Import Key feature to securely transfer the AWS KMS key over a VPN.
- E. Add the following condition to the AWS KMS key policy: "aws:Sourcelp": "10.0.0.0/16".

Answer: AC

Explanation:

An IAM policy can deny access to KMS except through your VPC endpoint with the following condition statement:

```
"Condition": {  
    "StringNotEquals": {  
        "aws:sourceVpce": "vpce-0295a3caf8414c94a"
```

}

}

If you select the Enable Private DNS Name option, the standard AWS KMS DNS hostname (<https://kms.<region>.amazonaws.com>) resolves to your VPC endpoint.

QUESTION 146

A company had one of its Amazon EC2 key pairs compromised. A Security Engineer must identify which current Linux EC2 instances were deployed and used the compromised key pair. How can this task be accomplished?

- Obtain the list of instances by directly querying Amazon EC2 using: `aws ec2 describe-instances --filters "Name=key-name,Values=KEYNAMEHERE"`.
- Obtain the fingerprint for the key pair from the AWS Management Console, then search for the fingerprint in the Amazon Inspector logs.
- Obtain the output from the EC2 instance metadata using: `curl http://169.254.169.254/latest/meta-data/public-keys/0/`.
- Obtain the fingerprint for the key pair from the AWS Management Console, then search for the fingerprint in Amazon CloudWatch Logs using: `aws logs filter-log-events`.

Answer: A

Explanation:

<https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-instances.html>

QUESTION 147

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

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

Answer: C

QUESTION 148

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

What policy should the Engineer implement?

A.

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

B.

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

C.

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

D.

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

Answer: C

QUESTION 149

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

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

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

Answer: B

Explanation:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-parameter-store.html>

QUESTION 150

A company is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information. The Security team has the following requirements for the architecture:

- Data must be encrypted in transit.
- Data must be encrypted at rest.
- The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential.

Which combination of steps would meet the requirements? (Choose two.)

- A. Enable AES-256 encryption using server-side encryption with Amazon S3-managed encryption keys (SSE-S3) on the S3 bucket.
- B. Enable default encryption with server-side encryption with AWS KMS-managed keys (SSE-KMS) on the S3 bucket.
- C. Add a bucket policy that includes a deny if a PutObject request does not include .aws:SecureTransport
- D. Add a bucket policy with aws:SourceIp to Allow uploads and downloads from the corporate intranet only.
- E. Add a bucket policy that includes a deny if a PutObject request does not include s3:x-amz-server-side-encryption: "aws:kms"
- F. Enable Amazon Macie to monitor and act on changes to the data lake's S3 bucket.

Answer: BC

QUESTION 151

A Security Engineer discovered a vulnerability in an application running on Amazon ECS. The vulnerability allowed attackers to install malicious code. Analysis of the code shows it exfiltrates data on port 5353 in batches at random time intervals.

While the code of the containers is being patched, how can Engineers quickly identify all compromised hosts and stop the egress of data on port 5353?

- A. Enable AWS Shield Advanced and AWS WAF. Configure an AWS WAF custom filter for egress traffic on port 5353
- B. Enable Amazon Inspector on Amazon ECS and configure a custom assessment to evaluate containers that have port 5353 open. Update the NACLs to block port 5353 outbound.

- C. Create an Amazon CloudWatch custom metric on the VPC Flow Logs identifying egress traffic on port 5353. Update the NACLs to block port 5353 outbound.
- D. Use Amazon Athena to query AWS CloudTrail logs in Amazon S3 and look for any traffic on port 5353.
Update the security groups to block port 5353 outbound.

Answer: C

QUESTION 152

An Amazon EC2 instance is denied access to a newly created AWS KMS CMK used for decrypt actions.

The environment has the following configuration:

- The instance is allowed the kms:Decrypt action in its IAM role for all resources
- The AWS KMS CMK status is set to enabled
- The instance can communicate with the KMS API using a configured VPC endpoint

What is causing the issue?

- A. The kms:GenerateDataKey permission is missing from the EC2 instance's IAM role
- B. The ARN tag on the CMK contains the EC2 instance's ID instead of the instance's ARN
- C. The kms:Encrypt permission is missing from the EC2 IAM role
- D. The KMS CMK key policy that enables IAM user permissions is missing

Answer: D

Explanation:

In a key policy, you use "*" for the resource, which means "this CMK." A key policy applies only to the CMK it is attached to

Reference: <https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html>

QUESTION 153

A company has enabled Amazon GuardDuty in all Regions as part of its security monitoring strategy. In one of the VPCs, the company hosts an Amazon EC2 instance working as an FTP server that is contacted by a high number of clients from multiple locations. This is identified by GuardDuty as a brute force attack due to the high number of connections that happen every hour.

The finding has been flagged as a false positive. However, GuardDuty keeps raising the issue. A Security Engineer has been asked to improve the signal-to-noise ratio. The Engineer needs to ensure that changes do not compromise the visibility of potential anomalous behavior.

How can the Security Engineer address the issue?

- A. Disable the FTP rule in GuardDuty in the Region where the FTP server is deployed
- B. Add the FTP server to a trusted IP list and deploy it to GuardDuty to stop receiving the notifications
- C. Use GuardDuty filters with auto archiving enabled to close the findings
- D. Create an AWS Lambda function that closes the finding whenever a new occurrence is reported

Answer: B

Explanation:

Trusted IP lists consist of IP addresses that you have whitelisted for secure communication with your AWS infrastructure and applications. GuardDuty does not generate findings for IP addresses on trusted IP lists.

At any given time, you can have only one uploaded trusted IP list per AWS account per region.
Reference: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_upload_lists.html

QUESTION 154

What are the MOST secure ways to protect the AWS account root user of a recently opened AWS account? (Choose two.)

- A. Use the AWS account root user access keys instead of the AWS Management Console
- B. Enable multi-factor authentication for the AWS IAM users with the AdministratorAccess managed policy attached to them
- C. Enable multi-factor authentication for the AWS account root user
- D. Use AWS KMS to encrypt all AWS account root user and AWS IAM access keys and set automatic rotation to 30 days
- E. Do not create access keys for the AWS account root user; instead, create AWS IAM users

Answer: CE

Explanation:

A: access key is the same with console, not help
B: MFA for IAM user will not help root account;
D: rotate will help a little, but the question is "The most";

QUESTION 155

A company has decided to migrate sensitive documents from on-premises data centers to Amazon S3. Currently, the hard drives are encrypted to meet a compliance requirement regarding data encryption. The CISO wants to improve security by encrypting each file using a different key instead of a single key. Using a different key would limit the security impact of a single exposed key.

Which of the following requires the LEAST amount of configuration when implementing this approach?

- A. Place each file into a different S3 bucket. Set the default encryption of each bucket to use a different AWS KMS customer managed key.
- B. Put all the files in the same S3 bucket. Using S3 events as a trigger, write an AWS Lambda function to encrypt each file as it is added using different AWS KMS data keys.
- C. Use the S3 encryption client to encrypt each file individually using S3-generated data keys
- D. Place all the files in the same S3 bucket. Use server-side encryption with AWS KMS-managed keys (SSE-KMS) to encrypt the data

Answer: D

Explanation:

<https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html>

QUESTION 156

A company has an encrypted Amazon S3 bucket. An Application Developer has an IAM policy that allows access to the S3 bucket, but the Application Developer is unable to access objects within the bucket.

What is a possible cause of the issue?

- A. The S3 ACL for the S3 bucket fails to explicitly grant access to the Application Developer
- B. The AWS KMS key for the S3 bucket fails to list the Application Developer as an administrator
- C. The S3 bucket policy fails to explicitly grant access to the Application Developer
- D. The S3 bucket policy explicitly denies access to the Application Developer

Answer: C

Explanation:

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

QUESTION 157

A Web Administrator for the website example.com has created an Amazon CloudFront distribution for dev.example.com, with a requirement to configure HTTPS using a custom TLS certificate imported to AWS Certificate Manager.

Which combination of steps is required to ensure availability of the certificate in the CloudFront console? (Choose two.)

- A. Call UploadServerCertificate with /cloudfront/dev/ in the path parameter.
- B. Import the certificate with a 4,096-bit RSA public key.
- C. Ensure that the certificate, private key, and certificate chain are PKCS #12-encoded.
- D. Import the certificate in the us-east-1 (N. Virginia) Region.
- E. Ensure that the certificate, private key, and certificate chain are PEM-encoded.

Answer: DE

Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/custom-ssl-certificate-cloudfront/>

QUESTION 158

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

What should the Security Engineer do to achieve this?

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

Answer: D

Explanation:

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

QUESTION 159

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

Engineer adds the following SCP to the OU:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowS3",  
            "Effect": "Allow",  
            "Action": "s3:*",  
            "Resource": "*"  
        }  
    ]  
}
```

The next day, API calls to AWS IAM appear in AWS CloudTrail logs in an account under that OU.

How should the Security Engineer resolve this issue?

- A. Move the account to a new OU and deny IAM:/* permissions.
- B. Add a Deny policy for all non-S3 services at the account level.
- C. Change the policy to:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowS3",  
            "Effect": "Allow",  
            "Action": "s3:*",  
            "Resource": "*/*"  
        }  
    ]  
}
```

- D. Detach the default FullAWSAccess SCP.

Answer: D

Explanation:

An allow list strategy has you remove the FullAWSAccess SCP that is attached by default to every OU and account. This means that no APIs are permitted anywhere unless you explicitly allow them.

QUESTION 160

A Developer is creating an AWS Lambda function that requires environment variables to store connection information and logging settings. The Developer is required to use an AWS KMS Customer Master Key (CMK) supplied by the Information Security department in order to adhere to company standards for securing Lambda environment variables.

Which of the following are required for this configuration to work? (Choose two.)

- A. The Developer must configure Lambda access to the VPC using the --vpc-config parameter.
- B. The Lambda function execution role must have the kms:Decrypt permission added in the AWS IAM policy.
- C. The KMS key policy must allow permissions for the Developer to use the KMS key.
- D. The AWS IAM policy assigned to the Developer must have the kms:GenerateDataKey permission added.
- E. The Lambda execution role must have the kms:Encrypt permission added in the AWS IAM policy.

Answer: DE

QUESTION 161

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

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

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

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

Answer: C

QUESTION 162

A company has several workloads running on AWS. Employees are required to authenticate using on-premises ADFS and SSO to access the AWS Management Console. Developers migrated an existing legacy web application to an Amazon EC2 instance. Employees need to access this application from anywhere on the internet, but currently, there is no authentication system built into the application.

How should the Security Engineer implement employee-only access to this system without changing the application?

- A. Place the application behind an Application Load Balancer (ALB). Use Amazon Cognito as authentication for the ALB.

- Define a SAML based Amazon Cognito user pool and connect it to ADFS.
- B. Implement AWS SSO in the master account and link it to ADFS as an identity provider.
Define the EC2 instance as a managed resource, then apply an IAM policy on the resource.
- C. Define an Amazon Cognito identity pool, then install the connector on the Active Directory server.
Use the Amazon Cognito SDK on the application instance to authenticate the employees using their Active Directory user names and passwords.
- D. Create an AWS Lambda custom authorizer as the authenticator for a reverse proxy on Amazon EC2.
Ensure the security group on Amazon EC2 only allows access from the Lambda function.

Answer: C

QUESTION 163

An Application Developer is using an AWS Lambda function that must use AWS KMS to perform encrypt and decrypt operations for API keys that are less than 2 KB.

Which key policy would allow the application to do this while granting least privilege?

- A. {
 "Sid": "AllowUserOfTheKey",
 "Effect": "Allow",
 "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
 >Action": [
 "kms:*"
],
 "Resource": "*"
}

B. {
 "Sid": "AllowUserOfTheKey",
 "Effect": "Allow",
 "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
 "Action": [
 "kms:Encrypt",
 "kms:Decrypt"
],
 "Resource": "*"
}

C. {
 "Sid": "AllowUserOfTheKey",
 "Effect": "Allow",
 "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
 "Action": [
 "kms:DescribeKey",
 "kms:GenerateDataKey*",
 "kms:Encrypt",
 "kms:ReEncrypt*",
 "kms:Decrypt"
],
 "Resource": "*"
}

```
D. {
    "Sid": "AllowUserOfTheKey",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
    "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey*",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "kms:Disable*",
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

Answer: C

QUESTION 164

A company is migrating its legacy workloads to AWS. The current security information events management (SIEM) system that analyzes logs is aging, and different SIEM systems are being evaluated to replace it. The company wants to change SIEMs without re-architecture the solution.

What should the Security Engineer do to accomplish this with minimal operational impact?

- A. Prepare an AMI with the SIEM log forwarder agent for each workload, and configure it to send logs to a centralized SIEM located in the Security team AWS account.
Configure an Amazon EC2 instance base AMI to forward logs to its local log forwarder agent.
Deploy an AMI in each workload.
- B. Configure an Amazon EC2 base AMI with an Amazon Kinesis Agent, and configure it to send to Amazon Kinesis Data Streams in the Security team AWS account.
Add an AWS Lambda function at Kinesis Data Streams to push streamed logs to the SIEM.
- C. Configure an Amazon EC2 base AMI to send logs to a local AWS CloudTrail log file.
Configure CloudTrail to send logs to Amazon CloudWatch.
Set up a central SIEM in the Security team AWS account and configure a puller to get information on CloudWatch.
- D. Select a pay-per-use SIEM in the AWS Marketplace.
Deploy the AMI in each workload to provide elasticity when required.
Use Amazon Athena to send real-time alerts.

Answer: B

QUESTION 165

An Application team has requested a new AWS KMS master key for use with Amazon S3, but the organizational security policy requires separate master keys for different AWS services to limit blast radius.

How can an AWS KMS customer master key (CMK) be constrained to work with only Amazon S3?

- A. Configure the CMK key policy to allow only the Amazon S3 service to use the kms:Encrypt action.
- B. Configure the CMK key policy to allow AWS KMS actions only when the kms:ViaService condition matches the Amazon S3 service name.
- C. Configure the IAM user's policy to allow KMS to pass a role to Amazon S3.

- D. Configure the IAM user's policy to allow only Amazon S3 operations when they are combined with the CMK.

Answer: B

Explanation:

<https://www.slideshare.net/AmazonWebServices/protecting-your-data-with-aws-kms-and-aws-cloudhsm> (17)

QUESTION 166

A company is developing a highly resilient application to be hosted on multiple Amazon EC2 instances. The application will store highly sensitive user data in Amazon RDS tables.

The application must:

- Include migration to a different AWS Region in the application disaster recovery plan.
- Provide a full audit trail of encryption key administration events.
- Allow only company administrators to administer keys.
- Protect data at rest using application layer encryption.

A Security Engineer is evaluating options for encryption key management.

Why should the Security Engineer choose AWS CloudHSM over AWS KMS for encryption key management in this situation?

- A. The key administration event logging generated by CloudHSM is significantly more extensive than AWS KMS.
- B. CloudHSM ensures that only company support staff can administer encryption keys, whereas AWS KMS allows AWS staff to administer keys.
- C. The ciphertext producer by CloudHSM provides more robust protection against brute force decryption attacks than the ciphertext produced by AWS KMS.
- D. CloudHSM provides the ability to copy keys to a different Region, whereas AWS KMS does not.

Answer: B

QUESTION 167

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

Which solution will meet these requirements?

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

Answer: C

Explanation:

<https://aws.amazon.com/shield/faqs/>

QUESTION 168

A Security Engineer signed in to the AWS Management Console as an IAM user and switched to the security role IAM role. To perform a maintenance operation, the Security Engineer needs to switch to the maintainer role IAM role, which lists the security role as a trusted entity. The Security Engineer attempts to switch to the maintainer role, but it fails.

What is the likely cause of the failure?

- A. The security role and the maintainer role are not assigned to the IAM user that the Security Engineer used to sign in to the account.
- B. The Security Engineer should have logged in as the AWS account root user, which is allowed to assume any role directly.
- C. The maintainer role does not include the IAM user as a trusted entity.
- D. The security role does not include a statement in its policy to allow an sts:AssumeRole action.

Answer: D

Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/troubleshoot-iam-policy-issues/>

QUESTION 169

A company is configuring three Amazon EC2 instances with each instance in a separate Availability Zone. The EC2 instances will be used as transparent proxies for outbound internet traffic for ports 80 and 443 so the proxies can block traffic to certain internet destinations as required by the company's security policies.

A Security Engineer completed the following:

- Set up the proxy software on the EC2 instances.
- Modified the route tables on the private subnets to use the proxy EC2 instances as the default route.
- Created a security group rule opening inbound port 80 and 443 TCP protocols on the proxy EC2 instance security group.

However, the proxy EC2 instances are not successfully forwarding traffic to the internet.

What should the Security Engineer do to make the proxy EC2 instances route traffic to the internet?

- A. Put all the proxy EC2 instances in a cluster placement group.
- B. Disable source and destination checks on the proxy EC2 instances.
- C. Open all inbound ports on the proxy EC2 instance security group.
- D. Change the VPC's DHCP domain-name-servers options set to the IP addresses of proxy EC2 instances.

Answer: B

Explanation:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_NAT_Instance.html

QUESTION 170

For compliance reasons, a Security Engineer must produce a weekly report that lists any instance that does not have the latest approved patches applied. The Engineer must also ensure that no system goes more than 30 days without the latest approved updates being applied.

What would be the MOST efficient way to achieve these goals?

- A. Use Amazon Inspector to determine which systems do not have the latest patches applied, and after 30 days, redeploy those instances with the latest AMI version.
- B. Configure Amazon EC2 Systems Manager to report on instance patch compliance, and enforce updates during the defined maintenance windows.
- C. Examine AWS CloudTrail logs to determine whether any instances have not restarted in the last 30 days, and redeploy those instances.
- D. Update the AMIs with the latest approved patches, and redeploy each instance during the defined maintenance window.

Answer: B

QUESTION 171

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

What should the Security Engineer do to meet these requirements?

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

Answer: A

QUESTION 172

A recent security audit found that AWS CloudTrail logs are insufficiently protected from tampering and unauthorized access.

Which actions must the Security Engineer take to access these audit findings? (Choose three.)

- A. Ensure CloudTrail log file validation is turned on.
- B. Configure an S3 lifecycle rule to periodically archive CloudTrail logs into Glacier for long-term storage.
- C. Use an S3 bucket with tight access controls that exists in a separate account.
- D. Use Amazon Inspector to monitor the file integrity of CloudTrail log files.
- E. Request a certificate through ACM and use a generated certificate private key to encrypt CloudTrail log files.
- F. Encrypt the CloudTrail log files with server-side encryption AWS KMS-managed keys (SSE-KMS).

Answer: ABF

Explanation:

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

QUESTION 173

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

- Block traffic from documented known bad IP addresses.
- Detect known software vulnerabilities and CIS Benchmarks compliance.

Which solution addresses these requirements?

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

Answer: C

QUESTION 174

A company needs to retain log data archives for several years to be compliant with regulations. The log data is no longer used, but it must be retained.

What is the MOST secure and cost-effective solution to meet these requirements?

- A. Archive the data to Amazon S3 and apply a restrictive bucket policy to deny the s3:DeleteObject API.
- B. Archive the data to Amazon S3 Glacier and apply a Vault Lock policy.
- C. Archive the data to Amazon S3 and replicated it to a second bucket in a second AWS Region. Choose the S3 Standard-Infrequent Access (S3 Standard-IA) storage class and apply a restrictive bucket policy to deny the s3:DeleteObject API.
- D. Migrate the log data to a 16 TB Amazon Elastic Block Store (Amazon EBS) volume. Create a snapshot of the EBS volume.

Answer: C

QUESTION 175

Developers in an organization have moved from a standard application deployment to containers. The Security Engineer is tasked with ensuring that containers are secure.

Which strategies will reduce the attack surface and enhance the security of the containers? (Choose two.)

- A. Use the containers to automate security deployments.
- B. Limit resource consumption (CPU, memory), networking connectors, ports, and unnecessary container libraries.
- C. Segregate container by host, function, and data classification.
- D. Use Docker Notary framework to sign task definitions.
- E. Enable container breakout at the host kernel.

Answer: BD

QUESTION 176

Auditors for a health care company have mandated that all data volumes be encrypted at rest. Infrastructure is deployed mainly via AWS CloudFormation; however, third-party frameworks and manual deployment are required on some legacy systems.

What is the BEST way to monitor, on a recurring basis, whether all EBS volumes are encrypted?

- A. On a recurring basis, update all IAM user policies to require that EC2 instances are created with an encrypted volume.
- B. Configure an AWS Config rule to run on a recurring basis for volume encryption.
- C. Set up Amazon Inspector rules for volume encryption to run on a recurring schedule.
- D. Use CloudWatch Logs to determine whether instances were created with an encrypted volume.

Answer: B

Explanation:

Using AWS Config Rules, you can run continuous assessment checks on your resources to verify that they comply with your own security policies, industry best practices, and compliance regimes such as PCI/ HIPAA. For example, AWS Config provides a managed AWS Config Rules to ensure that encryption is turned on for all EBS volumes in your account. You can also write a custom AWS Config Rule to essentially "codify" your own corporate security policies. AWS Config

alerts you in real time when a resource is misconfigured, or when a resource violates a particular security policy.

Reference: <https://d1.awsstatic.com/whitepapers/aws-security-whitepaper.pdf>

QUESTION 177

A company became aware that one of its access keys was exposed on a code sharing website 11 days ago. A Security Engineer must review all use of the exposed keys to determine the extent of the exposure. The company enabled AWS CloudTrail in all regions when it opened the account.

Which of the following will allow the Security Engineer to complete the task?

- A. Filter the event history on the exposed access key in the CloudTrail console.
Examine the data from the past 11 days.
- B. Use the AWS CLI to generate an IAM credential report.
Extract all the data from the past 11 days.
- C. Use Amazon Athena to query the CloudTrail logs from Amazon S3.
Retrieve the rows for the exposed access key for the past 11 days.
- D. Use the Access Advisor tab in the IAM console to view all of the access key activity for the past 11 days.

Answer: A

Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudtrail-search-for-activity/>

QUESTION 178

A Development team has built an experimental environment to test a simple static web application. It has built an isolated VPC with a private and a public subnet. The public subnet holds only an Application Load Balancer, a NAT gateway, and an internet gateway. The private subnet holds all of the Amazon EC2 instances.

There are 3 different types of servers. Each server type has its own Security Group that limits access to only required connectivity. The Security Groups have both inbound and outbound rules applied. Each subnet has both inbound and outbound network ACLs applied to limit access to only required connectivity.

Which of the following should the team check if a server cannot establish an outbound connection to the internet? (Choose three.)

- A. The route tables and the outbound rules on the appropriate private subnet security group.
- B. The outbound network ACL rules on the private subnet and the inbound network ACL rules on the public subnet.
- C. The outbound network ACL rules on the private subnet and both the inbound and outbound rules on the public subnet.
- D. The rules on any host-based firewall that may be applied on the Amazon EC2 instances.
- E. The Security Group applied to the Application Load Balancer and NAT gateway.
- F. That the 0.0.0.0/0 route in the private subnet route table points to the Internet gateway in the public subnet.

Answer: ACD

QUESTION 179

Example.com is hosted on Amazon EC2 instance behind an Application Load Balancer (ALB). Third-party host intrusion detection system (HIDS) agents that capture the traffic of the EC2 instance are running on each host. The company must ensure they are using privacy enhancing technologies for users, without losing the assurance the third-party solution offers.

What is the MOST secure way to meet these requirements?

- A. Enable TLS pass through on the ALB, and handle decryption at the server using Elliptic Curve Diffie-Hellman (ECDHE) cipher suites.
- B. Create a listener on the ALB that uses encrypted connections with Elliptic Curve Diffie-Hellman (ECDHE) cipher suites, and pass the traffic in the clear to the server.
- C. Create a listener on the ALB that uses encrypted connections with Elliptic Curve Diffie-Hellman (ECDHE) cipher suites, and use encrypted connections to the servers that do not enable Perfect Forward Security (PRS).
- D. Create a listener on the ALB that does not enable Perfect Forward Security (PFS) cipher suites, and use encrypted connections to the server using Elliptic Curve Diffie-Hellman (ECDHE) cipher suites.

Answer: C

QUESTION 180

A Website currently runs on Amazon EC2 with mostly static content on the site. Recently, the site was subjected to a DDoS attack, and a Security Engineer was tasked with redesigning the edge security to help mitigate this risk in the future.

What are some ways the Engineer could archive this? (Choose three.)

- A. Use AWS X-Ray to inspect the traffic going to the EC2 instances.
- B. Move the static content to Amazon S3, and front this with Amazon CloudFront distribution.
- C. Change the security group configuration to block the source of the attack traffic.
- D. Use AWS WAF security rules to inspect the inbound traffic.
- E. Use Amazon Inspector assessment templates to inspect the inbound traffic.
- F. Use Amazon Route 53 to distribute traffic.

Answer: ABE

QUESTION 181

A company manages three separate AWS accounts for its production, development, and test environments. Each Developer is assigned a unique IAM user under the development account. A new application hosted on an Amazon EC2 instance in the development account requires read access to the archived documents stored in an Amazon S3 bucket in the production account.

How should access be granted?

- A. Create an IAM role in the production account and allow EC2 instance in the development account to assume that role using the trust policy.
Provide read access for the required S3 bucket to this role.
- B. Use a custom identity broker to allow Developer IAM users to temporarily access the S3 bucket.
- C. Create a temporary IAM user for the application to use in the production account.
- D. Create a temporary IAM user in the production account and provide read access to Amazon S3.
Generate the temporary IAM user's access key and secret key and store these keys on the EC2 instance used by the application in the development account.

Answer: A

Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/cross-account-access-s3/>

QUESTION 182

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

How should a Security Engineer accomplish this?

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

Answer: D

QUESTION 183

An organizational must establish the ability to delete an AWS KMS Customer Master Key (CMK) within a 24-hour timeframe to keep it from being used for encrypt or decrypt operations.

Which of the following actions will address this requirement?

- A. Manually rotate a key within KMS to create a new CMK immediately.
- B. Use the KMS import key functionality to execute a delete key operation.
- C. Use the schedule key deletion function within KMS to specify the minimum wait period for deletion.
- D. Change the KMS CMK alias to immediately prevent any services from using the CMK.

Answer: C

Explanation:

<https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys.html>

QUESTION 184

A company is implementing a new application in a new AWS account. A VPC and subnets have been created for the application. The application has been peered to an existing VPC in another account in the same AWS Region for database access. Amazon EC2 instances will regularly be created and terminated in the application VPC, but only some of them will need access to the databases in the peered VPC over TCP port 1521. A security engineer must ensure that only the EC2 instances than need access to the databases can access them through the network.

How can the security engineer implement this solution?

- A. Create a new security group in the database VPC and create an inbound rule that allows all traffic from the IP address range of the application VPC.
Add a new network ACL rule on the database subnets.
Configure the rule to TCP port 1521 from the IP address range of the application VPC.
Attach the new security group to the database instances that the application instances need to access.
- B. Create a new security group in the application VPC with an inbound rule that allows the IP address range of the database VPC over TCP port 1521.
Create a new security group in the database VPC with an inbound rule that allows the IP address range of the application VPC over port 1521.
Attach the new security group to the database instances and the application instances that need database access.
- C. Create a new security group in the application VPC with no inbound rules.
Create a new security group in the database VPC with an inbound rule that allows TCP port 1521 from the new application security group in the application VPC.
Attach the application security group to the application instances that need database access, and attach the database security group to the database instances.
- D. Create a new security group in the application VPC with an inbound rule that allows the IP address range of the database VPC over TCP port 1521.
Add a new network ACL rule on the database subnets.
Configure the rule to allow all traffic from the IP address range of the application VPC.
Attach the new security group to the application instances that need database access.

Answer: A

QUESTION 185

A company wants to encrypt the private network between its on-premises environment and AWS. The company also wants a consistent network experience for its employees.

What should the company do to meet these requirements?

- A. Establish an AWS Direct Connect connection with AWS and set up a Direct Connect gateway. In the Direct Connect gateway configuration, enable IPsec and BGP, and then leverage native AWS network encryption between Availability Zones and Regions.
- B. Establish an AWS Direct Connect connection with AWS and set up a Direct Connect gateway. Using the Direct Connect gateway, create a private virtual interface and advertise the customer gateway private IP addresses.
Create a VPN connection using the customer gateway and the virtual private gateway.
- C. Establish a VPN connection with the AWS virtual private cloud over the Internet.
- D. Establish an AWS Direct Connect connection with AWS and establish a public virtual interface. For prefixes that need to be advertised, enter the customer gateway public IP addresses.
Create a VPN connection over Direct Connect using the customer gateway and the virtual private gateway.

Answer: C

QUESTION 186

A company's Security Engineer has been tasked with restricting a contractor's IAM account access to the company's Amazon EC2 console without providing access to any other AWS services. The contractor's IAM account must not be able to gain access to any other AWS service, even if the IAM account is assigned additional permissions based on IAM group membership.

What should the Security Engineer do to meet these requirements?

- A. Create an Inline IAM user policy that allows for Amazon EC2 access for the contractor's IAM user.
- B. Create an IAM permissions boundary policy that allows Amazon EC2 access.
Associate the contractor's IAM account with the IAM permissions boundary policy.
- C. Create an IAM group with an attached policy that allows for Amazon EC2 access.
Associate the contractor's IAM account with the IAM group.
- D. Create an IAM role that allows for EC2 and explicitly denies all other services.
Instruct the contractor to always assume this role.

Answer: B

QUESTION 187

A company recently performed an annual security assessment of its AWS environment. The assessment showed the audit logs are not available beyond 90 days and that unauthorized changes to IAM policies are made without detection.

How should a Security Engineer resolve these issues?

- A. Create an Amazon S3 lifecycle policy that archives AWS CloudTrail trail logs to Amazon S3 Glacier after 90 days.
Configure Amazon Inspector to provide a notification when a policy change is made to resources.
- B. Configure AWS Artifact to archive AWS CloudTrail logs.
Configure AWS Trusted Advisor to provide a notification when a policy change is made to resources.
- C. Configure Amazon CloudWatch to export log groups to Amazon S3.
Configure AWS CloudTrail to provide a notification when a policy change is made to resources.
- D. Create an AWS CloudTrail trail that stores audit logs in Amazon S3.
Configure an AWS Config rule to provide a notification when a policy change is made to resources.

Answer: A

QUESTION 188

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>

QUESTION 189

A company needs a forensic-logging solution for hundreds of applications running in Docker on Amazon EC2. The solution must perform real-time analytics on the logs, must support the replay of messages, and must persist the logs.

Which AWS services should be used to meet these requirements? (Choose two.)

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

Answer: BD

QUESTION 190

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

Which combination of activities must the company implement to meet its encryption requirements? (Choose two.)

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

Answer: AE

QUESTION 191

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

launched.

What could be causing these terminations?

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

Answer: B

Explanation:

The root EBS volume is encrypted and you do not have permissions to access the KMS key for decryption.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/troubleshooting-launch.html>

QUESTION 192

Authorized Administrators are unable to connect to an Amazon EC2 Linux bastion host using SSH over the Internet. The connection either fails to respond or generates the following error message:

Network error: Connection timed out.

What could be responsible for the connection failure? (Choose three.)

- A. The NAT gateway in the subnet where the EC2 instance is deployed has been misconfigured.
- B. The internet gateway of the VPC has been misconfigured.
- C. The security group denies outbound traffic on ephemeral ports.
- D. The route table is missing a route to the internet gateway.
- E. The NACL denies outbound traffic on ephemeral ports.
- F. The host-based firewall is denying SSH traffic.

Answer: BDF

Explanation:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html>

QUESTION 193

After multiple compromises of its Amazon EC2 instances, a company's Security Officer is mandating that memory dumps of compromised instances be captured for further analysis. A Security Engineer just received an EC2 abuse notification report from AWS stating that an EC2 instance running the most recent Windows Server 2019 Base AMI is compromised.

How should the Security Engineer collect a memory dump of the EC2 instance for forensic analysis?

- A. Give consent to the AWS Security team to dump the memory core on the compromised instance and provide it to AWS Support for analysis.
- B. Review memory dump data that the AWS Systems Manager Agent sent to Amazon CloudWatch Logs.
- C. Download and run the EC2Rescue for Windows Server utility from AWS.
- D. Reboot the EC2 Windows Server, enter safe mode, and select memory dump.

Answer: B

Explanation:

<https://www.giac.org/paper/gcfa/13310/digital-forensic-analysis-amazon-linux-ec2-instances/123500>

QUESTION 194

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

How should the Security Engineer do this?

- A. Log in to each account four times a day and filter the AWS CloudTrail log data, then copy and paste the logs in to the Amazon S3 bucket in the destination account.
- B. Set up Amazon CloudWatch to stream data to an Amazon S3 bucket in each source account. Set up bucket replication for each source account into a centralized bucket owned by the Security Engineer.
- C. Set up an AWS Config aggregator to collect AWS configuration data from multiple sources.
- D. Set up Amazon CloudWatch cross-account log data sharing with subscriptions in each account. Send the logs to Amazon Kinesis Data Firehose in the Security Engineer's account.

Answer: C

Explanation:

<https://docs.aws.amazon.com/organizations/latest/userguide/services-that-can-integrate-config.html>

QUESTION 195

Two Amazon EC2 instances in different subnets should be able to connect to each other but cannot. It has been confirmed that other hosts in the same subnets are able to communicate successfully, and that security groups have valid ALLOW rules in place to permit this traffic.

Which of the following troubleshooting steps should be performed?

- A. Check inbound and outbound security groups, looking for DENY rules
- B. Check inbound and outbound Network ACL rules, looking for DENY rules
- C. Review the rejected packet reason codes in the VPC Flow Logs
- D. Use AWS X-Ray to trace the end-to-end application flow

Answer: C

QUESTION 196

A Security Engineer creates an Amazon S3 bucket policy that denies access to all users. A few days later, the Security Engineer adds an additional statement to the bucket policy to allow read-only access to one other employee. Even after updating the policy, the employee still receives an access denied message.

What is the likely cause of this access denial?

- A. The ACL in the bucket needs to be updated

- B. The IAM policy does not allow the user to access the bucket
- C. It takes a few minutes for a bucket policy to take effect
- D. The allow permission is being overridden by the deny

Answer: B

Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/s3-access-denied-bucket-policy/>

QUESTION 197

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

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

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

Answer: D

Explanation:

<https://docs.aws.amazon.com/kms/latest/developerguide/key-policy-modifying-external-accounts.html>

QUESTION 198

An organization wants to log all AWS API calls made within all of its AWS accounts, and must have a central place to analyze these logs.

What steps should be taken to meet these requirements in the MOST secure manner? (Choose two.)

- A. Turn on AWS CloudTrail in each AWS account.
- B. Turn on CloudTrail in only the account that will be storing the logs.
- C. Update the bucket ACL of the bucket in the account that will be storing the logs so that other accounts can log to it.
- D. Create a service-based role for CloudTrail and associate it with CloudTrail in each account.
- E. Update the bucket policy of the bucket in the account that will be storing the logs so that other accounts can log to it.

Answer: BE

QUESTION 199

A company uses HTTP Live Streaming (HLS) to stream live video content to paying subscribers by using Amazon CloudFront. HLS splits the video content into chunks so that the user can request the right chunk based on different conditions. Because the video events last for several hours, the total video is made up of thousands of chunks.

The origin URL is not disclosed, and every user is forced to access the CloudFront URL. The company has a web application that authenticates the paying users against an internal repository and a CloudFront key pair that is already issued.

What is the simplest and MOST effective way to protect the content?

- A. Develop the application to use the CloudFront key pair to create signed URLs that users will use to access the content.
- B. Develop the application to use the CloudFront key pair to set the signed cookies that users will use to access the content.
- C. Develop the application to issue a security token that Lambda@Edge will receive to authenticate and authorize access to the content.
- D. Keep the CloudFront URL encrypted inside the application, and use AWS KMS to resolve the URL on-the-fly after the user is authenticated.

Answer: A

Explanation:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html>

QUESTION 200

A company uses an AWS Key Management Service (AWS KMS) CMK to encrypt application data before it is stored. The company's security policy was recently modified to require encryption key rotation annually. A security engineer must ensure that annual global key rotation is enabled for the key without making changes to the application.

What should the security engineer do to accomplish this requirement?

- A. Create new AWS managed keys. Configure the key schedule for the annual rotation.
Create an alias to point to the new keys.

- B. Enable automatic annual key rotation for the existing customer managed CMKs.
Update the application encryption library to use a new key ID for all encryption operations.
Fall back to the old key ID to decrypt data that was encrypted with previous versions of the key.
- C. Create new AWS managed CMKs. Configure the key schedule for annual rotation.
Create an alias to point to the new CMKs.
- D. Enable automatic annual key rotation for the existing customer managed CMKs.
Update the application encryption library to use a new key ID for all encryption operations.
Create a key grant for the old CMKs and update the code to point to the ARN of the grants.

Answer: D

Explanation:

<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>

QUESTION 201

A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running in Amazon Elastic Container Service (Amazon ECS). This solution will also handle volatile traffic patterns.

Which solution would have the MOST scalability and LOWEST latency?

- A. Configure a Network Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers.
- B. Configure an Application Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers.
- C. Configure a Network Load Balancer with a TCP listener to pass through TLS traffic to the containers.
- D. Configure Amazon Route 53 to use multivalue answer routing to send traffic to the containers.

Answer: C

QUESTION 202

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

Which of the following actions could fix this issue?

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

Answer: C

Explanation:

Logging server receives the traffic but doesn't know how to send it back. Its a routing issue.

QUESTION 203

A company has two software development teams that are creating applications that store sensitive data in Amazon S3. Each team's data must always be separate. The company's security team must design a data encryption strategy for both teams that provides the ability to audit key usage. The solution must also minimize operational overhead.

What should the security team recommend?

- A. Tell the application teams to use two different S3 buckets with separate AWS Key Management Service (AWS KMS) AWS managed CMKs.
 - Limit the key policies to allow encryption and decryption of the CMKs to their respective teams only.
 - Force the teams to use encryption context to encrypt and decrypt.
- B. Tell the application teams to use two different S3 buckets with a single AWS Key Management Service (AWS KMS) AWS managed CMK.
 - Limit the key policy to allow encryption and decryption of the CMK only.
 - Do not allow the teams to use encryption context to encrypt and decrypt.
- C. Tell the application teams to use two different S3 buckets with separate AWS Key Management Service (AWS KMS) customer managed CMKs.
 - Limit the key policies to allow encryption and decryption of the CMKs to their respective teams only.
 - Force the teams to use encryption context to encrypt and decrypt.
- D. Tell the application teams to use two different S3 buckets with a single AWS Key Management Service (AWS KMS) customer managed CMK.
 - Limit the key policy to allow encryption and decryption of the CMK only.
 - Do not allow the teams to use encryption context to encrypt and decrypt.

Answer: A

QUESTION 204

A company's Security Engineer is copying all application logs to centralized Amazon S3 buckets. Currently, each of the company's application is in its own AWS account, and logs are pushed into S3 buckets associated with each account. The Engineer will deploy an AWS Lambda function into each account that copies the relevant log files to the centralized S3 bucket.

The Security Engineer is unable to access the log files in the centralized S3 bucket. The Engineer's IAM user policy from the centralized account looks like this:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "s3:Put*",
            "Resource": "arn:aws:s3:::centralizedbucket/*",
            "Effect": "Deny"
        },
        {
            "Action": ["s3:Get*", "s3>List*"],
            "Resource": [
                "arn:aws:s3:::centralizedbucket/*",
                "arn:aws:s3:::centralizedbucket/"
            ],
            "Effect": "Allow"
        }
    ]
}
```

The centralized S3 bucket policy looks like this:

```
{
    "Version": "2012-10-17",      "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/LogCopier",
                    "arn:aws:iam::444455556666:role/LogCopier"
                ]
            },
            "Action": ["s3:PutObject", "s3:PutObjectAcl"],
            "Resource": "arn:aws:s3:::centralizedbucket/*"
        }
    ]
}
```

Why is the Security Engineer unable to access the log files?

- The S3 bucket policy does not explicitly allow the Security Engineer access to the objects in the bucket.
- The object ACLs are not being updated to allow the users within the centralized account to access the objects.
- The Security Engineer's IAM policy does not grant permissions to read objects in the S3 bucket.
- The s3:PutObject and s3:PutObjectAcl permissions should be applied at the S3 bucket level.

Answer: C

QUESTION 205

An application running on Amazon EC2 instances generates log files in a folder on a Linux file system. The instances block access to the console and file transfer utilities, such as Secure Copy

Protocol (SCP) and Secure File Transfer Protocol (SFTP). The Application Support team wants to automatically monitor the application log files so the team can set up notifications in the future.

A Security Engineer must design a solution that meets the following requirements:

- Make the log files available through an AWS managed service.
- Allow for automatic monitoring of the logs.
- Provide an interface for analyzing logs.
- Minimize effort.

Which approach meets these requirements?

- A. Modify the application to use the AWS SDK.
Write the application logs to an Amazon S3 bucket.
- B. Install the unified Amazon CloudWatch agent on the instances.
Configure the agent to collect the application log files on the EC2 file system and send them to Amazon CloudWatch Logs.
- C. Install AWS Systems Manager Agent on the instances.
Configure an automation document to copy the application log files to AWS DeepLens.
- D. Install Amazon Kinesis Agent on the instances.
Stream the application log files to Amazon Kinesis Data Firehose and set the destination to Amazon Elasticsearch Service.

Answer: B

Explanation:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/monitoring-cloudwatch-agent.html>

QUESTION 206

A company has multiple AWS accounts that are part of AWS Organizations. The company's Security team wants to ensure that even those Administrators with full access to the company's AWS accounts are unable to access the company's Amazon S3 buckets.

How should this be accomplished?

- A. Use SCPs.
- B. Add a permissions boundary to deny access to Amazon S3 and attach it to all roles.
- C. Use an S3 bucket policy.
- D. Create a VPC endpoint for Amazon S3 and deny statements for access to Amazon S3.

Answer: A

Explanation:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

QUESTION 207

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

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

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

Answer: CD

QUESTION 208

A company has decided to use encryption in its AWS account to secure the objects in Amazon S3 using server-side encryption. Object sizes range from 16,000 B to 5 MB. The requirements are as follows:

- The key material must be generated and stored in a certified Federal Information Processing Standard (FIPS) 140-2 Level 3 machine.
- The key material must be available in multiple Regions.

Which option meets these requirements?

- A. Use an AWS KMS customer managed key and store the key material in AWS with replication across Regions.
- B. Use an AWS customer managed key, import the key material into AWS KMS using in-house AWS CloudHSM, and store the key material securely in Amazon S3.
- C. Use an AWS KMS custom key store backed by AWS CloudHSM clusters, and copy backups across Regions.
- D. Use AWS CloudHSM to generate the key material and backup keys across Regions.
Use the Java Cryptography Extension (JCE) and Public Key Cryptography Standards #11 (PKCS #11) encryption libraries to encrypt and decrypt the data.

Answer: C

QUESTION 209

An organization has a multi-petabyte workload that it is moving to Amazon S3, but the CISO is concerned about cryptographic wear-out and the blast radius if a key is compromised.

How can the CISO be assured that AWS KMS and Amazon S3 are addressing the concerns?
(Choose two.)

- A. There is no API operation to retrieve an S3 object in its encrypted form.
- B. Encryption of S3 objects is performed within the secure boundary of the KMS service.
- C. S3 uses KMS to generate a unique data key for each individual object.
- D. Using a single master key to encrypt all data includes having a single place to perform audits and usage validation.
- E. The KMS encryption envelope digitally signs the master key during encryption to prevent cryptographic wear-out.

Answer: CD

QUESTION 210

A company has a compliance requirement to rotate its encryption keys on an annual basis. A Security Engineer needs a process to rotate the KMS Customer Master Keys (CMKs) that were created using imported key material.

How can the Engineer perform the key rotation process MOST efficiently?

- A. Create a new CMK, and redirect the existing Key Alias to the new CMK.
- B. Select the option to auto-rotate the key.
- C. Upload new key material into the existing CMK.
- D. Create a new CMK, and change the application to point to the new CMK.

Answer: D

QUESTION 211

You are responsible to deploying a critical application onto AWS. Part of the requirements for this application is to ensure that the controls set for this application met PCI compliance. Also there is a need to monitor web application logs to identify any malicious activity.

Which of the following services can be used to fulfil this requirement. Choose 2 answers from the options given below

- A. Amazon Cloudwatch Logs
- B. Amazon VPC Flow Logs
- C. Amazon AWS Config
- D. Amazon Cloudtrail

Answer: AD

Explanation:

The AWS Documentation mentions the following about these services AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

Option B is incorrect because VPC flow logs can only check for flow to instances in a VPC

Option C is incorrect because this can check for configuration changes only.

QUESTION 212

A large company wants its Compliance team to audit its Amazon S3 buckets to identify if personally identifiable information (PII) is stored in them. The company has hundreds of S3 buckets and has asked the Security Engineers to scan every bucket.

How can this task be accomplished?

- A. Configure Amazon CloudWatch Events to trigger Amazon Inspector to scan the S3 buckets daily for PII.
Configure Amazon Inspector to publish Amazon SNS notifications to the Compliance team if PII is

- detected.
- B. Configure Amazon Macie to classify data in the S3 buckets and check the dashboard for PII findings.
Configure Amazon CloudWatch Events to capture Macie alerts and target an Amazon SNS topic to be notified if PII is detected.
 - C. Check the AWS Trusted Advisor data loss prevention page in the AWS Management Console.
Download the Amazon S3 data confidentiality report and send it to the Compliance team.
Configure Amazon CloudWatch Events to capture Trusted Advisor alerts and target an Amazon SNS topic to be notified if PII is detected.
 - D. Enable Amazon GuardDuty in multiple Regions to scan the S3 buckets. Configure Amazon CloudWatch Events to capture GuardDuty alerts and target an Amazon SNS topic to be notified if PII is detected.

Answer: B

QUESTION 213

During a manual review of system logs from an Amazon Linux EC2 instance, a Security Engineer noticed that there are sudo commands that were never properly alerted or reported on the Amazon CloudWatch Logs agent.

Why were there no alerts on the sudo commands?

- A. There is a security group blocking outbound port 80 traffic that is preventing the agent from sending the logs.
- B. The IAM instance profile on the EC2 instance was not properly configured to allow the CloudWatch Logs agent to push the logs to CloudWatch.
- C. CloudWatch Logs status is set to ON versus SECURE, which prevents it from pulling in OS security event logs.
- D. The VPC requires that all traffic go through a proxy, and the CloudWatch Logs agent does not support a proxy configuration.

Answer: B

QUESTION 214

A company has an AWS account and allows a third-party contractor, who uses another AWS account, to assume certain IAM roles. The company wants to ensure that IAM roles can be assumed by the contractor only if the contractor has multi-factor authentication enabled on their IAM user accounts.

What should the company do to accomplish this?

- A. Add the following condition to the IAM policy attached to all IAM roles:
"Effect": "Deny",
"Condition" : { "BoolIfExists" : { "aws:MultiFactorAuthPresent" : false } }
- B. Add the following condition to the IAM policy attached to all IAM roles:
"Effect": "Deny",
"Condition" : { "Bool" : { "aws:MultiFactorAuthPresent" : false } }
- C. Add the following condition to the IAM policy attached to all IAM roles:
"Effect": "Allow",
"Condition" : { "Null" : { "aws:MultiFactorAuthPresent" : false } }
- D. Add the following condition to the IAM policy attached to all IAM roles:
"Effect": "Allow",

"Condition" : { "BoolIfExists" : { "aws:MultiFactorAuthPresent" : false } }

Answer: A

Explanation:

https://aws-orgs.readthedocs.io/_downloads/en/latest/pdf/ (18)

QUESTION 215

A large corporation is creating a multi-account strategy and needs to determine how its employees should access the AWS Infrastructure.

Which of the following solutions would provide the MOST scalable solution?

- A. Create dedicated IAM users within each AWS account that employees can assume through federation based upon group membership in their existing identity provider.
- B. Use a centralized account with IAM roles that employees can assume through federation with their existing identity provider.
Use cross-account roles to allow the federated users to assume their target role in the resource accounts.
- C. Configure the AWS Security Token Service to use Kerberos tokens so that users can use their existing corporate user names and passwords to access AWS resources directly.
- D. Configure the IAM trust policies within each account's role to set up a trust back to the corporation's existing identity provider, allowing users to assume the role based off their SAML token.

Answer: B

QUESTION 216

A company uses an external identity provider to allow federation into different AWS accounts. A security engineer for the company needs to identify the federated user that terminated a production Amazon EC2 instance a week ago.

What is the FASTEST way for the security engineer to identify the federated user?

- A. Review the AWS CloudTrail event history logs in an Amazon S3 bucket and look for the TerminateInstances event to identify the federated user from the role session name.
- B. Filter the AWS CloudTrail event history for the TerminateInstances event and identify the assumed IAM role.
Review the AssumeRoleWithSAML event call in CloudTrail to identify the corresponding username.
- C. Search the AWS CloudTrail logs for the TerminateInstances event and note the event time.
Review the IAM Access Advisor tab for all federated roles.
The last accessed time should match the time when the instance was terminated.
- D. Use Amazon Athena to run a SQL query on the AWS CloudTrail logs stored in an Amazon S3 bucket and filter on the TerminateInstances event.
Identify the corresponding role and run another query to filter the AssumeRoleWithWebIdentity event for the user name.

Answer: A

Explanation:

<https://aws.amazon.com/blogs/security/how-to-easily-identify-your-federated-users-by-using-aws-cloudtrail/>

QUESTION 217

A company's security officer is concerned about the risk of AWS account root user logins and has assigned a security engineer to implement a notification solution for near-real-time alerts upon account root user logins.

How should the security engineer meet these requirements?

- A. Create a cron job that runs a script to download the AWS IAM security credentials file, parse the file for account root user logins, and email the security team's distribution list.
- B. Run AWS CloudTrail logs through Amazon CloudWatch Events to detect account root user logins and trigger an AWS Lambda function to send an Amazon SNS notification to the security team's distribution list.
- C. Save AWS CloudTrail logs to an Amazon S3 bucket in the security team's account. Process the CloudTrail logs with the security engineer's logging solution for account root user logins.
Send an Amazon SNS notification to the security team upon encountering the account root user login events.
- D. Save VPC Flow Logs to an Amazon S3 bucket in the security team's account, and process the VPC Flow Logs with their logging solutions for account root user logins.
Send an Amazon SNS notification to the security team upon encountering the account root user login events.

Answer: B

Explanation:

<https://aws.amazon.com/blogs/mt/monitor-and-notify-on-aws-account-root-user-activity/>

QUESTION 218

A company has an application hosted in an Amazon EC2 instance and wants the application to access secure strings stored in AWS Systems Manager Parameter Store. When the application tries to access the secure string key value, it fails.

Which factors could be the cause of this failure? (Choose two.)

- A. The EC2 instance role does not have decrypt permissions on the AWS Key Management Service (AWS KMS) key used to encrypt the secret.
- B. The EC2 instance role does not have read permissions to read the parameters in Parameter Store.
- C. Parameter Store does not have permission to use AWS Key Management Service (AWS KMS) to decrypt the parameter.
- D. The EC2 instance role does not have encrypt permissions on the AWS Key Management Service (AWS KMS) key associated with the secret.
- E. The EC2 instance does not have any tags associated.

Answer: BC

QUESTION 219

A security engineer received an Amazon GuardDuty alert indicating a finding involving the Amazon EC2 instance that hosts the company's primary website. The GuardDuty finding received read:

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.

The security engineer confirmed that a malicious actor used API access keys intended for the EC2 instance from a country where the company does not operate. The security engineer needs to deny access to the malicious actor.

What is the first step the security engineer should take?

- A. Open the EC2 console and remove any security groups that allow inbound traffic from 0.0.0.0/0.
- B. Install the AWS Systems Manager Agent on the EC2 instance and run an inventory report.
- C. Install the Amazon Inspector agent on the host and run an assessment with the CVE rules package.
- D. Open the IAM console and revoke all IAM sessions that are associated with the instance profile.

Answer: B

QUESTION 220

A company manages multiple AWS accounts using AWS Organizations. The company's security team notices that some member accounts are not sending AWS CloudTrail logs to a centralized Amazon S3 logging bucket. The security team wants to ensure there is at least one trail configured for all existing accounts and for any account that is created in the future.

Which set of actions should the security team implement to accomplish this?

- A. Create a new trail and configure it to send CloudTrail logs to Amazon S3. Use Amazon EventBridge (Amazon CloudWatch Events) to send notification if a trail is deleted or stopped.
- B. Deploy an AWS Lambda function in every account to check if there is an existing trail and create a new trail, if needed.
- C. Edit the existing trail in the Organizations master account and apply it to the organization.
- D. Create an SCP to deny the clouptrail:Delete* and clouptrail:Stop* actions. Apply the SCP to all accounts.

Answer: C

QUESTION 221

A security engineer is setting up a new AWS account. The engineer has been asked to continuously monitor the company's AWS account using automated compliance checks based on AWS best practices and Center for Internet Security (CIS) AWS Foundations Benchmarks.

How can the security engineer accomplish this using AWS services?

- A. Enable AWS Config and set it to record all resources in all Regions and global resources. Then enable AWS Security Hub and confirm that the CIS AWS Foundations compliance standard is enabled.
- B. Enable Amazon Inspector and configure it to scan all Regions for the CIS AWS Foundations Benchmarks. Then enable AWS Security Hub and configure it to ingest the Amazon Inspector findings.
- C. Enable Amazon Inspector and configure it to scan all Regions for the CIS AWS Foundations Benchmarks. Then enable AWS Shield in all Regions to protect the account from DDoS attacks.
- D. Enable AWS Config and set it to record all resources in all Regions and global resources. Then enable Amazon Inspector and configure it to enforce CIS AWS Foundations Benchmarks using AWS Config rules.

Answer: D

Explanation:

<https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub.pdf>

QUESTION 222

A company has a VPC with several Amazon EC2 instances behind a NAT gateway. The company's security policy states that all network traffic must be logged and must include the original source and destination IP addresses. The existing VPC Flow Logs do not include this information. A security engineer needs to recommend a solution.

Which combination of steps should the security engineer recommend? (Choose two.)

- A. Edit the existing VPC Flow Logs.
Change the log format of the VPC Flow Logs from the Amazon default format to a custom format.
- B. Delete and recreate the existing VPC Flow Logs.
Change the log format of the VPC Flow Logs from the Amazon default format to a custom format.
- C. Change the destination to Amazon CloudWatch Logs.
- D. Include the pkt-srcaddr and pkt-dstaddr fields in the log format.
- E. Include the subnet-id and instance-id fields in the log format.

Answer: AE

Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>

QUESTION 223

A company has a VPC with an IPv6 address range and a public subnet with an IPv6 address block. The VPC currently hosts some public Amazon EC2 instances, but a security engineer needs to migrate a second application into the VPC that also requires IPv6 connectivity.

This new application will occasionally make API requests to an external, internet-accessible endpoint to receive updates. However, the security team does not want the application's EC2 instance exposed directly to the internet. The security engineer intends to create a private subnet with a custom route table and to associate the route table with the private subnet.

What else does the security engineer need to do to ensure the application will not be exposed directly to the internet, but can still communicate as required?

- A. Launch a NAT instance in the public subnet.
Update the custom route table with a new route to the NAT instance.
- B. Remove the internet gateway, and add AWS PrivateLink to the VPC.
Then update the custom route table with a new route to AWS PrivateLink.
- C. Add a managed NAT gateway to the VPC.
Update the custom route table with a new route to the gateway.
- D. Add an egress-only internet gateway to the VPC.
Update the custom route table with a new route to the gateway.

Answer: D

QUESTION 224

An ecommerce website was down for 1 hour following a DDoS attack. Users were unable to connect to the website during the attack period. The ecommerce company's security team is worried about future potential attacks and wants to prepare for such events. The company needs

to minimize downtime in its response to similar attacks in the future.

Which steps would help achieve this? (Choose two.)

- A. Enable Amazon GuardDuty to automatically monitor for malicious activity and block unauthorized access.
- B. Subscribe to AWS Shield Advanced and reach out to AWS Support in the event of an attack.
- C. Use VPC Flow Logs to monitor network traffic and an AWS Lambda function to automatically block an attacker's IP using security groups.
- D. Set up an Amazon CloudWatch Events rule to monitor the AWS CloudTrail events in real time, use AWS Config rules to audit the configuration, and use AWS Systems Manager for remediation.
- E. Use AWS WAF to create rules to respond to such attacks.

Answer: AB

QUESTION 225

A company's on-premises data center forwards DNS logs to a third-party security incident events management (SIEM) solution that alerts on suspicious behavior.

The company wants to introduce a similar capability to its AWS accounts that includes automatic remediation. The company expects to double in size within the next few months.

Which solution meets the company's current and future logging requirements?

- A. Enable Amazon GuardDuty and AWS Security Hub in all Regions and all accounts.
Designate a master security account to receive all alerts from the child accounts.
Set up specific rules within Amazon EventBridge to trigger an AWS Lambda function for remediation steps.
- B. Ingest all AWS CloudTrail logs, VPC Flow Logs, and DNS logs into a single Amazon S3 bucket in a designated security account.
Use the current on-premises SIEM to monitor the logs and send a notification to an Amazon SNS topic to alert the security team of remediation steps.
- C. Ingest all AWS CloudTrail logs, VPC Flow Logs, and DNS logs into a single Amazon S3 bucket in a designated security account.
Launch an Amazon EC2 instance and install the current SIEM to monitor the logs and send a notification to an Amazon SNS topic to alert the security team of remediation steps.
- D. Enable Amazon GuardDuty and AWS Security Hub in all Regions and all accounts.
Designate a master security account to receive all alerts from the child accounts.
Create an AWS Organizations SCP that denies access to certain API calls that are on an ignore list.

Answer: D

QUESTION 226

A company has a serverless application for internal users deployed on AWS. The application uses AWS Lambda for the front end and for business logic. The Lambda function accesses an Amazon RDS database inside a VPC. The company uses AWS Systems Manager Parameter Store for storing database credentials.

A recent security review highlighted the following issues:

- The Lambda function has internet access.

- The relational database is publicly accessible.
- The database credentials are not stored in an encrypted state.

Which combination of steps should the company take to resolve these security issues? (Choose three.)

- A. Disable public access to the RDS database inside the VPC.
- B. Move all the Lambda functions inside the VPC.
- C. Edit the IAM role used by Lambda to restrict internet access.
- D. Create a VPC endpoint for Systems Manager.
 - Store the credentials as a string parameter.
 - Change the parameter type to an advanced parameter.
- E. Edit the IAM role used by RDS to restrict internet access.
- F. Create a VPC endpoint for Systems Manager.
 - Store the credentials as a SecureString parameter.

Answer: BDE

Explanation:

https://docs.amazonaws.cn/en_us/config/latest/developerguide/operational-best-practices-for-hipaa_security.html (guidance)

QUESTION 227

A company wants to deploy an application in a private VPC that will not be connected to the internet. The company's security team will not allow bastion hosts or methods using SSH to log in to Amazon EC2 instances. The application team plans to use AWS Systems Manager Session Manager to connect to and manage the EC2 instances.

Which combination of steps should the security team take? (Choose three.)

- A. Make sure the Systems Manager Agent is installed and running on all EC2 instances inside the VPC.
- B. Ensure the IAM role attached to the EC2 instances in the VPC allows access to Systems Manager.
- C. Create an SCP that prevents the creation of SSH key pairs.
- D. Launch a NAT gateway in the VPC.
 - Update the routing policies to forward traffic to this NAT gateway.
- E. Ensure proper VPC endpoints are in place for Systems Manager and Amazon EC2.
- F. Ensure the VPC has a transit gateway attachment.
 - Update the routing policies to forward traffic to this transit gateway.

Answer: ABE

<https://aws.amazon.com/blogs/mt/replacing-a-bastion-host-with-amazon-ec2-systems-manager/>

QUESTION 228

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

A recent security audit found that the security groups are inconsistently implemented across accounts and that unauthorized changes have been made to the security groups. A security

engineer needs to recommend a solution to improve consistency and to prevent unauthorized changes in the individual accounts in the future.

Which solution should the security engineer recommend?

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

Answer: A

QUESTION 229

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

What should the security engineer do to meet these requirements?

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

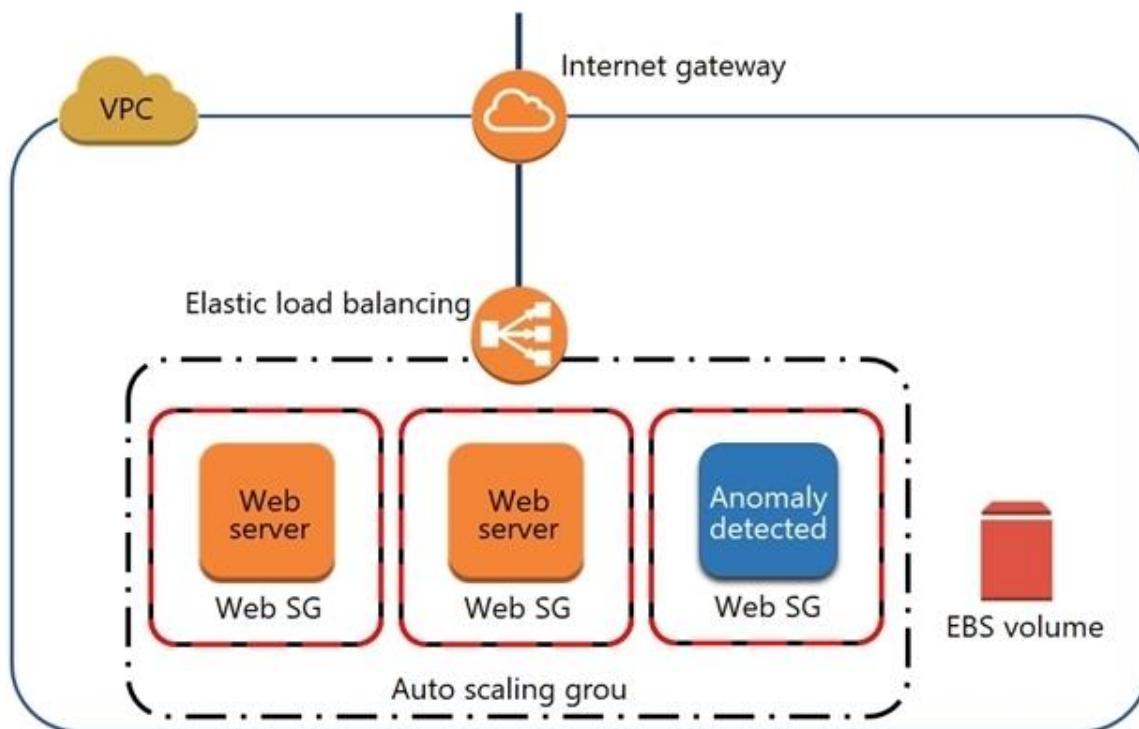
Answer: A

Explanation:

<https://docs.aws.amazon.com/ram/latest/userguide/ram-ug.pdf>

QUESTION 230

A security engineer noticed an anomaly within a company EC2 instance as shown in the image. The engineer must now investigate what is causing the anomaly.



What are the MOST effective steps to take to ensure that the instance is not further manipulated, while allowing the engineer to understand what happened?

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

Answer: D

QUESTION 231

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

- AWS IAM federated with on-premises Active Directory
- Amazon Cognito user pools to accessing an AWS Cloud application developed by the company

Which combination of actions should the security engineer take to solve this issue? (Choose two.)

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

Answer: BD

QUESTION 232

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

Which solution meets these requirements?

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

Answer: A

QUESTION 233

A company's security engineer has been asked to monitor and report all AWS account root user activities.

Which of the following would enable the security engineer to monitor and report all root user activities? (Choose two.)

- A. Configuring AWS Organizations to monitor root user API calls on the paying account
- B. Creating an Amazon CloudWatch Events rule that will trigger when any API call from the root user is reported
- C. Configuring Amazon Inspector to scan the AWS account for any root user activity
- D. Configuring AWS Trusted Advisor to send an email to the security team when the root user logs in to the console
- E. Using Amazon SNS to notify the target group

Answer: BE

QUESTION 234

A security engineer needs to ensure their company's use of AWS meets AWS security best practices. As part of this, the AWS account root user must not be used for daily work. The root

user must be monitored for use, and the security team must be alerted as quickly as possible if the root user is used.

Which solution meets these requirements?

- A. Set up an Amazon CloudWatch Events rule that triggers an Amazon SNS notification.
- B. Create root user access keys. Use an AWS Lambda function to parse AWS CloudTrail logs from Amazon S3 and generate notifications using Amazon SNS.
- C. Set up a rule in AWS Config to trigger root user events.
Trigger an AWS Lambda function and generate notifications using Amazon SNS.
- D. Use Amazon Inspector to monitor the usage of the root user and generate notifications using Amazon SNS.

Answer: C

QUESTION 235

A security engineer is designing an incident response plan to address the risk of a compromised Amazon EC2 instance. The plan must recommend a solution to meet the following requirements:

- A trusted forensic environment must be provisioned.
- Automated response processes must be orchestrated.

Which AWS services should be included in the plan? (Choose two.)

- A. AWS CloudFormation
- B. Amazon GuardDuty
- C. Amazon Inspector
- D. Amazon Macie
- E. AWS Step Functions

Answer: AB

Explanation:

<https://aws.amazon.com/blogs/security/how-to-automate-incident-response-in-aws-cloud-for-ec2-instances/>

QUESTION 236

A company is setting up products to deploy in AWS Service Catalog. Management is concerned that when users launch products, elevated IAM privileges will be required to create resources.

How should the company mitigate this concern?

- A. Add a template constraint to each product in the portfolio.
- B. Add a launch constraint to each product in the portfolio.
- C. Define resource update constraints for each product in the portfolio.
- D. Update the AWS CloudFormation template backing the product to include a service role configuration.

Answer: B

Explanation:

<https://aws.amazon.com/blogs/mt/how-to-launch-secure-and-governed-aws-resources-with-aws-cloudformation-and-aws-service-catalog/>

QUESTION 237

A security engineer has noticed that VPC Flow Logs are getting a lot of REJECT traffic originating from a single Amazon EC2 instance in an Auto Scaling group. The security engineer is concerned that this EC2 instance may be compromised.

What immediate action should the security engineer take?

- A. Remove the instance from the Auto Scaling group.
Close the security group with ingress only from a single forensic IP address to perform an analysis.
- B. Remove the instance from the Auto Scaling group.
Change the network ACL rules to allow traffic only from a single forensic IP address to perform an analysis.
Add a rule to deny all other traffic.
- C. Remove the instance from the Auto Scaling group.
Enable Amazon GuardDuty in that AWS account.
Install the Amazon Inspector agent on the suspicious EC2 instance to perform a scan.
- D. Take a snapshot of the suspicious EC2 instance.
Create a new EC2 instance from the snapshot in a closed security group with ingress only from a single forensic IP address to perform an analysis.

Answer: B

QUESTION 238

A company's director of information security wants a daily email report from AWS that contains recommendations for each company account to meet AWS Security best practices.

Which solution would meet these requirements?

- A. In every AWS account, configure AWS Lambda to query the AWS Support API for AWS Trusted Advisor security checks.
Send the results from Lambda to an Amazon SNS topic to send reports.
- B. Configure Amazon GuardDuty in a master account and invite all other accounts to be managed by the master account.
Use GuardDuty's integration with Amazon SNS to report on findings.
- C. Use Amazon Athena and Amazon QuickSight to build reports off of AWS CloudTrail.
Create a daily Amazon CloudWatch trigger to run the report daily and email it using Amazon SNS.
- D. Use AWS Artifact's prebuilt reports and subscriptions.
Subscribe the director of information security to the reports by adding the director as the security alternate contact for each account.

Answer: D

QUESTION 239

A company uses an Amazon S3 bucket to store reports. Management has mandated that all new objects stored in this bucket must be encrypted at rest using server-side encryption with a client specified AWS Key Management Service (AWS KMS) CMK owned by the same account as the S3 bucket. The AWS account number is 111122223333, and the bucket name is reportbucket. The company's security specialist must write the S3 bucket policy to ensure the mandate can be implemented.

Which statement should the security specialist include in the policy?

- A. {


```

                "Effect": "Deny",
                "Principal": "*",
                "Action": "s3:PutObject",
                "Resource": "arn:aws:s3:::reportbucket/*",
                "Condition": {
                    "StringEquals": {
                        "s3:x-amz-server-side-encryption": "AES256"
                    }
                }
            
```

}
- B. {


```

                "Effect": "Deny",
                "Principal": "*",
                "Action": "s3:PutObject",
                "Resource": "arn:aws:s3:::reportbucket/*",
                "Condition": {
                    "StringNotLike": {
                        "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:
                        *:111122223333:key/*"
                    }
                }
            
```

}
- C. {


```

                "Effect": "Deny",
                "Principal": "*",
                "Action": "s3:PutObject",
                "Resource": "arn:aws:s3:::reportbucket/*",
                "Condition": {
                    "StringNotLike": {
                        "s3:x-amz-server-side-encryption": "aws:kms"
                    }
                }
            
```

}
- D. {


```

                "Effect": "Deny",
                "Principal": "*",
                "Action": "s3:PutObject",
                "Resource": "arn:aws:s3:::reportbucket/*",
                "Condition": {
                    "StringNotLikeIfExists": {
                        "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:
                        *:111122223333:key/*"
                    }
                }
            
```

}

Answer: A

QUESTION 240

A company is designing the security architecture for a global latency-sensitive web application it plans to deploy to AWS. A security engineer needs to configure a highly available and secure two-tier architecture. The security design must include controls to prevent common attacks such as DDoS, cross-site scripting, and SQL injection.

Which solution meets these requirements?

- A. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Region.
 - Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region.
 - Create an Amazon CloudFront distribution that uses the ALB as its origin.
 - Create appropriate AWS WAF ACLs and enable them on the CloudFront distribution.
- B. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Region.
 - Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region.
 - Create an Amazon CloudFront distribution that uses the ALB as its origin.
 - Create appropriate AWS WAF ACLs and enable them on the CloudFront distribution.
- C. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Region.
 - Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region.
 - Create appropriate AWS WAF ACLs and enable them on the ALB.
- D. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Region.
 - Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region.
 - Create appropriate AWS WAF ACLs and enable them on the ALB.

Answer: B

QUESTION 241

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

What should a security engineer do to troubleshoot this error? (Choose three.)

- A. Ensure the KMS policy allows the AppUser role to have permission to decrypt for the CMK.
- B. Ensure the S3 bucket policy allows the AppUser role to have permission to get objects for the S3 bucket.
- C. Ensure the CMK was created before the S3 bucket.
- D. Ensure the S3 block public access feature is enabled for the S3 bucket.
- E. Ensure that automatic key rotation is disabled for the CMK.
- F. Ensure the SCPs within Organizations allow access to the S3 bucket.

Answer: BDE

QUESTION 242

A city is implementing an election results reporting website that will use Amazon CloudFront. The website runs on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. Election results are updated hourly and are stored as .pdf files in an Amazon S3 bucket. A security engineer needs to ensure that all external access to the website goes through CloudFront.

Which solution meets these requirements?

- A. Create an IAM role that allows CloudFront to access the specific S3 bucket.
Modify the S3 bucket policy to allow only the new IAM role to access its contents.
Create an interface VPC endpoint for CloudFront to securely communicate with the ALB.
- B. Create an IAM role that allows CloudFront to access the specific S3 bucket.
Modify the S3 bucket policy to allow only the new IAM role to access its contents.
Associate the ALB with a security group that allows only incoming traffic from the CloudFront service to communicate with the ALB.
- C. Create an origin access identity (OAI) in CloudFront. Modify the S3 bucket policy to allow only the new OAI to access the bucket contents.
Create an interface VPC endpoint for CloudFront to securely communicate with the ALB.
- D. Create an origin access identity (OAI) in CloudFront. Modify the S3 bucket policy to allow only the new OAI to access the bucket contents.
Associate the ALB with a security group that allows only incoming traffic from the CloudFront service to communicate with the ALB.

Answer: C

QUESTION 243

Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Choose three.)

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

Answer: ACD

QUESTION 244

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

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

After implementing the policy, the administrator receives reports that users are unable to perform Amazon EC2 commands using the AWS CLI.

What should the administrator do to resolve this problem while still enforcing multi-factor authentication?

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

Answer: D

QUESTION 245

A recent security audit identified that a company's application team injects database credentials into the environment variables of an AWS Fargate task. The company's security policy mandates that all sensitive data be encrypted at rest and in transit.

Which combination of actions should the security team take to make the application compliant with the security policy? (Choose three.)

- A. Store the credentials securely in a file in an Amazon S3 bucket with restricted access to the application team IAM role.
Ask the application team to read the credentials from the S3 object instead.
- B. Create an AWS Secrets Manager secret and specify the key/value pairs to be stored in this secret.
- C. Modify the application to pull credentials from the AWS Secrets Manager secret instead of the environment variables.
- D. Add the following statement to the container instance IAM role policy:

```
{
    "Effect": "Allow",
    "Action": [
        "ssm:GetParameters",
        "secretsmanager:GetSecretValue",
        "kms:Decrypt"
    ],
    "Resource": [
        "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:secret_name",
        "arn:aws:kms:<region>:<aws_account_id>:key/key_id"
    ]
}
```

- E. Add the following statement to the task execution role policy:

```
{
    "Effect": "Allow",
    "Action": [
        "ssm:GetParameters",
        "secretsmanager:GetSecretValue",
        "kms:Decrypt"
    ],
    "Resource": [
        "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:secret_name",
        "arn:aws:kms:<region>:<aws_account_id>:key/key_id"
    ]
}
```

- F. Log in to the AWS Fargate instance, create a script to read the secret value from AWS Secrets Manager, and inject the environment variables.
Ask the application team to redeploy the application.

Answer: AEF

QUESTION 246

A security engineer is responsible for providing secure access to AWS resources for thousands of developers in a company's corporate identity provider (IdP). The developers access a set of AWS services from their corporate premises using IAM credentials. Due to the volume of requests for provisioning new IAM users, it is taking a long time to grant access permissions. The security engineer receives reports that developers are sharing their IAM credentials with others to avoid provisioning delays. This causes concern about overall security for the security engineer.

Which actions will meet the program requirements that address security?

- A. Create an Amazon CloudWatch alarm for AWS CloudTrail events.
Create a metric filter to send a notification when the same set of IAM credentials is used by multiple developers.
- B. Create a federation between AWS and the existing corporate IdP.

- Leverage IAM roles to provide federated access to AWS resources.
- C. Create a VPN tunnel between the corporate premises and the VPC.
Allow permissions to all AWS services only if it originates from corporate premises.
 - D. Create multiple IAM roles for each IAM user.
Ensure that users who use the same IAM credentials cannot assume the same IAM role at the same time.

Answer: B

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html

QUESTION 247

A company's security team has defined a set of AWS Config rules that must be enforced globally in all AWS accounts the company owns.

What should be done to provide a consolidated compliance overview for the security team?

- A. Use AWS Organizations to limit AWS Config rules to the appropriate Regions, and then consolidate the Amazon CloudWatch dashboard into one AWS account.
- B. Use AWS Config aggregation to consolidate the views into one AWS account, and provide role access to the security team.
- C. Consolidate AWS Config rule results with an AWS Lambda function and push data to Amazon SQS.
Use Amazon SNS to consolidate and alert when some metrics are triggered.
- D. Use Amazon GuardDuty to load data results from the AWS Config rules compliance status, aggregate GuardDuty findings of all AWS accounts into one AWS account, and provide role access to the security team.

Answer: B

QUESTION 248

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

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

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

- Session Manager and attach to the team's IAM users.
- D. Enable AWS Systems Manager in the AWS Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM role.
Install the Systems Manager Agent on all EC2 Linux instances that need interactive access.
Configure IAM policies to allow development team access to the EC2 console and attach to the teams IAM users.

Answer: A

QUESTION 249

A large government organization is moving to the cloud and has specific encryption requirements. The first workload to move requires that a customer's data be immediately destroyed when the customer makes that request.

Management has asked the security team to provide a solution that will securely store the data, allow only authorized applications to perform encryption and decryption and allow for immediate destruction of the data.

Which solution will meet these requirements?

- A. Use AWS Secrets Manager and an AWS SDK to create a unique secret for the customer-specific data
- B. Use AWS Key Management Service (AWS KMS) and the AWS Encryption SDK to generate and store a data encryption key for each customer.
- C. Use AWS Key Management Service (AWS KMS) with service-managed keys to generate and store customer-specific data encryption keys
- D. Use AWS Key Management Service (AWS KMS) and create an AWS CloudHSM custom key store
Use CloudHSM to generate and store a new CMK for each customer.

Answer: A

QUESTION 250

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

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

- A. Configure the S3 bucket ACLs to allow AWS Config to record changes to the buckets.
- B. Configure policies attached to S3 buckets to allow AWS Config to record changes to the buckets.
- C. Attach the AmazonS3ReadOnryAccess managed policy to the IAM user.
- D. Verify the security engineer's IAM user has an attached policy that allows all AWS Config actions.
- E. Assign the AWSConfigRole managed policy to the AWS Config role

Answer: BE

QUESTION 251

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

- A. Create an Application Load Balancer with the existing EC2 instances as a target group
Create an AWS WAF web ACL containing rules mat protect the application from this attack, then apply it to the ALB
Test to ensure me vulnerability has been mitigated, then redirect thee Route 53 records to point to the ALB
Update security groups on the EC 2 instances to prevent direct access from the internet
- B. Create an Amazon CloudFront distribution specifying one EC2 instance as an origin
Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to me distribution
Test to ensure the vulnerability has mitigated, then redirect the Route 53 records to point to CloudFront
- C. Obtain me latest source code for the platform and make ire necessary updates
Test me updated code to ensure that the vulnerability has been irrigated, then deploy me patched version of the platform to the EC2 instances
- D. Update the security group mat is attached to the EC2 instances, removing access from the internet to the TCP port used by the SQL database
Create an AWS WAF web ACL containing rules mat protect me application from this attack, men apply it to the EC2 instances
Test to ensure me vulnerability has been mitigated. then restore the security group to me original setting

Answer: A

QUESTION 252

A security engineer has noticed that VPC Flow Logs are getting a lot REJECT traffic originating from a single Amazon EC2 instance in an Auto Scaling group. The security engineer is concerned that this EC2 instance may be compromised.

What immediate action should the security engineer take?

- A. Remove me instance from the Auto Seating group
Close me security group mm ingress only from a single forensic P address to perform an analysis.
- B. Remove me instance from the Auto Seating group
Change me network ACL rules to allow traffic only from a single forensic IP address to perform en analysis Add a rule to deny all other traffic.
- C. Remove the instance from the Auto Scaling group
Enable Amazon GuardDuty in that AWS account Install the Amazon Inspector agent cm the suspicious EC 2 instance to perform a scan.
- D. Take a snapshot of the suspicious EC2 instance
Create a new EC2 instance from me snapshot in a closed security group with ingress only from a single forensic IP address to perform an analysis

Answer: B

QUESTION 253

A company is collecting AWS CloudTrail log data from multiple AWS accounts by managing individual trails in each account and forwarding log data to a centralized Amazon S3 bucket residing in a log archive account. After CloudTrail introduced support for AWS Organizations trails, the company decided to further centralize management and automate deployment of the CloudTrail logging capability across all of its AWS accounts.

The company's security engineer created an AWS Organizations trail in the master account, enabled server-side encryption with AWS KMS managed keys (SSE-KMS) for the log files, and specified the same bucket as the storage location. However, the engineer noticed that logs recorded by the new trail were not delivered to the bucket.

Which factors could cause this issue? (Select TWO.)

- A. The CMK key policy does not allow CloudTrail to make encrypt and decrypt API calls against the key.
- B. The CMK key policy does not allow CloudTrail to make GenerateDataKey API calls against the key.
- C. The IAM role used by the CloudTrail trail does not have permissions to make PutObject API calls against a folder created for the Organizations trail.
- D. The S3 bucket policy does not allow CloudTrail to make PutObject API calls against a folder created for the Organizations trail.
- E. The CMK key policy does not allow the IAM role used by the CloudTrail trail to use the key for crypto graphical operations.

Answer: AD

QUESTION 254

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

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

Answer: ACD

QUESTION 255

A company has implemented centralized logging and monitoring of AWS CloudTrail logs from all Regions in an Amazon S3 bucket.

The log files are encrypted using AWS KMS. A Security Engineer is attempting to review the log files using a third-party tool hosted on an Amazon EC2 instance.

The Security Engineer is unable to access the logs in the S3 bucket and receives an access denied error message.

What should the Security Engineer do to fix this issue?

- A. Check that the role the Security Engineer uses grants permission to decrypt objects using the

- KMS CMK.
- B. Check that the role the Security Engineer uses grants permission to decrypt objects using the KMS CMK and gives access to the S3 bucket and objects
 - C. Check that the role the EC2 instance profile uses grants permission to decrypt objects using the KMS CMK and gives access to the S3 bucket and objects
 - D. Check that the role the EC2 instance profile uses grants permission to decrypt objects using the KMS CMK

Answer: C

QUESTION 256

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

What should a security engineer recommend to meet these requirements?

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

Answer: B

QUESTION 257

A company is running an application on Amazon EC2 instances in an Auto Scaling group. The application stores logs locally. A security engineer noticed that logs were lost after a scale-in event. The security engineer needs to recommend a solution to ensure the durability and availability of log data. All logs must be kept for a minimum of 1 year for auditing purposes.

What should the security engineer recommend?

- A. Within the Auto Scaling lifecycle, add a hook to create and attach an Amazon Elastic Block Store (Amazon EBS) log volume each time an EC2 instance is created.
When the instance is terminated, the EBS volume can be reattached to another instance for log review.
- B. Create an Amazon Elastic File System (Amazon EFS) file system and add a command in the user data section of the Auto Scaling launch template to mount the EFS file system during EC2 instance creation
Configure a process on the instance to copy the logs once a day from an instance Amazon Elastic Block Store (Amazon EBS) volume to a directory in the EFS file system.
- C. Build the Amazon CloudWatch agent into the AMI used in the Auto Scaling group.
Configure the CloudWatch agent to send the logs to Amazon CloudWatch Logs for review.
- D. Within the Auto Scaling lifecycle, add a lifecycle hook at the terminating state transition and alert the engineering team by using a lifecycle notification to Amazon Simple Notification Service (Amazon SNS).
Configure the hook to remain in the Terminating:Wait state for 1 hour to allow manual review of the security logs prior to instance termination.

Answer: C

QUESTION 258

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

- HTTPS needs to be enforced for all data in transit with specific ciphers.
- The CloudFront distribution needs to be accessible from the internet only.

Which solution will meet these requirements?

- A. Set up an S3 bucket policy with the awssecuretransport key
 - Configure the CloudFront origin access identity (OAI) with the S3 bucket
 - Configure CloudFront to use specific ciphers
 - Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers
 - Link the ALB with AWS WAF to allow access from the CloudFront IP ranges.
- B. Set up an S3 bucket policy with the aws:securetransport key
 - Configure the CloudFront origin access identity (OAI) with the S3 bucket
 - Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers.
- C. Modify the CloudFront distribution to use AWS WAF
 - Force HTTPS on the S3 bucket with specific ciphers in the bucket policy
 - Configure an HTTPS listener only for the ALB
 - Set up a security group to limit access to the ALB from the CloudFront IP ranges
- D. Modify the CloudFront distribution to use the ALB as the origin
 - Enforce an HTTPS listener on the ALB.
 - Create a path-based routing rule on the ALB with proxies that connect to Amazon S3
 - Create a bucket policy to allow access from these proxies only.

Answer: C

QUESTION 259

A company has recently recovered from a security incident that required the restoration of Amazon EC2 instances from snapshots.

After performing a gap analysis of its disaster recovery procedures and backup strategies, the company is concerned that, next time, it will not be able to recover the EC2 instances if the AWS account was compromised and Amazon EBS snapshots were deleted.

All EBS snapshots are encrypted using an AWS KMS CMK.

Which solution would solve this problem?

- A. Create a new Amazon S3 bucket Use EBS lifecycle policies to move EBS snapshots to the new S3 bucket.
 - Move snapshots to Amazon S3 Glacier using lifecycle policies, and apply Glacier Vault Lock policies to prevent deletion
- B. Use AWS Systems Manager to distribute a configuration that performs local backups of all attached disks to Amazon S3.
- C. Create a new AWS account with limited privileges.

- Allow the new account to access the AWS KMS key used to encrypt the EBS snapshots, and copy the encrypted snapshots to the new account on a recurring basis
- D. Use AWS Backup to copy EBS snapshots to Amazon S3.

Answer: A

QUESTION 260

A Security Architect has been asked to review an existing security architecture and identify why the application servers cannot successfully initiate a connection to the database servers. The following summary describes the architecture:

1. An Application Load Balancer, an internet gateway, and a NAT gateway are configured in the public subnet
2. Database, application, and web servers are configured on three different private subnets.
3. The VPC has two route tables: one for the public subnet and one for all other subnets
The route table for the public subnet has a 0.0.0.0/0 route to the internet gateway
The route table for all other subnets has a 0.0.0.0/0 route to the NAT gateway. All private subnets can route to each other.
4. Each subnet has a network ACL implemented that limits all inbound and outbound connectivity to only the required ports and protocols
5. There are 3 Security Groups (SGs) database application and web Each group limits all inbound and outbound connectivity to the minimum required

Which of the following accurately reflects the access control mechanisms the Architect should verify?

- A. Outbound SG configuration on database servers
Inbound SG configuration on application servers
Inbound and outbound network ACL configuration on the database subnet
Inbound and outbound network ACL configuration on the application server subnet
- B. Inbound SG configuration on database servers
Outbound SG configuration on application servers
Inbound and outbound network ACL configuration on the database subnet
Inbound and outbound network ACL configuration on the application server subnet
- C. Inbound and outbound SG configuration on database servers
Inbound and outbound SG configuration on application servers
Inbound network ACL configuration on the database subnet
Outbound network ACL configuration on the application server subnet
- D. Inbound SG configuration on database servers
Outbound SG configuration on application servers
Inbound network ACL configuration on the database subnet
Outbound network ACL configuration on the application server subnet.

Answer: B

QUESTION 261

A company hosts a web-based application that captures and stores sensitive data in an Amazon DynamoDB table. A security audit reveals that the application does not provide end-to-end data protection or the ability to detect unauthorized data changes. The software engineering team needs to make changes that will address the audit findings.

Which set of steps should the software engineering team take?

- A. Use an AWS Key Management Service (AWS KMS) CMK. Encrypt the data at rest.
- B. Use AWS Certificate Manager (ACM) Private Certificate Authority Encrypt the data in transit.
- C. Use a DynamoDB encryption client. Use client-side encryption and sign the table items
- D. Use the AWS Encryption SDK. Use client-side encryption and sign the table items.

Answer: A

QUESTION 262

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

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

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

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

Answer: C

QUESTION 263

A security engineer needs to configure monitoring and auditing for AWS Lambda.

Which combination of actions using AWS services should the security engineer take to accomplish this goal? (Select TWO.)

- A. Use AWS Config to track configuration changes to Lambda functions, runtime environments, tags, handler names, code sizes, memory allocation, timeout settings, and concurrency settings, along with Lambda IAM execution role, subnet, and security group associations.
- B. Use AWS CloudTrail to implement governance, compliance, operational, and risk auditing for Lambda.
- C. Use Amazon Inspector to automatically monitor for vulnerabilities and perform governance, compliance, operational, and risk auditing for Lambda.
- D. Use AWS Resource Access Manager to track configuration changes to Lambda functions, runtime environments, tags, handler names, code sizes, memory allocation, timeout settings, and concurrency settings, along with Lambda IAM execution role, subnet, and security group associations.
- E. Use Amazon Macie to discover, classify, and protect sensitive data being executed inside the Lambda function.

Answer: AB

QUESTION 264

A company uses Microsoft Active Directory for access management for on-premises resources and wants to use the same mechanism for accessing its AWS accounts. Additionally, the development team plans to launch a public-facing application for which they need a separate authentication solution.

Which combination of the following would satisfy these requirements? (Select TWO)

- A. Set up domain controllers on Amazon EC2 to extend the on-premises directory to AWS
- B. Establish network connectivity between on-premises and the user's VPC
- C. Use Amazon Cognito user pools for application authentication
- D. Use AD Connector for application authentication.
- E. Set up federated sign-in to AWS through ADFS and SAML.

Answer: CE

Explanation:

<https://aws.amazon.com/blogs/security/enabling-federation-to-aws-using-windows-active-directory-adfs-and-saml-2-0/>

QUESTION 265

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

Which approach MOST efficiently meets the company's needs?

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

Answer: A

QUESTION 266

A corporation is preparing to acquire several companies. A Security Engineer must design a solution to ensure that newly acquired AWS accounts follow the corporation's security best practices. The solution should monitor each Amazon S3 bucket for unrestricted public write access and use AWS managed services.

What should the Security Engineer do to meet these requirements?

- A. Configure Amazon Macie to continuously check the configuration of all S3 buckets.

- B. Enable AWS Config to check the configuration of each S3 bucket.
- C. Set up AWS Systems Manager to monitor S3 bucket policies for public write access.
- D. Configure an Amazon EC2 instance to have an IAM role and a cron job that checks the status of all S3 buckets.

Answer: C

QUESTION 267

A company hosts an application on Amazon EC2 that is subject to specific rules for regulatory compliance. One rule states that traffic to and from the workload must be inspected for network-level attacks. This involves inspecting the whole packet.

To comply with this regulatory rule, a security engineer must install intrusion detection software on a c5n.4xlarge EC2 instance. The engineer must then configure the software to monitor traffic to and from the application instances.

What should the security engineer do next?

- A. Place the network interface in promiscuous mode to capture the traffic.
- B. Configure VPC Flow Logs to send traffic to the monitoring EC2 instance using a Network Load Balancer.
- C. Configure VPC traffic mirroring to send traffic to the monitoring EC2 instance using a Network Load Balancer.
- D. Use Amazon Inspector to detect network-level attacks and trigger an AWS Lambda function to send the suspicious packets to the EC2 instance.

Answer: C

QUESTION 268

An application running on Amazon EC2 instances generates log files in a folder on a Linux file system. The instances block access to the console and file transfer utilities, such as Secure Copy Protocol (SCP) and Secure File Transfer Protocol (SFTP). The Application Support team wants to automatically monitor the application log files so the team can set up notifications in the future.

A Security Engineer must design a solution that meets the following requirements:

- Make the log files available through an AWS managed service.
- Allow for automatic monitoring of the logs.
- Provide an interface for analyzing logs.
- Minimize effort.

Which approach meets these requirements?

- A. Modify the application to use the AWS SDK Write the application logs to an Amazon S3 bucket
- B. Install the unified Amazon CloudWatch agent on the instances
Configure the agent to collect the application log files on the EC2 file system and send them to Amazon CloudWatch Logs
- C. Install AWS Systems Manager Agent on the instances
Configure an automation document to copy the application log files to AWS DeepLens
- D. Install Amazon Kinesis Agent on the instances
Stream the application log files to Amazon Kinesis Data Firehose and set the destination to Amazon Elasticsearch Service

Answer: D

QUESTION 269

A Security Engineer accidentally deleted the imported key material in an AWS KMS CMK. What should the Security Engineer do to restore the deleted key material?

- A. Create a new CMK.
Download a new wrapping key and a new import token to import the original key material
- B. Create a new CMK.
Use the original wrapping key and import token to import the original key material.
- C. Download a new wrapping key and a new import token.
Import the original key material into the existing CMK.
- D. Use the original wrapping key and import token.
Import the original key material into the existing CMK

Answer: D

QUESTION 270

Your company is planning on AWS on hosting its AWS resources. There is a company policy which mandates that all security keys are completely managed within the company itself. Which of the following is the correct measure of following this policy? Please select:

- A. Using the AWS KMS service for creation of the keys and the company managing the key lifecycle thereafter.
- B. Generating the key pairs for the EC2 Instances using puttygen
- C. Use the EC2 Key pairs that come with AWS
- D. Use S3 server-side encryption

Answer: B

Explanation:

By ensuring that you generate the key pairs for EC2 Instances, you will have complete control of the access keys.

Options A,C and D are invalid because all of these processes means that AWS has ownership of the keys.

And the question specifically mentions that you need ownership of the keys For information on security for Compute Resources, please visit the below URL:

<https://d1.awsstatic.com/whitepapers/Security/Security Compute Services Whitepaper.pdf>

QUESTION 271

A company website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Auto Scaling group across multiple Availability Zones. There is an Amazon CloudFront distribution in front of the ALB. Users are reporting performance problems. A security engineer discovers that the website is receiving a high rate of unwanted requests to the CloudFront distribution originating from a series of source IP addresses.

How should the security engineer address this problem?

- A. Using AWS Shield, configure a deny rule with an IP match condition containing the source IPs of the unwanted requests.
- B. Using Auto Scaling, configure the maximum instance value to an increased count that will

- absorb the unwanted requests.
- C. Using an Amazon VPC NACL, configure an inbound deny rule for each source IP CIDR address of the unwanted requests.
 - D. Using AWS WAF, configure a web ACL rate-based rule on the CloudFront distribution with a rate limit below that of the unwanted requests.

Answer: D

QUESTION 272

A Developer is building a serverless application that uses Amazon API Gateway as the front end. The application will not be publicly accessible. Other legacy applications running on Amazon EC2 will make calls to the application.

A Security Engineer Has been asked to review the security controls for authentication and authorization of the application.

Which combination of actions would provide the MOST secure solution? (Select TWO)

- A. Configure an IAM policy that allows the least permissive actions to communicate with the API Gateway Attach the policy to the role used by the legacy EC2 instances
- B. Enable AWS WAF for API Gateway Configure rules to explicitly allow connections from the legacy EC2 instances
- C. Create a VPC endpoint for API Gateway Attach an IAM resource policy that allows the role of the legacy EC2 instances to call specific APIs
- D. Create a usage plan Generate a set of API keys for each application that needs to call the API.
- E. Configure cross-origin resource sharing (CORS) in each API Share the CORS information with the applications that call the API.

Answer: AE

QUESTION 273

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

The operations team has observed some EC2 instances reboot at random. After rebooting, all access logs on the instances have been deleted. During an investigation, the operations team found that each reboot happened just after a PHP error occurred on the new-user-creation.php file.

The operations team needs to view log information to determine if the company is being attacked.

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

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

an S3 bucket

Use Amazon Athena to query the logs and find the new-user-creation php occurrences.

Answer: B

QUESTION 274

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

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

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

Answer: A

QUESTION 275

A company's security engineer is configuring Amazon S3 permissions to ban all current and future public buckets. However, the company hosts several websites directly off S3 buckets with public access enabled.

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

Which set of steps should the security engineer implement next?

- A. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution
Switch the DNS records from websites to point to the CloudFront distribution
Enable block public access settings at the account level
- B. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution
Switch the DNS records for the websites to point to the CloudFront distribution
Then, for each S3 bucket enable block public access settings
- C. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution
Enable block public access settings at the account level
- D. Configure an S3 bucket as the origin for the CloudFront distribution
Configure the S3 bucket policy to accept connections from the CloudFront points of presence only
Switch the DNS records for the websites to point to the CloudFront distribution
Enable block public access settings at the account level

Answer: A

QUESTION 276

A global company that deals with International finance is investing heavily in cryptocurrencies and

wants to experiment with mining technologies using AWS.

The company's security team has enabled Amazon GuardDuty and is concerned by the number of findings being generated by the accounts.

The security team wants to minimize the possibility of GuardDuty finding false negatives for compromised instances that are performing mining.

How can the security team continue using GuardDuty while meeting these requirements?

- A. In the GuardDuty console, select the CryptoCurrency:EC2/BitcoinTool B'DNS finding and use the suppress findings option
- B. Create a custom AWS Lambda function to process newly detected GuardDuty alerts Process the CryptoCurrency EC2/BitcoinTool BIDNS alert and filter out the high-severity finding types only.
- C. When creating a new Amazon EC2 Instance, provide the instance with a specific tag that indicates it is performing mining operations
Create a custom AWS Lambda function to process newly detected GuardDuty alerts and filter for the presence of this tag
- D. When GuardDuty produces a cryptocurrency finding, process the finding with a custom AWS Lambda function to extract the instance ID from the finding
Then use the AWS Systems Manager Run Command to check for a running process performing mining operations

Answer: A

QUESTION 277

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

Answer: B

QUESTION 278

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

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

- A. Encrypt the data in Amazon S3 using server-side encryption with Amazon S3 managed encryption keys (SSE-S3)
- B. Encrypt the data in Amazon S3 using server-side encryption with AWS KMS managed encryption keys (SSE-KMS)
- C. Create a new Amazon S3 VPC endpoint and modify the VPC's routing tables to use the new endpoint
- D. Use the Amazon S3 Block Public Access feature.

- E. Configure the bucket policy to allow access from the application instances only
- F. Use a NACL to filter traffic to Amazon S3

Answer: BCE

QUESTION 279

A security engineer is auditing a production system and discovers several additional IAM roles that are not required and were not previously documented during the last audit 90 days ago.

The engineer is trying to find out who created these IAM roles and when they were created. The solution must have the lowest operational overhead.

Which solution will meet this requirement?

- A. Import AWS CloudTrail logs from Amazon S3 into an Amazon Elasticsearch Service cluster, and search through the combined logs for CreateRole events.
- B. Create a table in Amazon Athena for AWS CloudTrail events.
Query the table in Amazon Athena for CreateRole events.
- C. Use AWS Config to look up the configuration timeline for the additional IAM roles and view the linked AWS CloudTrail event.
- D. Download the credentials report from the IAM console to view the details for each IAM entity, including the creation dates.

Answer: A

QUESTION 280

A security engineer must develop an encryption tool for a company. The company requires a cryptographic solution that supports the ability to perform cryptographic erasure on all resources protected by the key material in 15 minutes or less

Which AWS Key Management Service (AWS KMS) key solution will allow the security engineer to meet these requirements?

- A. Use Imported key material with CMK
- B. Use an AWS KMS CMK
- C. Use an AWS managed CMK.
- D. Use an AWS KMS customer managed CMK

Answer: C

QUESTION 281

A company is using AWS Organizations to manage multiple AWS member accounts. All of these accounts have Amazon GuardDuty enabled in all Regions. The company's AW5 Security Operations Center has a centralized security account for logging and monitoring. One of the member accounts has received an excessively high bill. A security engineer discovers that a compromised Amazon EC2 instance is being used to mine crypto currency. The Security Operations Center did not receive a GuardDuty finding in the central security account. But there was a GuardDuty finding in the account containing the compromised EC2 instance. The security engineer needs to ensure all GuardDuty findings are available in the security account.

What should the security engineer do to resolve this issue?

- A. Set up an Amazon CloudWatch Event rule to forward all GuardDuty findings to the security

- account
Use an AWS Lambda function as a target to raise findings
- B. Set up an Amazon CloudWatch Events rule to forward all GuardDuty findings to the security account
Use an AWS Lambda function as a target to raise findings in AWS Security Hub
- C. Check that GuardDuty in the security account is able to assume a role in the compromised account using the GuardDuty fast findings permission
Schedule an Amazon CloudWatch Events rule and an AWS Lambda function to periodically check for GuardDuty findings
- D. Use the aws GuardDuty get-members AWS CLI command in the security account to see if the account is listed
Send an invitation from GuardDuty in the security account to GuardDuty in the compromised account
Accept the invitation to forward all future GuardDuty findings

Answer: D

QUESTION 282

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

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

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

Answer: A

QUESTION 283

A website currently runs on Amazon EC2 with mostly static content on the site. Recently, the site was subjected to a DDoS attack, and a Security Engineer was tasked with redesigning the edge security to help mitigate this risk in the future,

What are some ways the Engineer could achieve this? (Select THREE)

- A. Use AWS X-Ray to inspect the traffic going to the EC2 instances

- B. Move the state content to Amazon S3 and font this with an Amazon CloudFront distribution
- C. Change the security group configuration to block the source of the attack traffic
- D. Use AWS WAF security rules to inspect the inbound traffic
- E. Use Amazon inspector assessment templates to inspect the inbound traffic
- F. Use Amazon Route 53 to distribute traffic

Answer: BDF

QUESTION 284

A company needs its Amazon Elastic Block Store (Amazon EBS) volumes to be encrypted at all times.

During a security incident. EBS snapshots of suspicious instances are shared to a forensics account for analysis.

A security engineer attempting to share a suspicious EBS snapshot to the forensics account receives the following error:

"Unable to share snapshot: An error occurred (OperationNotPermitted) when calling the ModifySnapshotAttribute operation: Encrypted snapshots with EBS default key cannot be shared."

Which combination of steps should the security engineer take in the incident account to complete the sharing operation? (Select THREE)

- A. Create a customer managed CMK
 - Copy the EBS snapshot encrypting the destination snapshot using the new CMKB
 - Allow forensics accounting principals to use the CMK by modifying its policy
- B. Create an Amazon EC2 instance
 - Attach the encrypted and suspicious EBS volume.
 - Copy data from the suspicious volume to an unencrypted volume. Snapshot the unencrypted volume
- C. Copy the EBS snapshot to the new decrypted snapshot
- D. Restore a volume from the suspicious EBS snapshot
 - Create an unencrypted EBS volume of the same size
- E. Share the target EBS snapshot with the forensics account

Answer: AB

QUESTION 285

A company is collecting AWS CloudTrail log data from multiple AWS accounts by managing individual trails in each account and forwarding log data to a centralized Amazon S3 bucket residing in a log archive account. After CloudTrail introduced support for AWS Organizations trails, the company decided to further centralize management and automate deployment of the CloudTrail logging capability across all of its AWS accounts.

The company's security engineer created an AWS Organizations trail in the master account, enabled server-side encryption with AWS KMS managed keys (SSE-KMS) for the log files, and specified the same bucket as the storage location. However, the engineer noticed that logs recorded by the new trail were not delivered to the bucket.

Which factors could cause this issue? (Choose two.)

- A. The CMK key policy does not allow CloudTrail to make encrypt and decrypt API calls against the

- key.
- B. The CMK key policy does not allow CloudTrail to make GenerateDatakey API calls against the key.
 - C. The IAM role used by the CloudTrail trail does not have permissions to make PutObject API calls against a folder created for the Organizations trail.
 - D. The S3 bucket policy does not allow CloudTrail to make PutObject API calls against a folder created for the Organizations trail.
 - E. The CMK key policy does not allow the IAM role used by the CloudTrail trail to use the key for cryptographical operations.

Answer: AD

QUESTION 286

Users report intermittent availability of a web application hosted on AWS. Monitoring systems report an excess of abnormal network traffic followed by high CPU utilization on the application web tier.

Which of the following techniques will improve the availability of the application? (Select TWO.)

- A. Deploy AWS WAF to block all unsecured web applications from accessing the internet.
- B. Deploy an Intrusion Detection/Prevention System (IDS/IPS) to monitor or block unusual incoming network traffic.
- C. Configure security groups to allow outgoing network traffic only from hosts that are protected with up-to-date antivirus software.
- D. Create Amazon CloudFront distribution and configure AWS WAF rules to protect the web applications from malicious traffic.
- E. Use the default Amazon VPC for external facing systems to allow AWS to actively block malicious network traffic affecting Amazon EC2 instances.

Answer: BD

QUESTION 287

A company wants to encrypt data locally while meeting regulatory requirements related to key exhaustion. The encryption key can be no more than 10 days old or encrypt more than 2^{16} objects. Any encryption key must be generated on a FIPS-validated hardware security module (HSM). The company is cost-conscious, as it plans to upload an average of 100 objects to Amazon S3 each second for sustained operations across 5 data producers.

Which approach MOST efficiently meets the company's needs?

- A. Use the AWS Encryption SDK and set the maximum age to 10 days and the maximum number of messages encrypted to 2^{16} .
Use AWS Key Management Service (AWS KMS) to generate the master key and data key. Use data key caching with the Encryption SDK during the encryption process.
- B. Use AWS Key Management Service (AWS KMS) to generate an AWS managed CMK.
Then use Amazon S3 client-side encryption configured to automatically rotate with every object.
- C. Use AWS CloudHSM to generate the master key and data keys.
Then use Boto 3 and Python to locally encrypt data before uploading the object.
Rotate the data key every 10 days or after 2^{16} objects have been uploaded to Amazon S3.
- D. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) and set the master key to automatically rotate.

Answer: C

QUESTION 288

A company's Security Officer is concerned about the risk of AWS account root user logins and has assigned a Security Engineer to implement a notification solution for near-real-time alerts upon account root user logins.

How should the Security Engineer meet these requirements?

- A. Create a cron job that runs a script to download the AWS IAM security credentials. We. parse the file for account root user logins and email the Security team's distribution list.
- B. Run AWS CloudTrail logs through Amazon CloudWatch Events to detect account root user logins and trigger an AWS Lambda function to send an Amazon SNS notification to the Security team's distribution list.
- C. Save AWS CloudTrail logs to an Amazon S3 bucket in the Security team's account. Process the CloudTrail logs with the Security Engineer's logging solution for account root user logins. Send an Amazon SNS notification to the Security team upon encountering the account root user login events.
- D. Save VPC Flow Logs to an Amazon S3 bucket in the Security team's account and process the VPC Flow Logs with their logging solutions for account root user logins. Send an Amazon SNS notification to the Security team upon encountering the account root user login events.

Answer: B

QUESTION 289

A security engineer has created an Amazon Cognito user pool.

The engineer needs to manually verify the ID and access token sent by the application for troubleshooting purposes.

What is the MOST secure way to accomplish this?

- A. Extract the subject (sub), audience (aud), and cognito:username from the ID token payload. Manually check the subject and audience for the user name In the user pool.
- B. Search for the public key with a key ID that matches the key ID In the header of the token. Then use a JSON Web Token (JWT) library to validate the signature of the token and extract values, such as the expiry date.
- C. Verify that the token is not expired. Then use the token_use claim function In Amazon Cognito to validate the key IDs.
- D. Copy the JSON Web Token (JWT) as a JSON document. Obtain the public JSON Web Key (JWK) and convert it to a pem file. Then use the file to validate the original JWT.

Answer: A

QUESTION 290

A company's security information events management (SIEM) tool receives new AWS CloudTrail logs from an Amazon S3 bucket that is configured to send all object created event notification to an Amazon SNS topic.

An Amazon SQS queue is subscribed to this SNS topic. The company's SEM tool then ports this SQS queue for new messages using an IAM role and fetches new log events from the S3 bucket based on the SQS messages.

After a recent security review that resulted in restricted permissions, the SEM tool has stopped

receiving new CloudTrail logs

Which of the following are possible causes of this issue? (Select THREE)

- A. The SQS queue does not allow the SQS SendMessage action from the SNS topic
- B. The SNS topic does not allow the SNS Publish action from Amazon S3
- C. The SNS topic is not delivering raw messages to the SQS queue
- D. The S3 bucket policy does not allow CloudTrail to perform the PutObject action
- E. The IAM role used by the 5EM tool does not have permission to subscribe to the SNS topic
- F. The IAM role used by the SEM tool does not allow the SQS DeleteMessage action.

Answer: ADF

QUESTION 291

An company is using AWS Secrets Manager to store secrets that are encrypted using a CMK and are stored in the security account 111122223333. One of the company's production accounts.

444455556666, must retrieve the secret values from the security account 111122223333.

A security engineer needs to apply a policy to the secret in the security account based on least privilege access so the production account can retrieve the secret value only.

Which policy should the security engineer apply?

A. {
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "secretsmanager:*",
 "Principal": {"AWS": "444455556666"},
 "Resource": "*"
 }
]
}

B. {
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "secretsmanager:*",
 "Principal": {"AWS": "111122223333"},
 "Resource": "*"
 }
]
}

```
C.  {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Principal": ("AWS": "111122223333"),
            "Resource": "*"
        }
    ]
}

D.  {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Principal": ("AWS": "444455556666"),
            "Resource": "*"
        }
    ]
}
```

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

Answer: A

QUESTION 292

Which of the below services can be integrated with the AWS Web application firewall service?
Choose 2 answers from the options given below

- A. AWS Cloudfront
- B. AWS Lambda
- C. AWS Application Load Balancer
- D. AWS Classic Load Balancer

Answer: AC

Explanation:

The AWS documentation mentions the following on the Application Load Balancer AWS WAF can be deployed on Amazon CloudFront and the Application Load Balancer (ALB). As part of Amazon CloudFront it can be part of your Content Distribution Network (CDN) protecting your resources and content at the Edge locations and as part of the Application Load Balancer it can protect your origin web servers running behind the ALBs. Options B and D are invalid because only Cloudfront and the Application Load Balancer services are supported by AWS WAF.

QUESTION 293

A company is outsourcing its operational support to an external company.
The company's security officer must implement an access solution for delegating operational support that minimizes overhead.

Which approach should the security officer take to meet these requirements?

- A. implement Amazon Cognito identity pools with a role that uses a policy that denies the actions related to Amazon Cognito API management
Allow the external company to federate through its identity provider
- B. Federate AWS Identity and Access Management (IAM) with the external company's identity provider
Create an IAM role and attach a policy with the necessary permissions
- C. Create an IAM group for the external company
Add a policy to the group that denies IAM modifications Securely provide the credentials to the external company.
- D. Use AWS SSO with the external company's identity provider.
Create an IAM group to map to the identity provider user group, and attach a policy with the necessary permissions.

Answer: B

QUESTION 294

A security engineer has noticed an unusually high amount of traffic coming from a single IP address. This was discovered by analyzing the Application Load Balancer's access logs. How can the security engineer limit the number of requests from a specific IP address without blocking the IP address?

- A. Add a rule to the Application Load Balancer to route the traffic originating from the IP address in question and show a static webpage.
- B. Implement a rate-based rule with AWS WAF
- C. Use AWS Shield to limit the originating traffic hit rate.
- D. Implement the GeoLocation feature in Amazon Route 53.

Answer: B

QUESTION 295

A company is developing a new mobile app for social media sharing. The company's development team has decided to use Amazon S3 to store media files generated by mobile app users. The company wants to allow users to control whether their own tiles are public, private, or shared with other users in their social network.

What should the development team do to implement the type of access control with the LEAST administrative effort?

- A. Use individual ACLs on each S3 object.
- B. Use IAM groups for sharing files between application social network users
- C. Store each user's files in a separate S3 bucket and apply a bucket policy based on the user's sharing settings
- D. Generate presigned URLs for each file access

Answer: A

QUESTION 296

A company hosts its public website on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an EC2 Auto Scaling group across multiple Availability Zones.

The website is under a DDoS attack by a specific IoT device brand that is visible in the user agent.

A security engineer needs to mitigate the attack without impacting the availability of the public website.

What should the security engineer do to accomplish this?

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

Answer: D

QUESTION 297

A company has hundreds of AWS accounts, and a centralized Amazon S3 bucket used to collect AWS CloudTrail for all of these accounts. A security engineer wants to create a solution that will enable the company to run ad hoc queries against its CloudTrail logs dating back 3 years from when the trails were first enabled in the company's AWS account.

How should the company accomplish this with the least amount of administrative overhead?

- A. Run an Amazon EMR cluster that uses a MapReduce job to examine the CloudTrail trails.
- B. Use the events history/feature of the CloudTrail console to query the CloudTrail trails.
- C. Write an AWS Lambda function to query the CloudTrail trails
Configure the Lambda function to be executed whenever a new file is created in the CloudTrail S3 bucket.
- D. Create an Amazon Athena table that points at the S3 bucket the CloudTrail trails are being written to use Athena to run queries against the trails.

Answer: D

QUESTION 298

A company uses SAML federation with AWS Identity and Access Management (IAM) to provide internal users with SSO for their AWS accounts.

The company's identity provider certificate was rotated as part of its normal lifecycle. Shortly after, users started receiving the following error when attempting to log in:

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

A security engineer needs to address the immediate issue and ensure that it will not occur again.

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

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

Answer: AD

QUESTION 299

Your company has just started using AWS and created an AWS account. They are aware of the potential issues when root access is enabled.

How can they best safeguard the account when it comes to root access? Choose 2 answers from the options given below

- A. Delete the root access account
- B. Create an Admin IAM user with the necessary permissions
- C. Change the password for the root account.
- D. Delete the root access keys

Answer: BD

Explanation:

The AWS Documentation mentions the following All AWS accounts have root user credentials (that is, the credentials of the account owner). These credentials allow full access to all resources in the account.

Because you can't restrict permissions for root user credentials, we recommend that you delete your root user access keys. Then create AWS Identity and Access Management (IAM) user credentials for everyday interaction with AWS.

Option A is incorrect since you cannot delete the root access account

Option C is partially correct but cannot be used as the ideal solution for safeguarding the account

QUESTION 300

A security team is creating a response plan in the event an employee executes unauthorized actions on AWS infrastructure. They want to include steps to determine if the employee's IAM permissions changed as part of the incident.

What steps should the team document in the plan?

- A. Use AWS Config to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.
- B. Use CloudTrail to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.
- C. Use Trusted Advisor to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.
- D. Use Lambda to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.

Answer: A

Explanation:

You can use the AWSConfig history to see the history of a particular item. The below snapshot shows an example configuration for a user in AWS Config



The screenshot shows a AWS Config history entry for a User configuration. The top right corner displays the date and time: 05th May 2018, 9:53:21 PM. Below this, the 'Configuration Details' section is expanded, showing the following information:

| | | | |
|----------------------|---------------------------------|-----------------------|-------|
| Amazon Resource Name | arn:aws:iam::1387512:user/UserA | User Name | UserA |
| Resource type | AWS::IAM::User | Inline Policy Details | |

Option B,C and D are all invalid because these services cannot be used to see the history of a particular configuration item. This can only be accomplished by AWS Config.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/TrackinChanges.html>

QUESTION 301

A company is hosting a website that must be accessible to users for HTTPS traffic. Also port 22 should be open for administrative purposes. The administrator's workstation has a static IP address of 203.0.113.1/32.

Which of the following security group configurations are the MOST secure but still functional to support these requirements? Choose 2 answers from the options given below

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

Answer: AD

Explanation:

Since HTTPS traffic is required for all users on the Internet, Port 443 should be open on all IP addresses.

For port 22, the traffic should be restricted to an internal subnet.

Option B is invalid, because this only allow traffic from a particular CIDR block and not from the internet

Option C is invalid because allowing port 22 from the internet is a security risk

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.html>

QUESTION 302

Your IT Security team has advised to carry out a penetration test on the resources in their company's AWS Account.

This is as part of their capability to analyze the security of the Infrastructure.

What should be done first in this regard?

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

Answer: C

Explanation:

This concept is given in the AWS Documentation How do I submit a penetration testing request for my AWS resources? Issue

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

Resolution

Before performing security testing on AWS resources, you must obtain approval from AWS.

After you submit your request AWS will reply in about two business days. AWS might have additional questions about your test which can extend the approval process, so plan accordingly and be sure that your initial request is as detailed as possible. If your request is approved, you'll receive an authorization number.

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

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

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

QUESTION 303

Your company has a requirement to monitor all root user activity by notification. How can this best be achieved? Choose 2 answers from the options given below. Each answer forms part of the solution

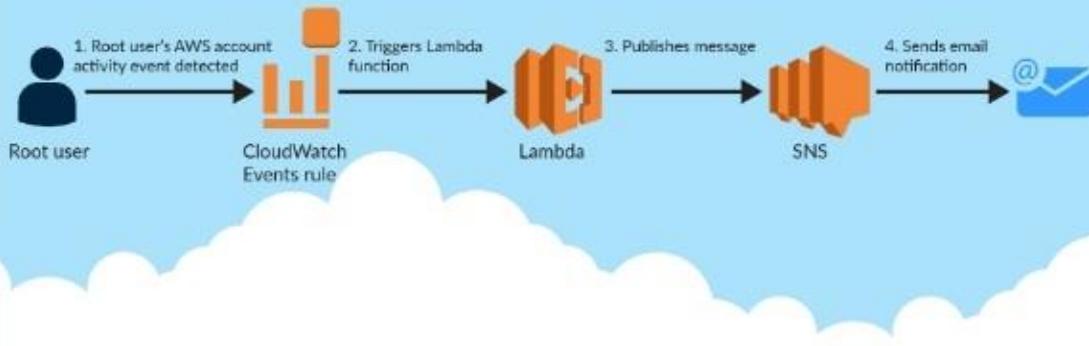
- A. Create a Cloudwatch Events Rule
- B. Create a Cloudwatch Logs Rule
- C. Use a Lambda function
- D. Use Cloudtrail API call

Answer: AC

Explanation:

Below is a snippet from the AWS blogs on a solution

Monitor and Notify on AWS Account Root User Activity



Option B is invalid because you need to create a Cloudwatch Events Rule and there is such thing as a Cloudwatch Logs Rule

Option D is invalid because Cloud Trail API calls can be recorded but cannot be used to send across notifications

<https://aws.amazon.com/blogs/mt/monitor-and-notify-on-aws-account-root-user-activity>

QUESTION 304

Your company is planning on hosting an internal network in AWS. They want machines in the VPC to authenticate using private certificates. They want to minimize the work and maintenance in working with certificates.

What is the ideal way to fulfil this requirement.

- A. Consider using Windows Server 2016 Certificate Manager
- B. Consider using AWS Certificate Manager
- C. Consider using AWS Access keys to generate the certificates
- D. Consider using AWS Trusted Advisor for managing the certificates

Answer: B

Explanation:

The AWS Documentation mentions the following ACM is tightly linked with AWS Certificate Manager Private Certificate Authority.

You can use ACM PCA to create a private certificate authority (CA) and then use ACM to issue private certificates. These are SSL/TLS X.509 certificates that identify users, computers, applications, services, servers, and other devices internally. Private certificates cannot be publicly trusted. Option A is partially invalid. Windows Server 2016 Certificate Manager can be used but since there is a requirement to "minimize the work and maintenance", AWS Certificate Manager should be used. Options C and D are invalid because these cannot be used for managing certificates.

<https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html>

QUESTION 305

A company wants to have a secure way of generating, storing and managing cryptographic

exclusive access for the keys.

Which of the following can be used for this purpose?

- A. Use KMS and the normal KMS encryption keys
- B. Use KMS and use an external key material
- C. Use S3 Server Side encryption
- D. Use Cloud HSM

Answer: D

Explanation:

The AWS Documentation mentions the following The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the AWS cloud. AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary. CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are designed and validated to government standards for secure key management. CloudHSM allows you to securely generate, store and manage cryptographic keys used for data encryption in a way that keys are accessible only by you. Option A, B and C are invalid because in all of these cases, the management of the key will be with AWS. Here the question specifically mentions that you want to have exclusive access over the keys. This can be achieved with Cloud HSM.
<https://aws.amazon.com/cloudhsm/faq>:

QUESTION 306

Your IT Security department has mandated that all data on EBS volumes created for underlying EC2 Instances need to be encrypted.

Which of the following can help achieve this?

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

Answer: A

Explanation:

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

Option B is incorrect - The AWS Certificate manager can be used to generate SSL certificates that can be used to encrypt traffic transit, but not at rest
Option C is incorrect as it is again used for issuing tokens when using API gateway for traffic in transit.
Option D is used for secure access to EC2 Instances
<https://docs.aws.amazon.com/kms/latest/developerguide/overview.html>

QUESTION 307

Your company has mandated that all calls to the AWS KMS service be recorded.

How can this be achieved?

- A. Enable logging on the KMS service
- B. Enable a trail in Cloudtrail
- C. Enable Cloudwatch logs
- D. Use Cloudwatch metrics

Answer: B

Explanation:

The AWS Documentation states the following AWS KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of AWS KMS in your AWS account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures API calls from the AWS KMS console or from the AWS KMS API. Using the information collected by CloudTrail, you can determine what request was made, the source IP address from which the request was made, who made the request when it was made, and so on.

Option A is invalid because logging is not possible in the KMS service

Option C and D are invalid because Cloudwatch cannot be used to monitor API calls
<https://docs.aws.amazon.com/kms/latest/developerguide/logging-using-cloudtrail.html>

QUESTION 308

You have an S3 bucket hosted in AWS. This is used to host promotional videos uploaded by yourself. You need to provide access to users for a limited duration of time.

How can this be achieved?

- A. Use versioning and enable a timestamp for each version
- B. Use Pre-signed URL's
- C. Use IAM Roles with a timestamp to limit the access
- D. Use IAM policies with a timestamp to limit the access

Answer: B

Explanation:

The AWS Documentation mentions the following All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL using their own security credentials, to grant time-limited permission to download the objects.

Option A is invalid because this can be used to prevent accidental deletion of objects

Option C is invalid because timestamps are not possible for Roles

Option D is invalid because policies is not the right way to limit access based on time
<https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.htm>

QUESTION 309

A company's AWS CloudTrail logs are all centrally stored in an Amazon S3 bucket. The security team controls the company's AWS account. The security team must prevent unauthorized access and tampering of the CloudTrail logs.

Which combination of steps should the security team take? (Choose three.)

- A. Configure server-side encryption with AWS KMS managed encryption keys (SSE-KMS)
- B. Compress log file with secure gzip.
- C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to notify the security team of any modifications on CloudTrail log files.
- D. Implement least privilege access to the S3 bucket by configuring a bucket policy.

- E. Configure CloudTrail log file integrity validation.
- F. Configure Access Analyzer for S3.

Answer: BCE

QUESTION 310

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

You define the below custom bucket policy

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

But when you try to apply the policy you get the error "Action does not apply to any resource(s) in statement."

What should be done to rectify the error?

- A. Change the IAM permissions by applying PutBucketPolicy permissions.
- B. Verify that the policy has the same name as the bucket name. If not, make it the same.
- C. Change the Resource section to "arn:aws:s3:::appbucket/*".
- D. Create the bucket "appbucket" and then apply the policy.

Answer: C

Explanation:

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

Option A is invalid because the right permissions are already provided as per the question requirement

Option B is invalid because it is not necessary that the policy has the same name as the bucket

Option D is invalid because this should be the default flow for applying the policy

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

QUESTION 311

Your company has an EC2 Instance that is hosted in an AWS VPC. There is a requirement to ensure that logs files from the EC2 Instance are stored accordingly. The access should also be limited for the destination of the log files.

How can this be accomplished? Choose 2 answers from the options given below. Each answer forms part of the solution

- A. Stream the log files to a separate Cloudtrail trail
- B. Stream the log files to a separate Cloudwatch Log group
- C. Create an IAM policy that gives the desired level of access to the Cloudtrail trail
- D. Create an IAM policy that gives the desired level of access to the Cloudwatch Log group

Answer: BD

Explanation:

You can create a Log group and send all logs from the EC2 Instance to that group. You can then limit the access to the Log groups via an IAM policy.

Option A is invalid because Cloudtrail is used to record API activity and not for storing log files

Option C is invalid because Cloudtrail is the wrong service to be used for this requirement

* <https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WorkingWithLogs.html>

* <https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/auth-and-access-control-cwl.html>

QUESTION 312

You have enabled Cloudtrail logs for your company's AWS account. In addition, the IT Security department has mentioned that the logs need to be encrypted.

How can this be achieved?

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

Answer: B

Explanation:

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

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

<https://docs.aws.amazon.com/awscloudtrail/latest/usereguide/how-cloudtrail-works.html>

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

QUESTION 313

You are hosting a web site via website hosting on an S3 bucket - <http://demo.s3-website-us-east-1.amazonaws.com>. You have some web pages that use Javascript that access resources in another bucket which has web site hosting also enabled. But when users access the web pages , they are getting a blocked Javascript error. How can you rectify this?

- A. Enable CORS for the bucket
- B. Enable versioning for the bucket
- C. Enable MFA for the bucket
- D. Enable CRR for the bucket

Answer: A

Explanation:

Use-case Scenarios

The following are example scenarios for using CORS:

Scenario 1: Suppose that you are hosting a website in an Amazon S3 bucket named website as described in Hosting a Static Website on Amazon S3. Your users load the website endpoint <http://website.s3-website-us-east-1.amazonaws.com>. Now you want to use JavaScript on the webpages that are stored in this bucket to be able to make authenticated GET and PUT requests against the same bucket by using the Amazon S3 API endpoint for the bucket website.s3.amazonaws.com. A browser would normally block JavaScript from allowing those requests, but with CORS you can configure your bucket to explicitly enable cross-origin requests from website.s3-website-us-east-1.amazonaws.com.

Scenario 2: Suppose that you want to host a web font from your S3 bucket. Again, browsers require a CORS check (also called a preflight check) for loading web fonts. You would configure the bucket that is hosting the web font to allow any origin to make these requests.

Option B is invalid because versioning is only to create multiple versions of an object and can help in accidental deletion of objects

Option C is invalid because this is used as an extra measure of caution for deletion of objects

Option D is invalid because this is used for Cross region replication of objects

<https://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html>

QUESTION 314

Compliance requirements state that all communications between company on-premises hosts and EC2 instances be encrypted in transit.

Hosts use custom proprietary protocols for their communication, and EC2 instances need to be fronted by a load balancer for increased availability.

Which of the following solutions will meet these requirements?

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

Answer: B

Explanation:

If you use HTTPS or SSL for your front-end connections, you must deploy an X.509 certificate (SSL server certificate) on your load balancer. The load balancer decrypts requests from clients before sending them to the back-end instances (known as SSL termination). For more information, see SSL/TLS Certificates for Classic Load Balancers.

If you don't want the load balancer to handle the SSL termination (known as SSL offloading), you can use TCP for both the front-end and back-end connections, and deploy certificates on the registered instances handling requests.

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-listener-config.html>

QUESTION 315

You have a 2 tier application hosted in AWS. It consists of a web server and database server (SQL Server) hosted on separate EC2 Instances. You are devising the security groups for these EC2 Instances. The Web tier needs to be accessed by users across the Internet. You have created a web security group(wg- 123) and database security group(db- 345). Which combination of the following security group rules will allow the application to be secure and functional. Choose 2 answers from the options given below.

- A. wg-123 -Allow ports 80 and 443 from 0.0.0.0/0
- B. db-345 - Allow port 1433 from wg-123
- C. wg-123 - Allow port 1433 from wg-123
- D. db-345 -Allow ports 1433 from 0.0.0.0/0

Answer: AB**Explanation:**

The Web security groups should allow access for ports 80 and 443 for HTTP and HTTPS traffic to all users from the internet. The database security group should just allow access from the web security group from port 1433.

Option C is invalid because this is not a valid configuration

Option D is invalid because database security should not be allowed on the internet

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.html>

QUESTION 316

A security team must present a daily briefing to the CISO that includes a report of which of the company's thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day's report. How can the security team fulfill these requirements?

- A. Use Amazon QuickSight and Cloud Trail to generate the report of out of compliance instances/servers.
Redeploy all out of compliance instances/servers using an AMI with the latest patches.
- B. Use Systems Manger Patch Manger to generate the report of out of compliance instances/servers.
Use Systems Manager Patch Manger to install the missing patches.
- C. Use Systems Manger Patch Manger to generate the report of out of compliance instances/servers.
Redeploy all out of compliance instances/servers using an AMI with the latest patches.
- D. Use Trusted Advisor to generate the report of out of compliance instances/servers.
Use Systems Manager Patch Manger to install the missing patches.

Answer: B**Explanation:**

Use the Systems Manager Patch Manager to generate the report and also install the missing patches The AWS Documentation mentions the following

AWS Systems Manager Patch Manager automates the process of patching managed instances with security-related updates.

For Linux-based instances, you can also install patches for non-security updates.

You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux.

You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.

Option A is invalid because Amazon

Quicksight and Cloud Trail cannot be used to generate the list of servers that don't meet

compliance needs.

Option C is wrong because deploying instances via new AMI'S would impact the applications hosted on these servers

Option D is invalid because Amazon Trusted Advisor cannot be used to generate the list of servers that don't meet compliance needs.

<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html>

QUESTION 317

You are designing a custom IAM policy that would allow users to list buckets in S3 only if they are MFA authenticated. \

Which of the following would best match this requirement?

- A. { "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Action": ["s3>ListAllMyBuckets", "s3:GetBucketLocation"], "Resource": "Resource": "arn:aws:s3:::*", "Condition": { "Bool": {"aws:MultiFactorAuthPresent": true} } } }
- B. { "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Action": ["s3>ListAllMyBuckets", "s3:GetBucketLocation"], "Resource": "Resource": "arn:aws:s3:::*", "Condition": { "Bool": {"aws:MultiFactorAuthPresent":false} } } }
- C. { "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Action": ["s3>ListAllMyBuckets", "s3:GetBucketLocation"], "Resource": "Resource": "arn:aws:s3:::*", "Condition": { "aws:MultiFactorAuthPresent":false } } } }
- D. { "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Action": ["s3>ListAllMyBuckets", "s3:GetBucketLocation"], "Resource": "Resource": "arn:aws:s3:::*", "Condition": { "aws:MultiFactorAuthPresent":true } } } }

Answer: A

Explanation:

The Condition clause can be used to ensure users can only work with resources if they are MFA authenticated.

Option B and C are wrong since the aws:MultiFactorAuthPresent clause should be marked as true. Here you are saying that only if the user has been MFA activated, that means it is true, then allow access.

Option D is invalid because the "boor clause is missing in the evaluation for the condition clause. Boolean conditions let you construct Condition elements that restrict access based on comparing a key to "true" or "false."

Here in this scenario the boot attribute in the condition element will return a value True for option A which will ensure that access is allowed on S3 resources.

QUESTION 318

A company hosts a critical web application on the AWS Cloud. This is a key revenue generating application for the company. The IT Security team is worried about potential DDos attacks against the web site. The senior management has also specified that immediate action needs to be taken in case of a potential DDos attack. What should be done in this regard?

- A. Consider using the AWS Shield Service
- B. Consider using VPC Flow logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.
- C. Consider using the AWS Shield Advanced Service
- D. Consider using Cloudwatch logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.

Answer: C

Explanation:

Option A is invalid because the normal AWS Shield Service will not help in immediate action against a DDoS attack. This can be done via the AWS Shield Advanced Service
 Option B is invalid because this is a logging service for VPCs traffic flow but cannot specifically protect against DDoS attacks.

Option D is invalid because this is a logging service for AWS Services but cannot specifically protect against DDoS attacks.

The AWS Documentation mentions the following

AWS Shield Advanced provides enhanced protections for your applications running on Amazon EC2.

Elastic Load Balancing (ELB), Amazon CloudFront and Route 53 against larger and more sophisticated attacks. AWS Shield Advanced is available to AWS Business Support and AWS Enterprise Support customers. AWS Shield Advanced protection provides always-on, flow-based monitoring of network traffic and active application monitoring to provide near real-time notifications of DDoS attacks. AWS Shield Advanced also gives customers highly flexible controls over attack mitigations to take actions instantly.

Customers can also engage the DDoS Response Team (DRT) 24X7 to manage and mitigate their application layer DDoS attacks.

QUESTION 319

A company wants to have an Intrusion detection system available for their VPC in AWS. They want to have complete control over the system.

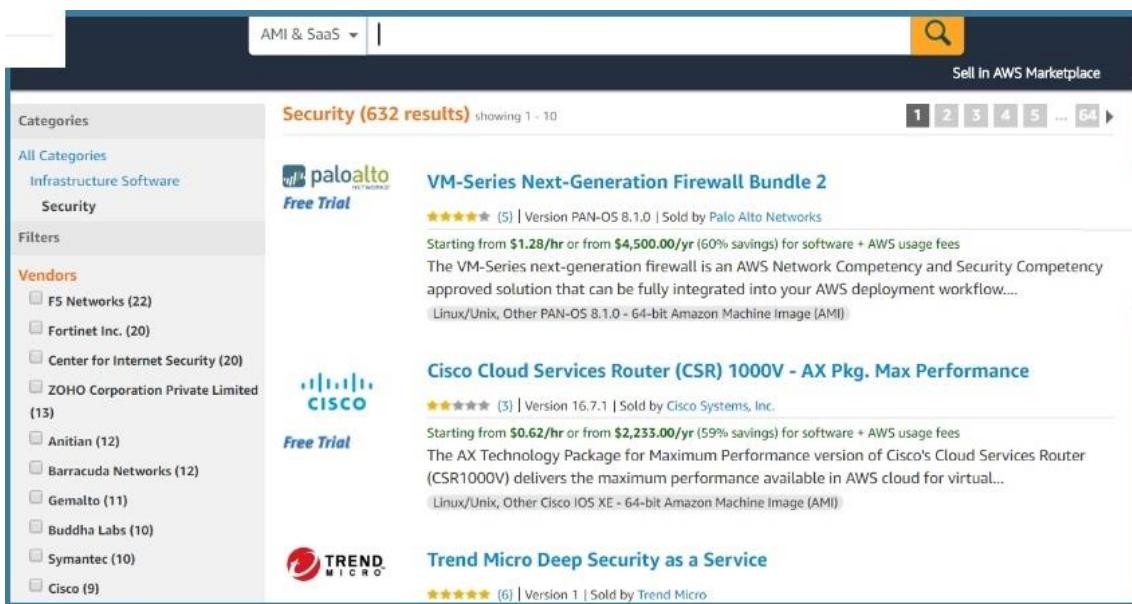
Which of the following would be ideal to implement?

- A. Use AWS WAF to catch all intrusions occurring on the systems in the VPC
- B. Use a custom solution available in the AWS Marketplace
- C. Use VPC Flow logs to detect the issues and flag them accordingly.
- D. Use AWS Cloudwatch to monitor all traffic

Answer: B

Explanation:

Sometimes companies want to have custom solutions in place for monitoring Intrusions to their systems. In such a case, you can use the AWS Marketplace for looking at custom solutions.



The screenshot shows the AWS Marketplace search results for 'Security' products. The search bar at the top has 'AMI & SaaS' selected. Below the search bar, there's a 'Sell in AWS Marketplace' button. The main area displays a grid of security products:

- Palo Alto Networks VM-Series Next-Generation Firewall Bundle 2**: Sold by Palo Alto Networks. Starting from \$1.28/hr or \$4,500.00/yr. Description: The VM-Series next-generation firewall is an AWS Network Competency and Security Competency approved solution that can be fully integrated into your AWS deployment workflow....
- Cisco Cloud Services Router (CSR) 1000V - AX Pkg. Max Performance**: Sold by Cisco Systems, Inc. Starting from \$0.62/hr or \$2,235.00/yr. Description: The AX Technology Package for Maximum Performance version of Cisco's Cloud Services Router (CSR1000V) delivers the maximum performance available in AWS cloud for virtual....
- Trend Micro Deep Security as a Service**: Sold by Trend Micro. Starting from \$0.00/hr or \$0.00/yr. Description: Trend Micro Deep Security as a Service provides advanced threat protection for your organization's endpoints, servers, and clouds.

On the left sidebar, there are filters for 'Categories' (All Categories, Infrastructure Software, Security) and 'Vendors' (F5 Networks, Fortinet, Center for Internet Security, ZOHO Corporation Private Limited, Anitian, Barracuda Networks, Gemalto, Buddha Labs, Symantec, Cisco).

Option A.C and D are all invalid because they cannot be used to conduct intrusion detection or prevention.

QUESTION 320

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

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

Answer: B

Explanation:

The AWS Documentation gives an example on such a case Inline policies are useful if you want to maintain a strict one-to-one relationship between a policy and the principal entity that it's applied to. For example, you want to be sure that the permissions in a policy are not inadvertently assigned to a principal entity other than the one they're intended for. When you use an inline policy, the permissions in the policy cannot be inadvertently attached to the wrong principal entity. In addition, when you use the AWS Management Console to delete that principal entity, the policies embedded in the principal entity are deleted as well. That's because they are part of the principal entity. Option A is invalid because AWS Managed Policies are ok for a group of users, but for individual users, inline policies are better.

Option C and D are invalid because they are specifically meant for access to S3 buckets

QUESTION 321

You have just recently set up a web and database tier in a VPC and hosted the application. When testing the app , you are not able to reach the home page for the app. You have verified the security groups.

What can help you diagnose the issue?

- A. Use the AWS Trusted Advisor to see what can be done.
- B. Use VPC Flow logs to diagnose the traffic
- C. Use AWS WAF to analyze the traffic
- D. Use AWS Guard Duty to analyze the traffic

Answer: B

Explanation:

Option A is invalid because this can be used to check for security issues in your account, but not verify as to why you cannot reach the home page for your application

Option C is invalid because this used to protect your app against application layer attacks, but not verify as to why you cannot reach the home page for your application

Option D is invalid because this used to protect your instance against attacks, but not verify as to why you cannot reach the home page for your application

QUESTION 322

Which of the following is used as a secure way to log into an EC2 Linux Instance?

- A. IAM User name and password
- B. Key pairs

- C. AWS Access keys
- D. AWS SDK keys

Answer: B

Explanation:

The AWS Documentation mentions the following Key pairs consist of a public key and a private key. You use the private key to create a digital signature, and then AWS uses the corresponding public key to validate the signature. Key pairs are used only for Amazon EC2 and Amazon CloudFront.

Option A.C and D are all wrong because these are not used to log into EC2 Linux Instances
<https://docs.aws.amazon.com/eeneral/latest/er/aws-sec-cred-types.html>

QUESTION 323

When you enable automatic key rotation for an existing CMK key where the backing key is managed by AWS, after how long is the key rotated?

- A. After 30 days
- B. After 128 days
- C. After 365 days
- D. After 3 years

Answer: D

Explanation:

The AWS Documentation states the following AWS managed CM Ks: You cannot manage key rotation for AWS managed CMKs. AWS KMS automatically rotates AWS managed keys every three years (1095 days).

Note: AWS-managed CMKs are rotated every 3yrs, Customer-Managed CMKs are rotated every 365-days from when rotation is enabled.

Option A, B, C are invalid because the dettings for automatic key rotation is not changeable.

QUESTION 324

You have just received an email from AWS Support stating that your AWS account might have been compromised.

Which of the following steps would you look to carry out immediately. Choose 3 answers from the options below.

- A. Change the root account password.
- B. Rotate all IAM access keys
- C. Keep all resources running to avoid disruption
- D. Change the password for all IAM users.

Answer: ABD

Explanation:

One of the articles from AWS mentions what should be done in such a scenario If you suspect that your account has been compromised, or if you have received a notification from AWS that the account has been compromised, perform the following tasks:

Change your AWS root account password and the passwords of any IAM users. Delete or rotate all root and AWS Identity and Access Management (IAM) access keys. Delete any resources on your account you didn't create, especially running EC2 instances, EC2 spot bids, or IAM users.

Respond to any notifications you received from AWS Support through the AWS Support Center.

Option C is invalid because there could be compromised instances or resources running on your environment. They should be shutdown or stopped immediately.

<https://aws.amazon.com/premiumsupport/knowledge-center/potential-account-compromise>

QUESTION 325

You have a web site that is sitting behind AWS Cloudfront. You need to protect the web site against threats such as SQL injection and Cross site scripting attacks.

Which of the following service can help in such a scenario

- A. AWS Trusted Advisor
- B. AWS WAF
- C. AWS Inspector
- D. AWS Config

Answer: B

Explanation:

The AWS Documentation mentions the following AWS WAF is a web application firewall that helps detect and block malicious web requests targeted at your web applications.

AWS WAF allows you to create rules that can help protect against common web exploits like SQL injection and cross-site scripting. With AWS WAF you first identify the resource (either an Amazon CloudFront distribution or an Application Load Balancer) that you need to protect.

Option A is invalid because this will only give advise on how you can better the security in your AWS account but not protect against threats mentioned in the question.

Option C is invalid because this can be used to scan EC2 Instances for vulnerabilities but not protect against threats mentioned in the question.

Option D is invalid because this can be used to check config changes but not protect against threats mentioned in the quest

<https://aws.amazon.com/waf/details/>

QUESTION 326

You have an Ec2 Instance in a private subnet which needs to access the KMS service.

Which of the following methods can help fulfil this requirement, keeping security in perspective

- A. Use a VPC endpoint
- B. Attach an Internet gateway to the subnet
- C. Attach a VPN connection to the VPC
- D. Use VPC Peering

Answer: A

Explanation:

The AWS Documentation mentions the following You can connect directly to AWS KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint communication between your VPC and AWS KMS is conducted entirely within the AWS network.

Option B is invalid because this could open threats from the internet Option C is invalid because this is normally used for communication between on-premise environments and AWS.

Option D is invalid because this is normally used for communication between VPCs

<https://docs.aws.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.html>

QUESTION 327

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings.

The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack?

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

Answer: C

Explanation:

Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL's as an additional security layer for the subnet to deny traffic.
Option D is invalid since just changing the Inbound Rules is sufficient.

QUESTION 328

You are trying to use the AWS Systems Manager run command on a set of Instances. The run command on a set of Instances.

What can you do to diagnose the issue? Choose 2 answers from the options given

- A. Ensure that the SSM agent is running on the target machine
- B. Check the /var/log/amazon/ssm/errors.log file
- C. Ensure the right AMI is used for the Instance
- D. Ensure the security groups allow outbound communication for the instance

Answer: AB

QUESTION 329

A user has enabled versioning on an S3 bucket. The user is using server side encryption for data at Rest.

If the user is supplying his own keys for encryption SSE-C, which of the below mentioned statements is true?

- A. The user should use the same encryption key for all versions of the same object
- B. It is possible to have different encryption keys for different versions of the same object
- C. AWS S3 does not allow the user to upload his own keys for server side encryption
- D. The SSE-C does not work when versioning is enabled

Answer: B

Explanation:

You can encrypt the object and send it across to S3

Option A is invalid because ideally you should use different encryption keys

Option C is invalid because you can use your own encryption keys

Option D is invalid because encryption works even if versioning is enabled

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html>

QUESTION 330

An application running on EC2 instances in a VPC must access sensitive data in the data center.

The access must be encrypted in transit and have consistent low latency.

Which hybrid architecture will meet these requirements?

- A. Expose the data with a public HTTPS endpoint.
- B. A VPN between the VPC and the data center over a Direct Connect connection

- C. A VPN between the VPC and the data center.
- D. A Direct Connect connection between the VPC and data center

Answer: B

Explanation:

Since this is required over a consistency low latency connection, you should use Direct Connect.

For encryption, you can make use of a VPN Option A is invalid because exposing an HTTPS endpoint will not help all traffic to flow between a VPC and the data center.

Option C is invalid because low latency is a key requirement

Option D is invalid because only Direct Connect will not suffice

<https://aws.amazon.com/answers/networking/aws-multiple-vpc-vpn-connection-share>

QUESTION 331

Which technique can be used to integrate AWS IAM (Identity and Access Management) with an on-premise LDAP (Lightweight Directory Access Protocol) directory service?

- A. Use an IAM policy that references the LDAP account identifiers and the AWS credentials.
- B. Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP.
- C. Use AWS Security Token Service from an identity broker to issue short-lived AWS credentials.
- D. Use IAM roles to automatically rotate the IAM credentials when LDAP credentials are updated.

Answer: B

Explanation:

On the AWS Blog site the following information is present to help on this context. The newly released whitepaper, Single Sign-On: Integrating AWS, OpenLDAP, and Shibboleth, will help you integrate your existing LDAP-based user directory with AWS. When you integrate your existing directory with AWS, your users can access AWS by using their existing credentials. This means that your users don't need to maintain yet another user name and password just to access AWS resources.

Options C and D are all invalid because in this sort of configuration, you have to use SAML to enable single sign on.

<https://aws.amazon.com/blogs/security/new-whitepaper-single-sign-on-integrating-aws-openldap-and-shibboleth/>

QUESTION 332

Your company has an external web site. This web site needs to access the objects in an S3 bucket.

Which of the following would allow the web site to access the objects in the most secure manner?

- A. Grant public access for the bucket via the bucket policy
- B. Use the aws:Referer key in the condition clause for the bucket policy
- C. Use the aws:sites key in the condition clause for the bucket policy
- D. Grant a role that can be assumed by the web site

Answer: B

Explanation:

An example of this is given in the AWS Documentation Restricting Access to a Specific HTTP Referrer. Suppose you have a website with domain name (www.example.com or example.com) with links to photos and videos stored in your S3 bucket examplebucket. By default, all the S3 resources are private, so only the AWS account that created the resources can access them. To allow read access to these objects from your website, you can add a bucket policy that allows

s3:GetObject permission with a condition, using the aws:referer key, that the get request must originate from specific webpages. The following policy specifies the StringLike condition with the aws:Referer condition key.

```
{  
    "Version": "2012-10-17",  
    "Id": "http referer policy example",  
    "Statement": [  
        {  
            "Sid": "Allow get requests originating from www.example.com and example.com.",  
            "Effect": "Allow",  
            "Principal": "*",  
            "Action": "s3:GetObject",  
            "Resource": "arn:aws:s3:::examplebucket/*",  
            "Condition": {  
                "StringLike": {"aws:Referer": ["http://www.example.com/*", "http://example.com/*"]}  
            }  
        }  
    ]  
}
```

Option A is invalid because giving public access is not a secure way to provide access

Option C is invalid because aws:sites is not a valid condition key

Option D is invalid because IAM roles will not be assigned to web sites

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

QUESTION 333

You have an EC2 instance with the following security configured:

- a. ICMP inbound allowed on Security Group
- b. ICMP outbound not configured on Security Group
- c. ICMP inbound allowed on Network ACL
- d. ICMP outbound denied on Network ACL

If Flow logs is enabled for the instance, which of the following flow records will be recorded?

Choose 3 answers from the options give below

- A. An ACCEPT record for the request based on the Security Group
- B. An ACCEPT record for the request based on the NACL
- C. A REJECT record for the response based on the Security Group

D. A REJECT record for the response based on the NACL

Answer: ABD

Explanation:

This example is given in the AWS documentation as well. For example, you use the ping command from your home computer (IP address is 203.0.113.12) to your instance (the network interface's private IP address is 172.31.16.139). Your security group's inbound rules allow ICMP traffic and the outbound rules do not allow ICMP traffic however, because security groups are stateful, the response ping from your instance is allowed. Your network ACL permits inbound ICMP traffic but does not permit outbound ICMP traffic. Because network ACLs are stateless, the response ping is dropped and will not reach your home computer. In a flow log, this is displayed as 2 flow log records:

An ACCEPT record for the originating ping that was allowed by both the network ACL and the security group, and therefore was allowed to reach your instance. A REJECT record for the response ping that the network ACL denied.

Option C is invalid because the REJECT record would not be present

<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-loes.html>

QUESTION 334

There are currently multiple applications hosted in a VPC. During monitoring it has been noticed that multiple port scans are coming in from a specific IP Address block. The internal security team has requested that all offending IP Addresses be denied for the next 24 hours.

Which of the following is the best method to quickly and temporarily deny access from the specified IP Address's?

- A. Create an AD policy to modify the Windows Firewall settings on all hosts in the VPC to deny access from the IP Address block.
- B. Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block.
- C. Add a rule to all of the VPC Security Groups to deny access from the IP Address block.
- D. Modify the Windows Firewall settings on all AMI'S that your organization uses in that VPC to deny access from the IP address block.

Answer: B

Explanation:

NACL acts as a firewall at the subnet level of the VPC and we can deny the offending IP address block at the subnet level using NACL rules to block the incoming traffic to the VPC instances.

Since NACL rules are applied as per the Rule numbers make sure that this rule number should take precedence over other rule numbers if there are any such rules that will allow traffic from these IP ranges. The lowest rule number has more precedence over a rule that has a higher number.

The AWS Documentation mentions the following as a best practices for IAM users. For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates a unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).

Options C is invalid because these options are not available

Option D is invalid because there is not root access for users

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

QUESTION 335

An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of IAM users should only access the test instances and not the production ones.

How can the organization set that as a part of the policy?

- A. Launch the test and production instances in separate regions and allow region wise access to the group
- B. Define the IAM policy which allows access based on the instance ID
- C. Create an IAM policy with a condition which allows access to only small instances
- D. Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specification tags

Answer: D

Explanation:

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type -- you can quickly identify a specific resource based on the tags you've assigned to it

Option A is invalid because this is not a recommended practices

Option B is invalid because this is an overhead to maintain this in policies

Option C is invalid because the instance type will not resolve the requirement

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

QUESTION 336

You company has mandated that all data in AWS be encrypted at rest. How can you achieve this for EBS volumes? Choose 2 answers from the options given below

- A. Use Windows bit locker for EBS volumes on Windows instances
- B. Use TrueEncrypt for EBS volumes on Linux instances
- C. Use AWS Systems Manager to encrypt the existing EBS volumes
- D. Boot EBS volume can be encrypted during launch without using custom AMI

Answer: AB

Explanation:

EBS encryption can also be enabled when the volume is created and not for existing volumes.

One can use existing tools for OS level encryption.

Option C is incorrect.

AWS Systems Manager is a management service that helps you automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems.

Option D is incorrect

You cannot choose to encrypt a non-encrypted boot volume on instance launch. To have encrypted boot volumes during launch , your custom AMI must have its boot volume encrypted before launch.

QUESTION 337

You currently operate a web application in the AWS US-East region. The application runs on an auto-scaled layer of EC2 instances and an RDS Multi-AZ database. Your IT security compliance officer has tasked you to develop a reliable and durable logging solution to track changes made to your EC2,IAM and RDS resources. The solution must ensure the integrity and confidentiality of your log data. Which of these solutions would you recommend?

- A. Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global

services

option selected. Use IAM roles S3 bucket policies and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.

- B. Create a new CloudTrail with one new S3 bucket to store the logs. Configure SNS to send log file delivery notifications to your management system. Use IAM roles and S3 bucket policies on the S3 bucket that stores your logs.
- C. Create a new CloudTrail trail with an existing S3 bucket to store the logs and with the global services option selected. Use S3 ACLs and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.
- D. Create three new CloudTrail trails with three new S3 buckets to store the logs one for the AWS Management console, one for AWS SDKs and one for command line tools. Use IAM roles and S3 bucket policies on the S3 buckets that store your logs.

Answer: A

Explanation:

AWS Identity and Access Management (IAM) is integrated with AWS CloudTrail, a service that logs AWS events made by or on behalf of your AWS account. CloudTrail logs authenticated AWS API calls and also AWS sign-in events, and collects this event information in files that are delivered to Amazon S3 buckets.

You need to ensure that all services are included. Hence option B is partially correct. Option B is invalid because you need to ensure that global services is selected. Option C is invalid because you should use bucket policies. Option D is invalid because you should ideally just create one S3 bucket.

<http://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html>

QUESTION 338

You need to create a Linux EC2 instance in AWS.

Which of the following steps is used to ensure secure authentication to the EC2 instance from a windows machine. Choose 2 answers from the options given below.

- A. Ensure to create a strong password for logging into the EC2 Instance
- B. Create a key pair using putty
- C. Use the private key to log into the instance
- D. Ensure the password is passed securely using SSL

Answer: BC

Explanation:

The AWS Documentation mentions the following. You can use Amazon EC2 to create your key pair.

Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. Each key pair requires a name. Be sure to choose a name that is easy to remember. Amazon EC2 associates the public key with the name that you specify as the key name.

Amazon EC2 stores the public key only, and you store the private key. Anyone who possesses your private key can decrypt login information, so it's important that you store your private keys in a secure place.

Options A and D are incorrect since you should use key pairs for secure access to EC2 Instances
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>

QUESTION 339

You have an S3 bucket defined in AWS. You want to ensure that you encrypt the data before sending it across the wire. What is the best way to achieve this?

- A. Enable server side encryption for the S3 bucket. This request will ensure that the data is encrypted first.
- B. Use the AWS Encryption CLI to encrypt the data first
- C. Use a Lambda function to encrypt the data before sending it to the S3 bucket.
- D. Enable client encryption for the bucket

Answer: B

Explanation:

One can use the AWS Encryption CLI to encrypt the data before sending it across to the S3 bucket.

Options A and C are invalid because this would still mean that data is transferred in plain text

Option D is invalid because you cannot just enable client side encryption for the S3 bucket

<https://aws.amazon.com/blogs/securiv/how-to-encrypt-and-decrypt-your-data-with-the-aws-encryption-cl>

QUESTION 340

You are working for a company and been allocated the task for ensuring that there is a federated authentication mechanism setup between AWS and their On-premise Active Directory.

Which of the following are important steps that need to be covered in this process? Choose 2 answers from the options given below.

- A. Ensure the right match is in place for On-premise AD Groups and IAM Roles.
- B. Ensure the right match is in place for On-premise AD Groups and IAM Groups.
- C. Configure AWS as the relying party in Active Directory
- D. Configure AWS as the relying party in Active Directory Federation services

Answer: AD

QUESTION 341

In your LAMP application, you have some developers that say they would like access to your logs. However, since you are using an AWS Auto Scaling group, your instances are constantly being re-created.

What would you do to make sure that these developers can access these log files? Choose the correct answer from the options below

- A. Give only the necessary access to the Apache servers so that the developers can gain access to the log files.
- B. Give root access to your Apache servers to the developers.
- C. Give read-only access to your developers to the Apache servers.
- D. Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.

Answer: D

Explanation:

One important security aspect is to never give access to actual servers, hence Option A,B and C are just totally wrong from a security perspective. The best option is to have a central logging server that can be used to archive logs. These logs can then be stored in S3.

Options A,B and C are all invalid because you should not give access to the developers on the Apache

QUESTION 342

Your company has defined a set of S3 buckets in AWS. They need to monitor the S3 buckets and know the source IP address and the person who make requests to the S3 bucket. How can this be achieved?

- A. Enable VPC flow logs to know the source IP addresses
- B. Monitor the S3 API calls by using Cloudtrail logging
- C. Monitor the S3 API calls by using Cloudwatch logging
- D. Enable AWS Inspector for the S3 bucket

Answer: B

Explanation:

The AWS Documentation mentions the following Amazon S3 is integrated with AWS CloudTrail. CloudTrail is a service that captures specific API calls made to Amazon S3 from your AWS account and delivers the log files to an Amazon S3 bucket that you specify. It captures API calls made from the Amazon S3 console or from the Amazon S3 API.

Using the information collected by CloudTrail, you can determine what request was made to Amazon S3, the source IP address from which the request was made, who made the request when it was made, and so on

Options A,C and D are invalid because these services cannot be used to get the source IP address of the calls to S3 buckets

<https://docs.aws.amazon.com/AmazonS3/latest/dev/cloudtrail-logins.html>

QUESTION 343

A company has set up the following structure to ensure that their S3 buckets always have logging enabled



If there are any changes to the configuration to an S3 bucket, a config rule gets checked. If logging is disabled , then Lambda function is invoked. This Lambda function will again enable logging on the S3 bucket. Now there is an issue being encountered with the entire flow. You have verified that the Lambda function is being invoked. But when logging is disabled for the bucket, the lambda function does not enable it again. Which of the following could be an issue?

- A. The AWS Config rule is not configured properly
- B. The AWS Lambda function does not have appropriate permissions for the bucket
- C. The AWS Lambda function should use Node.js instead of python.
- D. You need to also use the API gateway to invoke the lambda function

Answer: B

Explanation:

The most probable cause is that you have not allowed the Lambda functions to have the appropriate permissions on the S3 bucket to make the relevant changes. Option A is invalid because this is more of a permission instead of a configuration rule issue.

Option C is invalid because changing the language will not be the core solution.

Option D is invalid because you don't necessarily need to use the API gateway service

<https://docs.aws.amazon.com/lambda/latest/ds/accessing-resources.html>

QUESTION 344

A company needs to encrypt all of its data stored in Amazon S3. The company wants to use AWS Key Management Service (AWS KMS) to create and manage its encryption keys. The company's security policies require the ability to Import the company's own key material for the keys, set an expiration date on the keys, and delete keys immediately, if needed.

How should a security engineer set up AWS KMS to meet these requirements?

- A. Configure AWS KMS and use a custom key store.
Create a customer managed CMK with no key material Import the company's keys and key material into the CMK
- B. Configure AWS KMS and use the default Key store
Create an AWS managed CMK with no key material Import the company's key material into the CMK
- C. Configure AWS KMS and use the default key store
Create a customer managed CMK with no key material import the company's key material into the CMK
- D. Configure AWS KMS and use a custom key store.
Create an AWS managed CMK with no key material.
Import the company's key material into the CMK.

Answer: A

QUESTION 345

An application running on EC2 instances in a VPC must call an external web service via TLS (port 443).
The instances run in public subnets.

Which configurations below allow the application to function and minimize the exposure of the instances? Select 2 answers from the options given below

- A. A network ACL with a rule that allows outgoing traffic on port 443.
- B. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports
- C. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.
- D. A security group with a rule that allows outgoing traffic on port 443
- E. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports.
- F. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.

Answer: BD

Explanation:

Since here the traffic needs to flow outbound from the Instance to a web service on Port 443, the outbound rules on both the Network and Security Groups need to allow outbound traffic. The Incoming traffic should be allowed on ephemeral ports for the Operating System on the Instance to allow a connection to be established on any desired or available port.

Option A is invalid because this rule alone is not enough. You also need to ensure incoming traffic on ephemeral ports

Option C is invalid because need to ensure incoming traffic on ephemeral ports and not only port 443

Option E and F are invalid since here you are allowing additional ports on Security groups which are not required

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC_SecurityGroups.html

QUESTION 346

A company wishes to enable Single Sign On (SSO) so its employees can login to the management console using their corporate directory identity.

Which steps below are required as part of the process? Select 2 answers from the options given below.

- A. Create a Direct Connect connection between on-premise network and AWS. Use an AD connector for connecting AWS with on-premise active directory.
- B. Create IAM policies that can be mapped to group memberships in the corporate directory.
- C. Create a Lambda function to assign IAM roles to the temporary security tokens provided to the users.
- D. Create IAM users that can be mapped to the employees' corporate identities
- E. Create an IAM role that establishes a trust relationship between IAM and the corporate directory identity provider (IdP)

Answer: AE

Explanation:

Create a Direct Connect connection so that corporate users can access the AWS account

Option B is incorrect because IAM policies are not directly mapped to group memberships in the corporate directory. It is IAM roles which are mapped.

Option C is incorrect because Lambda functions is an incorrect option to assign roles.

Option D is incorrect because IAM users are not directly mapped to employees' corporate identities.

<https://aws.amazon.com/directconnect/>

QUESTION 347

A company hosts data in S3. There is a requirement to control access to the S3 buckets.

Which are the 2 ways in which this can be achieved?

- A. Use Bucket policies
- B. Use the Secure Token service
- C. Use IAM user policies
- D. Use AWS Access Keys

Answer: AC

Explanation:

The AWS Documentation mentions the following Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as resource-based policies. For example, bucket policies and access control lists (ACLs) are resource-based policies. You can also attach access policies to users in your account. These are called user policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources.

Option B and D are invalid because these cannot be used to control access to S3 buckets

<https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html>

QUESTION 348

A company needs to use HTTPS when connecting to its web applications to meet compliance requirements. These web applications run in Amazon VPC on Amazon EC2 instances behind an Application Load Balancer (ALB).

A security engineer wants to ensure that the load balancer will only accept connections over port

443. even if the ALB is mistakenly configured with an HTTP listener.

Which configuration steps should the security engineer take to accomplish this task?

- A. Create a security group with a rule that denies Inbound connections from 0.0.0.0/0 on port 00
Attach this security group to the ALB to overwrite more permissive rules from the ALB's default security group.
- B. Create a network ACL that denies inbound connections from 0.0.0.0/0 on port 80
Associate the network ACL with the VPC's internet gateway
- C. Create a network ACL that allows outbound connections to the VPC IP range on port 443 only.
Associate the network ACL with the VPC's internet gateway.
- D. Create a security group with a single inbound rule that allows connections from 0.0.0.0/0 on port 443.
Ensure this security group is the only one associated with the ALB

Answer: D

QUESTION 349

Your company currently has a set of EC2 Instances hosted in a VPC. The IT Security department is suspecting a possible DDos attack on the instances.

What can you do to zero in on the IP addresses which are receiving a flurry of requests.

- A. Use VPC Flow logs to get the IP addresses accessing the EC2 Instances
- B. Use AWS Cloud trail to get the IP addresses accessing the EC2 Instances
- C. Use AWS Config to get the IP addresses accessing the EC2 Instances
- D. Use AWS Trusted Advisor to get the IP addresses accessing the EC2 Instances

Answer: A

Explanation:

With VPC Flow logs you can get the list of IP addresses which are hitting the Instances in your VPC. You can then use the information in the logs to see which external IP addresses are sending a flurry of requests which could be the potential threat for a DDos attack.

Option B is incorrect Cloud Trail records AWS API calls for your account. VPC Flow logs logs network traffic for VPC, subnets, Network interfaces etc.

As per AWS,

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC whereas AWS CloudTrail, is a service that captures API calls and delivers the log files to an Amazon S3 bucket that you specify.

Option C is invalid this is a config service and will not be able to get the IP addresses

Option D is invalid because this is a recommendation service and will not be able to get the IP addresses

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html>

QUESTION 350

You need to inspect the running processes on an EC2 Instance that may have a security issue.

How can you achieve this in the easiest way possible. Also you need to ensure that the process does not interfere with the continuous running of the instance.

- A. Use AWS Cloudtrail to record the processes running on the server to an S3 bucket.
- B. Use AWS Cloudwatch to record the processes running on the server
- C. Use the SSM Run command to send the list of running processes information to an S3 bucket.
- D. Use AWS Config to see the changed process information on the server

Answer: C

Explanation:

The SSM Run command can be used to send OS specific commands to an Instance. Here you can check and see the running processes on an instance and then send the output to an S3 bucket.

Option A is invalid because this is used to record API activity and cannot be used to record running processes.

Option B is invalid because Cloudwatch is a logging and metric service and cannot be used to record running processes.

Option D is invalid because AWS Config is a configuration service and cannot be used to record running processes.

<https://docs.aws.amazon.com/systems-manage/latest/userguide/execute-remote-commands.html>

QUESTION 351

Which of the following is the responsibility of the customer? Choose 2 answers from the options given below

- A. Management of the Edge locations
- B. Encryption of data at rest
- C. Protection of data in transit
- D. Decommissioning of old storage devices

Answer: BC

QUESTION 352

You are planning on hosting a web application on AWS. You create an EC2 Instance in a public subnet. This instance needs to connect to an EC2 Instance that will host an Oracle database.

Which of the following steps should be followed to ensure a secure setup is in place? Select 2 answers.

- A. Place the EC2 Instance with the Oracle database in the same public subnet as the Web server for faster communication
- B. Place the EC2 Instance with the Oracle database in a separate private subnet
- C. Create a database security group and ensure the web security group to allowed incoming access
- D. Ensure the database security group allows incoming traffic from 0.0.0.0/0

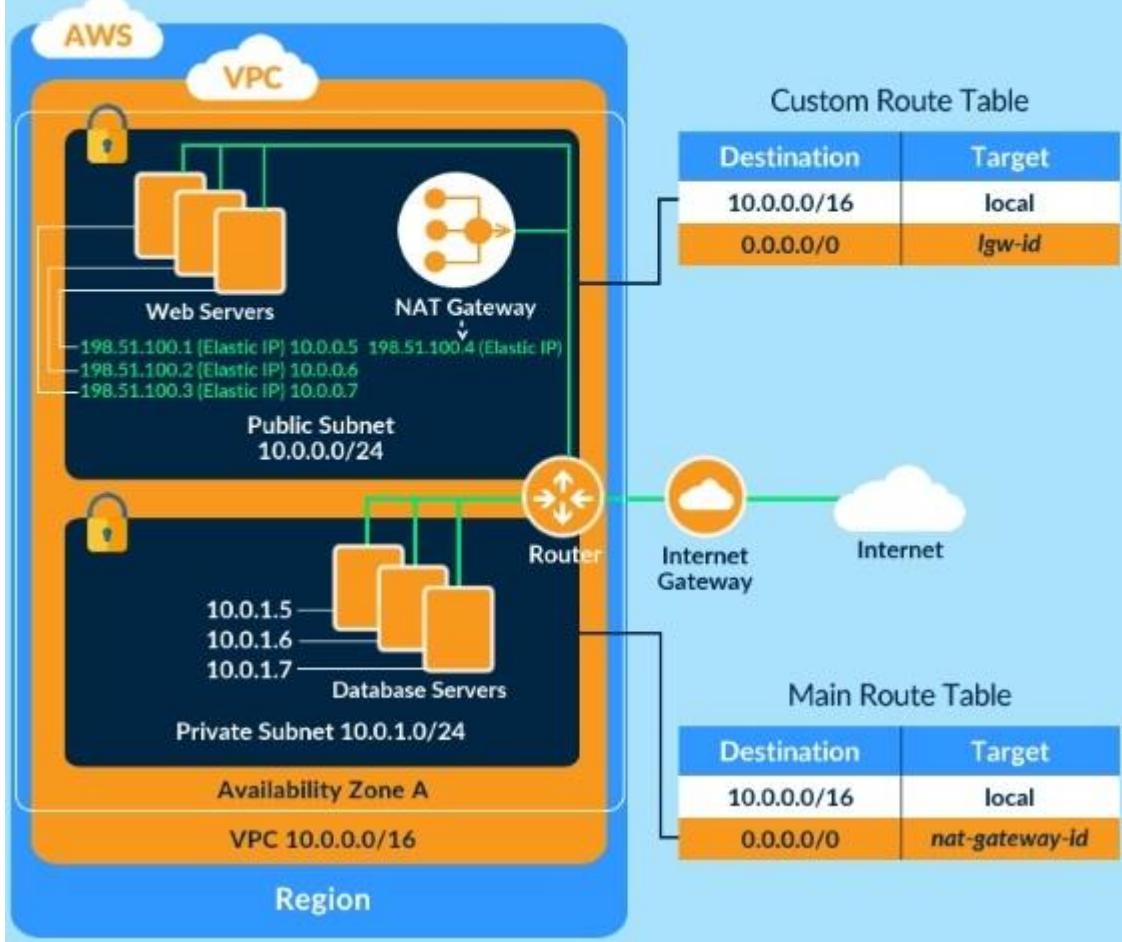
Answer: BC

Explanation:

The best secure option is to place the database in a private subnet. The below diagram from the AWS Documentation shows this setup. Also ensure that access is not allowed from all sources but just from the web servers.

VPC with Public and Private Subnets (NAT)

The following diagram shows the key components of the configuration for this scenario



Option A is invalid because databases should not be placed in the public subnet

Option D is invalid because the database security group should not allow traffic from the internet

QUESTION 353

A company hosts data in S3. There is now a mandate that going forward all data in the S3 bucket needs to encrypt at rest.

How can this be achieved? Please select:

- A. Use AWS Access keys to encrypt the data
- B. Use SSL certificates to encrypt the data
- C. Enable server side encryption on the S3 bucket
- D. Enable MFA on the S3 bucket

Answer: C

Explanation:

The AWS Documentation mentions the following Server-side encryption is about data encryption

at rest-- that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects. Options A and B are invalid because neither Access Keys nor SSL certificates can be used to encrypt data.

Option D is invalid because MFA is just used as an extra level of security for S3 buckets

QUESTION 354

A security engineer must troubleshoot an administrator's inability to make an existing Amazon S3 bucket public in an account that is part of an organization in AWS Organizations. The administrator switched the role from the master account to a member account and then attempted to make one S3 bucket public. This action was immediately denied.

Which actions should the security engineer take to troubleshoot the permissions issue? (Select TWO.)

- A. Review the cross-account role permissions and the S3 bucket policy Verify that the Amazon S3 block public access option in the member account is deactivated.
- B. Review the role permissions in the master account and ensure it has sufficient privileges to perform S3 operations
- C. Filter AWS CloudTrail logs for the master account to find the original deny event and update the cross-account role in the member account accordingly
Verify that the Amazon S3 block public access option in the master account is deactivated.
- D. Evaluate the SCPs covering the member account and the permissions boundary of the role in the member account for missing permissions and explicit denies.
- E. Ensure the S3 bucket policy explicitly allows the s3 PutBucketPublicAccess action for the role in the member account

Answer: BE

QUESTION 355

Your company has created a set of keys using the AWS KMS service. They need to ensure that each key is only used for certain services.

For example , they want one key to be used only for the S3 service. How can this be achieved?

- A. Create an IAM policy that allows the key to be accessed by only the S3 service.
- B. Create a bucket policy that allows the key to be accessed by only the S3 service.
- C. Use the kms:ViaService condition in the Key policy
- D. Define an IAM user, allocate the key and then assign the permissions to the required service

Answer: C

Explanation:

Option A and B are invalid because mapping keys to services cannot be done via either the IAM or bucket policy

Option D is invalid because keys for IAM users cannot be assigned to services

This is mentioned in the AWS Documentation

The kms:ViaService condition key limits use of a customer-managed CMK to requests from particular AWS services. (AWS managed CMKs in your account, such as aws/s3, are always restricted to the AWS service that created them.)

For example, you can use kms:ViaService to allow a user to use a customer managed CMK only for requests that Amazon S3 makes on their behalf.

Or you can use it to deny the user permission to a CMK when a request on their behalf comes

from AWS Lambda.

QUESTION 356

A company has a set of EC2 instances hosted in AWS. These instances have EBS volumes for storing critical information. There is a business continuity requirement and in order to boost the agility of the business and to ensure data durability which of the following options are not required?

- A. Use lifecycle policies for the EBS volumes
- B. Use EBS Snapshots
- C. Use EBS volume replication
- D. Use EBS volume encryption

Answer: CD

Explanation:

Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability. You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots taken to back up your Amazon EBS volumes.

With lifecycle management, you can be sure that snapshots are cleaned up regularly and keep costs under control.

EBS Lifecycle Policies

A lifecycle policy consists of these core settings:

Resource type--The AWS resource managed by the policy, in this case, EBS volumes. Target tag--The tag that must be associated with an EBS volume for it to be managed by the policy.

Schedule--Defines how often to create snapshots and the maximum number of snapshots to keep.

Snapshot creation starts within an hour of the specified start time. If creating a new snapshot exceeds the maximum number of snapshots to keep for the volume, the oldest snapshot is deleted.

Option C is correct. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. But it does not have an explicit feature like that. Option D is correct Encryption does not ensure data durability.

QUESTION 357

A company's Security Team received an email notification from the Amazon EC2 Abuse team that one or more of the company's Amazon EC2 instances may have been compromised

Which combination of actions should the Security team take to respond to (be current modem)? (Select TWO.)

- A. Open a support case with the AWS Security team and ask them to remove the malicious code from the affected instance
- B. Respond to the notification and list the actions that have been taken to address the incident
- C. Delete all IAM users and resources in the account
- D. Detach the internet gateway from the VPC remove all rules that contain 0.0.0.0/V0 from the security groups, and create a NACL rule to deny all traffic Inbound from the internet
- E. Delete the identified compromised instances and delete any associated resources that the Security team did not create.

Answer: DE

QUESTION 358

A company has been using the AW5 KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys which are no longer in use.

What are the ways that can be incorporated to see which keys are in use? Choose 2 answers from the options given below

- A. Determine the age of the master key
- B. See who is assigned permissions to the master key
- C. See Cloudtrail for usage of the key
- D. Use AWS cloudwatch events for events generated for the key

Answer: BC

Explanation:

The direct ways that can be used to see how the key is being used is to see the current access permissions and cloudtrail logs Option A is invalid because seeing how long ago the key was created would not determine the usage of the key

Option D is invalid because Cloudtrail Event is better for seeing for events generated by the key This is also mentioned in the AWS Documentation

Examining CMK Permissions to Determine the Scope of Potential Usage Determining who or what currently has access to a customer master key (CMK) might help you determine how widely the CM was used and whether it is still needed. To learn how to determine who or what currently has access to a CMK, go to Determining Access to an AWS KMS Customer Master Key.

Examining AWS CloudTrail Logs to Determine Actual Usage AWS KMS is integrated with AWS CloudTrail, so all AWS KMS API activity is recorded in CloudTrail log files. If you have CloudTrail turned on in the region where your customer master key (CMK) is located, you can examine your CloudTrail log files to view a history of all AWS KMS API activity for a particular CMK, and thus its usage history. You might be able to use a CMK's usage history to help you determine whether or not you still need it.

QUESTION 359

A company is deploying a new web application on AWS. Based on their other web applications, they anticipate being the target of frequent DDoS attacks.

Which steps can the company use to protect their application? Select 2 answers from the options given below.

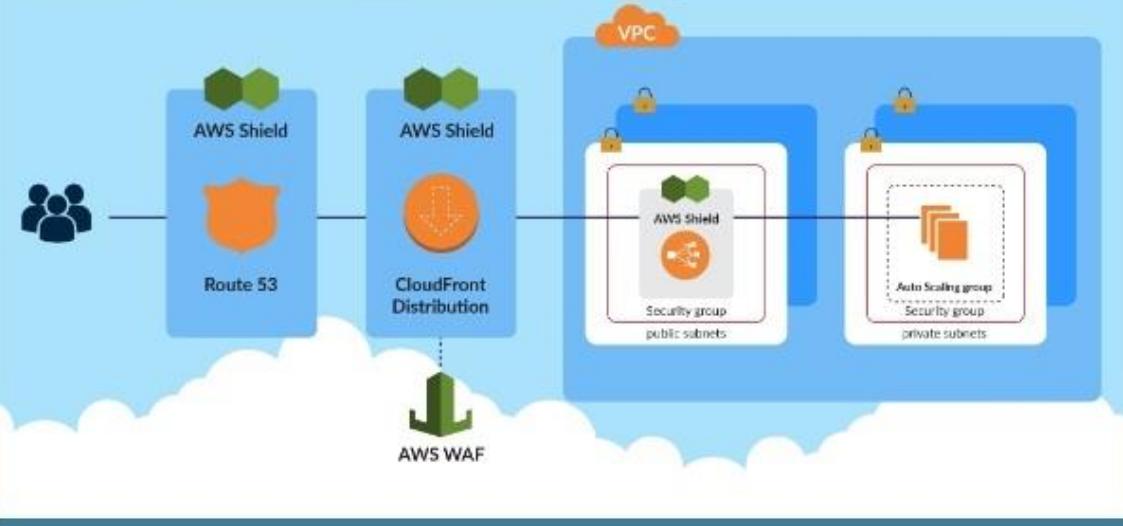
- A. Associate the EC2 instances with a security group that blocks traffic from blacklisted IP addresses.
- B. Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic.
- C. Use Amazon Inspector on the EC2 instances to examine incoming traffic and discard malicious traffic.
- D. Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application
- E. Enable GuardDuty to block malicious traffic from reaching the application

Answer: BD

Explanation:

The below diagram from AWS shows the best case scenario for avoiding DDos attacks using services such as AWS Cloudfront WAF, ELB and Autoscaling

Avoiding DDoS attacks using services such as AWS Cloudfront, WAF, ELB and Autoscaling



Option A is invalid because by default security groups don't allow access

Option C is invalid because AWS Inspector cannot be used to examine traffic

Option E is invalid because this can be used for attacks on EC2 Instances but not against DDoS attacks on the entire application

<https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation>

QUESTION 360

A company is using AWS Secrets Manager to store secrets for its production Amazon RDS database. The Security Officer has asked that secrets be rotated every 3 months.

Which solution would allow the company to securely rotate the secrets? (Select TWO.)

- Place the RDS instance in a public subnet and an AWS Lambda function outside the VPC. Schedule the Lambda function to run every 3 months to rotate the secrets.
- Place the RDS instance in a private subnet and an AWS Lambda function inside the VPC in the private subnet. Configure the private subnet to use a NAT gateway. Schedule the Lambda function to run every 3 months to rotate the secrets.
- Place the RDS instance in a private subnet and an AWS Lambda function outside the VPC. Configure the private subnet to use an internet gateway. Schedule the Lambda function to run every 3 months to rotate the secrets.
- Place the RDS instance in a private subnet and an AWS Lambda function inside the VPC in the private subnet. Schedule the Lambda function to run quarterly to rotate the secrets.
- Place the RDS instance in a private subnet and an AWS Lambda function inside the VPC in the private subnet. Configure a Secrets Manager interface endpoint. Schedule the Lambda function to run every 3 months to rotate the secrets.

Answer: BE

QUESTION 361

An employee keeps terminating EC2 instances on the production environment. You've determined the best way to ensure this doesn't happen is to add an extra layer of defense against terminating the instances.

What is the best method to ensure the employee does not terminate the production instances? Choose the 2 correct answers from the options below

- A. Tag the instance with a production-identifying tag and add resource-level permissions to the employee user with an explicit deny on the terminate API call to instances with the production tag.
<
- B. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance call.
- C. Modify the IAM policy on the user to require MFA before deleting EC2 instances and disable MFA access to the employee
- D. Modify the IAM policy on the user to require MFA before deleting EC2 instances

Answer: AB

Explanation:

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type -- you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define

Options C&D are incorrect because it will not ensure that the employee cannot terminate the instance.

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Usins_Tags.html

QUESTION 362

An organization has setup multiple IAM users. The organization wants that each IAM user accesses the IAM console only within the organization and not from outside. How can it achieve this?

- A. Create an IAM policy with the security group and use that security group for AWS console login
- B. Create an IAM policy with a condition which denies access when the IP address range is not from the organization
- C. Configure the EC2 instance security group which allows traffic only from the organization's IP range
- D. Create an IAM policy with VPC and allow a secure gateway between the organization and AWS Console

Answer: B

Explanation:

You can actually use a Deny condition which will not allow the person to log in from outside. The below example shows the Deny condition to ensure that any address specified in the source address is not allowed to access the resources in aws.

Option A is invalid because you don't mention the security group in the IAM policy

Option C is invalid because security groups by default don't allow traffic

Option D is invalid because the IAM policy does not have such an option.

http://docs.aws.amazon.com/IAM/latest/UserGuide/access_pol_examples.htm#iam-policy-example-ec2-two-condition

QUESTION 363

A company has a set of EC2 Instances hosted in AWS. The EC2 Instances have EBS volumes which is used to store critical information. There is a business continuity requirement to ensure high availability for the EBS volumes. How can you achieve this?

- A. Use lifecycle policies for the EBS volumes
- B. Use EBS Snapshots
- C. Use EBS volume replication
- D. Use EBS volume encryption

Answer: B

Explanation:

Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability

Option A is invalid because there is no lifecycle policy for EBS volumes

Option C is invalid because there is no EBS volume replication

Option D is invalid because EBS volume encryption will not ensure business continuity.

https://d1.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf

QUESTION 364

You need to have a cloud security device which would allow to generate encryption keys based on FIPS 140-2 Level 3.

Which of the following can be used for this purpose?

- A. AWS KMS
- B. AWS Customer Keys
- C. AWS managed keys
- D. AWS Cloud HSM

Answer: AD

QUESTION 365

Attach the following SCP to the OU that contains this account:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:*"],  
            "Resource": "arn:aws:ec2:*:*:snapshot/*"  
        },  
        {"Condition": {"StringLikeIfExists": {"ec2:ImageType": "encrypted"}}}  
    ]  
}
```

- A. For each finding in the audit report, run the ec2 copy-snapshot command and use the encrypted flag specifying an AWS Key Management Service (AWS KMS) CMK
- B. Create a private AMI for the company Configure encryption for the private AMI by selecting the custom AMI in the Amazon EC2 console, the destination AWS Region and the source account's AWS Key Management Service (AWS KMS) master key.
- C. In the Amazon EC2 console, select the Always Encrypt new EBS volumes setting for each AWS Region.

Answer: A

QUESTION 366

Your company has a set of 1000 EC2 Instances defined in an AWS Account. They want to effectively automate several administrative tasks on these instances.

Which of the following would be an effective way to achieve this?

- A. Use the AWS Systems Manager Parameter Store
- B. Use the AWS Systems Manager Run Command
- C. Use the AWS Inspector
- D. Use AWS Config

Answer: B

Explanation:

The AWS Documentation mentions the following AWS Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the AWS console, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the AWS SDKs. Run Command is offered at no additional cost.

Option A is invalid because this service is used to store parameter

Option C is invalid because this service is used to scan vulnerabilities in an EC2 Instance.

Option D is invalid because this service is used to check for configuration changes

<https://docs.aws.amazon.com/systems-manager/latest/userguide/execute-remote-commands.html>

QUESTION 367

There is a set of Ec2 Instances in a private subnet. The application hosted on these EC2 Instances need to access a DynamoDB table. It needs to be ensured that traffic does not flow out to the internet. How can this be achieved?

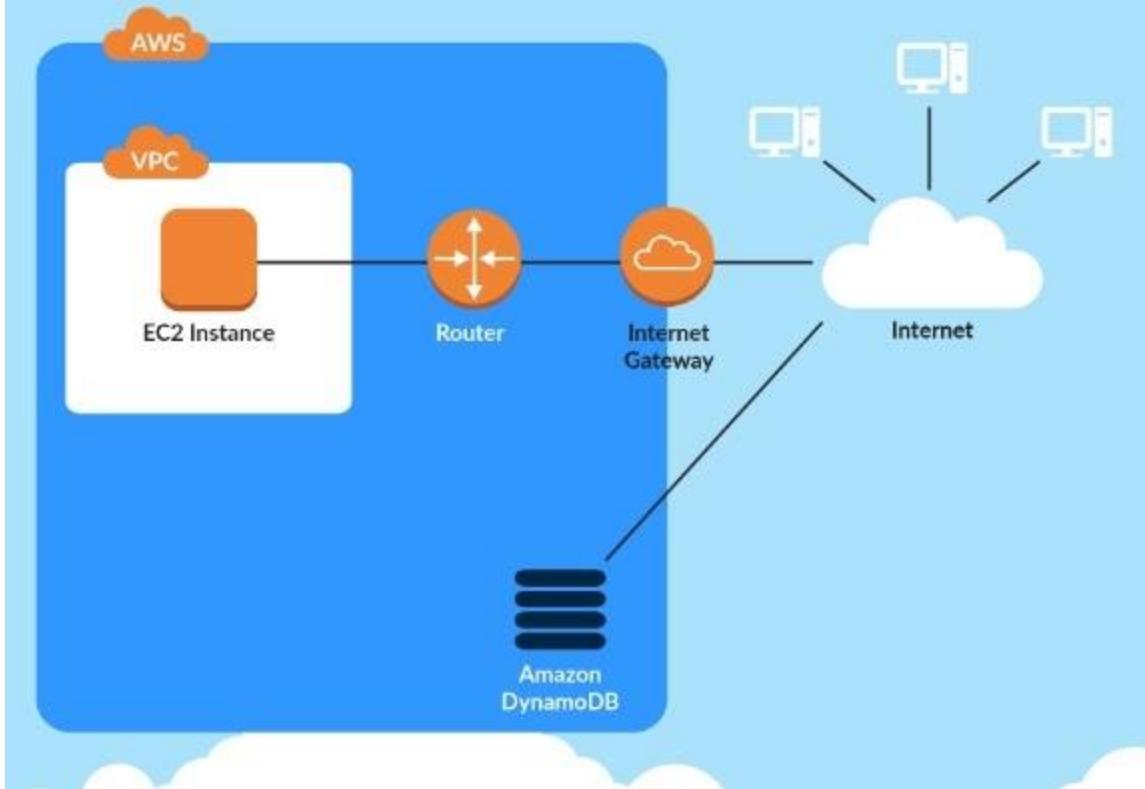
- A. Use a VPC endpoint to the DynamoDB table
- B. Use a VPN connection from the VPC
- C. Use a VPC gateway from the VPC
- D. Use a VPC Peering connection to the DynamoDB table

Answer: A

Explanation:

The following diagram from the AWS Documentation shows how you can access the DynamoDB service from within a V without going to the Internet This can be done with the help of a VPC endpoint

How you can access the DynamoDB service from within a VPC without going to the Internet



Option B is invalid because this is used for connection between an on-premise solution and AWS
 Option C is invalid because there is no such option
 Option D is invalid because this is used to connect 2 VPCs

QUESTION 368

Your company hosts a large section of EC2 instances in AWS. There are strict security rules governing the EC2 Instances. During a potential security breach , you need to ensure quick investigation of the underlying EC2 Instance.

Which of the following service can help you quickly provision a test environment to look into the breached instance?

- A. AWS Cloudwatch
- B. AWS Cloudformation
- C. AWS Cloudtrail
- D. AWS Config

Answer: B

Explanation:

The AWS Security best practises mentions the following Unique to AWS, security practitioners can use CloudFormation to quickly create a new, trusted environment in which to conduct deeper investigation. The CloudFormation template can pre-configure instances in an isolated environment that contains all the necessary tools forensic teams need to determine the cause of the incident This cuts down on the time it takes to gather necessary tools, isolates systems under

examination, and ensures that the team is operating in a clean room.

Option A is incorrect since this is a logging service and cannot be used to provision a test environment

Option C is incorrect since this is an API logging service and cannot be used to provision a test environment

Option D is incorrect since this is a configuration service and cannot be used to provision a test environment

QUESTION 369

A company stores critical data in an S3 bucket. There is a requirement to ensure that an extra level of security is added to the S3 bucket. In addition , it should be ensured that objects are available in a secondary region if the primary one goes down.

Which of the following can help fulfil these requirements? Choose 2 answers from the options given below

- A. Enable bucket versioning and also enable CRR
- B. Enable bucket versioning and enable Master Pays
- C. For the Bucket policy add a condition for {"Null": {"aws:MultiFactorAuthAge": true}} i
- D. Enable the Bucket ACL and add a condition for {"Null": {"aws:MultiFactorAuthAge": true}}

Answer: AC

Explanation:

The AWS Documentation mentions the following Adding a Bucket Policy to Require MFA Amazon S3 supports MFA-protected API access, a feature that can enforce multi-factor authentication (MFA) for access to your Amazon S3 resources. Multi-factor authentication provides an extra level of security you can apply to your AWS environment. It is a security feature that requires users to prove physical possession of an MFA device by providing a valid MFA code. For more information, go to AWS Multi-Factor Authentication. You can require MFA authentication for any requests to access your Amazoi.

S3 resources. You can enforce the MFA authentication requirement using the aws:MultiFactorAuthAge key in a bucket policy. IAM users car access Amazon S3 resources by using temporary credentials issued by the AWS Security Token Service (STS). You provide the MFA code at the time of the STS request.

When Amazon S3 receives a request with MFA authentication, the aws:MultiFactorAuthAge key provides a numeric value indicating how long ago (in seconds) the temporary credential was created. If the temporary credential provided in the request was not created using an MFA device, this key value is null (absent). In a bucket policy, you can add a condition to check this value, as shown in the following example bucket policy. The policy denies any Amazon S3 operation on the /taxdocuments folder in the examplebucket bucket if the request is not MFA authenticated. To learn more about MFA authentication, see Using Multi- Factor Authentication (MFA) in AWS in the IAM User Guide.

```
{  
    "Version": "2012-10-17",  
    "Id": "123",  
    "Statement": [  
        {  
            "Sid": "",  
            "Effect": "Deny",  
            "Principal": "*",  
            "Action": "s3:*",  
            "Resource": "arn:aws:s3:::examplebucket/taxdocuments/*",  
            "Condition": { "Null": { "aws:MultiFactorAuthAge": true } }  
        }  
    ]  
}
```

Option B is invalid because just enabling bucket versioning will not guarantee replication of objects

Option D is invalid because the condition for the bucket policy needs to be set accordingly
<https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

QUESTION 370

You need to have a requirement to store objects in an S3 bucket with a key that is automatically managed and rotated.

Which of the following can be used for this purpose?

- A. AWS KMS
- B. AWS S3 Server side encryption
- C. AWS Customer Keys
- D. AWS Cloud HSM

Answer: B

Explanation:

The AWS Documentation mentions the following Server-side encryption protects data at rest. Server-side encryption with Amazon S3- managed encryption keys (SSE-S3) uses strong multi-factor encryption.

Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES- 256), to encrypt your data.

All other options are invalid since here you need to ensure the keys are manually rotated since you manage the entire key set Using AWS S3 Server side encryption, AWS will manage the rotation of keys

automatically.

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html>

QUESTION 371

One of the EC2 Instances in your company has been compromised.

What steps would you take to ensure that you could apply digital forensics on the Instance. Select 2 answers from the options given below

- A. Remove the role applied to the Ec2 Instance
- B. Create a separate forensic instance
- C. Ensure that the security groups only allow communication to this forensic instance
- D. Terminate the instance

Answer: BC

Explanation:

Option A is invalid because removing the role will not help completely in such a situation

Option D is invalid because terminating the instance means that you cannot conduct forensic analysis on the instance

One way to isolate an affected EC2 instance for investigation is to place it in a Security Group that only the forensic investigators can access. Close all ports except to receive inbound SSH or RDP traffic from one single IP address from which the investigators can safely examine the instance.

QUESTION 372

Your company has a set of EC2 Instances defined in AWS. These Ec2 Instances have strict security groups attached to them. You need to ensure that changes to the Security groups are noted and acted on accordingly.

How can you achieve this?

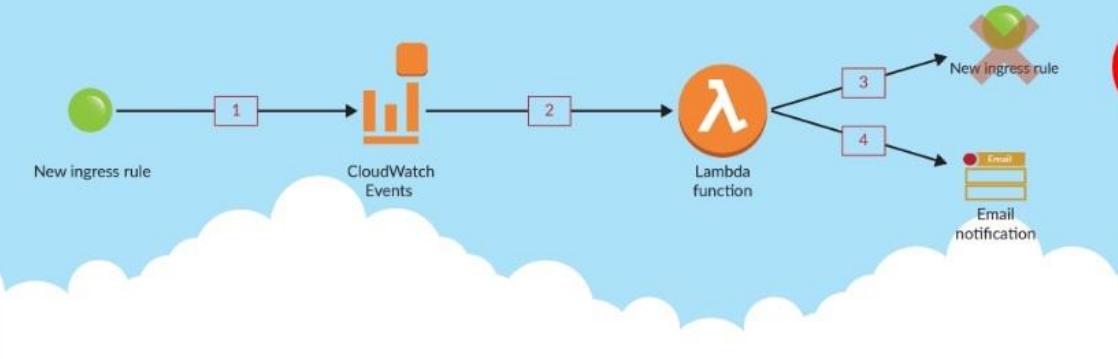
- A. Use Cloudwatch logs to monitor the activity on the Security Groups. Use filters to search for the changes and use SNS for the notification.
- B. Use Cloudwatch metrics to monitor the activity on the Security Groups. Use filters to search for the changes and use SNS for the notification.
- C. Use AWS inspector to monitor the activity on the Security Groups. Use filters to search for the changes and use SNS f the notification.
- D. Use Cloudwatch events to be triggered for any changes to the Security Groups. Configure the Lambda function for email notification as well.

Answer: D

Explanation:

The below diagram from an AWS blog shows how security groups can be monitored

How to Automatically Revert and Receive Notifications About Changes to Your Amazon VPC Security Groups



Option A is invalid because you need to use Cloudwatch Events to check for chan

Option B is invalid because you need to use Cloudwatch Events to check for chang

Option C is invalid because AWS inspector is not used to monitor the activity on Security Groups

QUESTION 373

Your company has a set of EC2 Instances defined in AWS. They need to ensure that all traffic packets are monitored and inspected for any security threats.

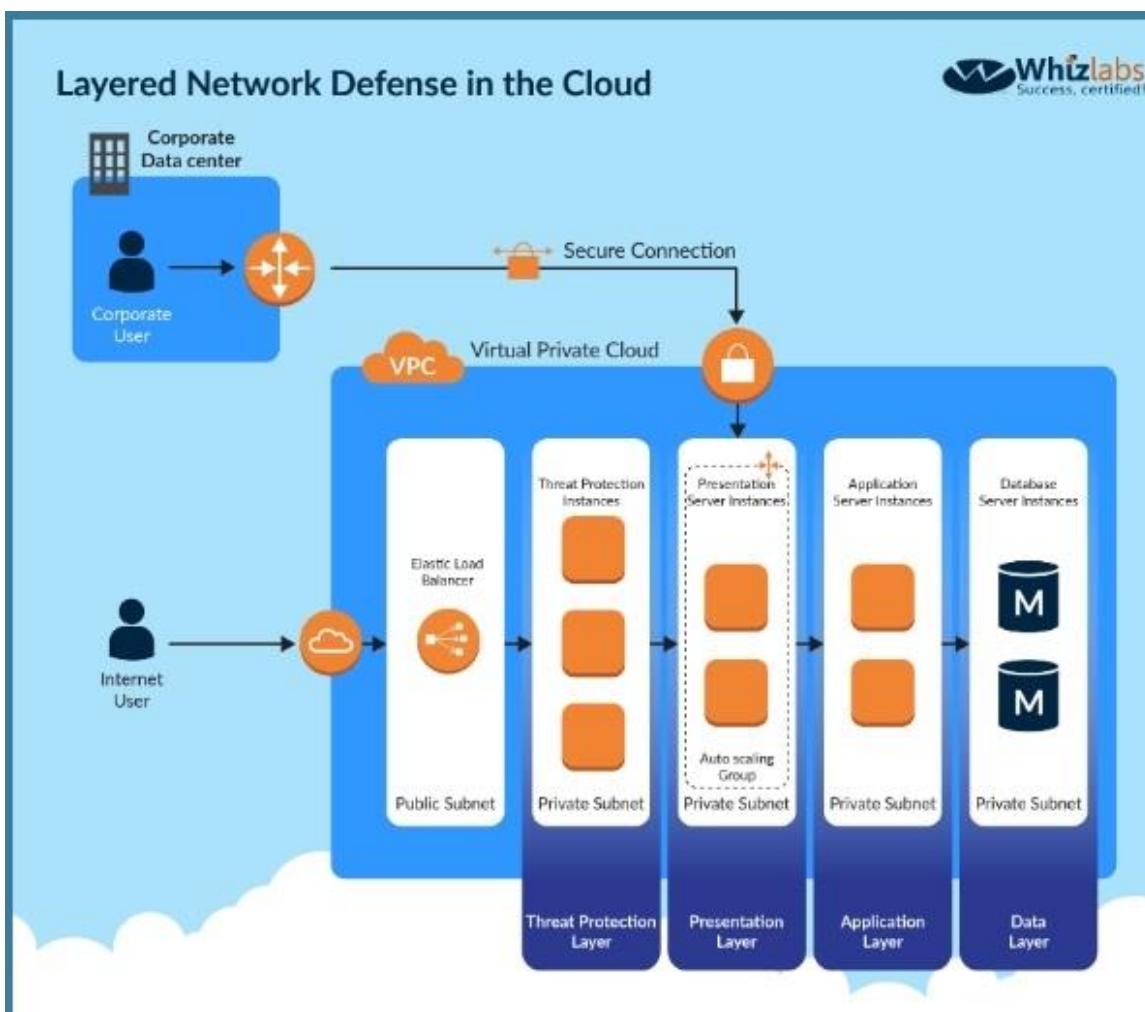
How can this be achieved? Choose 2 answers from the options given below

- A. Use a host based intrusion detection system
- B. Use a third party firewall installed on a central EC2 instance
- C. Use VPC Flow logs
- D. Use Network Access control lists logging

Answer: AB

Explanation:

If you want to inspect the packets themselves, then you need to use custom based software A diagram representation of this is given in the AWS Security best practices



Option C is invalid because VPC Flow logs cannot conduct packet inspection.

QUESTION 374

A company had developed an incident response plan 18 months ago. Regular implementations of the response plan are carried out. No changes have been made to the response plan have been made since its creation.

Which of the following is a right statement with regards to the plan?

- It places too much emphasis on already implemented security controls.
- The response plan is not implemented on a regular basis
- The response plan does not cater to new services
- The response plan is complete in its entirety

Answer: C

Explanation:

So definitely the case here is that the incident response plan is not catering to newly created services.

AWS keeps on changing and adding new services and hence the response plan must cater to these new services.

Option A and B are invalid because we don't know this for a fact. Option D is invalid because we

know that the response plan is not complete, because it does not cater to new features of AWS
<https://aws.amazon.com/blogs/publicsector/buildins-a-cloud-specific-incident-response-plan>

QUESTION 375

You are planning to use AWS Config to check the configuration of the resources in your AWS account. You are planning on using an existing IAM role and using it for the AWS Config resource.

Which of the following is required to ensure the AWS config service can work as required?

- A. Ensure that there is a trust policy in place for the AWS Config service within the role
- B. Ensure that there is a grant policy in place for the AWS Config service within the role
- C. Ensure that there is a user policy in place for the AWS Config service within the role
- D. Ensure that there is a group policy in place for the AWS Config service within the role

Answer: A

Explanation:

| VPN Connections | |
|---|---|
| You can connect your Amazon VPC to remote networks by using a VPN connection. The following are some of the connectivity options available to you. | |
| VPN connectivity option | Description |
| AWS managed VPN | You can create an IPsec VPN connection between your VPC and your remote network. On the AWS side of the VPN connection, a <i>virtual private gateway</i> provides two VPN endpoints (tunnels) for automatic failover. You configure your <i>customer gateway</i> on the remote side of the VPN connection. For more information, see AWS Managed VPN Connections , and the Amazon VPC Network Administrator Guide . |
| AWS VPN CloudHub | If you have more than one remote network (for example, multiple branch offices), you can create multiple AWS managed VPN connections via your virtual private gateway to enable communication between these networks. For more information, see Providing Secure Communication Between Sites Using VPN CloudHub . |
| Third party software VPN appliance | You can create a VPN connection to your remote network by using an Amazon EC2 instance in your VPC that's running a third party software VPN appliance. AWS does not provide or maintain third party software VPN appliances; however, you can choose from a range of products provided by partners and open source communities. Find third party software VPN appliances on the AWS Marketplace . |
| You can also use AWS Direct Connect to create a dedicated private connection from a remote network to your VPC. You can combine this connection with an AWS managed VPN connection to create an IPsec-encrypted connection. For more information, see What is AWS Direct Connect? in the AWS Direct Connect User Guide . For more information about the different VPC and VPN connectivity options, see the Amazon Virtual Private Cloud Connectivity Options whitepaper. | |

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "",  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "config.amazonaws.com"  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}
```

Options B,C and D are invalid because you need to ensure a trust policy is in place and not a grant.

<https://docs.aws.amazon.com/config/latest/developerguide/iamrole-permissions.html>

QUESTION 376

You are planning on using the AWS KMS service for managing keys for your application. For which of the following can the KMS CMK keys be used for encrypting? Choose 2 answers from the options given below

- A. Image Objects
- B. Large files
- C. Password
- D. RSA Keys

Answer: CD

Explanation:

The CMK keys themselves can only be used for encrypting data that is maximum 4KB in size. Hence it can be used for encrypting information such as passwords and RSA keys.

Option A and B are invalid because the actual CMK key can only be used to encrypt small amounts of data and not large amounts of data. You have to generate the data key from the CMK key in order to encrypt high amounts of data.

<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html>

QUESTION 377

A company is using a Redshift cluster to store their data warehouse. There is a requirement from the Internal IT Security team to ensure that data gets encrypted for the Redshift database. How can this be achieved?

- A. Encrypt the EBS volumes of the underlying EC2 Instances
- B. Use AWS KMS Customer Default master key
- C. Use SSL/TLS for encrypting the data
- D. Use S3 Encryption

Answer: B

Explanation:

The AWS Documentation mentions the following Amazon Redshift uses a hierarchy of encryption keys to encrypt the database. You can use either AWS Key Management Service (AWS KMS) or a hardware security module (HSM) to manage the top-level encryption keys in this hierarchy.

The process that Amazon Redshift uses for encryption differs depending on how you manage keys.

Option A is invalid because it's the cluster that needs to be encrypted

Option C is invalid because this encrypts objects in transit and not objects at rest

Option D is invalid because this is used only for objects in S3 buckets.

<https://docs.aws.amazon.com/redshift/latest/memt/working-with-db-encryption.html>

QUESTION 378

Your company is planning on developing an application in AWS. This is a web based application.

The application user will use their Facebook or Google identities for authentication.

You want to have the ability to manage user profiles without having to add extra coding to manage this.

Which of the below would assist in this?

- A. Create an OIDC identity provider in AWS
- B. Create a SAML provider in AWS
- C. Use AWS Cognito to manage the user profiles
- D. Use IAM users to manage the user profiles

Answer: C

Explanation:

The AWS Documentation mentions the following A user pool is a user directory in Amazon Cognito. With a user pool, your users can sign in to your web or mobile app through Amazon Cognito. Your users can also sign in through social identity providers like Facebook or Amazon, and through SAML identity providers.

Whether your users sign in directly or through a third party, all members of the user pool have a directory profile that you can access through an SDK.

User pools provide:

Sign-up and sign-in services.

A built-in, customizable web UI to sign in users. Social sign-in with Facebook, Google, and Login with Amazon, as well as sign-in with SAML identity providers from your user pool.

User directory management and user profiles.

Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification. Customized workflows and user migration through AWS Lambda triggers.

Options A and B are invalid because these are not used to manage users

Option D is invalid because this would be a maintenance overhead

<https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools.html>

QUESTION 379

You have just developed a new mobile application that handles analytics workloads on large scale datasets that are stored on Amazon Redshift. Consequently, the application needs to access Amazon Redshift tables.

Which of the below methods would be the best both practically and security-wise, to access the tables? Choose the correct answer from the options below

- A. Create an IAM user and generate encryption keys for that user. Create a policy for Redshift read-only access. Embed those keys in the application.
- B. Create an HSM client certificate in Redshift and authenticate using this certificate.
- C. Create a Redshift read-only access policy in IAM and embed those credentials in the application.
- D. Use roles that allow a web identity federated user to assume a role that allows access to the Redshift table by providing temporary credentials.

Answer: D

Explanation:

The AWS Documentation mentions the following "When you write such an app, you'll make requests to AWS services that must be signed with an AWS access key. However, we strongly recommend that you do not embed or distribute long-term AWS credentials with apps that a user downloads to a device, even in an encrypted store. Instead, build your app so that it requests temporary AWS security credentials dynamically when needed using web identity federation. The supplied temporary credentials map to an AWS role that has only the permissions needed to perform the tasks required by the mobile app".

Option A, B and C are all automatically incorrect because you need to use IAM Roles for Secure access to services

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html

QUESTION 380

Your company makes use of S3 buckets for storing data. There is a company policy that all services should have logging enabled.

How can you ensure that logging is always enabled for created S3 buckets in the AWS Account?

- A. Use AWS Inspector to inspect all S3 buckets and enable logging for those where it is not enabled
- B. Use AWS Config Rules to check whether logging is enabled for buckets
- C. Use AWS Cloudwatch metrics to check whether logging is enabled for buckets
- D. Use AWS Cloudwatch logs to check whether logging is enabled for buckets

Answer: B

Explanation:

This is given in the AWS Documentation as an example rule in AWS Config Example rules with triggers Example rule with configuration change trigger

1. You add the AWS Config managed rule, S3_BUCKET_LOGGING_ENABLED, to your account to check whether your Amazon S3 buckets have logging enabled.
2. The trigger type for the rule is configuration changes. AWS Config runs the evaluations for the rule when an Amazon S3 bucket is created, changed, or deleted.
3. When a bucket is updated, the configuration change triggers the rule and AWS Config evaluates whether the bucket is compliant against the rule.

Option A is invalid because AWS Inspector cannot be used to scan all buckets

Option C and D are invalid because Cloudwatch cannot be used to check for logging enablement for buckets.

<https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html>

QUESTION 381

A company is operating a website using Amazon CloudFront. CloudFront servers some content from Amazon S3 and other from web servers running EC2 instances behind an Application Load Balancer (ALB). Amazon DynamoDB is used as the data store. The company already uses AWS Certificate Manager (ACM) to store a public TLS certificate that can optionally secure connections

between the website users and CloudFront. The company has a new requirement to enforce end-to-end encryption in transit.

Which combination of steps should the company take to meet this requirement? (Select THREE.)

- A. Update the CloudFront distribution, configuring it to optionally use HTTPS when connecting to origins on Amazon S3
- B. Update the web application configuration on the web servers to use HTTPS instead of HTTP when connecting to DynamoDB
- C. Update the CloudFront distribution to redirect HTTP corrections to HTTPS
- D. Configure the web servers on the EC2 instances to listen using HTTPS using the public ACM TLS certificate
 - Update the ALB to connect to the target group using HTTPS
- E. Update the ALB listen to listen using HTTPS using the public ACM TLS certificate.
 - Update the CloudFront distribution to connect to the HTTPS listener.
- F. Create a TLS certificate Configure the web servers on the EC2 instances to use HTTPS only with that certificate.
 - Update the ALB to connect to the target group using HTTPS.

Answer: BCE

QUESTION 382

Your company has many AWS accounts defined and all are managed via AWS Organizations. One AWS account has a S3 bucket that has critical data.

How can we ensure that all the users in the AWS organisation have access to this bucket?

- A. Ensure the bucket policy has a condition which involves aws:PrincipalOrgID
- B. Ensure the bucket policy has a condition which involves aws:AccountNumber
- C. Ensure the bucket policy has a condition which involves aws:PrincipalId
- D. Ensure the bucket policy has a condition which involves aws:OrgID

Answer: A

Explanation:

The AWS Documentation mentions the following AWS Identity and Access Management (IAM) now makes it easier for you to control access to your AWS resources by using the AWS organization of IAM principals (users and roles). For some services, you grant permissions using resource-based policies to specify the accounts and principals that can access the resource and what actions they can perform on it. Now, you can use a new condition key, aws:PrincipalOrgID, in these policies to require all principals accessing the resource to be from an account in the organization

Option B.C and D are invalid because the condition in the bucket policy has to mention aws:PrincipalOrgID

<https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-usins-the-aws-organization-of-iam-principal>

QUESTION 383

A company is planning on extending their on-premise AWS Infrastructure to the AWS Cloud. They need to have a solution that would give core benefits of traffic encryption and ensure latency is kept to a minimum.

Which of the following would help fulfil this requirement? Choose 2 answers from the options given below

- A. AWS VPN
- B. AWS VPC Peering
- C. AWS NAT gateways
- D. AWS Direct Connect

Answer: AD

Explanation:

The AWS Document mention the following which supports the requirement

| VPN Connections | |
|--|---|
| You can connect your Amazon VPC to remote networks by using a VPN connection. The following are some of the connectivity options available to you. | |
| VPN connectivity option | Description |
| AWS managed VPN | You can create an IPsec VPN connection between your VPC and your remote network. On the AWS side of the VPN connection, a virtual private gateway provides two VPN endpoints (tunnels) for automatic failover. You configure your customer gateway on the remote side of the VPN connection. For more information, see AWS Managed VPN Connections , and the Amazon VPC Network Administrator Guide . |
| AWS VPN CloudHub | If you have more than one remote network (for example, multiple branch offices), you can create multiple AWS managed VPN connections via your virtual private gateway to enable communication between these networks. For more information, see Providing Secure Communication Between Sites Using VPN CloudHub . |
| Third party software VPN appliance | You can create a VPN connection to your remote network by using an Amazon EC2 instance in your VPC that's running a third party software VPN appliance. AWS does not provide or maintain third party software VPN appliances; however, you can choose from a range of products provided by partners and open source communities. Find third party software VPN appliances on the AWS Marketplace . |
| You can also use AWS Direct Connect to create a dedicated private connection from a remote network to your VPC. You can combine this connection with an AWS managed VPN connection to create an IPsec-encrypted connection. For more information, see What is AWS Direct Connect? in the AWS Direct Connect User Guide . For more information about the different VPC and VPN connectivity options, see the Amazon Virtual Private Cloud Connectivity Options whitepaper . | |

Option B is invalid because VPC peering is only used for connection between VPCs and cannot be used to connect On-premise infrastructure to the AWS Cloud.

Option C is invalid because NAT gateways is used to connect instances in a private subnet to the internet

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/pn-connections.html>

QUESTION 384

You need to create a policy and apply it for just an individual user. How could you accomplish this in the right way?

- A. Add an AWS managed policy for the user
- B. Add a service policy for the user
- C. Add an IAM role for the user
- D. Add an inline policy for the user

Answer: D

Explanation:

Options A and B are incorrect since you need to add an inline policy just for the user

Option C is invalid because you don't assign an IAM role to a user

QUESTION 385

You have a set of Keys defined using the AWS KMS service. You want to stop using a couple of keys , but are not sure of which services are currently using the keys.

Which of the following would be a safe option to stop using the keys from further usage.

- A. Delete the keys since anyway there is a 7 day waiting period before deletion
- B. Disable the keys
- C. Set an alias for the key
- D. Change the key material for the key

Answer: B**Explanation:**

Option A is invalid because once you schedule the deletion and waiting period ends, you cannot come back from the deletion process. Option C and D are invalid because these will not check to see if the keys are being used or not.

The AWS Documentation mentions the following

Deleting a customer master key (CMK) in AWS Key Management Service (AWS KMS) is destructive and potentially dangerous. It deletes the key material and all metadata associated with the CMK, and is irreversible. After a CMK is deleted you can no longer decrypt the data that was encrypted under that CMK, which means that data becomes unrecoverable. You should delete a CMK only when you are sure that you don't need to use it anymore. If you are not sure, consider disabling the CMK instead of deleting it.

You can re-enable a disabled CMK if you need to use it again later, but you cannot recover a deleted CMK.

<https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys.html>

QUESTION 386

You have a set of application , database and web servers hosted in AWS. The web servers are placed behind an ELB. There are separate security groups for the application, database and web servers. The network security groups have been defined accordingly. There is an issue with the communication between the application and database servers. In order to troubleshoot the issue between just the application and database server, what is the ideal set of MINIMAL steps you would take?

- A. Check the Inbound security rules for the database security group Check the Outbound security rules for the application security group
- B. Check the Outbound security rules for the database security group | Check the inbound security rules for the application security group
- C. Check the both the Inbound and Outbound security rules for the database security group Check the inbound security rules for the application security group
- D. Check the Outbound security rules for the database security group Check the both the Inbound and Outbound security rules for the application security group

Answer: A**Explanation:**

Here since the communication would be established inward to the database server and outward from the application server, you need to ensure that just the Outbound rules for application server security groups are checked. And then just the Inbound rules for database server security groups are checked.

Option B can't be the correct answer. It says that we need to check the outbound security group which is not needed.

We need to check the inbound for DB SG and outbound of Application SG. Because, this two group need to communicate with each other to function properly.

Option C is invalid because you don't need to check for Outbound security rules for the database security group

Option D is invalid because you don't need to check for Inbound security rules for the application security group

QUESTION 387

Your company has confidential documents stored in the simple storage service. Due to compliance requirements, you have to ensure that the data in the S3 bucket is available in a

different geographical location.

As an architect what is the change you would make to comply with this requirement?

- A. Apply Multi-AZ for the underlying S3 bucket
- B. Copy the data to an EBS Volume in another Region
- C. Create a snapshot of the S3 bucket and copy it to another region
- D. Enable Cross region replication for the S3 bucket

Answer: D

Explanation:

This is mentioned clearly as a use case for S3 cross-region replication. You might configure cross-region

replication on a bucket for various reasons, including the following:

Compliance requirements - Although, by default Amazon S3 stores your data across multiple geographically distant Availability Zones, compliance requirements might dictate that you store data at even further distances.

Cross-region replication allows you to replicate data between distant AWS Regions to satisfy these compliance requirements.

Option A is invalid because Multi-AZ cannot be used to S3 buckets. Option B is invalid because copying it to an EBS volume is not a recommended practice.

Option C is invalid because creating snapshots is not possible in S3.

QUESTION 388

Your current setup in AWS consists of the following architecture. 2 public subnets, one subnet which has the web servers accessed by users across the internet and the other subnet for the database server.

Which of the following changes to the architecture would add a better security boundary to the resources hosted in your setup?

- A. Consider moving the web server to a private subnet
- B. Consider moving the database server to a private subnet
- C. Consider moving both the web and database server to a private subnet
- D. Consider creating a private subnet and adding a NAT instance to that subnet

Answer: B

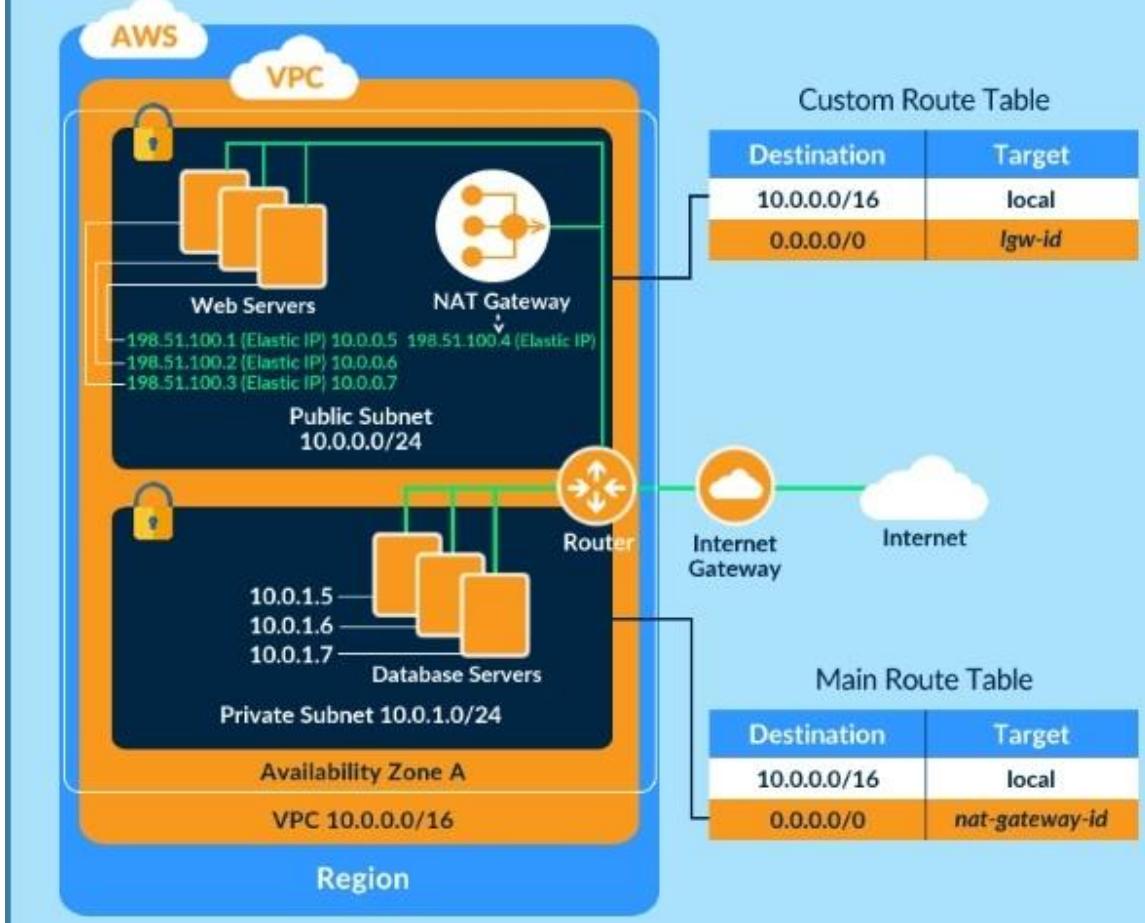
Explanation:

The ideal setup is to ensure that the web server is hosted in the public subnet so that it can be accessed by users on the internet. The database server can be hosted in the private subnet.

The below diagram from the AWS Documentation shows how this can be setup

VPC with Public and Private Subnets (NAT)

The following diagram shows the key components of the configuration for this scenario



Option A and C are invalid because if you move the web server to a private subnet, then it cannot be accessed by users

Option D is invalid because NAT instances should be present in the public subnet

QUESTION 389

An auditor needs access to logs that record all API events on AWS. The auditor only needs read-only access to the log files and does not need access to each AWS account. The company has multiple AWS accounts, and the auditor needs access to all the logs for all the accounts.

What is the best way to configure access for the auditor to view event logs from all accounts?

Choose the correct answer from the options below

- Configure the CloudTrail service in each AWS account, and have the logs delivered to an AWS bucket on each account, while granting the auditor permissions to the bucket via roles in the secondary accounts and a single primary IAM account that can assume a read-only role in the secondary AWS accounts.
- Configure the CloudTrail service in the primary AWS account and configure consolidated billing for all the secondary accounts.

- Then grant the auditor access to the S3 bucket that receives the CloudTrail log files.
- C. Configure the CloudTrail service in each AWS account and enable consolidated logging inside of CloudTrail.
 - D. Configure the CloudTrail service in each AWS account and have the logs delivered to a single AWS bucket in the primary account and grant the auditor access to that single bucket in the primary account.

Answer: D

Explanation:

Given the current requirements, assume the method of "least privilege" security design and only allow the auditor access to the minimum amount of AWS resources as possible. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure. CloudTrail provides a history of AWS API calls for your account including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting.

Option A is incorrect since the auditor should have access to the logs.
Option B is incorrect since consolidated billing is not a key requirement as part of the question.

Option C is incorrect since there is no consolidated logging.

QUESTION 390

A company has a requirement to create a DynamoDB table. The company's software architect has provided the following CLI command for the DynamoDB table

```
--table-name Customers \
--attribute-definitions \
   AttributeName=ID,AttributeType=S \
   AttributeName=Name,AttributeType=S \
--key-schema \
   AttributeName=ID,KeyType=HASH \
   AttributeName=Name,KeyType=RANGE \
--provisioned-throughput \
    ReadCapacityUnits=10,WriteCapacityUnits=5 \
--sse-specification Enabled=true
```

Which of the following has been taken from a security perspective from the above command?

- A. Since the ID is hashed, it ensures security of the underlying table.
- B. The above command ensures data encryption at rest for the Customer table.
- C. The above command ensures data encryption in transit for the Customer table.
- D. The right throughput has been specified from a security perspective.

Answer: B

Explanation:

The above command with the "-sse-specification Enabled=true" parameter ensures that the data for the DynamoDB table is encrypted at rest.

Options A, C and D are all invalid because this command is specifically used to ensure data

encryption at rest

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/encryption.tutorial.html>

QUESTION 391

A company is planning to run a number of Admin related scripts using the AWS Lambda service. There is a need to understand if there are any errors encountered when the script run. How can this be accomplished in the most effective manner.

- A. Use Cloudwatch metrics and logs to watch for errors
- B. Use Cloudtrail to monitor for errors
- C. Use the AWS Config service to monitor for errors
- D. Use the AWS inspector service to monitor for errors

Answer: A

Explanation:

The AWS Documentation mentions the following AWS Lambda automatically monitors Lambda functions on your behalf, reporting metrics through Amazon CloudWatch. To help you troubleshoot failures in a function. Lambda logs all requests handled by your function and also automatically stores logs generated by your code through Amazon CloudWatch Logs. Option B,C and D are all invalid because these services cannot be used to monitor for errors.

QUESTION 392

An IT department currently has a Java web application deployed on Apache Tomcat running on Amazon EC2 instances. All traffic to the EC2 instances is sent through an internet-facing Application Load Balancer (ALB).

The Security team has noticed during the past two days thousands of unusual read requests coming from hundreds of IP addresses. This is causing the Tomcat server to run out of threads and reject new connections

Which the SIMPLEST change that would address this server issue?

- A. Create an Amazon CloudFront distribution and configure the ALB as the origin
- B. Block the malicious IPs with a network access list (NACL).
- C. Create an AWS Web Application Firewall (WAF). and attach it to the ALB
- D. Map the application domain name to use Route 53

Answer: A

QUESTION 393

A windows machine in one VPC needs to join the AD domain in another VPC. VPC Peering has been established. But the domain join is not working.

What is the other step that needs to be followed to ensure that the AD domain join can work as intended?

- A. Change the VPC peering connection to a VPN connection
- B. Change the VPC peering connection to a Direct Connect connection
- C. Ensure the security groups for the AD hosted subnet has the right rule for relevant subnets
- D. Ensure that the AD is placed in a public subnet

Answer: C

Explanation:

In addition to VPC peering and setting the right route tables, the security groups for the AD EC2 instance needs to ensure the right rules are put in place for allowing incoming traffic. Option A and B is invalid because changing the connection type will not help. This is a problem with the Security Groups.

Option D is invalid since the AD should not be placed in a public subnet

<https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/ingress.html>

QUESTION 394

How can you ensure that instance in an VPC does not use AWS DNS for routing DNS requests. You want to use your own managed DNS instance. How can this be achieved?

- A. Change the existing DHCP options set
- B. Create a new DHCP options set and replace the existing one.
- C. Change the route table for the VPC
- D. Change the subnet configuration to allow DNS requests from the new DNS Server

Answer: B

Explanation:

In order to use your own DNS server, you need to ensure that you create a new custom DHCP options set with the IP of the custom DNS server. You cannot modify the existing set, so you need to create a new one.

Option A is invalid because you cannot make changes to an existing DHCP options Set.

Option C is invalid because this can only be used to work with Routes and not with a custom DNS solution.

Option D is invalid because this needs to be done at the VPC level and not at the Subnet level

QUESTION 395

A company continually generates sensitive records that it stores in an S3 bucket. All objects in the bucket are encrypted using SSE-KMS using one of the company's CMKs. Company compliance policies require that no more than one month of data be encrypted using the same encryption key. What solution below will meet the company's requirements?

- A. Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK and updates the S3 bucket to use the new CMK.
- B. Configure the CMK to rotate the key material every month.
- C. Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK, updates the S3 bucket to use the new CMK, and deletes the old CMK.
- D. Trigger a Lambda function with a monthly CloudWatch event that rotates the key material in the CMK.

Answer: A

Explanation:

You can use a Lambda function to create a new key and then update the S3 bucket to use the new key.

Remember not to delete the old key, else you will not be able to decrypt the documents stored in the S3 bucket using the older key.

Option B is incorrect because AWS KMS cannot rotate keys on a monthly basis

Option C is incorrect because deleting the old key means that you cannot access the older objects

Option D is incorrect because rotating key material is not possible.

<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html>

QUESTION 396

An EC2 Instance hosts a Java based application that access a DynamoDB table. This EC2 Instance is currently serving production based users.

Which of the following is a secure way of ensuring that the EC2 Instance access the Dynamo table?

- A. Use IAM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance
- B. Use KMS keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- C. Use IAM Access Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- D. Use IAM Access Groups with the right permissions to interact with DynamoDB and assign it to the EC2 Instance

Answer: A

Explanation:

To always ensure secure access to AWS resources from EC2 Instances, always ensure to assign a Role to the EC2 Instance

Option B is invalid because KMS keys are not used as a mechanism for providing EC2 Instances access to AWS services.

Option C is invalid Access keys is not a safe mechanism for providing EC2 Instances access to AWS services.

Option D is invalid because there is no way access groups can be assigned to EC2 Instances.

QUESTION 397

Your company looks at the gaming domain and hosts several Ec2 Instances as game servers.

The servers each experience user loads in the thousands. There is a concern of DDoS attacks on the EC2 Instances which could cause a huge revenue loss to the company.

Which of the following can help mitigate this security concern and also ensure minimum downtime for the servers?

- A. Use VPC Flow logs to monitor the VPC and then implement NACL's to mitigate attacks
- B. Use AWS Shield Advanced to protect the EC2 Instances
- C. Use AWS Inspector to protect the EC2 Instances
- D. Use AWS Trusted Advisor to protect the EC2 Instances

Answer: B

Explanation:

Below is an excerpt from the AWS Documentation on some of the use cases for AWS Shield

| Example AWS Shield Advanced Use Cases | | |
|--|---|---|
| Goal | Suggested services | Related service documentation |
| Protect a web application and RESTful APIs against a DDoS attack | Shield Advanced protecting an Amazon CloudFront distribution and an Application Load Balancer | Amazon Elastic Load Balancing Documentation , Amazon CloudFront Documentation |
| Protect a TCP-based application against a DDoS attack | Shield Advanced protecting a Network Load Balancer attached to an Elastic IP address | Amazon Elastic Load Balancing Documentation |
| Protect a UDP-based game server against a DDoS attack | Shield Advanced protecting an Amazon EC2 instance attached to an Elastic IP address | Amazon Elastic Compute Cloud Documentation |

QUESTION 398

DDoS attacks that happen at the application layer commonly target web applications with lower volumes of traffic compared to infrastructure attacks. To mitigate these types of attacks, you should probably want to include a WAF (Web Application Firewall) as part of your infrastructure. To inspect all HTTP requests, WAFs sit in-line with your application traffic. Unfortunately, this creates a scenario where WAFs can become a point of failure or bottleneck. To mitigate this problem, you need the ability to run multiple WAFs on demand during traffic spikes. This type of scaling for WAF is done via a "WAF sandwich."

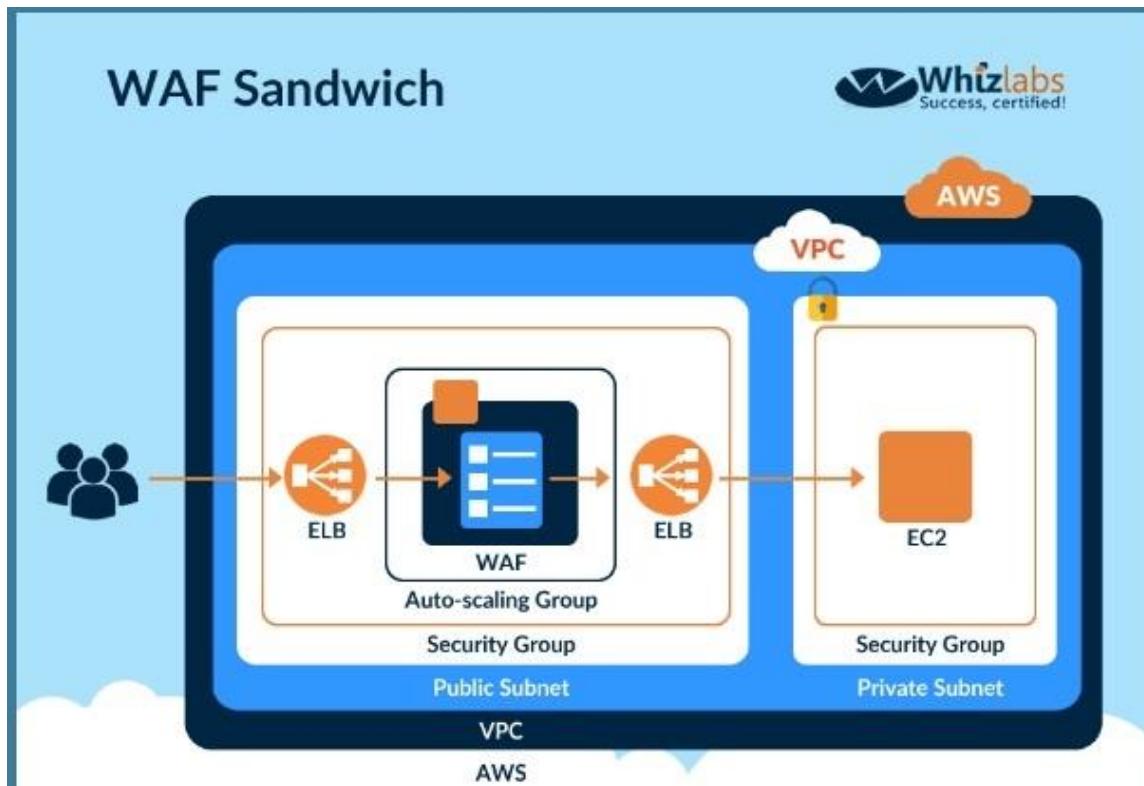
Which of the following statements best describes what a "WAF sandwich" is? Choose the correct answer from the options below

- A. The EC2 instance running your WAF software is placed between your private subnets and any NATed connections to the internet.
- B. The EC2 instance running your WAF software is placed between your public subnets and your Internet Gateway.
- C. The EC2 instance running your WAF software is placed between your public subnets and your private subnets.
- D. The EC2 instance running your WAF software is included in an Auto Scaling group and placed in between two Elastic load balancers.

Answer: D

Explanation:

The below diagram shows how a WAF sandwich is created. Its the concept of placing the Ec2 instance which hosts the WAF software in between 2 elastic load balancers.



Option A.B and C are incorrect since the EC2 Instance with the WAF software needs to be placed in an Autoscaling Group.

QUESTION 399

A company is hosting sensitive data in an AWS S3 bucket. It needs to be ensured that the bucket always remains private.

How can this be ensured continually? Choose 2 answers from the options given below Please select:

- A. Use AWS Config to monitor changes to the AWS Bucket
- B. Use AWS Lambda function to change the bucket policy
- C. Use AWS Trusted Advisor API to monitor the changes to the AWS Bucket
- D. Use AWS Lambda function to change the bucket ACL

Answer: AD

QUESTION 400

You need to ensure that the CloudTrail logs which are being delivered in your AWS account is encrypted.

How can this be achieved in the easiest way possible?

- A. Don't do anything since CloudTrail logs are automatically encrypted.
- B. Enable S3-SSE for the underlying bucket which receives the log files
- C. Enable S3-KMS for the underlying bucket which receives the log files
- D. Enable KMS encryption for the logs which are sent to Cloudwatch

Answer: A

Explanation:

The AWS Documentation mentions the following By default the log files delivered by CloudTrail to your bucket are encrypted by Amazon server-side encryption with Amazon S3-managed encryption keys (SSE-S3) Option B,C and D are all invalid because by default all logs are encrypted when they sent by Cloudtrail to S3 buckets
[https://docs.aws.amazon.com/awscloudtrail/latest/usereuide/encrypting-cloudtrail-log-files-with-aws-kms.html](https://docs.aws.amazon.com/awscloudtrail/latest/usereguide/encrypting-cloudtrail-log-files-with-aws-kms.html)

QUESTION 401

Your company has a hybrid environment, with on-premise servers and servers hosted in the AWS cloud. They are planning to use the Systems Manager for patching servers.

Which of the following is a pre-requisite for this to work;

- A. Ensure that the on-premise servers are running on Hyper-V.
- B. Ensure that an IAM service role is created
- C. Ensure that an IAM User is created
- D. Ensure that an IAM Group is created for the on-premise servers

Answer: B

Explanation:

You need to ensure that an IAM service role is created for allowing the on-premise servers to communicate with the AWS Systems Manager.

Option A is incorrect since it is not necessary that servers should only be running Hyper-V Options C and D are incorrect since it is not necessary that IAM users and groups are created.

QUESTION 402

A company is using Amazon Elastic Container Service (Amazon ECS) to deploy an application

that deals with sensitive data. During a recent security audit, the company identified a security issue in which Amazon RDS credentials were stored with the application code in the company's source code repository.

A security engineer needs to develop a solution to ensure that database credentials are stored securely and rotated periodically. The credentials should be accessible to the application only. The engineer also needs to prevent database administrators from sharing database credentials as plaintext with other teammates. The solution must also minimize administrative overhead.

Which solution meets these requirements?

- A. Use the AWS Systems Manager Parameter Store to generate database credentials.
Use an IAM profile for ECS tasks to restrict access to database credentials to specific containers only.
- B. Use AWS Secrets Manager to store database credentials.
Use an IAM inline policy for ECS tasks to restrict access to database credentials to specific containers only.
- C. Use the AWS Systems Manager Parameter Store to store database credentials. Use IAM roles for
ECS tasks to restrict access to database credentials to specific containers only.
- D. Use AWS Secrets Manager to store database credentials.
Use IAM roles for ECS tasks to restrict access to database credentials to specific containers only.

Answer: D

QUESTION 403

You are building a large-scale confidential documentation web server on AWS and all of the documentation for it will be stored on S3. One of the requirements is that it cannot be publicly accessible from S3 directly, and you will need to use CloudFront to accomplish this. Which of the methods listed below would satisfy the requirements as outlined? Choose an answer from the options below

- A. Create an Identity and Access Management (IAM) user for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
- B. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
- C. Create individual policies for each bucket the documents are stored in and in that policy grant access to only CloudFront.
- D. Create an S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

Answer: B

Explanation:

If you want to use CloudFront signed URLs or signed cookies to provide access to objects in your Amazon S3 bucket you probably also want to prevent users from accessing your Amazon S3 objects using Amazon S3 URLs. If users access your objects directly in Amazon S3, they bypass the controls provided by CloudFront signed URLs or signed cookies, for example, control over the date and time that a user can no longer access your content and control over which IP addresses can be used to access content. In addition, if user's access objects both through CloudFront and directly by using Amazon S3 URLs, CloudFront access logs are less useful because they're incomplete.

Option A is invalid because you need to create an Origin Access Identity for Cloudfront and not an IAM user.

Option C and D are invalid because using policies will not help fulfil the requirement.

<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

QUESTION 404

You have a bucket and a VPC defined in AWS. You need to ensure that the bucket can only be accessed by the VPC endpoint. How can you accomplish this?

- A. Modify the security groups for the VPC to allow access to the S3 bucket
- B. Modify the route tables to allow access for the VPC endpoint
- C. Modify the IAM Policy for the bucket to allow access for the VPC endpoint
- D. Modify the bucket Policy for the bucket to allow access for the VPC endpoint

Answer: D

Explanation:

This is mentioned in the AWS Documentation Restricting Access to a Specific VPC Endpoint. The following is an example of an S3 bucket policy that restricts access to a specific bucket, examplebucket only from the VPC endpoint with the ID vpce-1a2b3c4d. The policy denies all access to the bucket if the specified endpoint is not being used. The aws:sourceVpce condition is used to specify the endpoint. The aws:sourceVpce condition does not require an ARN for the VPC endpoint resource, only the VPC endpoint ID. For more information about using conditions in a policy, see Specifying Conditions in a Policy.

```
{  
    "Version": "2012-10-17",  
    "Id": "Policy1415115909152",  
    "Statement": [  
        {  
            "Sid": "Access-to-specific-VPCE-only",  
            "Principal": "*",  
            "Action": "s3:*",  
            "Effect": "Deny",  
            "Resource": ["arn:aws:s3:::examplebucket",  
                        "arn:aws:s3:::examplebucket/*"],  
            "Condition": {  
                "StringNotEquals": {  
                    "aws:sourceVpce": "vpce-1a2b3c4d"  
                }  
            }  
        }  
    ]  
}
```

Options A and B are incorrect because using Security Groups nor route tables will help to allow access specifically for that bucke via the VPC endpoint Here you specifically need to ensure the bucket policy is changed.

Option C is incorrect because it is the bucket policy that needs to be changed and not the IAM policy.

QUESTION 405

An Incident Response team is investigating an AWS access key leak that resulted in Amazon EC2 instances being launched.

The company did not discover the incident until many months later.

The Director of Information Security wants to implement new controls that will alert when similar incidents happen in the future.

Which controls should the company implement to achieve this? {Select TWO.)

- A. Enable VPC Flow Logs in all VPCs Create a scheduled AWS Lambda function that downloads and parses the logs, and sends an Amazon SNS notification for violations.
- B. Use AWS CloudTrail to make a trail, and apply it to all Regions Specify an Amazon S3 bucket to receive all the CloudTrail log files

- C. Add the following bucket policy to the company's AWS CloudTrail bucket to prevent log tampering
- ```
{
 "Version": "2012-10-17-",
 "Statement": {
 "Effect": "Deny",
 "Action": "s3:PutObject",
 "Principal": "-"
 },
 "Resource": "arn:aws:s3:::cloudtrail/AWSLogs/111122223333/*" } }
```
- Create an Amazon S3 data event for an PutObject attempts, which sends notifications to an Amazon SNS topic.
- D. Create a Security Auditor role with permissions to access Amazon CloudWatch Logs in all Regions Ship the logs to an Amazon S3 bucket and make a lifecycle policy to ship the logs to Amazon S3 Glacier.
- E. Verify that Amazon GuardDuty is enabled in all Regions, and create an Amazon CloudWatch Events rule for Amazon GuardDuty findings Add an Amazon SNS topic as the rule's target

**Answer:** AE

#### **QUESTION 406**

You have an Amazon VPC that has a private subnet and a public subnet in which you have a NAT instance server. You have created a group of EC2 instances that configure themselves at startup by downloading a bootstrapping script from S3 that deploys an application via GIT.

Which one of the following setups would give us the highest level of security? Choose the correct answer from the options given below.

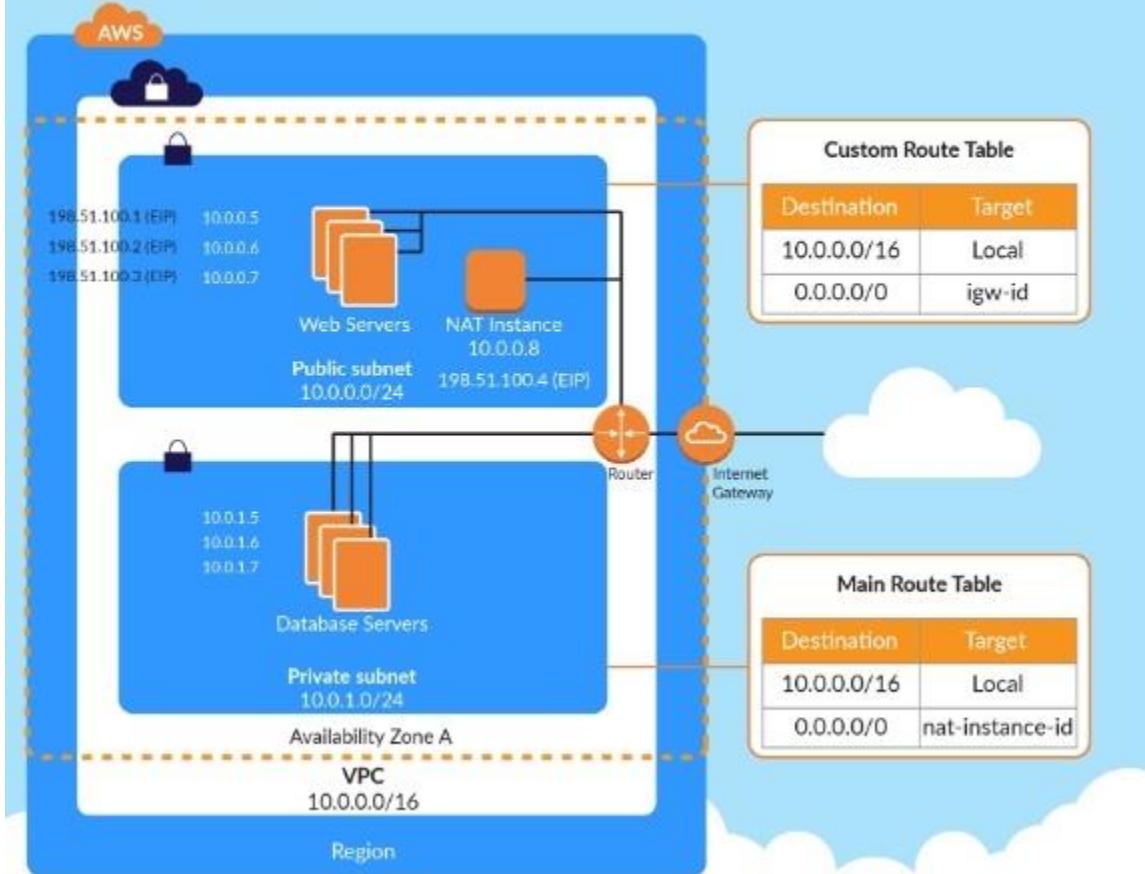
- A. EC2 instances in our public subnet, no EIPs, route outgoing traffic via the IGW
- B. EC2 instances in our public subnet, assigned EIPs, and route outgoing traffic via the NAT
- C. EC2 instance in our private subnet, assigned EIPs, and route our outgoing traffic via our IGW
- D. EC2 instances in our private subnet, no EIPs, route outgoing traffic via the NAT

**Answer:** D

**Explanation:**

The below diagram shows how the NAT instance works. To make EC2 instances very secure, they need to be in a private sub such as the database server shown below with no EIP and all traffic routed via the NAT.

## AWS VPC with public and private subnets using NAT instance



Options A and B are invalid because the instances need to be in the private subnet  
 Option C is invalid because since the instance needs to be in the private subnet, you should not attach an EIP to the instance.

### QUESTION 407

Every application in a company's portfolio has a separate AWS account for development and production. The security team wants to prevent the root user and all IAM users in the production accounts from accessing a specific set of unneeded services.

How can they control this functionality?

- Create a Service Control Policy that denies access to the services. Assemble all production accounts in an organizational unit. Apply the policy to that organizational unit.
- Create a Service Control Policy that denies access to the services. Apply the policy to the root account.
- Create an IAM policy that denies access to the services. Associate the policy with an IAM group and enlist all users and the root users in this group.
- Create an IAM policy that denies access to the services. Create a Config Rule that checks that all users have the policy assigned. Trigger a Lambda function that adds the policy when found missing.

**Answer:** A

**Explanation:**

As an administrator of the master account of an organization, you can restrict which AWS services and individual API actions the users and roles in each member account can access. This restriction even overrides the administrators of member accounts in the organization. When AWS Organizations blocks access to a service or API action for a member account a user or role in that account can't access any prohibited service or API action, even if an administrator of a member account explicitly grants such permissions in an IAM policy. Organization permissions overrule account permissions.

Option B is invalid because service policies cannot be assigned to the root account at the account level.

Option C and D are invalid because IAM policies alone at the account level would not be able to suffice the requirement

## QUESTION 408

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

- A. Create a new role and add each user to the IAM role
- B. Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group
- C. Create a policy and apply it to multiple users using a JSON script
- D. Create an S3 bucket policy with unlimited access which includes each user's AWS account ID

**Answer:** B

**Explanation:**

Option A is incorrect since you don't add a user to the IAM Role Option C is incorrect since you don't assign multiple users to a policy

Option D is incorrect since this is not an ideal approach An IAM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group.

## QUESTION 409

Your company manages thousands of EC2 Instances. There is a mandate to ensure that all servers don't have any critical security flaws. Which of the following can be done to ensure this? Choose 2 answers from the options given below.

- A. Use AWS Config to ensure that the servers have no critical flaws.
- B. Use AWS inspector to ensure that the servers have no critical flaws.
- C. Use AWS inspector to patch the servers
- D. Use AWS SSM to patch the servers

**Answer:** BD

**Explanation:**

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

the Amazon Inspector console or API.

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

Option C is invalid because the AWS Inspector service is not used to patch servers

## QUESTION 410

A company hosts critical data in an S3 bucket. Even though they have assigned the appropriate permissions to the bucket, they are still worried about data deletion.

What measures can be taken to restrict the risk of data deletion on the bucket. Choose 2 answers from the options given below Please select:

- A. Enable versioning on the S3 bucket
- B. Enable data at rest for the objects in the bucket
- C. Enable MFA Delete in the bucket policy
- D. Enable data in transit for the objects in the bucket

**Answer:** AC

**Explanation:**

One of the AWS Security blogs mentions the following: Versioning keeps multiple versions of an object in the same bucket. When you enable it on a bucket Amazon S3 automatically adds a unique version ID to every object stored in the bucket. At that point, a simple DELETE action does not permanently delete an object version; it merely associates a delete marker with the object. If you want to permanently delete an object version, you must specify its version ID in your DELETE request. You can add another layer of protection by enabling MFA Delete on a versioned bucket. Once you do so, you must provide your AWS accounts access keys and a valid code from the account's MFA device in order to permanently delete an object version or suspend or reactivate versioning on the bucket.

Option B is invalid because enabling encryption does not guarantee risk of data deletion.

Option D is invalid because this option does not guarantee risk of data deletion.

<https://aws.amazon.com/blogs/security/securing-access-to-aws-using-mfa-part-3/>

## QUESTION 411

Your company has been using AWS for hosting EC2 Instances for their web and database applications.

They want to have a compliance check to see the following

Whether any ports are left open other than admin ones like SSH and RDP

Whether any ports to the database server other than ones from the web server security group are open.

Which of the following can help achieve this in the easiest way possible. You don't want to carry out an extra configuration changes?

- A. AWS Config
- B. AWS Trusted Advisor
- C. AWS Inspector D.AWSGuardDuty

**Answer:** B

**Explanation:**

Trusted Advisor checks for compliance with the following security recommendations:

Limited access to common administrative ports to only a small subset of addresses. This includes ports 22 (SSH), 23 (Telnet) 3389 (RDP), and 5500 (VNC). Limited access to common database ports. This includes ports 1433 (MSSQL Server), 1434 (MSSQL Monitor), 3306 (MySQL), Oracle (1521) and 5432 (PostgreSQL). Option A is partially correct but then you would need to write custom rules for this. The AWS trusted advisor can give you all of these checks on its dashboard

Option C is incorrect. Amazon Inspector needs a software agent to be installed on all EC2 instances that are included in th.  
assessment target, the security of which you want to evaluate with Amazon Inspector. It monitors the behavior of the EC2 instance on which it is installed, including network, file system, and process activity, and collects a wide set of behavior and configuration data (telemetry), which it then passes to the Amazon Inspector service. Our question's requirement is to choose a choice that is easy to implement. Hence Trusted Advisor is more appropriate for this ) question.

Options D is invalid because this service dont provide these details.

#### QUESTION 412

A company wants to deploy a distributed web application on a fleet of EC2 instances. The fleet will be fronted by a Classic Load Balancer that will be configured to terminate the TLS connection. The company wants to make sure that all past and current TLS traffic to the Classic Load Balancer stays secure even if the certificate private key is leaked.

To ensure the company meets these requirements, a Security Engineer can configure a Classic Load Balancer with:

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

**Answer:** C

#### QUESTION 413

A company requires that data stored in AWS be encrypted at rest.

Which of the following approaches achieve this requirement? Select 2 answers from the options given below.

- A. When storing data in Amazon EBS, use only EBS-optimized Amazon EC2 instances.
- B. When storing data in EBS, encrypt the volume by using AWS KMS.
- C. When storing data in Amazon S3, use object versioning and MFA Delete.
- D. When storing data in Amazon EC2 Instance Store, encrypt the volume by using KMS.
- E. When storing data in S3, enable server-side encryption.

**Answer:** BE

#### Explanation:

The AWS Documentation mentions the following To create an encrypted Amazon EBS volume, select the appropriate box in the Amazon EBS section of the Amazon EC2 console. You can use a custom customer master key (CMK) by choosing one from the list that appears below the encryption box. If you do not specify a custom CMK, Amazon EBS uses the AWS-managed CMK for Amazon EBS in your account. If there is no AWS-managed CMK for Amazon EBS in your account, Amazon EBS creates one.

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by

using SSL or by using client-side encryption. You have the following options of protecting data at rest in Amazon S3.

Use Server-Side Encryption - You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects. Use Client-Side Encryption - You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Option A is invalid because using EBS-optimized Amazon EC2 instances alone will not guarantee protection of instances at rest.

Option C is invalid because this will not encrypt data at rest for S3 objects.

Option D is invalid because you don't store data in Instance store.

<https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

#### QUESTION 414

A new application will be deployed on EC2 instances in private subnets. The application will transfer sensitive data to and from an S3 bucket. Compliance requirements state that the data must not traverse the public internet.

Which solution meets the compliance requirement?

- A. Access the S3 bucket through a proxy server
- B. Access the S3 bucket through a NAT gateway.
- C. Access the S3 bucket through a VPC endpoint for S3
- D. Access the S3 bucket through the SSL protected S3 endpoint

**Answer:** C

**Explanation:**

The AWS Documentation mentions the following A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Option A is invalid because using a proxy server is not sufficient enough

Option B and D are invalid because you need secure communication which should not traverse the internet

#### QUESTION 415

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

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

- A. Open inbound port 22 to 0.0.0.0/0 on all Linux servers.
- B. Enable the advanced-instances tier in Systems Manager.
- C. Create a managed-instance activation for the on-premises servers.
- D. Reconfigure the Systems Manager Agent with the activation code and ID.
- E. Assign an IAM role to all of the on-premises servers.
- F. Initiate an inventory collection with Systems Manager on the on-premises servers

**Answer:** CEF

**QUESTION 416**

Your company is planning on using AWS EC2 and ELB for deployment for their web applications. The security policy mandates that all traffic should be encrypted.

Which of the following options will ensure that this requirement is met. Choose 2 answers from the options below.

- A. Ensure the load balancer listens on port 80
- B. Ensure the load balancer listens on port 443
- C. Ensure the HTTPS listener sends requests to the instances on port 443
- D. Ensure the HTTPS listener sends requests to the instances on port 80

**Answer:** BC

**Explanation:**

The AWS Documentation mentions the following You can create a load balancer that listens on both the HTTP (80) and HTTPS (443) ports. If you specify that the HTTPS listener sends requests to the instances on port 80, the load balancer terminates the requests and communication from the load balancer to the instances is not encrypted, if the HTTPS listener sends requests to the instances on port 443, communication from the load balancer to the instances is encrypted.

Option A is invalid because there is a need for secure traffic, so port 80 should not be used

Option D is invalid because for the HTTPS listener you need to use port 443

**QUESTION 417**

An enterprise wants to use a third-party SaaS application. The SaaS application needs to have access to issue several API commands to discover Amazon EC2 resources running within the enterprise's account. The enterprise has internal security policies that require any outside access to their environment must conform to the principles of least privilege and there must be controls in place to ensure that the credentials used by the SaaS vendor cannot be used by any other third party. Which of the following would meet all of these conditions?

- A. From the AWS Management Console, navigate to the Security Credentials page and retrieve the access and secret key for your account.
- B. Create an IAM user within the enterprise account assign a user policy to the IAM user that allows only the actions required by the SaaS application.  
Create a new access and secret key for the user and provide these credentials to the SaaS provider.
- C. Create an IAM role for cross-account access allows the SaaS provider's account to assume the role  
and assign it a policy that allows only the actions required by the SaaS application.
- D. Create an IAM role for EC2 instances, assign it a policy that allows only the actions required for the SaaS application to work, provide the role ARN to the SaaS provider to use when launching their application instances.

**Answer:** C

**Explanation:**

The below diagram from an AWS blog shows how access is given to other accounts for the services in your own account

## How to Best Architect Your AWS Marketplace SaaS Subscription Across Multiple AWS Accounts



Options A and B are invalid because you should not user IAM users or IAM Access keys  
 Options D is invalid because you need to create a role for cross account access

### QUESTION 418

You have private video content in S3 that you want to serve to subscribed users on the Internet. User IDs, credentials, and subscriptions are stored in an Amazon RDS database. Which configuration will allow you to securely serve private content to your users?

- Generate pre-signed URLs for each user as they request access to protected S3 content
- Create an IAM user for each subscribed user and assign the GetObject permission to each IAM user
- Create an S3 bucket policy that limits access to your private content to only your subscribed users'credentials
- Crpafp a Cloud Front Clriein Identity user for vnur suhsrrihprl users and assign the GptOhiprt oprmissinn to this user

**Answer:** A

**Explanation:**

All objects and buckets by default are private. The pre-signed URLs are useful if you want your user/ customer to be able upload a specific object to your bucket but you don't require them to have AWS security credentials or permissions. When you create a pre-signed URL, you must provide your security credentials, specify a bucket name, an object key, an HTTP method (PUT for uploading objects), and an expiration date and time. The pre-signed URLs are valid only for the specified duration.

Option B is invalid because this would be too difficult to implement at a user level.

Option C is invalid because this is not possible

Option D is invalid because this is used to serve private content via Cloudfront

<http://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html>

### QUESTION 419

A Security Engineer is troubleshooting an issue with a company's custom logging application. The application logs are written to an Amazon S3 bucket with event notifications enabled to send events to an Amazon SNS topic. All logs are encrypted at rest using an AWS KMS CMK. The

SNS topic is subscribed to an encrypted Amazon SQS queue. The logging application polls the queue for new messages that contain metadata about the S3 object. The application then reads the content of the object from the S3 bucket for indexing.

The Logging team reported that Amazon CloudWatch metrics for the number of messages sent or received is showing zero. No logs are being received.

What should the Security Engineer do to troubleshoot this issue?

- A. Add the following statement to the AWS managed CMKs:

```
{
 "Sid": "Allow Amazon SNS to use this key",
 "Effect": "Allow",
 "Principal": {
 "Service": ["sns.amazonaws.com", "sqs.amazonaws.com", "s3.amazonaws.com"]
 },
 "Action": [
 "kms:Decrypt",
 "kms:GenerateDataKey"
],
 "Resource": "*"
}
```

- B. Add the following statement to the CMK key policy:

```
{
 "Sid": "Allow Amazon SNS to use this key",
 "Effect": "Allow",
 "Principal": {
 "Service": "sns.amazonaws.com"
 },
 "Action": [
 "kms:Decrypt",
 "kms:GenerateDataKey"
],
 "Resource": "*"
}
```

- C. Add the following statement to the CMK key policy:

```
{
 "Sid": "Allow Amazon SNS to use this key",
 "Effect": "Allow",
 "Principal": {
 "Service": "sns.amazonaws.com"
 },
 "Action": [
 "kms:Decrypt",
 "kms:GenerateDataKey*"
],
 "Resource": "*"
}
```

- D. Add the following statement to the CMK key policy:

```
{
 "Sid": "Allow Amazon SNS to use this key",
 "Effect": "Allow",
 "Principal": {
 "Service": "sns.amazonaws.com"
 },
 "Action": [
 "kms:Decrypt",
 "kms:GenerateDataKey*"
],
 "Resource": "*"
}
```

**Answer:** D

#### QUESTION 420

A large organization is planning on AWS to host their resources. They have a number of autonomous departments that wish to use AWS.

What could be the strategy to adopt for managing the accounts?

- A. Use multiple VPCs in the account each VPC for each department
- B. Use multiple IAM groups, each group for each department
- C. Use multiple IAM roles, each group for each department
- D. Use multiple AWS accounts, each account for each department

**Answer:** D

**Explanation:**

A recommendation for this is given in the AWS Security best practices

C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option A is incorrect since this would be applicable for resources in a VPC

Options B and C are incorrect since operationally it would be difficult to manage

#### QUESTION 421

You want to track access requests for a particular S3 bucket. How can you achieve this in the easiest possible way?

- A. Enable server access logging for the bucket
- B. Enable Cloudwatch metrics for the bucket
- C. Enable Cloudwatch logs for the bucket
- D. Enable AWS Config for the S3 bucket

**Answer:** A

**Explanation:**

The AWS Documentation mentions the following: To track requests for access to your bucket you can enable access logging.

Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code, if any.

Options B and C are incorrect: Cloudwatch is used for metrics and logging and cannot be used to track access requests.

Option D is incorrect since this can be used for Configuration management but not for tracking S3 bucket requests.

#### QUESTION 422

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

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

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

- A. For each team, create an IAM policy similar to the one that follows. Populate the ec2:ResourceTag/Team condition key with a proper team name. Attach resulting policies to the corresponding IAM roles.
- B. For each team, create an IAM policy similar to the one that follows. Populate the aws:TagKeys/Team condition key with a proper team name. Attach the resulting policies to the corresponding IAM roles.
- C. Tag each IAM role with a Team tag key, and use the team name in the tag value. Create an IAM policy similar to the one that follows, and attach it to all the IAM roles used by developers.
- D. Tag each IAM role with the Team key, and use the team name in the tag value. Create an IAM policy similar to the one that follows, and attach it to all the IAM roles used by developers.

**Answer:** A

#### QUESTION 423

Your company has the following setup in AWS

- a. A set of EC2 Instances hosting a web application
- b. An application load balancer placed in front of the EC2 Instances

There seems to be a set of malicious requests coming from a set of IP addresses. Which of the following can be used to protect against these requests?

- A. Use Security Groups to block the IP addresses
- B. Use VPC Flow Logs to block the IP addresses
- C. Use AWS inspector to block the IP addresses
- D. Use AWS WAF to block the IP addresses

**Answer:** D

**Explanation:**

The AWS Documentation mentions the following on AWS WAF which can be used to protect Application Load Balancers and Cloud front A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon CloudFront distributions or Application Load Balancers respond to.

You can allow or block the following types of requests:

Originate from an IP address or a range of IP addresses

Originate from a specific country or countries

Contain a specified string or match a regular expression (regex) pattern in a particular part of requests  
Exceed a specified length

Appear to contain malicious SQL code (known as SQL injection)

Appear to contain malicious scripts (known as cross-site scripting)

Option A is invalid because by default Security Groups have the Deny policy

Options B and C are invalid because these services cannot be used to block IP addresses

#### **QUESTION 424**

What is the result of the following bucket policy?

```
{
 "Statement": [
 {
 "Sid": "Sid1",
 "Action": "s3:*",
 "Effect": "Allow",
 "Resource": "arn:aws:s3:::mybucket/*",
 "Principal": {"
 "AWS": ["arn:aws:iam::1111111111:user/mark"]}
 }
 },
 {
 "Sid": "Sid2",
 "Action": "s3:*",
 "Effect": "Deny",
 "Resource": "arn:aws:s3:::mybucket/*",
 "Principal": {"
 "AWS": [
 "*"
]
 }
 }
]
}
```

Choose the correct answer:

- A. It will allow all access to the bucket mybucket
- B. It will allow the user mark from AWS account number 1111111111 all access to the bucket but deny everyone else all access to the bucket
- C. It will deny all access to the bucket mybucket
- D. None of these

**Answer: C**

**Explanation:**

The policy consists of 2 statements, one is the allow for the user mark to the bucket and the next is the deny policy for all other users. The deny permission will override the allow and hence all users will not have access to the bucket.

Options A,B and D are all invalid because this policy is used to deny all access to the bucket mybucket.

**QUESTION 425**

Your company uses AWS KMS for management of its customer keys. From time to time, there is a requirement to delete existing keys as part of housekeeping activities.

What can be done during the deletion process to verify that the key is no longer being used.

- A. Use CloudTrail to see if any KMS API request has been issued against existing keys
- B. Use Key policies to see the access level for the keys
- C. Rotate the keys once before deletion to see if other services are using the keys
- D. Change the IAM policy for the keys to see if other services are using the keys

**Answer:** A

**Explanation:**

The AWS documentation mentions the following: You can use a combination of AWS CloudTrail, Amazon CloudWatch Logs, and Amazon Simple Notification Service (Amazon SNS) to create an alarm that notifies you of AWS KMS API requests that attempt to use a customer master key (CMK) that is pending deletion.

If you receive a notification from such an alarm, you might want to cancel deletion of the CMK to give yourself more time to determine whether you want to delete it.

Options B and D are incorrect because Key policies nor IAM policies can be used to check if the keys are being used.

Option C is incorrect since rotation will not help you check if the keys are being used.

<https://docs.aws.amazon.com/kms/latest/developerguide/delete-keys-create-cloudwatch-alarm.html>

**QUESTION 426**

Which of the following is the correct sequence of how KMS manages the keys when used along with the Redshift cluster service?

- A. The master key encrypts the cluster key.  
The cluster key encrypts the database key.  
The database key encrypts the data encryption keys.
- B. The master key encrypts the database key.  
The database key encrypts the data encryption keys.
- C. The master key encrypts the data encryption keys.  
The data encryption keys encrypt the database key
- D. The master key encrypts the cluster key, database key and data encryption keys

**Answer:** A

**Explanation:**

This is mentioned in the AWS Documentation: Amazon Redshift uses a four-tier, key-based architecture for encryption. The architecture consists of data encryption keys, a database key, a cluster key, and a master key. Data encryption keys encrypt data blocks in the cluster. Each data block is assigned a randomly-generated AES-256 key. These keys are encrypted by using the database key for the cluster.

The database key encrypts data encryption keys in the cluster. The database key is a randomly-generated AES-256 key. It is stored on disk in a separate network from the Amazon Redshift cluster and passed to the cluster across a secure channel. The cluster key encrypts the database key for the Amazon Redshift cluster.

Option B is incorrect because the master key encrypts the cluster key and not the database key.  
Option C is incorrect because the master key encrypts the cluster key and not the data encryption keys.

Option D is incorrect because the master key encrypts the cluster key only.

**QUESTION 427**

You need to establish a secure backup and archiving solution for your company, using AWS. Documents should be immediately accessible for three months and available for five years for compliance reasons.

Which AWS service fulfills these requirements in the most cost-effective way? Choose the correct answer:

- A. Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.
- B. Upload the data on EBS, use lifecycle policies to move EBS snapshots into S3 and later into Glacier for long-term archiving.
- C. Use Direct Connect to upload data to S3 and use IAM policies to move the data into Glacier for long-term archiving.
- D. Use Storage Gateway to store data to S3 and use lifecycle policies to move the data into Redshift for long-term archiving.

**Answer:** A

**Explanation:**

Amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. Customers can reliably store large or small amounts of data for as little as \$0.004 per gigabyte per month, a significant savings compared to on-premises solutions.

With Amazon lifecycle policies you can create transition actions in which you define when objects transition to another Amazon S3 storage class.

For example, you may choose to transition objects to the STANDARDIA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.

Option B is invalid because lifecycle policies are not available for EBS volumes

Option C is invalid because IAM policies cannot be used to move data to Glacier

Option D is invalid because lifecycle policies are not used to move data to Redshift

<http://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

**QUESTION 428**

A Security Engineer receives alerts that an Amazon EC2 instance on a public subnet is under an SFTP brute force attack from a specific IP address, which is a known malicious bot.

What should the Security Engineer do to block the malicious bot?

- A. Add a deny rule to the public VPC security group to block the malicious IP
- B. Add the malicious IP to AWS WAF backhosted IPs
- C. Configure Linux iptables or Windows Firewall to block any traffic from the malicious IP
- D. Modify the hosted zone in Amazon Route 53 and create a DNS sinkhole for the malicious IP

**Answer:** D

**QUESTION 429**

A company is planning on using AWS for hosting their applications. They want complete separation and isolation of their production, testing and development environments.

Which of the following is an ideal way to design such a setup?

- A. Use separate VPCs for each of the environments
- B. Use separate IAM Roles for each of the environments
- C. Use separate IAM Policies for each of the environments
- D. Use separate AWS accounts for each of the environments

**Answer:** D

**Explanation:**

A recommendation from the AWS Security Best practices highlights this as well

### Strategies for Using Multiple AWS Accounts

Design your AWS account strategy to maximize security and follow your business and governance requirements. Table 3 discusses possible strategies.

| Business Requirement                                            | Proposed Design    | Comments                                                                                  |
|-----------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------------------|
| Centralized security management                                 | Single AWS account | Centralize information security management and minimize overhead.                         |
| Separation of production, development, and testing environments | Three AWS accounts | Create one AWS account for production services, one for development, and one for testing. |

Option A is partially valid , you can segregate resources , but a best practise is to have multiple accounts for this setup.

Options B and C are invalid because from a maintenance perspective this could become very difficult

For more information on the Security Best practices, please visit the following URL:

Option A is partially valid, you can segregate resources, but a best practise is to have multiple accounts for this setup.

Options B and C are invalid because from a maintenance perspective this could become very difficult

[https://dl.awsstatic.com/whitepapers/Security/AWS\\_Security\\_Best\\_Practices.pdf](https://dl.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf)

### QUESTION 430

You have a requirement to conduct penetration testing on the AWS Cloud for a couple of EC2 Instances.

How could you go about doing this? Choose 2 right answers from the options given below.

- A. Get prior approval from AWS for conducting the test
- B. Use a pre-approved penetration testing tool.
- C. Work with an AWS partner and no need for prior approval request from AWS
- D. Choose any of the AWS instance type

**Answer:** AB

**Explanation:**

You can use a pre-approved solution from the AWS Marketplace.

But till date the AWS Documentation still mentions that you have to get prior approval before conducting a test on the AWS Cloud for EC2 Instances.

Option C and D are invalid because you have to get prior approval first.

AWS Docs Provides following details:

"For performing a penetration test on AWS resources first of all we need to take permission from AWS and

complete a requisition form and submit it for approval. The form should contain information about the instances you wish to test identify the expected start and end dates/times of your test and requires you to read and agree to Terms and Conditions specific to penetration testing and to the

use of appropriate tools for testing. Note that the end date may not be more than 90 days from the start date." ( At this time, our policy does not permit testing small or micro RDS instance types. Testing of ml .small, t1 .micro or t2.nano EC2 instance types is not permitted.

**QUESTION 431**

Your company is hosting a set of EC2 Instances in AWS. They want to have the ability to detect if any port scans occur on their AWS EC2 Instances.  
Which of the following can help in this regard?

- A. Use AWS inspector to consciously inspect the instances for port scans
- B. Use AWS Trusted Advisor to notify of any malicious port scans
- C. Use AWS Config to notify of any malicious port scans
- D. Use AWS Guard Duty to monitor any malicious port scans

**Answer:** D

**Explanation:**

The AWS blogs mention the following to support the use of AWS GuardDuty. GuardDuty voraciously consumes multiple data streams, including several threat intelligence feeds, staying aware of malicious addresses, devious domains, and more importantly, learning to accurately identify malicious or unauthorized behavior in your AWS accounts. In combination with information gleaned from your VPC Flow Logs, AWS CloudTrail Event Logs, and DNS logs, this allows GuardDuty to detect many different types of dangerous and mischievous behavior including probes for known vulnerabilities, port scans and probes, and access from unusual locations. On the AWS side, it looks for suspicious AWS account activity such as unauthorized deployments, unusual CloudTrail activity, patterns of access to AWS API functions, and attempts to exceed multiple service limits. GuardDuty will also look for compromised EC2 instances talking to malicious entities or services, data exfiltration attempts, and instances that are mining cryptocurrency.

Options A, B and C are invalid because these services cannot be used to detect port scans  
<https://aws.amazon.com/blogs/aws/amazon-guardduty-continuous-security-monitoring-threat-detection>

**QUESTION 432**

An application running on EC2 instances processes sensitive information stored on Amazon S3. The information is accessed over the Internet. The security team is concerned that the Internet connectivity to Amazon S3 is a security risk.  
Which solution will resolve the security concern?

- A. Access the data through an Internet Gateway.
- B. Access the data through a VPN connection.
- C. Access the data through a NAT Gateway.
- D. Access the data through a VPC endpoint for Amazon S3

**Answer:** D

**Explanation:**

The AWS Documentation mentions the following: A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network. Option A, B and C are all invalid because the question specifically mentions that access should not be provided via the Internet.

**QUESTION 433**

Your IT Security team has identified a number of vulnerabilities across critical EC2 Instances in the company's AWS Account.

Which would be the easiest way to ensure these vulnerabilities are remediated?

- A. Create AWS Lambda functions to download the updates and patch the servers.
- B. Use AWS CLI commands to download the updates and patch the servers.
- C. Use AWS inspector to patch the servers
- D. Use AWS Systems Manager to patch the servers

**Answer:** D

**Explanation:**

The AWS Documentation mentions the following You can quickly remediate patch and association compliance issues by using Systems Manager Run Command. You can tag either instance IDs or Amazon EC2 tags and execute the AWS-RefreshAssociation document or the AWS-RunPatchBaseline document.

If refreshing the association or re-running the patch baseline fails to resolve the compliance issue, then you need to investigate your associations, patch baselines, or instance configurations to understand why the Run Command executions did not resolve the problem

Options A and B are invalid because even though this is possible, still from a maintenance perspective it would be difficult to maintain the Lambda functions

Option C is invalid because this service cannot be used to patch servers

<https://docs.aws.amazon.com/systems-manager/latest/usereguide/sysman-compliance-fixing.html>

**QUESTION 434**

A company has set up EC2 instances on the AW5 Cloud. There is a need to see all the IP addresses which are accessing the EC2 Instances.

Which service can help achieve this?

- A. Use the AWS Inspector service
- B. Use AWS VPC Flow Logs
- C. Use Network ACL's
- D. Use Security Groups

**Answer:** B

**Explanation:**

The AWS Documentation mentions the following A flow log record represents a network flow in your flow log.

Each record captures the network flow for a specific 5-tuple, for a specific capture window. A 5-tuple is a set of five different values that specify the source, destination, and protocol for an internet protocol (IP) flow.

Options A,C and D are all invalid because these services/tools cannot be used to get the the IP addresses

**QUESTION 435**

A company has an existing AWS account and a set of critical resources hosted in that account.

The employee who was in-charge of the root account has left the company.

What must be now done to secure the account. Choose 3 answers from the options given below.

- A. Change the access keys for all IAM users.
- B. Delete all custom created IAM policies

- C. Delete the access keys for the root account
- D. Confirm MFA to a secure device
- E. Change the password for the root account
- F. Change the password for all IAM users

**Answer:** CDE

**Explanation:**

Now if the root account has a chance to be compromised, then you have to carry out the below steps

- 1. Delete the access keys for the root account
- 2. Confirm MFA to a secure device
- 3. Change the password for the root account

This will ensure the employee who has left has no chance to compromise the resources in AWS.

Option A is invalid because this would hamper the working of the current IAM users

Option B is invalid because this could hamper the current working of services in your AWS account

Option F is invalid because this would hamper the working of the current IAM users

#### QUESTION 436

You want to ensure that you keep a check on the Active EBS Volumes, Active snapshots and Elastic IP addresses you use so that you don't go beyond the service limit. Which of the below services can help in this regard?

- A. AWS Cloudwatch
- B. AWS EC2
- C. AWS Trusted Advisor
- D. AWS SNS

**Answer:** C

**Explanation:**

Below is a snapshot of the service limits that the Trusted Advisor can monitor

| Service                                      | Limits                                                                                                                                                                               |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Amazon Elastic Compute Cloud<br>(Amazon EC2) | Elastic IP addresses (EIPs)<br>Reserved Instances - purchase limit (monthly)                                                                                                         |
| Amazon Elastic Block Store<br>(Amazon EBS)   | Active volumes<br>Active snapshots<br>General Purpose (SSD) volume storage (GiB)<br>Provisioned IOPS<br>Provisioned IOPS (SSD) volume storage (GiB)<br>Magnetic volume storage (GiB) |
| Amazon Kinesis Streams                       | Shards                                                                                                                                                                               |

Option A is invalid because even though you can monitor resources, it cannot be checked against the service limit.

Option B is invalid because this is the Elastic Compute cloud service

Option D is invalid because it can send notifications but not check on service limit

#### QUESTION 437

A company's Security Auditor discovers that users are able to assume roles without using multi-factor authentication (MFA). An example of a current policy being applied to these users is as follows:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Deny",
 "Principal": {
 "AWS": "arn:aws:iam::555555555555:root"
 },
 "Action": "sts:AssumeRole",
 "Condition": {
 "Bool": { "aws:MultiFactorAuthPresent": false}
 }
 }
]
}
```

The Security Auditor finds that the users who are able to assume roles without MFA are also coming from the AWS CLI.

These users are using long-term AWS credentials.

Which changes should a Security Engineer implement to resolve this security issue? (Select TWO.)

A)

```
"Effect": "Deny",
"Condition": { "Bool": { "aws:MultiFactorAuthPresent": false} }
```

B)

```
"Effect": "Allow",
"Condition": { "Bool": { "aws:MultiFactorAuthPresent": true} }
```

C)

```
"Effect": "Allow", "Condition": { "BoolIfExists": { "aws:MultiFactorAuthPresent": true} }
```

D)

```
"Effect": "Deny", "Condition": { "BoolIfExists": { "aws:MultiFactorAuthPresent": false} }
```

E)

```
"Effect": "Deny", "Condition": { "BoolIfNotExist": { "aws:MultiFactorAuthPresent": true} }
```

A. Option A

- B. Option B
- C. Option C
- D. Option D
- E. Option E

**Answer:** AD

**QUESTION 438**

A company has external vendors that must deliver files to the company. These vendors have cross-account that gives them permission to upload objects to one of the company's S3 buckets.

What combination of steps must the vendor follow to successfully deliver a file to the company?  
Select 2 answers from the options given below

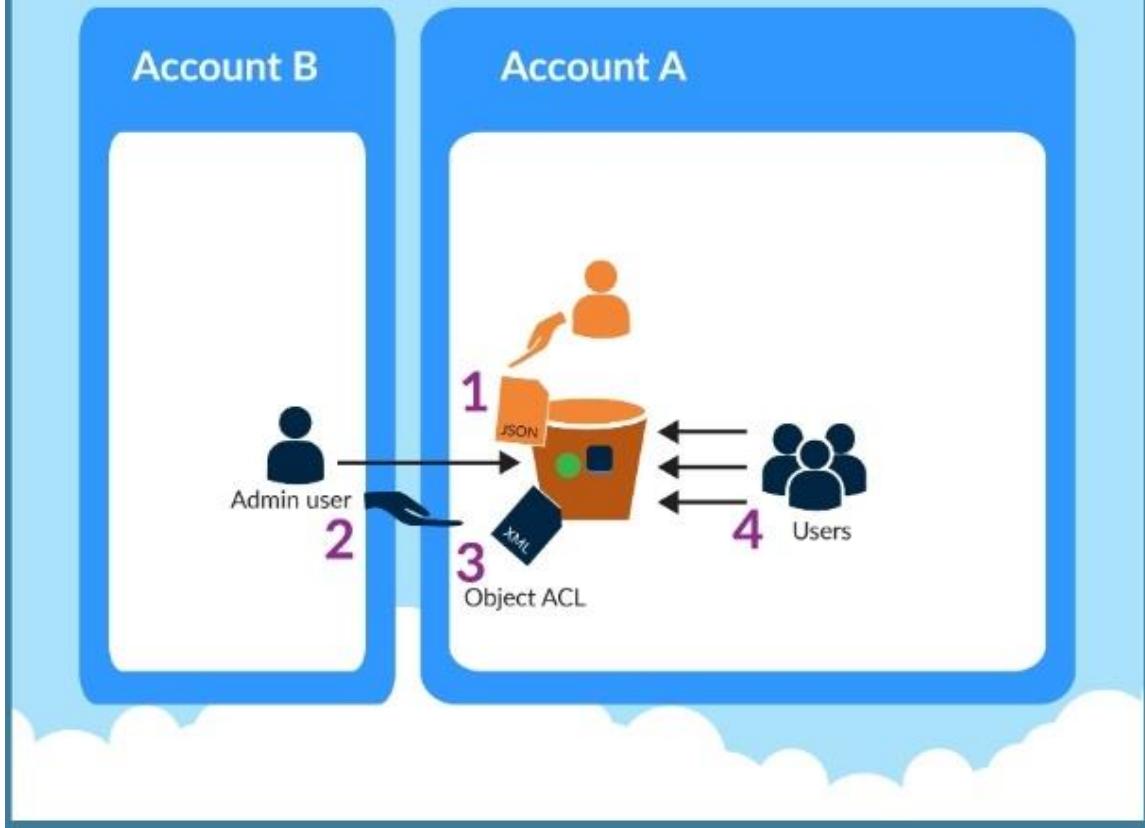
- A. Attach an IAM role to the bucket that grants the bucket owner full permissions to the object
- B. Add a grant to the objects ACL giving full permissions to bucket owner.
- C. Encrypt the object with a KMS key controlled by the company.
- D. Add a bucket policy to the bucket that grants the bucket owner full permissions to the object
- E. Upload the file to the company's S3 bucket

**Answer:** BE

**Explanation:**

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

Bucket Owner Granting Its Users  
Permissions to Objects It Does Not Own



Option A and D are invalid because bucket ACL's are used to give grants to bucket  
 Option C is not required since encryption is not part of the requirement

**QUESTION 439**

A company is deploying an Amazon EC2-based application. The application will include a custom health- checking component that produces health status data in JSON format. A Security Engineer must implement a secure solution to monitor application availability in near-real time by analyzing the hearth status data.

Which approach should the Security Engineer use?

- Use Amazon CloudWatch monitoring to capture Amazon EC2 and networking metrics Visualize metrics using Amazon CloudWatch dashboards.
- Run the Amazon Kinesis Agent to write the status data to Amazon Kinesis Data Firehose Store the streaming data from Kinesis Data Firehose in Amazon Redshift. (hen run a script on the pool data and analyze the data in Amazon Redshift)
- Write the status data directly to a public Amazon S3 bucket from the health-checking component Configure S3 events to invoke an AWS Lambda function that analyzes the data
- Generate events from the health-checking component and send them to Amazon CloudWatch Events.  
 Include the status data as event payloads

Use CloudWatch Events rules to invoke an AWS Lambda function that analyzes the data.

**Answer:** A

**QUESTION 440**

You have a requirement to serve up private content using the keys available with Cloudfront. How can this be achieved?

- A. Add the keys to the backend distribution.
- B. Add the keys to the S3 bucket
- C. Create pre-signed URL's
- D. Use AWS Access keys

**Answer:** C

**Explanation:**

Option A and B are invalid because you will not add keys to either the backend distribution or the S3 bucket.

Option D is invalid because this is used for programmatic access to AWS resources. You can use Cloudfront key pairs to create a trusted pre-signed URL which can be distributed to users Specifying the AWS Accounts

**QUESTION 441**

You have a set of Customer keys created using the AWS KMS service. These keys have been used for around 6 months. You are now trying to use the new KMS features for the existing set of key's but are not able to do so.

What could be the reason for this?

- A. You have not explicitly given access via the key policy
- B. You have not explicitly given access via the IAM policy
- C. You have not given access via the IAM roles
- D. You have not explicitly given access via IAM users

**Answer:** A

**Explanation:**

By default, keys created in KMS are created with the default key policy. When features are added to KMS, you need to explicitly update the default key policy for these keys.

Option B,C and D are invalid because the key policy is the main entity used to provide access to the key.

**QUESTION 442**

You are creating a Lambda function which will be triggered by a Cloudwatch Event. The data from these events needs to be stored in a DynamoDB table.

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

- A. Put the AWS Access keys in the Lambda function since the Lambda function by default is secure
- B. Use an IAM role which has permissions to the DynamoDB table and attach it to the Lambda function.
- C. Use the AWS Access keys which has access to DynamoDB and then place it in an S3 bucket.
- D. Create a VPC endpoint for the DynamoDB table. Access the VPC endpoint from the Lambda function.

**Answer:** B

**Explanation:**

AWS Lambda functions uses roles to interact with other AWS services. So use an IAM role which has permissions to the DynamoDB table and attach it to the Lambda function.

Options A and C are all invalid because you should never use AWS keys for access.

Option D is invalid because the VPC endpoint is used for VPCs

#### **QUESTION 443**

A company has hired a third-party security auditor, and the auditor needs read-only access to all AWS resources and logs of all VPC records and events that have occurred on AWS.

How can the company meet the auditor's requirements without comprising security in the AWS environment? Choose the correct answer from the options below

- A. Create a role that has the required permissions for the auditor.
- B. Create an SNS notification that sends the CloudTrail log files to the auditor's email when CloudTrail delivers the logs to S3, but do not allow the auditor access to the AWS environment.
- C. The company should contact AWS as part of the shared responsibility model, and AWS will grant required access to the third-party auditor.
- D. Enable CloudTrail logging and create an IAM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs.

**Answer:** D

**Explanation:**

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure. CloudTrail provides a history of AWS API calls for your account including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting.

Option A and C are incorrect since Cloudtrail needs to be used as part of the solution

Option B is incorrect since the auditor needs to have access to Cloudtrail

#### **QUESTION 444**

A company has a set of resources defined in AWS. It is mandated that all API calls to the resources be monitored. Also all API calls must be stored for lookup purposes. Any log data greater than 6 months must be archived. Which of the following meets these requirements? Choose 2 answers from the options given below. Each answer forms part of the solution.

- A. Enable CloudTrail logging in all accounts into S3 buckets
- B. Enable CloudTrail logging in all accounts into Amazon Glacier
- C. Ensure a lifecycle policy is defined on the S3 bucket to move the data to EBS volumes after 6 months.
- D. Ensure a lifecycle policy is defined on the S3 bucket to move the data to Amazon Glacier after 6 months.

**Answer:** AD

**Explanation:**

Cloudtrail publishes the trail of API logs to an S3 bucket

Option B is invalid because you cannot put the logs into Glacier from CloudTrail

Option C is invalid because lifecycle policies cannot be used to move data to EBS volumes

#### **QUESTION 445**

Your company has an EC2 Instance hosted in AWS. This EC2 Instance hosts an application. Currently this application is experiencing a number of issues. You need to inspect the network packets to see what the type of error that is occurring.  
Which one of the below steps can help address this issue?

- A. Use the VPC Flow Logs.
- B. Use a network monitoring tool provided by an AWS partner.
- C. Use another instance. Setup a port to "promiscuous mode" and sniff the traffic to analyze the packets. -
- D. Use Cloudwatch metric

**Answer:** B

#### QUESTION 446

A company has multiple Amazon S3 buckets encrypted with customer-managed CMKs Due to regulatory requirements the keys must be rotated every year. The company's Security Engineer has enabled automatic key rotation for the CMKs; however the company wants to verify that the rotation has occurred.

What should the Security Engineer do to accomplish this?

- A. Filter AWS CloudTrail logs for KeyRotaton events
- B. Monitor Amazon CloudWatch Events for any AWS KMS CMK rotation events
- C. Using the AWS CLI. run the aws kms get-key-relation-status operation with the --key-id parameter to check the CMK rotation date
- D. Use Amazon Athena to query AWS CloudTrail logs saved in an S3 bucket to filter Generate New Key events

**Answer:** C

#### QUESTION 447

Your CTO is very worried about the security of your AWS account. How best can you prevent hackers from completely hijacking your account?

- A. Use short but complex password on the root account and any administrators.
- B. Use AWS IAM Geo-Lock and disallow anyone from logging in except for in your city.
- C. Use MFA on all users and accounts, especially on the root account.
- D. Don't write down or remember the root account password after creating the AWS account.

**Answer:** C

**Explanation:**

Multi-factor authentication can add one more layer of security to your AWS account Even when you go to your Security Credentials dashboard one of the items is to enable MFA on your root account

## Security Status

3 out of 5 complete.

- |                                                                                                                     |   |
|---------------------------------------------------------------------------------------------------------------------|---|
|  Delete your root access keys      | ▼ |
|  Activate MFA on your root account | ▼ |
|  Create individual IAM users       | ▼ |
|  Use groups to assign permissions  | ▼ |
|  Apply an IAM password policy      | ▼ |

Option A is invalid because you need to have a good password policy

Option B is invalid because there is no IAM Geo-Lock

Option D is invalid because this is not a recommended practices

**QUESTION 448**

Your company is planning on using bastion hosts for administering the servers in AWS.

Which of the following is the best description of a bastion host from a security perspective?

- A. A Bastion host should be on a private subnet and never a public subnet due to security concerns
- B. A Bastion host sits on the outside of an internal network and is used as a gateway into the private network and is considered the critical strong point of the network
- C. Bastion hosts allow users to log in using RDP or SSH and use that session to SSH into internal network to access private subnet resources.
- D. A Bastion host should maintain extremely tight security and monitoring as it is available to the public

**Answer:** C

**Explanation:**

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.

In AWS, A bastion host is kept on a public subnet. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets.

Options A and B are invalid because the bastion host needs to sit on the public network.

Option D is invalid because bastion hosts are not used for monitoring

<https://docsaws.amazon.com/quickstart/latest/linux-bastion/architecture.html>

**QUESTION 449**

Your company has a set of EC2 Instances that are placed behind an ELB. Some of the applications hosted on these instances communicate via a legacy protocol.

There is a security mandate that all traffic between the client and the EC2 Instances need to be secure.

How would you accomplish this?

- A. Use an Application Load balancer and terminate the SSL connection at the ELB
- B. Use a Classic Load balancer and terminate the SSL connection at the ELB
- C. Use an Application Load balancer and terminate the SSL connection at the EC2 Instances
- D. Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances

**Answer:** D

**Explanation:**

Since there are applications which work on legacy protocols, you need to ensure that the ELB can be used at the network layer as well and hence you should choose the Classic ELB. Since the traffic needs to be secure till the EC2 Instances, the SSL termination should occur on the Ec2 Instances.

Option A and C are invalid because you need to use a Classic Load balancer since this is a legacy application.

Option B is incorrect since encryption is required until the EC2 Instance

## QUESTION 450

You have a set of 100 EC2 Instances in an AWS account. You need to ensure that all of these instances are patched and kept to date. All of the instances are in a private subnet.

How can you achieve this?

Choose 2 answers from the options given below

- A. Ensure a NAT gateway is present to download the updates
- B. Use the Systems Manager to patch the instances
- C. Ensure an internet gateway is present to download the updates
- D. Use the AWS inspector to patch the updates

**Answer:** AB

**Explanation:**

Option C is invalid because the instances need to remain in the private:

Option D is invalid because AWS inspector can only detect the patches

One of the AWS Blogs mentions how patching of Linux servers can be accomplished.

## QUESTION 451

Development teams in your organization use S3 buckets to store the log files for various applications hosted ir development environments in AWS.

The developers want to keep the logs for one month for troubleshooting purposes, and then purge the logs.

What feature will enable this requirement?

- A. Adding a bucket policy on the S3 bucket.
- B. Configuring lifecycle configuration rules on the S3 bucket.
- C. Creating an IAM policy for the S3 bucket.
- D. Enabling CORS on the S3 bucket.

**Answer:** B

**Explanation:**

The AWS Documentation mentions the following on lifecycle policies Lifecycle configuration enables you to specify the lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects. These actions can be classified a?follows:

Transition actions - In which you define when objects transition to another. For example, you may choose to transition objects to the STANDARDIA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.

Expiration actions - In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.

Option A and C are invalid because neither bucket policies neither IAM policy's can control the purging of logs

Option D is invalid CORS is used for accessing objects across domains and not for purging of

logs

**QUESTION 452**

A System Administrator is unable to start an Amazon EC2 instance in the eu-west-1 Region using an IAM role. The same System Administrator is able to start an EC2 instance in the eu-west-2 and eu-west-3 Regions. The AWSSystemAdministrator access policy attached to the System Administrator IAM role allows unconditional access to all AWS services and resources within the account.

Which configuration caused this issue?

- A. An SCP is attached to the account with the following permission statement:
- B. A permission boundary policy is attached to the System Administrator role with the following permission statement:
- C. A permission boundary is attached to the System Administrator role with the following permission statement:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ec2:*"
],
 "Resource": "*"
 }
],
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ec2:*,",
 "Resource": "*",
 "Condition": {
 "StringEquals": {
 "AWS:RequestedRegion": [
 "eu-west-1"
]
 }
 }
 }
]
}
```

- D. An SCP is attached to the account with the following statement:

```

 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "*",
 "Resource": "*"
 },
 {
 "Effect": "Deny",
 "NotAction": [
 "iam::*",
 "organizations::*",
 "route53::*",
 "budgets::*",
 "waf::*",
 "cloudfront::*",
 "globalaccelerator::*",
 "importexport::*",
 "support::*",
 "ec2r::*"
],
 "Resource": "*",
 "Condition": {
 "StringEquals": [
 "aws:RequestedRegion": [
 "eu-west-1"
]
]
 }
 }
]
}

```

- E. Option A
- F. Option B
- G. Option C
- H. Option D

**Answer:** B

#### QUESTION 453

A company has a web-based application using Amazon CloudFront and running on Amazon Elastic Container Service (Amazon ECS) behind an Application Load Balancer (ALB). The ALB is terminating TLS and balancing load across ECS service tasks. A security engineer needs to design a solution to ensure that application content is accessible only through CloudFront and that it is never accessible directly.

How should the security engineer build the MOST secure solution?

- A. Add an origin custom header Set the viewer protocol policy to HTTP and HTTPS  
Set the origin protocol policy to HTTPS only Update the application to validate the CloudFront custom header
- B. Add an origin custom header Set the viewer protocol policy to HTTPS only  
Set the origin protocol policy to match viewer Update the application to validate the CloudFront custom header.
- C. Add an origin custom header Set the viewer protocol policy to redirect HTTP to HTTPS  
Set the origin protocol policy to HTTP only Update the application to validate the CloudFront custom header.
- D. Add an origin custom header Set the viewer protocol policy to redirect HTTP to HTTPS.  
Set the origin protocol policy to HTTPS only Update the application to validate the CloudFront custom header

**Answer:** D

**QUESTION 454**

A customer has an instance hosted in the AWS Public Cloud. The VPC and subnet used to host the Instance have been created with the default settings for the Network Access Control Lists. They need to provide an IT Administrator secure access to the underlying instance. How can this be accomplished.

- A. Ensure the Network Access Control Lists allow Inbound SSH traffic from the IT Administrator's Workstation
- B. Ensure the Network Access Control Lists allow Outbound SSH traffic from the IT Administrator's Workstation
- C. Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation
- D. Ensure that the security group allows Outbound SSH traffic from the IT Administrator's Workstation

**Answer:** C

**Explanation:**

Options A & B are invalid as default NACL rule will allow all inbound and outbound traffic. The requirement is that the IT administrator should be able to access this EC2 instance from his workstation.

For that we need to enable the Security Group of EC2 instance to allow traffic from the IT administrator's workstation.

Hence option C is correct. Option D is incorrect as we need to enable the Inbound SSH traffic on the EC2 instance Security Group since the traffic originate' , from the IT admin's workstation.

**QUESTION 455**

You want to launch an EC2 Instance with your own key pair in AWS. How can you achieve this? Choose 3 answers from the options given below.

- A. Use a third party tool to create the Key pair
- B. Create a new key pair using the AWS CLI
- C. Import the public key into EC2
- D. Import the private key into EC2

**Answer:** ABC

**Explanation:**

This is given in the AWS Documentation Creating a Key Pair You can use Amazon EC2 to create your key pair. For more information, see Creating a Key Pair Using Amazon EC2.

Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. For more information, see Importing Your Own Public Key to Amazon EC2.

Option B is Correct, because you can use the AWS CLI to create a new key pair 1

<https://docs.aws.amazon.com/cli/latest/userguide/cli-ec2-keypairs.html>

Option D is invalid because the public key needs to be stored in the EC2 Instance

**QUESTION 456**

A Security Engineer has been tasked with enabling AWS Security Hub to monitor Amazon EC2 instances fix CVE in a single AWS account The Engineer has already enabled AWS Security Hub and Amazon Inspector in the AWS Management Console and has installed the Amazon Inspector agent on an EC2 instances that need to be monitored.

Which additional steps should the Security Engineer take to meet this requirement?

- A. Configure the Amazon inspector agent to use the CVE rule package
- B. Configure the Amazon Inspector agent to use the CVE rule package Configure Security Hub to ingest from AWS inspector by writing a custom resource policy
- C. Configure the Security Hub agent to use the CVE rule package Configure AWS Inspector to ingest from Security Hub by writing a custom resource policy
- D. Configure the Amazon Inspector agent to use the CVE rule package Install an additional Integration library Allow the Amazon Inspector agent to communicate with Security Hub

**Answer:** D

#### **QUESTION 457**

When managing permissions for the API gateway, what can be used to ensure that the right level of permissions are given to developers, IT admins and users? These permissions should be easily managed.

- A. Use the secure token service to manage the permissions for the different users
- B. Use IAM Policies to create different policies for the different types of users.
- C. Use the AWS Config tool to manage the permissions for the different users
- D. Use IAM Access Keys to create sets of keys for the different types of users.

**Answer:** B

**Explanation:**

The AWS Documentation mentions the following You control access to Amazon API Gateway with IAM permissions by controlling access to the following two API Gateway component processes:

- \* To create, deploy, and manage an API in API Gateway, you must grant the API developer permissions to perform the required actions supported by the API management component of API Gateway.
  - \* To call a deployed API or to refresh the API caching, you must grant the API caller permissions to perform required IAM actions supported by the API execution component of API Gateway.
- Option A, C and D are invalid because these cannot be used to control access to AWS services. This needs to be done via policies.

<https://docs.aws.amazon.com/apisateway/latest/developerguide/permissions.html>

#### **QUESTION 458**

You have an EBS volume attached to an EC2 Instance which uses KMS for Encryption. Someone has now gone ahead and deleted the Customer Key which was used for the EBS encryption.

What should be done to ensure the data can be decrypted.

- A. Create a new Customer Key using KMS and attach it to the existing volume
- B. You cannot decrypt the data that was encrypted under the CMK, and the data is not recoverable.
- C. Request AWS Support to recover the key
- D. Use AWS Config to recover the key

**Answer:** B

#### **QUESTION 459**

Your company has been using AWS for the past 2 years. They have separate S3 buckets for logging the various AWS services that have been used. They have hired an external vendor for analyzing their log files. They have their own AWS account.

What is the best way to ensure that the partner account can access the log files in the company account for analysis? Choose 2 answers from the options given below

- A. Create an IAM user in the company account
- B. Create an IAM Role in the company account
- C. Ensure the IAM user has access for read-only to the S3 buckets
- D. Ensure the IAM Role has access for read-only to the S3 buckets

**Answer:** BD

**Explanation:**

The AWS Documentation mentions the following

To share log files between multiple AWS accounts, you must perform the following general steps. These steps are explained in detail later in this section. Create an IAM role for each account that you want to share log files with.

For each of these IAM roles, create an access policy that grants read-only access to the account you want to share the log files with.

Have an IAM user in each account programmatically assume the appropriate role and retrieve the log files.

Options A and C are invalid because creating an IAM user and then sharing the IAM user credentials with the vendor is a direct 'NO' practise from a security perspective.

#### QUESTION 460

A company has two AW5 accounts within AWS Organizations. In Account-1. Amazon EC2 Auto Scaling is launched using a service-linked role. In Account-2. Amazon EBS volumes are encrypted with an AWS KMS key A Security Engineer needs to ensure that the service- linked role can launch instances with these encrypted volumes.

Which combination of steps should the Security Engineer take in both accounts? (Select TWO.)

- A. Allow Account-1 to access the KMS key in Account-2 using a key policy
- B. Attach an IAM policy to the service-linked role in Account-1 that allows these actions CreateGrant, DescnbeKey, Encrypt, GenerateDataKey, Decrypt, and ReEncrypt
- C. Create a KMS grant for the service-linked role with these actions CreateGrant, DescnbeKey Encrypt GenerateDataKey Decrypt, and ReEncrypt
- D. Attach an IAM policy to the role attached to the EC2 instances with KMS actions and then allow Account-1 in the KMS key policy.
- E. Attach an IAM policy to the user who is launching EC2 instances and allow the user to access the KMS key policy of Account-2.

**Answer:** CD

#### QUESTION 461

Your team is experimenting with the API gateway service for an application. There is a need to implement a custom module which can be used for authentication/authorization for calls made to the API gateway.

How can this be achieved?

- A. Use the request parameters for authorization
- B. Use a Lambda authorizer
- C. Use the gateway authorizer
- D. Use CORS on the API gateway

**Answer:** B

**Explanation:**

The AWS Documentation mentions the following An Amazon API Gateway Lambda authorizer (formerly known as a custom authorize?) is a Lambda function that you provide to control access to your API methods. A Lambda authorizer uses bearer token authentication strategies, such as OAuth or SAML. It can also use information described by headers, paths, query strings, stage variables, or context variables request parameters.

Options A,C and D are invalid because these cannot be used if you need a custom authentication/authorization for calls made to the API gateway

**QUESTION 462**

Your company has a requirement to work with a DynamoDB table. There is a security mandate that all data should be encrypted at rest.

What is the easiest way to accomplish this for DynamoDB?

- A. Use the AWS SDK to encrypt the data before sending it to the DynamoDB table
- B. Encrypt the DynamoDB table using KMS during its creation
- C. Encrypt the table using AWS KMS after it is created
- D. Use S3 buckets to encrypt the data before sending it to DynamoDB

**Answer:** B

**Explanation:**

The most easiest option is to enable encryption when the DynamoDB table is created.

The AWS Documentation mentions the following

Amazon DynamoDB offers fully managed encryption at rest. DynamoDB encryption at rest provides enhanced security by encrypting your data at rest using an AWS Key Management Service (AWS KMS) managed encryption key for DynamoDB. This functionality eliminates the operational burden and complexity involved in protecting sensitive data.

Option A is partially correct, you can use the AWS SDK to encrypt the data, but the easier option would be to encrypt the table before hand.

Option C is invalid because you cannot encrypt the table after it is created

Option D is invalid because encryption for S3 buckets is for the objects in S3 only

**QUESTION 463**

A company has resources hosted in their AWS Account. There is a requirement to monitor all API activity for all regions. The audit needs to be applied for future regions as well.

Which of the following can be used to fulfil this requirement?

- A. Ensure Cloudtrail for each region. Then enable for each future region.
- B. Ensure one Cloudtrail trail is enabled for all regions.
- C. Create a Cloudtrail for each region. Use Cloudformation to enable the trail for all future regions.
- D. Create a Cloudtrail for each region. Use AWS Config to enable the trail for all future regions.

**Answer:** B

**Explanation:**

The AWS Documentation mentions the following You can now turn on a trail across all regions for your AWS account. CloudTrail will deliver log files from all regions to the Amazon S3 bucket and an optional CloudWatch Logs log group you specified. Additionally, when AWS launches a new region, CloudTrail will create the same trail in the new region. As a result you will receive log files containing API activity for the new region without taking any action.

Option A and C is invalid because this would be a maintenance overhead to enable clouptrail for every region

Option D is invalid because this AWS Config cannot be used to enable trails

<https://aws.amazon.com/about-aws/whats-new/2015/12/turn-on-cloudtrail-across-all-regions-and-support-for-multiple-trails>

**QUESTION 464**

A company has several Customer Master Keys (CMK), some of which have imported key material. Each CMK must be rotated annually.

What two methods can the security team use to rotate each key? Select 2 answers from the options given below

- A. Enable automatic key rotation for a CMK
- B. Import new key material to an existing CMK
- C. Use the CLI or console to explicitly rotate an existing CMK
- D. Import new key material to a new CMK; Point the key alias to the new CMK.
- E. Delete an existing CMK and a new default CMK will be created.

**Answer:** AD

**Explanation:**

The AWS Documentation mentions the following Automatic key rotation is available for all customer managed CMKs with KMS-generated key material. It is not available for CMKs that have imported key material (the value of the Origin field is External), but you can rotate these CMKs manually.

Rotating Keys Manually

You might want to create a new CMK and use it in place of a current CMK instead of enabling automatic key rotation. When the new CMK has different cryptographic material than the current CMK, using the new CMK has the same effect as changing the backing key in an existing CMK. The process of replacing one CMK with another is known as manual key rotation.

When you begin using the new CMK, be sure to keep the original CMK enabled so that AWS KMS can decrypt data that the original CMK encrypted. When decrypting data, KMS identifies the CMK that was used to encrypt the data, and it uses the same CMK to decrypt the data. As long as you keep both the original and new CMKs enabled, AWS KMS can decrypt any data that was encrypted by either CMK.

Option B is invalid because you also need to point the key alias to the new key

Option C is invalid because existing CMK keys cannot be rotated as they are

Option E is invalid because deleting existing keys will not guarantee the creation of a new default CMK key

<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>

**QUESTION 465**

The CFO of a company wants to allow one of his employees to view only the AWS usage report page.

Which of the below mentioned IAM policy statements allows the user to have access to the AWS usage report page?

- A. "Effect": "Allow", "Action": ["Describe"], "Resource": "Billing"
- B. "Effect": "Allow", "Action": ["AccountUsage"], "Resource": "\*"
- C. "Effect": "Allow", "Action": ["aws-portal:ViewUsage", "aws-portal:ViewBilling"], "Resource": "\*"
- D. "Effect": "Allow", "Action": ["aws-portal:ViewBilling"], "Resource": "\*"

**Answer:** C

**Explanation:**

the AWS documentation, below is the access required for a user to access the Usage reports page

and as per this, Option C is the right answer.

**Example 2: Allow IAM users to access the Reports console page**

To allow an IAM user to access the **Reports** console page and to view the usage reports that contain account activity information, you would use a policy similar to this example policy.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "aws-portal:ViewUsage",
 "aws-portal:ViewBilling"
],
 "Resource": "*"
 }
]
}
```

**QUESTION 466**

You currently have an S3 bucket hosted in an AWS Account. It holds information that needs be accessed by a partner account.

Which is the MOST secure way to allow the partner account to access the S3 bucket in your account? Select 3 options.

- A. Ensure an IAM role is created which can be assumed by the partner account.
- B. Ensure an IAM user is created which can be assumed by the partner account.
- C. Ensure the partner uses an external id when making the request
- D. Provide the ARN for the role to the partner account
- E. Provide the Account Id to the partner account
- F. Provide access keys for your account to the partner account

**Answer:** ACD

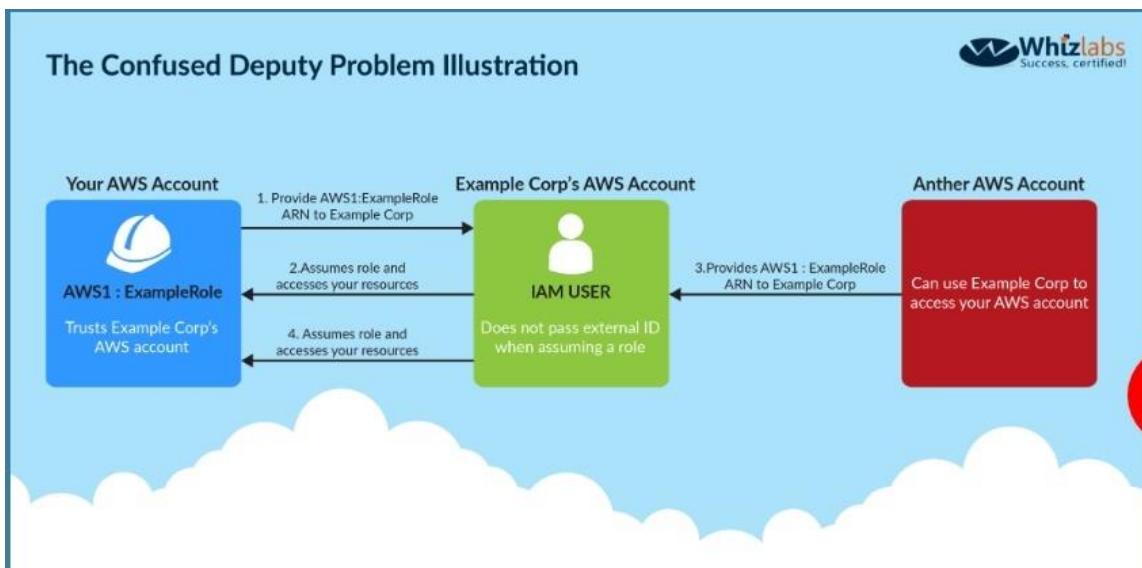
**Explanation:**

Option B is invalid because Roles are assumed and not IAM users

Option E is invalid because you should not give the account ID to the partner

Option F is invalid because you should not give the access keys to the partner

The below diagram from the AWS documentation showcases an example on this wherein an IAM role and external ID is used to access an AWS account resources



#### QUESTION 467

You work as an administrator for a company. The company hosts a number of resources using AWS. There is an incident of a suspicious API activity which occurred 11 days ago. The Security Admin has asked to get the API activity from that point in time. How can this be achieved?

- A. Search the Cloud Watch logs to find for the suspicious activity which occurred 11 days ago
- B. Search the Cloudtrail event history on the API events which occurred 11 days ago.
- C. Search the Cloud Watch metrics to find for the suspicious activity which occurred 11 days ago
- D. Use AWS Config to get the API calls which were made 11 days ago.

**Answer:** B

**Explanation:**

The Cloud Trail event history allows to view events which are recorded for 90 days. So one can use a metric filter to gather the API calls from 11 days ago. Option A and C is invalid because Cloudwatch is used for logging and not for monitoring API activity

Option D is invalid because AWSConfig is a configuration service and not for monitoring API activity

In this question we assume that the customer has enabled cloud trail service. AWS CloudTrail is enabled by default for ALL CUSTOMERS and will provide visibility into the past seven days of account activity without the need for you to configure a trail in the service to get started. So for an activity that happened 11 days ago to be stored in the cloud trail we need to configure the trail manually to ensure that it is stored in the events history.

#### QUESTION 468

Your application currently use AWS Cognito for authenticating users. Your application consists of different types of users. Some users are only allowed read access to the application and others are given contributor access. How would you manage the access effectively?

- A. Create different cognito endpoints, one for the readers and the other for the contributors.
- B. Create different cognito groups, one for the readers and the other for the contributors.
- C. You need to manage this within the application itself
- D. This needs to be managed via Web security tokens

**Answer:** B

**Explanation:**

The AWS Documentation mentions the following You can use groups to create a collection of users in a user pool, which is often done to set the permissions for those users. For example, you can create separate groups for users who are readers, contributors, and editors of your website and app. Option A is incorrect since you need to create cognito groups and not endpoints Options C and D are incorrect since these would be overheads when you can use AWS Cognito  
<https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-user-groups.html>

## QUESTION 469

There is a requirement for a company to transfer large amounts of data between AWS and an on-premise location. There is an additional requirement for low latency and high consistency traffic to AWS.

Given these requirements how would you design a hybrid architecture? Choose the correct answer from the options below

- A. Provision a Direct Connect connection to an AWS region using a Direct Connect partner.
- B. Create a VPN tunnel for private connectivity, which increases network consistency and reduces latency.
- C. Create an iPSec tunnel for private connectivity, which increases network consistency and reduces latency.
- D. Create a VPC peering connection between AWS and the Customer gateway.

**Answer:** A

**Explanation:**

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect you can establish private connectivity between AWS and your datacenter, office, or colocation environment which in many cases can reduce your network costs, increase bandwidth throughput and provide a more consistent network experience than Internet-based connections.

Options B and C are invalid because these options will not reduce network latency

Options D is invalid because this is only used to connect 2 VPC's

## QUESTION 470

One of your company's EC2 Instances have been compromised. The company has strict policy for thorough investigation on finding the culprit for the security breach.

What would you do in from the options given below.

- A. Take a snapshot of the EBS volume
- B. Isolate the machine from the network
- C. Make sure that logs are stored securely for auditing and troubleshooting purpose
- D. Ensure all passwords for all IAM users are changed
- E. Ensure that all access keys are rotated.

**Answer:** ABC

## QUESTION 471

Your team is designing a web application. The users for this web application would need to sign in via an external ID provider such as Facebook or Google.

Which of the following AWS service would you use for authentication?

- A. AWS Cognito
- B. AWS SAML
- C. AWS IAM
- D. AWS Config

**Answer:** A

**Explanation:**

The AWS Documentation mentions the following Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps. Your users can sign in directly with a user name and password, or through a third party such as Facebook, Amazon, or Google. Option B is incorrect since this is used for identity federation Option C is incorrect since this is pure Identity and Access management

Option D is incorrect since AWS is a configuration service

#### **QUESTION 472**

You have setup a set of applications across 2 VPC's. You have also setup VPC Peering. The applications are still not able to communicate across the Peering connection.

Which network troubleshooting steps should be taken to resolve the issue?

- A. Ensure the applications are hosted in a public subnet
- B. Check to see if the VPC has an Internet gateway attached.
- C. Check to see if the VPC has a NAT gateway attached.
- D. Check the Route tables for the VPC's

**Answer:** D

**Explanation:**

After the VPC peering connection is established, you need to ensure that the route tables are modified to ensure traffic can between the VPCs

Option A ,B and C are invalid because allowing access the Internet gateway and usage of public subnets can help for Inter, access, but not for VPC Peering.

#### **QUESTION 473**

Which of the following bucket policies will ensure that objects being uploaded to a bucket called 'demo' are encrypted.

- A. "Version":"2012-10-17",  
"Id":"PutObj",  
"Statement":[{  
"Sid":"DenyUploads",  
"Effect":"Deny",  
"Principal":"\*",  
"Action":"s3:PutObject",  
"Resource":"arn:aws:s3:::demo/\*",  
"Condition":{  
"StringNotEquals":{  
"s3:x-amz-server-side-encryption":"aws:kms"  
}  
}  
}  
]  
}
- B. "Version":"2012-10-17",  
"Id":"PutObj",  
"Statement":[{  
"Sid":"DenyUploads",  
"Effect":"Deny",  
"Principal":"\*",  
"Action":"s3:PutObject",  
"Resource":"arn:aws:s3:::demo/\*",  
"Condition":{  
"StringEquals":{  
"s3:x-amz-server-side-encryption":"aws:kms"  
}  
}  
}  
]  
}
- C. "Version":"2012-10-17",  
"Id":"PutObj",  
"Statement":[{  
"Sid":"DenyUploads",  
"Effect":"Deny",  
"Principal":"\*",  
"Action":"s3:PutObject",  
"Resource":"arn:aws:s3:::demo/\*"  
}  
]  
}

D. "Version":"2012-10-17",  
"Id":"PutObj",  
"Statement":[(  
"Sid":"DenyUploads",  
"Effect":"Deny",  
"Principal":"\*",  
"Action":"s3:PutObjectEncrypted",  
"Resource":"arn:aws:s3:::demo/\*"  
)  
)  
]  
)

**Answer:** A

**Explanation:**

The condition of "s3:x-amz-server-side-encryption":"aws:kms" ensures that objects uploaded need to be encrypted.

Options B,C and D are invalid because you have to ensure the condition of ns3:x-amz- server-side- encryption":"aws:kms" is present

#### QUESTION 474

You have been given a new brief from your supervisor for a client who needs a web application set up on AWS. The most important requirement is that MySQL must be used as the database, and this database must not be hosted in the public cloud, but rather at the client's data center due to security risks.

Which of the following solutions would be the best to assure that the client's requirements are met? Choose the correct answer from the options below

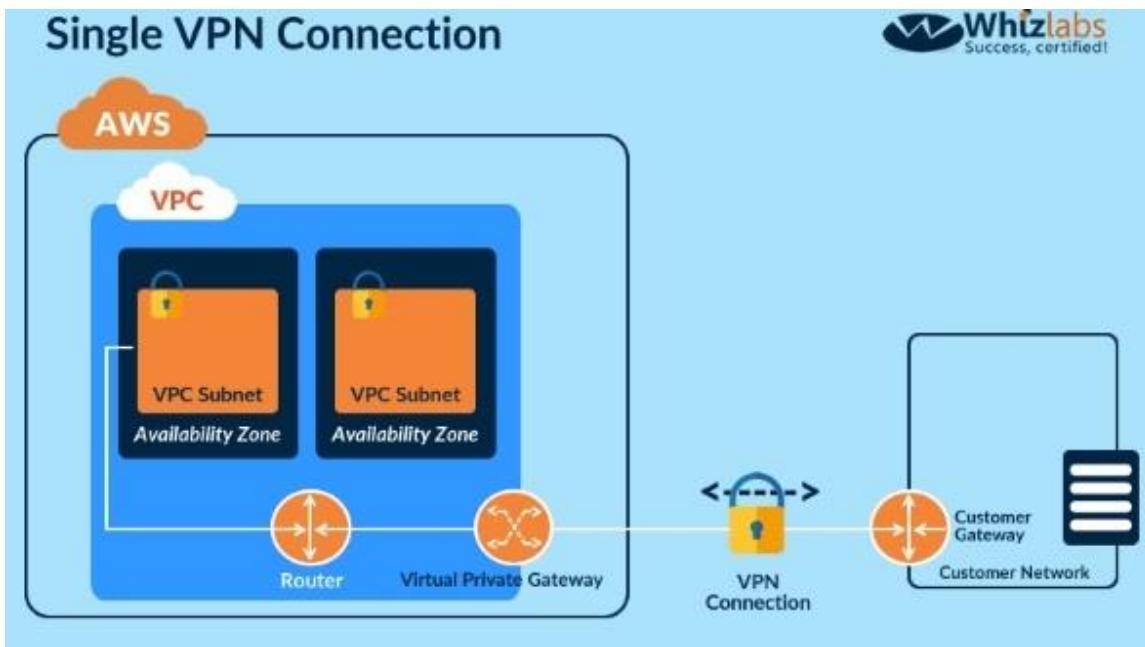
- A. Build the application server on a public subnet and the database at the client's data center. Connect them with a VPN connection which uses IPsec.
- B. Use the public subnet for the application server and use RDS with a storage gateway to access and synchronize the data securely from the local data center.
- C. Build the application server on a public subnet and the database on a private subnet with a NAT instance between them.
- D. Build the application server on a public subnet and build the database in a private subnet with a secure ssh connection to the private subnet from the client's data center.

**Answer:** A

**Explanation:**

Since the database should not be hosted on the cloud all other options are invalid.

The best option is to create a VPN connection for securing traffic as shown below.



Option B is invalid because this is the incorrect use of the Storage gateway

Option C is invalid since this is the incorrect use of the NAT instance

Option D is invalid since this is an incorrect configuration

#### QUESTION 475

Your organization is preparing for a security assessment of your use of AWS. In preparation for this assessment, which three IAM best practices should you consider implementing?

- Create individual IAM users
- Configure MFA on the root account and for privileged IAM users
- Assign IAM users and groups configured with policies granting least privilege access
- Ensure all users have been assigned and are frequently rotating a password, access ID/secret key, and X.509 certificate

**Answer:** ABC

**Explanation:**

When you go to the security dashboard, the security status will show the best practices for initiating the first level of security.

| Security Status                       |                                   | 2 out of 5 complete. |
|---------------------------------------|-----------------------------------|----------------------|
| <span style="color: orange;">⚠</span> | Delete your root access keys      | ▼                    |
| <span style="color: orange;">⚠</span> | Activate MFA on your root account | ▼                    |
| <span style="color: green;">✓</span>  | Create individual IAM users       | ▼                    |
| <span style="color: green;">✓</span>  | Use groups to assign permissions  | ▼                    |
| <span style="color: orange;">⚠</span> | Apply an IAM password policy      | ▼                    |

Option D is invalid because as per the dashboard, this is not part of the security recommendation

### QUESTION 476

Your company uses AWS to host its resources. They have the following requirements

- 1) Record all API calls and Transitions
- 2) Help in understanding what resources are there in the account
- 3) Facility to allow auditing credentials and logins

Which services would suffice the above requirements?

- A. AWS Inspector, CloudTrail, IAM Credential Reports
- B. CloudTrail, IAM Credential Reports, AWS SNS
- C. CloudTrail, AWS Config, IAM Credential Reports
- D. AWS SQS, IAM Credential Reports, CloudTrail

**Answer:** C

**Explanation:**

You can use AWS CloudTrail to get a history of AWS API calls and related events for your account. This history includes calls made with the AWS Management Console, AWS Command Line Interface, AWS SDKs, and other AWS services.

Options A,B and D are invalid because you need to ensure that you use the services of CloudTrail, AWS Config, IAM Credential Reports.

### QUESTION 477

You have several S3 buckets defined in your AWS account. You need to give access to external AWS accounts to these S3 buckets.

Which of the following can allow you to define the permissions for the external accounts? Choose 2 answers from the options given below

- A. IAM policies
- B. Buckets ACL's
- C. IAM users
- D. Bucket policies

**Answer:** BD

**Explanation:**

The AWS Security whitepaper gives the type of access control and to what level the control can be given

| Type of Access Control | AWS Account-Level Control? | User-Level Control? |
|------------------------|----------------------------|---------------------|
| IAM Policies           | No                         | Yes                 |
| ACLs                   | Yes                        | No                  |
| Bucket Policies        | Yes                        | Yes                 |

Options A and C are incorrect since for external access to buckets.

**QUESTION 478**

Your CTO thinks your AWS account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated AWS engineers and doing everything they can to cover their tracks?

- A. Use CloudTrail Log File Integrity Validation.
- B. Use AWS Config SNS Subscriptions and process events in real time.
- C. Use CloudTrail backed up to AWS S3 and Glacier.
- D. Use AWS Config Timeline forensics.

**Answer:** A

**Explanation:**

The AWS Documentation mentions the following To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log file integrity validation. This feature is

built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing.

This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.

You can use the AWS CLI to validate the files in the location where CloudTrail delivered them Validated log files are invaluable in security and forensic investigations.

For example, a validated log file enables you to assert positively that the log file itself has not changed, or that particular user credentials performed specific API activity. The CloudTrail log file integrity validation process also lets you know if a log file has been deleted or changed, or assert positively that no log files were delivered to your account during a given period of time.

Options B.C and D is invalid because you need to check for log File Integrity Validation for cloudtrail logs.

**QUESTION 479**

A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The public subnet uses CIDR 20.0.1.0/24. The user is planning to host a web server in the public subnet with port 80 and a Database server in the private subnet with port 3306. The user is configuring a security group for the public subnet (WebSecGrp) and the private subnet (DBSecGrp). which of the below mentioned entries is required in the private subnet database security group DBSecGrp?

- A. Allow Inbound on port 3306 for Source Web Server Security Group WebSecGrp.
- B. Allow Inbound on port 3306 from source 20.0.0.0/16
- C. Allow Outbound on port 3306 for Destination Web Server Security Group WebSecGrp.
- D. Allow Outbound on port 80 for Destination NAT Instance IP

**Answer:** A

**Explanation:**

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

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

Option B is invalid because you need to allow incoming access for the database server from the WebSecGrp security group.

Options C and D are invalid because you need to allow Outbound traffic and not inbound traffic.

#### QUESTION 480

A company is planning on using AWS EC2 and AWS Cloudfront for their web application. For which one of the below attacks is usage of Cloudfront most suited for?

- A. Cross side scripting
- B. SQL injection
- C. DDoS attacks
- D. Malware attacks

**Answer:** C

**Explanation:**

The below table from AWS shows the security capabilities of AWS Cloudfront. AWS Cloudfront is more prominent for DDoS attacks.

| Table 2: Overview of CloudFront security capabilities |                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Vulnerability                                         | CloudFront Security Capabilities                                                                                                                                                                                                                                                                                                                                   |
| <b>Cryptographic attacks</b>                          | CloudFront frequently reviews the latest security standards and supports only viewer requests using SSL v3 and TLS v1.0, 1.1, and 1.2. When available, TLS v1.3 will also be supported.<br><br>CloudFront supports the strongest ciphers (ECDHE, RSA-AES128, GCM-SHA256) and offers them to the client in preferential sequence. Export ciphers are not supported. |
| <b>Patching</b>                                       | Dedicated teams are responsible for monitoring the threat landscape, handling security events, and patching software. Under the shared security model, AWS will take the necessary measures to remediate vulnerabilities with methods such as patching, deprecation, and revocation.                                                                               |
| <b>DDoS attacks</b>                                   | CloudFront has extensive mitigation techniques for standard flood-type attacks against SSL. To thwart SSL renegotiation-type attacks, CloudFront disables renegotiation.                                                                                                                                                                                           |

Options A, B and D are invalid because Cloudfront is specifically used to protect sites against DDoS attacks.

**QUESTION 481**

A Devops team is currently looking at the security aspect of their CI/CD pipeline. They are making use of AWS resource? for their infrastructure. They want to ensure that the EC2 Instances don't have any high security vulnerabilities. They want to ensure a complete DevSecOps process. How can this be achieved?

- A. Use AWS Config to check the state of the EC2 instance for any sort of security issues.
- B. Use AWS Inspector API's in the pipeline for the EC2 Instances
- C. Use AWS Trusted Advisor API's in the pipeline for the EC2 Instances
- D. Use AWS Security Groups to ensure no vulnerabilities are present

**Answer:** B

**Explanation:**

Amazon Inspector offers a programmatic way to find security defects or misconfigurations in your operating systems and applications. Because you can use API calls to access both the processing of assessments and the results of your assessments, integration of the findings into workflow and notification systems is simple. DevOps teams can integrate Amazon Inspector into their CI/CD pipelines and use it to identify any pre-existing issues or when new issues are introduced.

Option A.C and D are all incorrect since these services cannot check for Security Vulnerabilities. These can only be checked by the AWS Inspector service.

**QUESTION 482**

An application is designed to run on an EC2 Instance. The applications needs to work with an S3 bucket. From a security perspective , what is the ideal way for the EC2 instance/ application to be configured?

- A. Use the AWS access keys ensuring that they are frequently rotated.
- B. Assign an IAM user to the application that has specific access to only that S3 bucket
- C. Assign an IAM Role and assign it to the EC2 Instance
- D. Assign an IAM group and assign it to the EC2 Instance

**Answer:** C

**Explanation:**

The below diagram from the AWS whitepaper shows the best security practice of allocating a role that has access to the S3 bucket

## How Roles for EC2 Work

### AWS Account

1. Admin creates role that grants read access to *photos* bucket



Role : Get-pics



Amazon S3 bucket : photos

2. Developer launches an instance with the role



Photo app

Amazon EC2 instance

3. App retrieves role credentials from the instance

4. App gets photos by using the role credentials

Options A,B and D are invalid because using users, groups or access keys is an invalid security practise when giving access to resources from other AWS resources.

### QUESTION 483

A web application runs in a VPC on EC2 instances behind an ELB Application Load Balancer. The application stores data in an RDS MySQL DB instance. A Linux bastion host is used to apply schema updates to the database - administrators connect to the host via SSH from a corporate workstation. The following security groups are applied to the infrastructure-

- \* sgLB - associated with the ELB
- \* sgWeb - associated with the EC2 instances.
- \* sgDB - associated with the database
- \* sgBastion - associated with the bastion host

Which security group configuration will allow the application to be secure and functional?

- A. sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from 0.0.0.0/0 sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range
- B. sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB sgDB :allow port 3306 traffic from sgWeb and sgLB sgBastion: allow port 22 traffic from the VPC IP address range
- C. sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the VPC IP address range
- D. sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range

**Answer:** D

**Explanation:**

The Load Balancer should accept traffic on port 80 and 443 traffic from 0.0.0.0/0

The backend EC2 Instances should accept traffic from the Load Balancer

The database should allow traffic from the Web server

And the Bastion host should only allow traffic from a specific corporate IP address range Option A is incorrect because the Web group should only allow traffic from the Load balancer  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.html>

**QUESTION 484**

A company hosts multiple externally facing applications, each isolated in its own AWS account. The company's Security team has enabled AWS WAF, AWS Config, and Amazon GuardDuty on all accounts. The company's Operations team has also joined all of the accounts to AWS Organizations and established centralized logging for CloudTrail, AWS Config, and GuardDuty. The company wants the Security team to take a reactive remediation in one account, and automate implementing this remediation as proactive prevention in all the other accounts. How should the Security team accomplish this?

- A. Update the AWS WAF rules in the affected account and use AWS Firewall Manager to push updated AWS WAF rules across all other accounts.
- B. Use GuardDuty centralized logging and Amazon SNS to set up alerts to notify all application teams of security incidents.
- C. Use GuardDuty alerts to write an AWS Lambda function that updates all accounts by adding additional NACLs on the Amazon EC2 instances to block known malicious IP addresses.
- D. Use AWS Shield Advanced to identify threats in each individual account and then apply the account-based protections to all other accounts through Organizations.

**Answer:** C

**QUESTION 485**

Company policy requires that all insecure server protocols, such as FTP, Telnet, HTTP, etc be disabled on all servers. The security team would like to regularly check all servers to ensure compliance with this requirement by using a scheduled CloudWatch event to trigger a review of the current infrastructure.

What process will check compliance of the company's EC2 instances?

- A. Trigger an AWS Config Rules evaluation of the restricted-common-ports rule against every EC2 instance.
- B. Query the Trusted Advisor API for all best practice security checks and check for "action recommended" status.
- C. Enable a GuardDuty threat detection analysis targeting the port configuration on every EC2 instance.
- D. Run an Amazon Inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.

**Answer:** D

**Explanation:**

Option B is incorrect because querying Trusted Advisor API's are not possible. Option C is incorrect because GuardDuty should be used to detect threats and not check the compliance of security protocols.

Option D states that Run Amazon Inspector using runtime behavior analysis rules which will analyze the behavior of your instances during an assessment run, and provide guidance about how to make your EC2 instances more secure.

**Insecure Server Protocols**

This rule helps determine whether your EC2 instances allow support for insecure and unencrypted ports/ services such as FTP, Telnet, HTTP, IMAP, POP version 3, SMTP, SNMP versions 1 and 2, rsh, and rlogin.

[https://docs.aws.amazon.com/mspector/latest/userguide/inspector\\_runtime-behavior-](https://docs.aws.amazon.com/mspector/latest/userguide/inspector_runtime-behavior-)

analysis.html#insecure-protocols

#### QUESTION 486

Your development team is using access keys to develop an application that has access to S3 and DynamoDB. A new security policy has outlined that the credentials should not be older than 2 months, and should be rotated. How can you achieve this?

- A. Use the application to rotate the keys in every 2 months via the SDK
- B. Use a script to query the creation date of the keys. If older than 2 months, create new access key and update all applications to use it deactivate the old key and delete it.
- C. Delete the user associated with the keys after every 2 months. Then recreate the user again.
- D. Delete the IAM Role associated with the keys after every 2 months. Then recreate the IAM Role again.

**Answer:** B

**Explanation:**

One can use the CLI command list-access-keys to get the access keys. This command also returns the "CreateDate" of the keys. If the CreateDate is older than 2 months, then the keys can be deleted.

The Returns list-access-keys CLI command returns information about the access key IDs associated with the specified IAM user. If there are none, the action returns an empty list

Option A is incorrect because you might as well use a script for such maintenance activities

Option C is incorrect because you would not rotate the users themselves

Option D is incorrect because you don't use IAM roles for such a purpose

#### QUESTION 487

A security engineer must ensure that all infrastructure launched in the company AWS account be monitored for deviation from compliance rules, specifically that all EC2 instances are launched from one of a specified list of AMIs and that all attached EBS volumes are encrypted.

Infrastructure not in compliance should be terminated. What combination of steps should the Engineer implement? Select 2 answers from the options given below.

- A. Set up a CloudWatch event based on Trusted Advisor metrics
- B. Trigger a Lambda function from a scheduled CloudWatch event that terminates non-compliant infrastructure.
- C. Set up a CloudWatch event based on Amazon Inspector findings
- D. Monitor compliance with AWS Config Rules triggered by configuration changes
- E. Trigger a CLI command from a CloudWatch event that terminates the infrastructure

**Answer:** BD

**Explanation:**

You can use AWS Config to monitor for such events. Option A is invalid because you cannot set Cloudwatch events based on Trusted Advisor checks.

Option C is invalid. Amazon Inspector cannot be used to check whether instances are launched from a specific AMI.

Option E is invalid because triggering a CLI command is not the preferred option, instead you should use Lambda functions for all automation purposes.

#### QUESTION 488

You are building a system to distribute confidential training videos to employees. Using CloudFront, what method could be used to serve content that is stored in S3, but not publicly

accessible from S3 directly?

- A. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
- B. Add the CloudFront account security group "amazon-cf/amazon-cf-sg" to the appropriate S3 bucket policy.
- C. Create an Identity and Access Management (IAM) User for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
- D. Create a S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

**Answer:** A

**Explanation:**

You can optionally secure the content in your Amazon S3 bucket so users can access it through CloudFront but cannot access it directly by using Amazon S3 URLs. This prevents anyone from bypassing CloudFront and using the Amazon S3 URL to get content that you want to restrict access to. This step isn't required to use signed URLs, but we recommend it

To require that users access your content through CloudFront URLs, you perform the following tasks:

Create a special CloudFront user called an origin access identity. Give the origin access identity permission to read the objects in your bucket. Remove permission for anyone else to use Amazon S3 URLs to read the objects. Option B,C and D are all automatically invalid, because the right way is to

ensure to create Origin Access Identity (OAI) for CloudFront and grant access accordingly. For more information on serving private content via Cloudfront, please visit the following URL:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>  
The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI. You can optionally secure the content in your Amazon S3 bucket so users can access it through CloudFront but cannot access it directly by using Amazon S3 URLs. This prevents anyone from bypassing CloudFront and using the Amazon S3 URL to get content that you want to restrict access to. This step isn't required to use signed URLs, but we recommend it To require that users access your content through CloudFront URLs, you perform the following tasks:

Create a special CloudFront user called an origin access identity. Give the origin access identity permission to read the objects in your bucket. Remove permission for anyone else to use Amazon S3 URLs to read the objects.

Option B,C and D are all automatically invalid, because the right way is to ensure to create Origin Access Identity (OAI) for CloudFront and grant access accordingly.

#### QUESTION 489

A company has a large set of keys defined in AWS KMS. Their developers frequently use the keys for the applications being developed.

What is one of the ways that can be used to reduce the cost of accessing the keys in the AWS KMS service.

- A. Enable rotation of the keys
- B. Use Data key caching
- C. Create an alias of the key
- D. Use the right key policy

**Answer:** B

**Explanation:**

The AWS Documentation mentions the following Data key caching stores data keys and related cryptographic material in a cache. When you encrypt or decrypt data, the AWS Encryption SDK

looks for a matching data key in the cache. If it finds a match, it uses the cached data key rather than generatir a new one. Data key caching can improve performance, reduce cost, and help you stay within service limits as your application scales.

Option A.C and D are all incorrect since these options will not impact how the key is used.

**QUESTION 490**

You need to ensure that objects in an S3 bucket are available in another region. This is because of the criticality of the data that is hosted in the S3 bucket.

How can you achieve this in the easiest way possible?

- A. Enable cross region replication for the bucket
- B. Write a script to copy the objects to another bucket in the destination region
- C. Create an S3 snapshot in the destination region
- D. Enable versioning which will copy the objects to the destination region

**Answer:** A

**Explanation:**

Option B is partially correct but a big maintenance over head to create and maintain a script when the functionality is already available in S3 Option C is invalid because snapshots are not available in S3 Option D is invalid because versioning will not replicate objects The AWS Documentation mentions the following

Cross-region replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buck in different AWS Regions.

**QUESTION 491**

A company's Chief Security Officer has requested that a Security Analyst review and improve the security posture of each company AWS account.

The Security Analyst decides to do this by Improving AWS account root user security.

Which actions should the Security Analyst take to meet these requirements? (Select THREE.)

- A. Delete the access keys for the account root user in every account.
- B. Create an admin IAM user with administrative privileges and delete the account root user in every account.
- C. Implement a strong password to help protect account-level access to the AWS Management Console by the account root user.
- D. Enable multi-factor authentication (MFA) on every account root user in all accounts.
- E. Create a custom IAM policy to limit permissions to required actions for the account root user and attach the policy to the account root user.
- F. Attach an IAM role to the account root user to make use of the automated credential rotation in AWS STS.

**Answer:** ACD

**Explanation:**

- If you do have an access key for your AWS account root user, delete it.
- Use a strong password to help protect account-level access to the AWS Management Console.
- Enable AWS multi-factor authentication (MFA) on your AWS account root user account  
<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#create-iam-users>

**QUESTION 492**

Your company has just set up a new central server in a VPC. There is a requirement for other

teams who have their servers located in different VPC's in the same region to connect to the central server.

Which of the below options is best suited to achieve this requirement.

- A. Set up VPC peering between the central server VPC and each of the teams VPCs.
- B. Set up AWS DirectConnect between the central server VPC and each of the teams VPCs.
- C. Set up an IPSec Tunnel between the central server VPC and each of the teams VPCs.
- D. None of the above options will work.

**Answer:** A

**Explanation:**

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a single region.

Options B and C are invalid because you need to use VPC Peering  
Option D is invalid because VPC Peering is available

### QUESTION 493

Your developer is using the KMS service and an assigned key in their Java program. They get the below error when running the code

arn:aws:iam::113745388712:user/UserB is not authorized to perform: kms:DescribeKey

Which of the following could help resolve the issue?

- A. Ensure that UserB is given the right IAM role to access the key
- B. Ensure that UserB is given the right permissions in the IAM policy
- C. Ensure that UserB is given the right permissions in the Key policy
- D. Ensure that UserB is given the right permissions in the Bucket policy

**Answer:** C

**Explanation:**

You need to ensure that UserB is given access via the Key policy for the Key

**This Account**

The following IAM users and roles can use this key to encrypt and decrypt data from within applications and when using AWS services integrated with KMS. [Learn more](#).

| <input type="checkbox"/> | Name <span style="font-size: small;">▼</span> | Path <span style="font-size: small;">▼</span> | Type <span style="font-size: small;">▼</span> |
|--------------------------|-----------------------------------------------|-----------------------------------------------|-----------------------------------------------|
| <input type="checkbox"/> | UserA                                         | /                                             | User                                          |
| <input type="checkbox"/> | UserB                                         | /                                             | User                                          |

Showing 2 results

### QUESTION 494

You are trying to use the Systems Manager to patch a set of EC2 systems. Some of the systems are not getting covered in the patching process.

Which of the following can be used to troubleshoot the issue? Choose 3 answers from the options given below.

- A. Check to see if the right role has been assigned to the EC2 instances
- B. Check to see if the IAM user has the right permissions for EC2
- C. Ensure that agent is running on the instances.
- D. Check the Instance status by using the Health API.

**Answer:** ACD

**Explanation:**

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

- 1) You installed the latest version of the SSM Agent on your instance
  - 2) Your instance is configured with an AWS Identity and Access Management (IAM) role that enables the instance to communicate with the Systems Manager API
  - 3) You can use the Amazon EC2 Health API to quickly determine the following information about Amazon EC2 instances The status of one or more instances The last time the instance sent a heartbeat value The version of the SSM Agent  
The operating system  
The version of the EC2Config service (Windows)  
The status of the EC2Config service (Windows)
- Option B is invalid because IAM users are not supposed to be directly granted permissions to EC2 Instances

### QUESTION 495

You are designing a connectivity solution between on-premises infrastructure and Amazon VPC. Your server's on-premises will be communicating with your VPC instances. You will be establishing IPsec tunnels over the internet. Yo will be using VPN gateways and terminating the IPsec tunnels on AWS- supported customer gateways. Which of the following objectives would you achieve by implementing an IPsec tunnel as outlined above? Choose 4 answers form the options below

- A. End-to-end protection of data in transit
- B. End-to-end Identity authentication
- C. Data encryption across the internet
- D. Protection of data in transit over the Internet
- E. Peer identity authentication between VPN gateway and customer gateway
- F. Data integrity protection across the Internet

**Answer:** CDEF

**Explanation:**

IPSec is a widely adopted protocol that can be used to provide end to end protection for data.

### QUESTION 496

A company uses a third-party application to store encrypted data in Amazon S3. The company uses another third-party application trial decrypts the data from Amazon S3 to ensure separation of duties Between the applications A Security Engineer warns to separate the permissions using IAM roles attached to Amazon EC2 instances. The company prefers to use native AWS services.

Which encryption method will meet these requirements?

- A. Use encrypted Amazon EBS volumes with Amazon default keys (AWS EBS)
- B. Use server-side encryption with customer-provided keys (SSE-C)

- C. Use server-side encryption with AWS KMS managed keys (SSE-KMS)
- D. Use server-side encryption with Amazon S3 managed keys (SSE-S3)

**Answer:** C

**QUESTION 497**

A company wants to use Cloudtrail for logging all API activity. They want to segregate the logging of data events and management events.

How can this be achieved? Choose 2 answers from the options given below

- A. Create one Cloudtrail log group for data events
- B. Create one trail that logs data events to an S3 bucket
- C. Create another trail that logs management events to another S3 bucket
- D. Create another Cloudtrail log group for management events

**Answer:** BC

**Explanation:**

The AWS Documentation mentions the following You can configure multiple trails differently so that the trails process and log only the events that you specify. For example, one trail can log read-only data and management events, so that all read-only events are delivered to one S3 bucket. Another trail can log only write-only data and management events, so that all write-only events are delivered to a separate S3 bucket

Options A and D are invalid because you have to create a trail and not a log group.

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/loHEing-manasement-and-data-events-with-cloudtrai>

**QUESTION 498**

Your company has a set of EBS volumes defined in AWS. The security mandate is that all EBS volumes are encrypted. What can be done to notify the IT admin staff if there are any unencrypted volumes in the account?

- A. Use AWS Inspector to inspect all the EBS volumes
- B. Use AWS Config to check for unencrypted EBS volumes
- C. Use AWS Guard duty to check for the unencrypted EBS volumes
- D. Use AWS Lambda to check for the unencrypted EBS volumes

**Answer:** B

**Explanation:**

The enc config rule for AWS Config can be used to check for unencrypted volumes.  
encrypted-volurnn

5 volumes that are in an attached state are encrypted. If you specify the ID of a KMS key for encryptio using the kmsId parameter, the rule checks if the EBS volumes in an attached state are encrypted with that KMS key\*1.

Options A and C are incorrect since these services cannot be used to check for unencrypted EBS volumes

Option D is incorrect because even though this is possible, trying to implement the solution alone with just the Lambda servk would be too difficult.

**QUESTION 499**

You are working in the media industry and you have created a web application where users will

be able to upload photos they create to your website. This web application must be able to call the S3 API in order to be able to function.

Where should you store your API credentials whilst maintaining the maximum level of security?

- A. Save the API credentials to your PHP files.
- B. Don't save your API credentials, instead create a role in IAM and assign this role to an EC2 instance when you first create it.
- C. Save your API credentials in a public Github repository.
- D. Pass API credentials to the instance using instance userdata.

**Answer:** B

**Explanation:**

Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances.

For example, you can securely distribute your AWS credentials to the instances, enabling the applications

on those instances to use your credentials to sign requests, while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance, especially those that AWS creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.

IAM roles are designed so that your applications can securely make API requests from your instances, without requiring you manage the security credentials that the applications use.

Option A.C and D are invalid because using AWS Credentials in an application in production is a direct no recommendation 1 secure access.

## QUESTION 500

A company has a legacy application that outputs all logs to a local text file. Logs from all applications running on AWS must be continually monitored for security related messages.

What can be done to allow the company to deploy the legacy application on Amazon EC2 and still meet the monitoring requirement?

- A. Create a Lambda function that mounts the EBS volume with the logs and scans the logs for security incidents. Trigger the function every 5 minutes with a scheduled Cloudwatch event.
- B. Send the local text log files to CloudWatch Logs and configure a CloudWatch metric filter. Trigger cloudwatch alarms based on the metrics.
- C. Install the Amazon inspector agent on any EC2 instance running the legacy application. Generate CloudWatch alerts a based on any Amazon inspector findings.
- D. Export the local text log files to CloudTrail. Create a Lambda function that queries the CloudTrail logs for security ' incidents using Athena.

**Answer:** B

**Explanation:**

One can send the log files to Cloudwatch Logs. Log files can also be sent from On-premise servers. You can then specify metrii to search the logs for any specific values. And then create alarms based on these metrics.

Option A is invalid because this will be just a long over drawn process to achieve this requirement  
Option C is invalid because AWS Inspector cannot be used to monitor for security related messages.

Option D is invalid because files cannot be exported to AWS Cloudtrail.

**QUESTION 501**

You work at a company that makes use of AWS resources. One of the key security policies is to ensure that all data is encrypted both at rest and in transit.

Which of the following is one of the right ways to implement this?

- A. Use S3 SSE and use SSL for data in transit
- B. SSL termination on the ELB
- C. Enabling Proxy Protocol
- D. Enabling sticky sessions on your load balancer

**Answer:** A

**Explanation:**

By disabling SSL termination, you are leaving an unsecure connection from the ELB to the back end instances. Hence this means that part of the data transit is not being encrypted.

Option B is incorrect because this would not guarantee complete encryption of data in transit

Option C and D are incorrect because these would not guarantee encryption

**QUESTION 502**

In order to encrypt data in transit for a connection to an AWS RDS instance, which of the following would you implement?

- A. Transparent data encryption
- B. SSL from your application
- C. Data keys from AWS KMS
- D. Data Keys from CloudHSM

**Answer:** B

**Explanation:**

This is mentioned in the AWS Documentation You can use SSL from your application to encrypt a connection to a DB instance running MySQL MariaDB, Amazon Aurora, SQL Server, Oracle, or PostgreSQL.

Option A is incorrect since Transparent data encryption is used for data at rest and not in transit

Options C and D are incorrect since keys can be used for encryption of data at rest.

**QUESTION 503**

A company needs to migrate several applications to AWS. This will require storing more than 5,000 credentials. To meet compliance requirements, the company will use its existing password management system for key rotation, auditing, and integration with third-party secrets containers. The company has a limited budget and is seeking the most cost-effective solution that is still secure.

How should the company accomplish this at the LOWEST cost?

- A. Configure the company's key management solution to integrate with AWS Systems Manager Parameter Store.
- B. Configure the company's key management solution to integrate with AWS Secrets Manager.
- C. Use an Amazon S3 encrypted bucket to store the secrets and configure the applications with the appropriate roles to access the secrets.
- D. Configure the company's key management solution to integrate with AWS CloudHSM.

**Answer:** D

**QUESTION 504**

A company has a web-based application using Amazon CloudFront and running on Amazon Elastic Container Service (Amazon ECS) behind an Application Load Balancer (ALB). The ALB is terminating TLS and balancing load across ECS service tasks.

A security engineer needs to design a solution to ensure that application content is accessible only through CloudFront and that it is never accessible directly.

How should the security engineer build the MOST secure solution?

- A. Add an origin custom header. Set the viewer protocol policy to HTTP and HTTPS.  
Set the origin protocol policy to HTTPS only.  
Update the application to validate the CloudFront custom header.
- B. Add an origin custom header. Set the viewer protocol policy to HTTPS only.  
Set the origin protocol policy to match viewer.  
Update the application to validate the CloudFront custom header.
- C. Add an origin custom header. Set the viewer protocol policy to redirect HTTP to HTTPS.  
Set the origin protocol policy to HTTP only.  
Update the application to validate the CloudFront custom header.
- D. Add an origin custom header. Set the viewer protocol policy to redirect HTTP to HTTPS.  
Set the origin protocol policy to HTTPS only.  
Update the application to validate the CloudFront custom header.

**Answer:** C

**QUESTION 505**

A large government organization is moving to the cloud and has specific encryption requirements. The first workload to move requires that a customer's data be immediately destroyed when the customer makes that request.

Management has asked the security team to provide a solution that will securely store the data, allow only authorized applications to perform encryption and decryption, and allow for immediate destruction of the data.

Which solution will meet these requirements?

- A. Use AWS Secrets Manager and an AWS SDK to create a unique secret for the customer-specific data.
- B. Use AWS Key Management Service (AWS KMS) and the AWS Encryption SDK to generate and store a data encryption key for each customer.
- C. Use AWS Key Management Service (AWS KMS) with service-managed keys to generate and store customer-specific data encryption keys.
- D. Use AWS Key Management Service (AWS KMS) and create an AWS CloudHSM custom key store.  
Use CloudHSM to generate and store a new CMK for each customer.

**Answer:** A

**QUESTION 506**

A security engineer is defining the controls required to protect the AWS account root user credentials in an AWS Organizations hierarchy. The controls should also limit the impact in case these credentials have been compromised.

Which combination of controls should the security engineer propose? (Choose three.)

- A. Apply the following SCP:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "GRRESTRICTROOTUSER",
 "Effect": "Deny",
 "Action": "*",
 "Resource": [
 "*"
],
 "Condition": {
 "StringLike": {
 "aws:PrincipalArn": [
 "arn:aws:iam::*:root"
]
 }
 }
 }
]
}
```

lab51793

- B. Apply the following SCP:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "GRRESTRICTROOTUSER",
 "Effect": "Deny",
 "Principal": "arn:aws:iam::*:root",
 "Action": "*",
 "Resource": [
 "*"
],
 "Condition": {
 "StringLike": {
 "aws:PrincipalArn": [
 "arn:aws:iam::*:root"
]
 }
 }
 }
]
}
```

lab51793

- C. Enable multi-factor authentication (MFA) for the root user.  
D. Set a strong randomized password and store it in a secure location.  
E. Create an access key ID and secret access key, and store them in a secure location.  
F. Apply the following permissions boundary to the root user:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "GRRESTRICTROOTUSER",
 "Effect": "Deny",
 "Action": "*",
 "Resource": [
 "*"
],
 "Condition": {
 "StringLike": {
 "aws:PrincipalArn": [
 "arn:aws:iam::*:root"
]
 }
 }
 }
]
}
```

abs51793

**Answer:** ADF**QUESTION 507**

A VPC endpoint for Amazon CloudWatch Logs was recently added to a company's VPC. The company's system administrator has verified that private DNS is enabled and that the appropriate route tables and security groups have been updated. The role attached to the Amazon EC2 instance is:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "logs>CreateLogGroup",
 "logs>CreateLogStream",
 "logs>PutLogEvents",
 "logs>DescribeLogStreams"
],
 "Resource": [
 "arn:aws:logs:*:*:
]
 }
]
}
```

abs51793

The CloudWatch Logs agent is running and attempting to write to a CloudWatch Logs stream in

the same AWS account. However, no logs are being updated in CloudWatch Logs.

What is the likely cause of this issue?

- A. The EC2 instance role is not allowing the appropriate Put actions.
- B. The EC2 instance role policy is incorrect and should be changed to:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "logs:CreateLogGroup",
 "logs:CreateLogStream",
 "logs:PutLogEvents",
 "logs:DescribeLogStreams"
],
 "Resource": [
 "*"
]
 }
]
}
```

- C. The CloudWatch Logs endpoint policy is not allowing the appropriate Put actions.
- D. The CloudWatch Logs resource policy is not allowing the appropriate List actions.

**Answer:** C

### QUESTION 508

Amazon GuardDuty has detected communications to a known command and control endpoint from a company's Amazon EC2 instance. The instance was found to be running a vulnerable version of a common web framework. The company's security operations team wants to quickly identify other compute resources with the specific version of that framework installed.

Which approach should the team take to accomplish this task?

- A. Scan all the EC2 instances for noncompliance with AWS Config.  
Use Amazon Athena to query AWS CloudTrail logs for the framework installation.
- B. Scan all the EC2 instances with the Amazon Inspector Network Reachability rules package to identify instances running a web server with RecognizedPortWithListener findings.
- C. Scan all the EC2 instances with AWS Systems Manager to identify the vulnerable version of the web framework.
- D. Scan all the EC2 instances with AWS Resource Access Manager to identify the vulnerable version of the web framework.

**Answer:** B

### QUESTION 509

A security engineer has noticed an unusually high amount of traffic coming from a single IP address. This was discovered by analyzing the Application Load Balancer's access logs.

How can the security engineer limit the number of requests from a specific IP address without blocking the IP address?

- A. Add a rule to the Application Load Balancer to route the traffic originating from the IP address in QUESTION 5and show a static webpage.
- B. Implement a rate-based rule with AWS WAF.
- C. Use AWS Shield to limit the originating traffic hit rate.
- D. Implement the GeoLocation feature in Amazon Route 53.

**Answer:** B

#### **QUESTION 510**

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

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

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

**Answer:** AD

**Explanation:**

<https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-buckets-allowing-public-access/>

#### **QUESTION 511**

A security engineer must develop an encryption tool for a company. The company requires a cryptographic solution that supports the ability to perform cryptographic erasure on all resources protected by the key material in 15 minutes or less.

Which Aws Key Management Service (AWS KMS) key solution will allow the security engineer to meet these requirements?

- A. Use imported key material with CMK.
- B. Use an AWS KMS CMK.
- C. Use an AWS managed CMK.
- D. Use an AWS KMS customer managed CMK.

**Answer:** A

**QUESTION 512**

A company deployed an Amazon EC2 instance to a VPC on AWS. A recent alert indicates that the EC2 instance is receiving a suspicious number of requests over an open TCP port from an external source. The TCP port remains open for long periods of time.

The company's security team needs to stop all activity to this port from the external source to ensure that the EC2 instance is not being compromised. The application must remain available to other users.

Which solution will meet these requirements?

- A. Update the network ACL that is attached to the subnet that is associated with the EC2 instance.  
Add a Deny statement for the port and the source IP addresses.
- B. Update the elastic network interface security group that is attached to the EC2 instance to remove the port from the inbound rule list.
- C. Update the elastic network interface security group that is attached to the EC2 instance by adding a Deny entry in the inbound list for the port and the source IP addresses.
- D. Create a new network ACL for the subnet.  
Deny all traffic from the EC2 instance to prevent data from being removed.

**Answer:** D

**QUESTION 513**

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

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

PassLeader

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

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

**Answer:** A

**QUESTION 514**

A security engineer needs to build a solution to turn AWS CloudTrail back on in multiple AWS Regions in case it is ever turned off.

What is the MOST efficient way to implement this solution?

- A. Use AWS Config with a managed rule to trigger the AWS-EnableCloudTrail remediation.
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) event with a cloudtrail.amazonaws.com event source and a StartLogging event name to trigger an AWS Lambda function to call the StartLogging API.
- C. Create an Amazon CloudWatch alarm with a cloudtrail.amazonaws.com event source and a StopLogging event name to trigger an AWS Lambda function to call the StartLogging API.
- D. Monitor AWS Trusted Advisor to ensure CloudTrail logging is enabled.

**Answer:** C

**QUESTION 515**

A company needs to encrypt all of its data stored in Amazon S3. The company wants to use AWS Key Management Service (AWS KMS) to create and manage its encryption keys. The company's security policies require the ability to import the company's own key material for the keys, set an expiration date on the keys, and delete keys immediately, if needed.

How should a security engineer set up AWS KMS to meet these requirements?

- A. Configure AWS KMS and use a custom key store.  
Create a customer managed CMK with no key material. Import the company's keys and key material into the CMK.
- B. Configure AWS KMS and use the default key store.  
Create an AWS managed CMK with no key material. Import the company's keys and key material into the CMK.
- C. Configure AWS KMS and use the default key store.  
Create a customer managed CMK with no key material. Import the company's keys and key material into the CMK.
- D. Configure AWS KMS and use a custom key store.  
Create an AWS managed CMK with no key material.  
Import the company's keys and key material into the CMK.

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/kms/latest/developerguide/overview.html>

**QUESTION 516**

A company has an application that uses an Amazon RDS PostgreSQL database. The company is developing an application feature that will store sensitive information for an individual in the database.

During a security review of the environment, the company discovers that the RDS DB instance is not encrypting data at rest. The company needs a solution that will provide encryption at rest for all the existing data and for any new data that is entered for an individual.

Which combination of options can the company use to meet these requirements? (Choose two.)

- A. Create a snapshot of the DB instance.  
Copy the snapshot to a new snapshot, and enable encryption for the copy process.  
Use the new snapshot to restore the DB instance.
- B. Modify the configuration of the DB instance by enabling encryption.  
Create a snapshot of the DB instance. Use the snapshot to restore the DB instance.
- C. Use AWS Key Management Service (AWS KMS) to create a new default AWS managed aws/rds key.  
Select this key as the encryption key for operations with Amazon RDS.
- D. Use AWS Key Management Service (AWS KMS) to create a new CMK.  
Select this key as the encryption key for operations with Amazon RDS.
- E. Create a snapshot of the DB instance.  
Enable encryption on the snapshot.  
Use the snapshot to restore the DB instance.

**Answer:** AD

**Explanation:**

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_CopySnapshot.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_CopySnapshot.html)

**QUESTION 517**

A security engineer needs to create an Amazon S3 bucket policy to grant least privilege read access to IAM user accounts that are named User1, User2 and User3. These IAM user accounts are members of the AuthorizedPeople IAM group. The security engineer drafts the following S3 bucket policy:

```
{
 "Version": "2012-10-17",
 "Id": "AuthorizedPeoplePolicy",
 "Statement": [
 {
 "Sid": "Actions-Authorized-People",
 "Effect": "Allow",
 "Action": [
 "s3:GetObject"
],
 "Resource": "arn:aws:s3:::authorized-people-bucket/*"
 }
]
}
```

lab051793

When the security engineer tries to add the policy to the S3 bucket, the following message appears:

"Missing required field Principal."

The security engineer is adding a Principal element to the policy. The addition must provide read access to only User1, User2 and User3.

Which solution meets these requirements?

- A.    "Principal": {  
        "AWS": [  
            "arn:aws:iam::1234567890:user/User1",  
            "arn:aws:iam::1234567890:user/User2",  
            "arn:aws:iam::1234567890:user/User3"  
        ]  
    }
- B.    "Principal": {  
        "AWS": [  
            "arn:aws:iam::1234567890:root"  
        ]  
    }
- C.    "Principal": {  
        "AWS": [  
            "\*"  
        ]  
    }
- D.    "Principal": {  
        "AWS": "arn:aws:iam::1234567890:group/AuthorizedPeople"  
    }

**Answer: B**

**Explanation:**

[https://docs.amazonaws.cn/en\\_us/AmazonS3/latest/userguide/example-bucket-policies.html](https://docs.amazonaws.cn/en_us/AmazonS3/latest/userguide/example-bucket-policies.html)

**QUESTION 518**

A company is hosting a web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The application has become the target of a DoS attack. Application logging shows that requests are coming from small number of client IP addresses, but the addresses change regularly.

The company needs to block the malicious traffic with a solution that requires the least amount of ongoing effort.

Which solution meets these requirements?

- A. Create an AWS WAF rate-based rule, and attach it to the ALB.
- B. Update the security group that is attached to the ALB to block the attacking IP addresses.
- C. Update the ALB subnet's network ACL to block the attacking client IP addresses.
- D. Create a AWS WAF rate-based rule, and attach it to the security group of the EC2 instances.

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/aws-best-practices-ddos-resiliency.pdf>

**QUESTION 519**

A public subnet contains two Amazon EC2 instances. The subnet has a custom network ACL. A security engineer is designing a solution to improve the subnet security.

The solution must allow outbound traffic to an internet service that uses TLS through port 443. The solution also must deny inbound traffic that is destined for MySQL port 3306.

Which network ACL rule set meets these requirements?

- A. Use inbound rule 100 to allow traffic on TCP port 443.  
Use inbound rule 200 to deny traffic on TCP port 3306.  
Use outbound rule 100 to allow traffic on TCP port 443.
- B. Use inbound rule 100 to deny traffic on TCP port 3306.  
Use inbound rule 200 to allow traffic on TCP port range 1024-65535.  
Use outbound rule 100 to allow traffic on TCP port 443.
- C. Use inbound rule 100 to allow traffic on TCP port range 1024-65535.  
Use inbound rule 200 to deny traffic on TCP port 3306.  
Use outbound rule 100 to allow traffic on TCP port 443.
- D. Use inbound rule 100 to deny traffic on TCP port 3306.  
Use inbound rule 200 to allow traffic on TCP port 443.  
Use outbound rule 100 to allow traffic on TCP port 443.

**Answer:** A

**QUESTION 520**

A company has developed a new Amazon RDS database application. The company must secure the RDS database credentials for encryption in transit and encryption at rest. The company also must rotate the credentials automatically on a regular basis.

Which solution meets these requirements?

- A. Use AWS Systems Manager Parameter Store to store the database credentials.  
Configure automatic rotation of the credentials.
- B. Use AWS Secrets Manager to store the database credentials.  
Configure automatic rotation of the credentials.
- C. Store the database credentials in an Amazon S3 bucket that is configured with server-side encryption with S3 managed encryption keys (SSE-S3).  
Rotate the credentials with IAM database authentication.
- D. Store the database credentials in Amazon S3 Glacier, and use S3 Glacier Vault Lock.  
Configure an AWS Lambda function to rotate credentials on a scheduled basis.

**Answer:** C

#### QUESTION 521

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

The solution must minimize management overhead.

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

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

**Answer:** C

#### QUESTION 522

A security engineer has enabled AWS Security Hub in their AWS account, and has enabled the Center for Internet Security (CIS) AWS Foundations compliance standard. No evaluation results on compliance are returned in the Security Hub console after several hours. The engineer wants to ensure that Security Hub can evaluate their resources for CIS AWS Foundations compliance.

Which steps should the security engineer take to meet these requirements?

- A. Add full Amazon Inspector IAM permissions to the Security Hub service role to allow it to perform the CIS compliance evaluation.
- B. Ensure that AWS Trusted Advisor is enabled in the account, and that the Security Hub service role has permissions to retrieve the Trusted Advisor security-related recommended actions.
- C. Ensure that AWS Config is enabled in the account, and that the required AWS Config rules

- have been created for the CIS compliance evaluation.
- D. Ensure that the correct trail in AWS CloudTrail has been configured for monitoring by Security Hub, and that the Security Hub service role has permissions to perform the GetObject operation on CloudTrail's Amazon S3 bucket.

**Answer:** B

**Explanation:**

<https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub.pdf>

### QUESTION 523

A company has two AWS accounts: Account A and Account B. Account A has an IAM role that IAM users in Account B assume when they need to upload sensitive documents to Amazon S3 buckets in Account A.

A new requirement mandates that users can assume the role only if they are authenticated with multi-factor authentication (MFA). A security engineer must recommend a solution that meets this requirement with minimum risk and effort.

Which solution should the security engineer recommend?

- A. Add an aws:MultiFactorAuthPresent condition to the role's permissions policy.
- B. Add an aws:MultiFactorAuthPresent condition to the role's trust policy.
- C. Add an aws:MultiFactorAuthPresent condition to the session policy.
- D. Add an aws:MultiFactorAuthPresent condition to the S3 bucket policies.

**Answer:** D

### QUESTION 524

A company is developing an ecommerce application. The application uses Amazon EC2 instances and an Amazon RDS MySQL database. For compliance reasons, data must be secured in transit and at rest. The company needs a solution that minimizes operational overhead and minimizes cost.

Which solution meets these requirements?

- A. Use TLS certificates from AWS Certificate Manager (ACM) with an Application Load Balancer. Deploy self-signed certificates on the EC2 instances.  
Ensure that the database client software uses a TLS connection to Amazon RDS.  
Enable encryption of the RDS DB instance.  
Enable encryption on the Amazon Elastic Block Store (Amazon EBS) volumes that support the EC2 instances.
- B. Use TLS certificates from a third-party vendor with an Application Load Balancer.  
Install the same certificates on the EC2 instances.  
Ensure that the database client software uses a TLS connection to Amazon RDS.  
Use AWS Secrets Manager for client-side encryption of application data.
- C. Use AWS CloudHSM to generate TLS certificates for the EC2 instances.  
Install the TLS certificates on the EC2 instances.  
Ensure that the database client software uses a TLS connection to Amazon RDS.  
Use the encryption keys from CloudHSM for client-side encryption of application data.
- D. Use Amazon CloudFront with AWS WAF. Send HTTP connections to the origin EC2 instances.  
Ensure that the database client software uses a TLS connection to Amazon RDS.

Use AWS Key Management Service (AWS KMS) for client-side encryption of application data before the data is stored in the RDS database.

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html>

**QUESTION 525**

A company is undergoing a layer 3 and layer 4 DDoS attack on its web servers running on AWS.

Which combination of AWS services and features will provide protection in this scenario?  
(Choose three.)

- A. Amazon Route 53
- B. AWS Certificate Manager (ACM)
- C. Amazon S3
- D. AWS Shield
- E. Elastic Load Balancer
- F. Amazon GuardDuty

**Answer:** ACD

**Explanation:**

<https://aws.amazon.com/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

**QUESTION 526**

A user in account 111122223333 is receiving an access denied error message while calling the AWS Key Management Service (AWS KMS) GenerateDataKey API operation. The key policy contains the following statement:

```
{
 "Effect": "Allow",
 "Principal": {
 "AWS": "arn:aws:iam::111122223333:user/KMSUser"
 },
 "Action": [
 "kms:GenerateDataKey",
 "kms:Encrypt",
 "kms:Decrypt"
],
 "Resource": "*",
 "Condition": {
 "StringEquals": {
 "kms:EncryptionContext:AppName": "CorpApp"
 }
 }
}
```

Account 111122223333 is not using AWS Organizations SCPs.

Which combination of steps should a security engineer take to ensure that KMSUser can perform the action on the key? (Choose two.)

- A. Modify the key policy to include the key's key ID in the Resource field.
- B. Verify that KMSUser has no explicit denies for the GenerateDataKey action in its attached IAM policies.
- C. Verify that KMSUser is allowed to perform the GenerateDataKey action in its attached IAM policies for the encryption context.
- D. Ensure that KMSUser is including the encryption context key-value pair in its GenerateDataKey.
- E. Revoke any KMS grants on the key that are denying the GenerateDataKey action for KMSUser.

**Answer:** AC

#### QUESTION 527

A company is building an application on AWS that will store sensitive information. The company has a support team with access to the IT infrastructure, including databases. The company's security engineer must introduce measures to protect the sensitive data against any data breach while minimizing management overhead. The credentials must be regularly rotated.

What should the security engineer recommend?

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

- B. Install a database on an Amazon EC2 instance.
  - Enable third-party disk encryption to encrypt Amazon Elastic Block Store (Amazon EBS) volume.
  - Store the database credentials in AWS CloudHSM with automatic rotation.
  - Set up TLS for the connection to the database.
- C. Enable Amazon RDS encryption to encrypt the database and snapshots.
  - Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instances.
  - Store the database credentials in AWS Secrets Manager with automatic rotation.
  - Set up TLS for the connection to the RDS hosted database.
- D. Set up an AWS CloudHSM cluster with AWS Key Management Service (AWS KMS) to store KMS keys.
  - Set up Amazon RDS encryption using AWS KSM to encrypt the database.
  - Store the database credentials in AWS Systems Manager Parameter Store with automatic rotation.
  - Set up TLS for the connection to the RDS hosted database.

**Answer:** D

#### QUESTION 528

A company is developing a mobile shopping web app. The company needs an environment that is configured to encrypt all resources in transit and at rest.

A security engineer must develop a solution that will encrypt traffic in transit to the company's Application Load Balancer and Amazon API Gateway resources. The solution also must encrypt traffic at rest for Amazon S3 storage.

What should the security engineer do to meet these requirements?

- A. Use AWS Certificate Manager (ACM) for encryption in transit.
  - Use AWS Key Management Service for encryption at rest.
- B. Use AWS Certificate Manager (ACM) for encryption in transit and encryption at rest.
- C. Use AWS Key Management Service for encryption in transit.
  - Use AWS Certificate Manager (ACM) for encryption at rest.
- D. Use AWS Key Management Service for encryption in transit and encryption at rest.

**Answer:** A

#### QUESTION 529

A security team is implementing a centralized logging solution to meet requirements for auditing. The solution must be able to aggregate logs from Amazon CloudWatch and AWS CloudTrail to an account that is controlled by the security team. This approach must be usable across the entire organization in AWS Organizations.

Which solution meets these requirements in the MOST operationally efficient manner?

- A. In each AWS account, create an Amazon Kinesis Data Firehose delivery stream that has a destination of Amazon S3 in the security team's account.
  - Create a subscription for each Amazon CloudWatch Logs log group in each AWS account to the Kinesis Data Firehose delivery stream in the same account.
  - For the organization, create a CloudTrail trail that has a destination of Amazon S3.
- B. In the security team's account, create an Amazon Kinesis Data Firehose delivery stream that has a destination of Amazon S3 in the same account.

Create a subscription for each Amazon CloudWatch Logs log group in each AWS account to the Kinesis Data Firehose delivery stream in the security team's account.

For each AWS account, create a CloudTrail trail that has a destination of Amazon S3.

- C. In each AWS account, create an Amazon Kinesis data stream that has a destination of Amazon S3 in the security team's account.  
Create a subscription for each Amazon CloudWatch Logs log group in each AWS account to the Kinesis data stream in the same account.  
For the organization, create a CloudTrail trail that has a destination of Amazon S3.
- D. In the security team's account, create an Amazon Kinesis data stream that has a destination of Amazon S3 in the same account.  
Create a subscription for each Amazon CloudWatch Logs log group in each AWS account to the Kinesis data stream in the security team's account.  
For each AWS account, create a CloudTrail trail that has a destination of Amazon S3.

**Answer:** A

### QUESTION 530

A company needs its Amazon Elastic Block Store (Amazon EBS) volumes to be encrypted at all times. During a security incident, EBS snapshots of suspicious instances are shared to a forensics account for analysis. A security engineer attempting to share a suspicious EBS snapshot to the forensics account receives the following error:

"Unable to share snapshot. An error occurred (OperationNotPermitted) when calling the ModifySnapshotAttribute operation: Encrypted snapshots with EBS default key cannot be shared"

Which combination of steps should the security engineer take in the incident account to complete the sharing operation? (Choose three.)

- A. Create a customer managed CMK.  
Copy the EBS snapshot encrypting the destination snapshot using the new CMK.
- B. Allow forensics accounting principals to use the CMK by modifying its policy.
- C. Create an Amazon EC2 instance.  
Attach the encrypted and suspicious EBS volume.  
Copy data from the suspicious volume to an unencrypted volume.  
Snapshot the unencrypted volume.
- D. Copy the EBS snapshot to the new decrypted snapshot.
- E. Restore a volume from the suspicious EBS snapshot.  
Create an unencrypted EBS volume of the same size.
- F. Share the target EBS snapshot with the forensics account.

**Answer:** CDE

### QUESTION 531

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 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:** D

**Explanation:**

<https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-regex-conditions.html>

### QUESTION 532

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 engineers 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 to a new IAM group.  
Have team members use individual IAM accounts that are members of the new IAM group.

**Answer:** D

### QUESTION 533

A company has an IAM group. All of the IAM users in the group have been assigned a multi-factor authentication (MFA) device and have full access to Amazon S3.

The company needs to ensure that users in the group can perform S3 actions only after the users authenticate with MFA. A security engineer must design a solution that accomplishes this goal with the least maintenance overhead.

Which combination of actions will meet these requirements? (Choose two.)

- A. Add a customer managed Deny policy to users in the group for s3:\*actions.
- B. Add a customer managed Deny policy to the group for s3:\*actions.
- C. Add a customer managed Allow policy to the group for s3:\*actions.
- D. Add a condition to the policy:  
"Condition" : { "BoolIfExists" : { "aws:MultiFactorAuthPresent" : false } }
- E. Add a condition to the policy:  
"Condition" : { "Bool" : { "aws:MultiFactorAuthPresent" : false } }

**Answer:** CE

**Explanation:**

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_mfa\\_configure-api-require.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html)

**QUESTION 534**

A company uses Amazon RDS for MySQL as a database engine for its applications. A recent security audit revealed an RDS instance that is not compliant with company policy for encrypting data at rest. A security engineer at the company needs to ensure that all existing RDS databases are encrypted using server-side encryption and that any future deviations from the policy are detected.

Which combination of steps should the security engineer take to accomplish this? (Choose two.)

- A. Create an AWS Config rule to detect the creation of encrypted RDS databases.  
Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger on the AWS Config rules compliance state change and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.
- B. Use AWS System Manager State Manager to detect RDS database encryption configuration drift.  
Create an Amazon EventBridge (Amazon CloudWatch Events) rule to track state changes and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.
- C. Create a read replica for the existing unencrypted RDS database and enable replica encryption in the process.  
Once the replica becomes active, promote it into a standalone database instance and terminate the unencrypted database instance.
- D. Take a snapshot of the unencrypted RDS database.  
Copy the snapshot and enable snapshot encryption in the process.  
Restore the database instance from the newly created encrypted snapshot. Terminate the unencrypted database instance.
- E. Enable encryption for the identified unencrypted RDS instance by changing the configurations of the existing database.

**Answer:** DE

**QUESTION 535**

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

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

- A. Enable AWS Systems Manager in the AWS Management Console and configure for access to EC2 instances using the default AmazonEC2RoleforSSM role.  
Install the Systems Manager Agent on all EC2 Linux instances that need interactive access.  
Configure IAM user policies to allow development team access to the Systems Manager Session Manager and attach to the team's IAM users.
- B. Enable console SSH access in the EC2 console.  
Configure IAM user policies to allow development team access to the AWS Systems Manager Session Manager and attach to the development team's IAM users.
- C. Enable AWS Systems Manager in the AWS Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM role.  
Install the Systems Manager Agent on all EC2 Linux instances that need interactive access.

Configure a security group that allows SSH port 22 from all published IP addresses.  
Configure IAM user policies to allow development team access to the AWS Systems Manager Session Manager and attach to the team's IAM users.

- D. Enable AWS Systems Manager in the AWS Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM role.  
Install the Systems Manager Agent on all EC2 Linux instances that need interactive access.  
Configure IAM user policies to allow development team access to the EC2 console and attach to the team's IAM users.

**Answer:** D

### QUESTION 536

A company's on-premises networks are connected to VPCs using an AWS Direct Connect gateway. The company's on-premises application needs to stream data using an existing Amazon Kinesis Data Firehose delivery stream. The company's security policy requires that data be encrypted in transit using a private network.

How should the company meet these requirements?

- A. Create a VPC endpoint for Kinesis Data Firehose.  
Configure the application to connect to the VPC endpoint.
- B. Configure an IAM policy to restrict access to Kinesis Data Firehose using a source IP condition.  
Configure the application to connect to the existing Firehose delivery stream.
- C. Create a new TLS certificate in AWS Certificate Manager (ACM).  
Create a public-facing Network Load Balancer (NLB) and select the newly created TLS certificate.  
Configure the NLB to forward all traffic to Kinesis Data Firehose.  
Configure the application to connect to the NLB.
- D. Peer the on-premises network with the Kinesis Data Firehose VPC using Direct Connect.  
Configure the application to connect to the existing Firehose delivery stream.

**Answer:** B

### QUESTION 537

A company has implemented AWS WAF and Amazon CloudFront for an application. The application runs on Amazon EC2 instances that are part of an Auto Scaling group. The Auto Scaling group is behind an Application Load Balancer (ALB).

The AWS WAF web ACL uses an AWS Managed Rules rule group and is associated with the CloudFront distribution. CloudFront receives the request from AWS WAF and the uses the ALB as the distribution's origin.

During a security review, a security engineer discovers that the infrastructure is susceptible to a large, layer 7 DDoS attack.

How can the security engineer improve the security at the edge of the solution to defend against this type of attack?

- A. Configure the CloudFront distribution to use the Lambda@Edge feature.  
Create an AWS Lambda function that imposes a rate limit on CloudFront viewer requests.  
Block the request if the rate limit is exceeded.
- B. Configure the AWS WAF web ACL so that the web ACL has more capacity units to process all

- AWS WAF rules faster.
- C. Configure AWS WAF with a rate-based rule that imposes a rate limit that automatically blocks requests when the rate limit is exceeded.
  - D. Configure the CloudFront distribution to use AWS WAF as its origin instead of the ALB.

**Answer:** A

### QUESTION 538

A development team is using an AWS Key Management Service (AWS KMS) CMK to try to encrypt and decrypt a secure string parameter from AWS Systems Manager Parameter Store. However, the development team receives an error message on each attempt.

Which issues that are related to the CMK could be reasons for the error? (Choose two.)

- A. The CMK is used in the attempt does not exist.
- B. The CMK is used in the attempt needs to be rotated.
- C. The CMK is used in the attempt is using the CMK's key ID instead of the CMK ARN.
- D. The CMK is used in the attempt is not enabled.
- E. The CMK is used in the attempt is using an alias.

**Answer:** BE

### QUESTION 539

A company uses AWS Config and AWS Organizations. One of the company's account administrators recently turned off AWS Config recording, and a critical security incident was not logged properly.

The company's security engineer must create an SCP that will deny all users the ability to stop AWS Config. The SCP also must allow the ApprovedAdministrator role to edit AWS Config settings.

Which SCP meets these requirements?

- A. {  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "config:DeleteConfigRule",  
                "config:DeleteConfigurationRecorder",  
                "config:DeleteDeliveryChannel",  
                "config:StopConfigurationRecorder"  
            ],  
            "Resource": "\*",  
            "Condition": {  
                "ArnEquals": {  
                    "aws:PrincipalArn": "arn:aws:iam::\*:role/ApprovedAdministrator"  
                }  
            }  
        }  
    ]  
}

11051703

B. {  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": [  
                "config:DeleteConfigRule",  
                "config:DeleteConfigurationRecorder",  
                "config:DeleteDeliveryChannel",  
                "config:StopConfigurationRecorder"  
            ],  
            "Resource": "\*",  
            "Condition": {  
                "ArnEquals": {  
                    "aws:PrincipalArn": "arn:aws:iam::\*:role/ApprovedAdministrator"  
                }  
            }  
        }  
    ]  
}

C. {  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "config:DeleteConfigRule",  
                "config:DeleteConfigurationRecorder",  
                "config:DeleteDeliveryChannel",  
                "config:StopConfigurationRecorder"  
            ],  
            "Resource": "\*",  
            "Principal": {  
                "AWS": [  
                    "arn:aws:iam::\*:role/ApprovedAdministrator"  
                ]  
            }  
        }  
    ]  
}

D. {  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": [  
                "config>DeleteConfigRule",  
                "config>DeleteConfigurationRecorder",  
                "config>DeleteDeliveryChannel",  
                "config>StopConfigurationRecorder"  
            ],  
            "Resource": "\*",  
            "NotPrincipal": {  
                "AWS": [  
                    "arn:aws:iam::\*:role/ApprovedAdministrator"  
                ]  
            }  
        }  
    ]  
}

11151783

**Answer:** A

**QUESTION 540**

A company stores images for a website in an Amazon S3 bucket. The company is using Amazon CloudFront to serve the images to the 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 identity (OAI).
- 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:** AE

**QUESTION 541**

An audit determined that a company's Amazon EC2 instance security group violated company policy by allowing unrestricted incoming SSH traffic. A security engineer must implement a near-real-time monitoring and alerting solution that will notify administrators of such violations.

Which solution meets these requirements with the MOST operational efficiency?

- A. Create a recurring Amazon Inspector assessment run that runs every day and uses the Network Reachability package.  
Create an Amazon CloudWatch rule that invokes an AWS Lambda function when an assessment run starts.  
Configure the Lambda function to retrieve and evaluate the assessment run report when it completes.  
Configure the Lambda function also to publish an Amazon Simple Notification Service (Amazon SNS) notification if there are any violations for unrestricted incoming SSH traffic.
- B. Use the restricted-ssh AWS Config managed rule that is invoked by security group configuration changes that are not compliant.  
Use the AWS Config remediation feature to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.
- C. Configure VPC Flow Logs for the VPC, and specify an Amazon CloudWatch Logs group.  
Subscribe the CloudWatch Logs group to an AWS Lambda function that parses new log entries, detects successful connections on port 22, and publishes a notification through Amazon Simple Notification Service (Amazon SNS).
- D. Create a recurring Amazon Inspector assessment run that runs every day and uses the Security Best Practices package.  
Create an Amazon CloudWatch rule that invokes an AWS Lambda function when an assessment run starts.  
Configure the Lambda function to retrieve and evaluate the assessment run report when it completes.  
Configure the Lambda function also to publish an Amazon Simple Notification Service (Amazon SNS) notification if there are any violations for unrestricted incoming SSH traffic.

**Answer:** A

**Explanation:**

[https://docs.aws.amazon.com/inspector/latest/userguide/inspector\\_assessments.html](https://docs.aws.amazon.com/inspector/latest/userguide/inspector_assessments.html)

#### **QUESTION 542**

A large company has hundreds of AWS accounts. The company needs to provide its employees with access to these accounts. The solution must maximize scalability and operational efficiency.

Which solution meets these requirements?

- A. With each AWS account, create dedicated IAM users that employees can assume through federation based upon group membership in their existing identity provider.
- B. Use a centralized account with IAM roles that employees can assume through federation with their existing identity provider.  
Create a custom authorizer by using AWS SDK to give federated users the ability to assume their target role in the resource accounts.
- C. Implement AWS Control Tower for multi-account management by integrating AWS Single Sign-On with the company's existing identity provider.  
Create IAM roles for the identity provider to assume.
- D. Configure the IAM trust policies within each account's role to set up a trust back to the company's existing identity provider.  
Allow users to assume the role based on their SAML token.

**Answer:** B

#### **QUESTION 543**

A company's security team suspects that an insider threat is present. The security team is basing its suspicion on activity that occurred in one of the company's AWS accounts. The activity was

performed with the AWS account root user credentials. The root user has no access keys. The company uses AWS Organizations, and the account where the activity occurred is in an OU.

A security engineer needs to take away the root user's ability to make any updates to the account. The root user password cannot be changed to accomplish this goal.

Which solution will meet these requirements?

- A. Attach the following SCP to the account:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Action": "*",
 "Resource": "*",
 "Effect": "Deny",
 "Condition": {
 "StringLike": {
 "aws:PrincipalArn": [
 "arn:aws:root"
]
 }
 }
 }
]
}
```

- B. Attach the following SCP to the account:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Action": "*",
 "Resource": "*",
 "Effect": "Deny",
 "Condition": {
 "StringLike": {
 "aws:PrincipalArn": [
 "arn:aws:iam::*:root"
]
 }
 }
 }
]
}
```

ht051793

C. Attach the following SCP to the account:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Action": "*",
 "Resource": "*",
 "Effect": "Deny",
 "Principal": {
 "AWS": "arn:aws:iam::*:root"
 }
 }
]
}
```

ht051793

D. Attach the following inline IAM policy to the root user:

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

**Answer:** C

**QUESTION 544**

A user is implementing a third-party web application on an Amazon EC2 instance. All client communications must be over HTTPS, and traffic must be terminated before it reaches the instance. Communication to the instance must be over port 80. Company policy requires that workloads reside in private subnets.

Which solution meets these requirements?

- A. Create an Application Load Balancer. Add an HTTP listener for port 80 to redirect traffic to HTTPS on port 443.  
Add another listener with an AWS Certificate Manager (ACM) certificate for termination and a rule that forwards to the target instance through port 80.
- B. Allocate an Elastic IP address that has SSL termination activated.  
Associate the Elastic IP address with the instance on port 80.
- C. Create a Gateway Load Balancer. Add an HTTP listener for port 80 to redirect traffic to HTTPS on port 443.  
Add another listener with an AWS Certificate Manager (ACM) certificate for termination and a rule that forwards to the target instance through port 80.
- D. Implement a Network Load Balancer. Add an HTTP listener for port 80 to redirect traffic to HTTPS on port 443.  
Add another listener with an AWS Certificate Manager (ACM) certificate for termination and a rule that forwards to the target instance through port 80.

**Answer:** D

**QUESTION 545**

A company uses AWS CodePipeline for its software builds. Company policy mandates that code must be deployed to the staging environment before it is deployed to the production environment. The company needs to implement monitoring and alerting to detect when a CodePipeline pipeline is used to deploy code to production without the code first being deployed to staging.

What should a security engineer do to meet these requirements?

- A. Enable Amazon GuardDuty to monitor AWS CloudTrail for CodePipeline.  
Configure findings through AWS Security Hub, and create a custom action in Security Hub to send to Amazon Simple Notification Service (Amazon SNS).

- B. Use the AWS Cloud Development Kit (AWS CDK) to model reference-architecture CodePipeline pipeline that deploys application code through the staging environment and then the production environment.
- C. Turn on AWS Config recording. Use a custom AWS Config rule to examine each CodePipeline pipeline for compliance.  
Configure an Amazon Simple Notification Service (Amazon SNS) notification on any change that is not in compliance with the rule.  
Add the desired receiver of the notification as a subscriber to the SNS topic.
- D. Use Amazon Inspector to conduct an assessment of the CodePipeline pipelines and send a notification upon the discovery of a pipeline that is not in compliance.  
Add the desired receiver of the notification as a subscriber to the Amazon Simple Notification Service (Amazon SNS) topic.

**Answer:** A

**QUESTION 546**

An application is running on an Amazon EC2 instance that has an IAM role attached. The IAM role provides access to an AWS Key Management Service (AWS KMS) customer managed key and an Amazon S3 bucket.

A security engineer discovers a potential vulnerability on the EC2 instance that could result in the compromise of the sensitive data. Due to other critical operations, the security engineer cannot immediately shut down the EC2 instance for vulnerability patching.

What is the FASTEST way to prevent the sensitive data from being exposed?

- A. Download the data from the existing S3 bucket to a new EC2 instance.  
Then delete the data from the S3 bucket. Re-encrypt the data with a client-based key.  
Upload the data to a new S3 bucket.
- B. Block access to the public range of S3 endpoint IP addresses by using a host-based firewall.  
Ensure that internet-bound traffic from the affected EC2 instance is routed through the host-based firewall.
- C. Revoke the IAM role's active session permissions.  
Update the S3 bucket policy to deny access to the IAM role.  
Remove the IAM role from the EC2 instance profile.
- D. Disable the current key.  
Create a new KMS key that the IAM role does not have access to, and re-encrypt all the data with the new key.  
Schedule the compromised key for deletion.

**Answer:** C

**QUESTION 547**

A company stores sensitive documents in Amazon S3 by using server-side encryption with an AWS Key Management Service (AWS KMS) CMK. A new requirement mandates that the CMK that is used for these documents can be used only for S3 actions.

Which statement should the company add to the key policy to meet this requirement?

- A. {  
    "Effect": "Deny",  
    "Principal": "\*",  
    >Action": "kms:\*",  
    "Resource": "\*",  
    "Condition": {  
        "StringNotEquals": {  
            "kms:CallerAccount": "s3.amazonaws.com"  
        }  
    }  
}  
    b0051793
- B. {  
    "Effect": "Deny",  
    "Principal": "\*",  
    "Action": "s3:\*",  
    "Resource": "\*",  
    "Condition": {  
        "StringNotEquals": {  
            "kms:ViaService": "kms.\*amazonaws.com"  
        }  
    }  
}  
    b0051793
- C. {  
    "Effect": "Deny",  
    "Principal": "\*",  
    "Action": "kms:\*",  
    "Resource": "\*",  
    "Condition": {  
        "StringNotEquals": {  
            "kms:ViaService": "s3.\*amazonaws.com"  
        }  
    }  
}  
    b0051793

D. {  
    "Effect": "Deny",  
    "Principal": "\*",  
    >Action": "s3:\*",  
    "Resource": "\*",  
    "Condition": {  
        "StringNotEquals": {  
            "kms:CallerAccount": "kms.amazonaws.com"  
        }  
    }  
}

10051793

**Answer:** B

**QUESTION 548**

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 signed 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 549**

A company is planning to use Amazon Elastic File System (Amazon EFS) with its on-premises servers. The company has an existing AWS Direct Connect connection established between its on-premises data center and an AWS Region. Security policy states that the company's on-premises firewall should only have specific IP addresses added to the allow list and not a CIDR range. The company also wants to restrict access so that only certain data center-based servers have access to Amazon EFS. How should a security engineer implement this solution?

- A. Add the file-system-id efs aws-region amazonaws.com URL to the allow list for the data center firewall  
Install the AWS CLI on the data center-based servers to mount the EFS file system in the EFS security group add the data center IP range to the allow list  
Mount the EFS using the EFS file system name
- B. Assign an Elastic IP address to Amazon EFS and add the Elastic IP address to the allow list for the data center firewall  
Install the AWS CLI on the data center-based servers to mount the EFS file system  
In the EFS security group, add the IP addresses of the data center servers to the allow list  
Mount the EFS using the Elastic IP address
- C. Add the EFS file system mount target IP addresses to the allow list for the data center firewall  
In the EFS security group, add the data center server IP addresses to the allow list  
Use the Linux terminal to mount the EFS file system using the IP address of one of the mount targets
- D. Assign a static range of IP addresses for the EFS file system by contacting AWS Support  
In the EFS security group add the data center server IP addresses to the allow list  
Use the Linux terminal to mount the EFS file system using one of the static IP addresses

**Answer:** B

#### **QUESTION 550**

A company is running workloads in a single AWS account on Amazon EC2 instances and Amazon EMR clusters a recent security audit revealed that multiple Amazon Elastic Block Store (Amazon EBS) volumes and snapshots are not encrypted.

The company's security engineer is working on a solution that will allow users to deploy EC2 Instances and EMR clusters while ensuring that all new EBS volumes and EBS snapshots are encrypted at rest. The solution must also minimize operational overhead.

Which steps should the security engineer take to meet these requirements?

- A. Create an Amazon Event Bridge (Amazon Cloud watch Events) event with an EC2 instance as the source and create volume as the event trigger.  
When the event is triggered invoke an AWS Lambda function to evaluate and notify the security engineer if the EBS volume that was created is not encrypted.
- B. Use a customer managed IAM policy that will verify that the encryption flag of the Createvolume context is set to true.  
Apply this rule to all users.
- C. Create an AWS Config rule to evaluate the configuration of each EC2 instance on creation or modification.  
Have the AWS Config rule trigger an AWS Lambda function to alert the security team and terminate the instance if the EBS volume is not encrypted.
- D. Use the AWS Management Console or AWS CLI to enable encryption by default for EBS volumes in each AWS Region where the company operates.

**Answer:** D

#### **QUESTION 551**

A company needs a security engineer to implement a scalable solution for multi-account authentication and authorization. The solution should not introduce additional user-managed architectural components. Native AWS features should be used as much as possible. The security engineer has set up AWS Organizations with all features activated and AWS SSO enabled. Which additional steps should the security engineer take to complete the task?

- A. Use AD Connector to create users and groups for all employees that require access to AWS accounts.  
Assign AD Connector groups to AWS accounts and link to the IAM roles in accordance with the employees' job functions and access requirements.  
Instruct employees to access AWS accounts by using the AWS Directory Service user portal.
- B. Use an AW5 SSO default directory to create users and groups for all employees that require access to AWS accounts.  
Assign groups to AWS accounts and link to permission sets in accordance with the employees' job functions and access requirements. Instruct employees to access AWS accounts by using the AWS SSO user portal.
- C. Use an AWS SSO default directory to create users and groups for all employees that require access to AWS accounts.  
Link AWS SSO groups to the IAM users present in all accounts to inherit existing permissions.  
Instruct employees to access AWS accounts by using the AW5 SSO user portal.
- D. Use AWS Directory Service or Microsoft Active Directory to create users and groups for all employees that require access to AWS accounts  
Enable AWS Management Console access in the created directory and specify AWS SSO as a source of information for integrated accounts and permission sets.  
Instruct employees to access AWS accounts by using the AWS Directory Service user portal.

**Answer:** B

#### **QUESTION 552**

A company deployed AWS Organizations to help manage its increasing number of AWS accounts. A security engineer wants to ensure only principals in the Organization structure can access a specific Amazon S3 bucket. The solution must also minimize operational overhead. Which solution will meet these requirements?

- A. Put all users into an IAM group with an access policy granting access to the J bucket.
- B. Have the account creation trigger an AWS Lambda function that manages the bucket policy, allowing access to accounts listed in the policy only.
- C. Add an SCP to the Organizations master account, allowing all principals access to the bucket.
- D. Specify the organization ID in the global key condition element of a bucket policy, allowing all principals access.

**Answer:** D

#### **QUESTION 553**

A company's engineering team is developing a new application that creates AWS Key Management Service (AWS KMS) CMK grants for users immediately after a grant is created. Users must be able to use the CMK to encrypt a 512-byte payload. During load testing, a bug appears intermittently where AccessDeniedExceptions are occasionally triggered when a user first attempts to encrypt using the CMK.

Which solution should the company's security specialist recommend?

- A. Instruct users to implement a retry mechanism every 2 minutes until the call succeeds.
- B. Instruct the engineering team to consume a random grant token from users, and to call the CreateGrant operation, passing it the grant token.  
Instruct users to use that grant token in their call to encrypt.
- C. Instruct the engineering team to create a random name for the grant when calling the CreateGrant operation.  
Return the name to the users and instruct them to provide the name as the grant token in the call

- to encrypt.
- D. Instruct the engineering team to pass the grant token returned in the CreateGrant response to users.  
Instruct users to use that grant token in their call to encrypt.

**Answer:** D

**QUESTION 554**

A website currently runs on Amazon EC2, with mostly static content on the site. Recently the site was subjected to a DDoS attack and a security engineer was asked to redesign the edge security to help mitigate this risk in the future.

What are some ways the engineer could achieve this? (Select THREE)

- A. Use AWS X-Ray to inspect the traffic going to the EC2 instances.
- B. Move the static content to Amazon S3, and front this with an Amazon CloudFront distribution.
- C. Change the security group configuration to block the source of the attack traffic.
- D. Use AWS WAF security rules to inspect the inbound traffic.
- E. Use Amazon Inspector assessment templates to inspect the inbound traffic.
- F. Use Amazon Route 53 to distribute traffic.

**Answer:** BDF

**QUESTION 555**

A company deployed Amazon GuardDuty in the us-east-1 Region.

The company wants all DNS logs that relate to the company's Amazon EC2 instances to be inspected.

What should a security engineer do to ensure that the EC2 instances are logged?

- A. Use IPv6 addresses that are configured for hostnames.
- B. Configure external DNS resolvers as internal resolvers that are visible only to AWS.
- C. Use AWS DNS resolvers for all EC2 instances.
- D. Configure a third-party DNS resolver with logging for all EC2 instances.

**Answer:** C

**QUESTION 556**

A company wants to establish separate AWS Key Management Service (AWS KMS) keys to use for different AWS services. The company's security engineer created the following key policy to allow the infrastructure deployment team to create encrypted Amazon Elastic Block Store (Amazon EBS) volumes by assuming the InfrastructureDeployment IAM role:

```

{
 "Version": "2012-10-17",
 "Id": "key-policy-eba",
 "Statement": [
 {
 "Sid": "Enable IAM User Permissions",
 "Effect": "Allow",
 "Principal": [
 "AWS": "arn:aws:iam::123456789012:root"
],
 "Action": "kms:*",
 "Resource": "*"
 },
 {
 "Sid": "Allow use of the key",
 "Effect": "Allow",
 "Principal": [
 "AWS": "arn:aws:iam::123456789012:role/aws-reserved/sso.amazonaws.com/InfrastructureDeployment"
],
 "Action": [
 "kms:Encrypt",
 "kms:Decrypt",
 "kms:ReEncrypt*",
 "kms:GenerateDataKey*",
 "kms:DescribeKey",
 "kms>CreateGrant",
 "kms>ListGrants",
 "kms:RevokeGrant"
],
 "Resource": "*",
 "Condition": [
 "StringEquals": [
 "kms:ViaService": "ec2.us-west-2.amazonaws.com"
]
]
 }
]
}

```

The security engineer recently discovered that IAM roles other than the InfrastructureDeployment role used this key (or other services).

Which change to the policy should the security engineer make to resolve these issues?

- In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change StringEquals to StringLike.
- In the policy document, remove the statement block that contains the Sid "Enable IAM User Permissions".  
Add key management policies to the KMS policy.
- In the statement block that contains the Sid "Allow use of the Key", under the "Condition" block, change the Kms:ViaService value to ec2.us-east-1 .amazonaws.com.
- In the policy document, add a new statement block that grants the kms:Disable' permission to the security engineer's IAM role.

**Answer:** C

#### QUESTION 557

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? (Select TWO.)

- Update the S3 bucket policy to restrict access to a CloudFront origin access identity (OAI).

- 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

#### **QUESTION 558**

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:** A

#### **QUESTION 559**

A developer at a company uses an SSH key to access multiple Amazon EC2 instances. The company discovers that the SSH key has been posted on a public GitHub repository. A security engineer verifies that the key has not been used recently.

How should the security engineer prevent unauthorized access to the EC2 instances?

- A. Delete the key pair from the EC2 console. Create a new key pair.
- B. Use the ModifyInstanceAttribute API operation to change the key on any EC2 instance that is using the key.
- C. Restrict SSH access in the security group to only known corporate IP addresses.
- D. Update the key pair in any AMI that is used to launch the EC2 instances. Restart the EC2 instances.

**Answer:** C

#### **QUESTION 560**

A company's cloud operations team is responsible for building effective security for AWS cross-account access. The team asks a security engineer to help troubleshoot why some developers in the developer account (123456789012) in the developers group are not able to assume a cross-account role (ReadS3) into a production account (999999999999) to read the contents of an Amazon S3 bucket (productionapp).

The two account policies are as follows:

Which recommendations should the security engineer make to resolve this issue? (Select TWO.)

- A. Ask the developers to change their password and use a different web browser.
- B. Ensure that developers are using multi-factor authentication (MFA) when they log in to their developer account as the developer role.
- C. Modify the production account ReadS3 role policy to allow the PutBucketPolicy action on the productionapp S3 bucket.
- D. Update the trust relationship policy on the production account S3 role to allow the account number of the developer account.
- E. Update the developer group permissions in the developer account to allow access to the productionapp S3 bucket.

**Answer:** AD

#### QUESTION 561

A company is using AWS Organizations to develop a multi-account secure networking strategy. The company plans to use separate centrally managed accounts for shared services, auditing, and security inspection. The company plans to provide dozens of additional accounts to application owners for production and development environments.

Company security policy requires that all internet traffic be routed through a centrally managed security inspection layer in the security inspection account. A security engineer must recommend a solution that minimizes administrative overhead and complexity.

Which solution meets these requirements?

- A. Use AWS Control Tower.  
Modify the default Account Factory networking template to automatically associate new accounts with a centrally managed VPC through a VPC peering connection and to create a default route to the VPC peer in the default route table.  
Create an SCP that denies the CreateInternetGateway action.  
Attach the SCP to all accounts except the security inspection account.
- B. Create a centrally managed VPC in the security inspection account.  
Establish VPC peering connections between the security inspection account and other accounts.  
Instruct account owners to create default routes in their account route tables that point to the VPC peer.  
Create an SCP that denies the AttachInternetGateway action.  
Attach the SCP to all accounts except the security inspection account.
- C. Use AWS Control Tower.  
Modify the default Account Factory networking template to automatically associate new accounts with a centrally managed transit gateway and to create a default route to the transit gateway in the default route table.  
Create an SCP that denies the AttachInternetGateway action.  
Attach the SCP to all accounts except the security inspection account.
- D. Enable AWS Resource Access Manager (AWS RAM) for AWS Organizations.  
Create a shared transit gateway, and make it available by using an AWS RAM resource share.  
Create an SCP that denies the CreateInternetGateway action.  
Attach the SCP to all accounts except the security inspection account.  
Create routes in the route tables of all accounts that point to the shared transit gateway.

**Answer:** C

#### QUESTION 562

A company is running an application in The eu-west-1 Region. The application uses an AWS Key Management Service (AWS KMS) CMK to encrypt sensitive data. The company plans to deploy

the application in the eu-north-1 Region.

A security engineer needs to implement a key management solution for the application deployment in the new Region.

The security engineer must minimize changes to the application code.

Which change should the security engineer make to the AWS KMS configuration to meet these requirements?

- A. Update the key policies in eu-west-1.  
Point the application in eu-north-1 to use the same CMK as the application in eu-west-1.
- B. Allocate a new CMK to eu-north-1 to be used by the application that is deployed in that Region.
- C. Allocate a new CMK to eu-north-1.  
Create the same alias name for both keys.  
Configure the application deployment to use the key alias.
- D. Allocate a new CMK to eu-north-1.  
Create an alias for eu-'-1.  
Change the application code to point to the alias for eu-'-1.

**Answer:** B

#### **QUESTION 563**

A company wants to ensure that its AWS resources can be launched only in the us-east-1 and us-west-2 Regions.

What is the MOST operationally efficient solution that will prevent developers from launching Amazon EC2 instances in other Regions?

- A. Enable Amazon GuardDuty in all Regions.  
Create alerts to detect unauthorized activity outside us-east-1 and us-west-2.
- B. Use an organization in AWS Organizations.  
Attach an SCP that allows all actions when the aws:  
Requested Region condition key is either us-east-1 or us-west-2.  
Delete the FullAWSAccess policy.
- C. Provision EC2 resources by using AWS Cloud Formation templates through AWS CodePipeline.  
Allow only the values of us-east-1 and us-west-2 in the AWS CloudFormation template's parameters.
- D. Create an AWS Config rule to prevent unauthorized activity outside us-east-1 and us-west-2.

**Answer:** C

#### **QUESTION 564**

A company is using AWS Organizations. The company wants to restrict AWS usage to the eu-west-1 Region for all accounts under an OU that is named "development." The solution must persist restrictions to existing and new AWS accounts under the development OU.

A.

- A. Include the following SCP on the development OU:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "DenyNonDefaultRegions",
 "Effect": "Deny",
 "NotAction": [
 <Desired Global Services>],
 "Resource": "*",
 "Condition": {
 "StringNotEquals": {
 "aws:RequestedRegion": [
 "eu-west-1"
]
 },
 "ArnNotLike": {
 "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
 }
 }
 }
]
}
```

B.

- B. Include the following SCP on the development account:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "DenyNonDefaultRegions",
 "Effect": "Deny",
 "NotAction": [
 <Desired Global Services>],
 "Resource": "*",
 "Condition": {
 "StringNotEquals": {
 "aws:RequestedRegion": [
 "eu-west-1"
]
 },
 "ArnNotLike": {
 "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
 }
 }
 }
]
}
```

C.

- Ⓐ C. Include the following SCP on the development OU:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "DenyNonDefaultRegions",
 "Effect": "Deny",
 "NotAction": [
 <Desired Global Services>],
 "Resource": "*",
 "Condition": {
 "StringEquals": {
 "aws:RequestedRegion": [
 "eu-west-1"
]
 },
 "ArnNotLike": {
 "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
 }
 }
 }
]
}
```

D.

- Ⓑ D. Include the following SCP on the development OU:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "DenyNonDefaultRegions",
 "Effect": "Allow",
 "NotAction": [
 <Desired Global Services>],
 "Resource": "*",
 "Condition": {
 "StringNotEquals": {
 "aws:RequestedRegion": [
 "us-east-1"
]
 },
 "ArnNotLike": {
 "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
 }
 }
 }
]
}
```

**Answer: A**

**QUESTION 565**

A company deploys a set of standard IAM roles in AWS accounts. The IAM roles are based on

job functions within the company. To balance operational efficiency and security, a security engineer implemented AWS Organizations SCPs to restrict access to critical security services in all company accounts.

All of the company's accounts and OUs within AWS Organizations have a default FullAWSAccess SCP that is attached.

The security engineer needs to ensure that no one can disable Amazon GuardDuty and AWS Security Hub.

The security engineer also must not override other permissions that are granted by IAM policies that are defined in the accounts.

Which SCP should the security engineer attach to the root of the organization to meet these requirements?

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

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

A.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Deny",
 "Action": [
 "guardduty:DeleteDetector",
 "guardduty:UpdateDetector",
 "securityhub:DisableSecurityH
],
 "Resource": [
 "*"
]
 }
]
}
```

B.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "*",
 "Resource": "*"
 },
 {
 "Effect": "Deny",
 "NotAction": [
 "guardduty:DeleteDetector",
 "guardduty:UpdateDetector",
 "securityhub:DisableSecurityHub"
],
 "Resource": [
 "*"
]
 }
]
}
```

```
C. {
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "NotAction": [
 "guardduty:DeleteDetector",
 "guardduty:UpdateDetector",
 "securityhub:DisableSecurityHub"
],
 "Resource": [
 "*"
]
 }
]
}
```

**Answer:** C

#### QUESTION 566

A company deploys a distributed web application on a fleet of Amazon EC2 instances. The fleet is behind an Application Load Balancer (ALB) that will be configured to terminate the TLS connection. All TLS traffic to the ALB must stay secure, even if the certificate private key is compromised.

How can a security engineer meet this requirement?

- A. Create an HTTPS listener that uses a certificate that is managed by AWS Certificate Manager (ACM).
- B. Create an HTTPS listener that uses a security policy that uses a cipher suite with perfect forward secrecy (PFS).
- C. Create an HTTPS listener that uses the Server Order Preference security feature.
- D. Create a TCP listener that uses a custom security policy that allows only cipher suites with perfect forward secrecy (PFS).

**Answer:** A

#### QUESTION 567

A company's application team wants to replace an internal application with a new AWS architecture that consists of Amazon EC2 instances, an AWS Lambda function, and an Amazon S3 bucket in a single AWS Region. After an architecture review, the security team mandates that no application network traffic can traverse the public internet at any point. The security team already has an SCP in place for the company's organization in AWS Organizations to restrict the creation of internet gateways, NAT gateways, and egress-only gateways.

Which combination of steps should the application team take to meet these requirements? (Select THREE.)

- A. Create an S3 endpoint that has a full-access policy for the application's VPC.
- B. Create an S3 access point for the S3 bucket. Include a policy that restricts the network origin to VPCs.
- C. Launch the Lambda function. Enable the block public access configuration.
- D. Create a security group that has an outbound rule over port 443 with a destination of the S3 endpoint.  
Associate the security group with the EC2 instances.
- E. Create a security group that has an outbound rule over port 443 with a destination of the S3 access point.  
Associate the security group with the EC2 instances.
- F. Launch the Lambda function in a VPC.

**Answer:** ADF

#### QUESTION 568

A security engineer receives an AWS abuse email message. According to the message, an Amazon EC2 instance that is running in the security engineer's AWS account is sending phishing email messages.

The EC2 instance is part of an application that is deployed in production. The application runs on many EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple subnets and multiple Availability Zones. The instances normally communicate only over the HTTP, HTTPS, and MySQL protocols. Upon investigation, the security engineer discovers that email messages are being sent over port 587. All other traffic is normal.

The security engineer must create a solution that contains the compromised EC2 instance, preserves forensic evidence for analysis, and minimizes application downtime.

Which combination of steps must the security engineer take to meet these requirements? (Select THREE.)

- A. Add an outbound rule to the security group that is attached to the compromised EC2 instance to deny traffic to 0.0.0.0/0 and port 587.
- B. Add an outbound rule to the network ACL for the subnet that contains the compromised EC2 instance to deny traffic to 0.0.0.0/0 and port 587.
- C. Gather volatile memory from the compromised EC2 instance.  
Suspend the compromised EC2 instance from the Auto Scaling group.  
Then take a snapshot of the compromised EC2 instance.
- D. Take a snapshot of the compromised EC2 instance.  
Suspend the compromised EC2 instance from the Auto Scaling group.  
Then gather volatile memory from the compromised EC2 instance.
- E. Move the compromised EC2 instance to an isolated subnet that has a network ACL that has no inbound rules or outbound rules.
- F. Replace the existing security group that is attached to the compromised EC2 instance with a new security group that has no inbound rules or outbound rules.

**Answer:** ACE

#### QUESTION 569

A company's application team needs to host a MySQL database on AWS. According to the company's security policy, all data that is stored on AWS must be encrypted at rest. In addition, all cryptographic material must be compliant with FIPS 140-2 Level 3 validation. The application team needs a solution that satisfies the company's security requirements and minimizes

operational overhead.

Which solution will meet these requirements?

- A. Host the database on Amazon RDS.
  - Use Amazon Elastic Block Store (Amazon EBS) for encryption.
  - Use an AWS Key Management Service (AWS KMS) custom key store that is backed by AWS CloudHSM for key management.
- B. Host the database on Amazon RDS.
  - Use Amazon Elastic Block Store (Amazon EBS) for encryption.
  - Use an AWS managed CMK in AWS Key Management Service (AWS KMS) for key management.
- C. Host the database on an Amazon EC2 instance.
  - Use Amazon Elastic Block Store (Amazon EBS) for encryption.
  - Use a customer managed CMK in AWS Key Management Service (AWS KMS) for key management.
- D. Host the database on an Amazon EC2 instance.
  - Use Transparent Data Encryption (TDE) for encryption and key management.

**Answer:** B

#### **QUESTION 570**

A Network Load Balancer (NLB) target instance is not entering the InService state.

A security engineer determines that health checks are failing.

Which factors could cause the health check failures? (Select THREE.)

- A. The target instance's security group does not allow traffic from the NLB.
- B. The target instance's security group is not attached to the NLB.
- C. The NLB's security group is not attached to the target instance.
- D. The target instance's subnet network ACL does not allow traffic from the NLB.
- E. The target instance's security group is not using IP addresses to allow traffic from the NLB.
- F. The target network ACL is not attached to the NLB.

**Answer:** ACD

#### **QUESTION 571**

A security engineer creates an Amazon S3 bucket policy that denies access to all users.

A few days later, the security engineer adds an additional statement to the bucket policy to allow read-only access to one other employee.

Even after updating the policy, the employee still receives an access denied message.

What is the likely cause of this access denial?

A security engineer is working with a company to design an ecommerce application. The application will run on Amazon EC2 instances that run in an Auto Scaling group behind an Application Load Balancer (ALB). The application will use an Amazon RDS DB instance for its database. The only required connectivity from the internet is for HTTP and HTTPS traffic to the application. The application must communicate with an external payment provider that allows traffic only from a preconfigured allow list of IP addresses. The company must ensure that communications with the external payment provider are not interrupted as the environment scales.

Which combination of actions should the security engineer recommend to meet these requirements? (Select THREE.)

- A. Deploy a NAT gateway in each private subnet for every Availability Zone that is in use.

- B. Place the DB instance in a public subnet.
- C. Place the DB instance in a private subnet.
- D. Configure the Auto Scaling group to place the EC2 instances in a public subnet.
- E. Configure the Auto Scaling group to place the EC2 instances in a private subnet.
- F. Deploy the ALB in a private subnet.

**Answer:** ACE

### QUESTION 572

A company has two teams, and each team needs to access its respective Amazon S3 buckets. The company anticipates adding more teams that also will have their own S3 buckets. When the company adds these teams, team members will need the ability to be assigned to multiple teams. Team members also will need the ability to change teams. Additional S3 buckets can be created or deleted.

An IAM administrator must design a solution to accomplish these goals.

The solution also must be scalable and must require the least possible operational overhead. Which solution meets these requirements?

- A. Add users to groups that represent the teams.  
Create a policy for each team that allows the team to access its respective S3 buckets only.  
Attach the policy to the corresponding group.
- B. Create an IAM role for each team.  
Create a policy for each team that allows the team to access its respective S3 buckets only.  
Attach the policy to the corresponding role.
- C. Create IAM roles that are labeled with an access tag value of a team.  
Create one policy that allows dynamic access to S3 buckets with the same tag.  
Attach the policy to the IAM roles. Tag the S3 buckets accordingly.
- D. Implement a role-based access control (RBAC) authorization model.  
Create the corresponding policies, and attach them to the IAM users.

**Answer:** A

### QUESTION 573

A company wants to monitor the deletion of customer managed CMKs. A security engineer must create an alarm that will notify the company before a CMK is deleted. The security engineer has configured the integration of AWS CloudTrail with Amazon CloudWatch. What should the security engineer do next to meet this requirement? Within AWS Key Management Service (AWS KMS) specify the deletion time of the key material during CMK creation. AWS KMS will automatically create a CloudWatch. Create an Amazon Eventbridge (Amazon CloudWatch Events) rule to look for API calls of DeleteAlias. Create an AWS Lambda function to send an Amazon Simple Notification Service (Amazon SNS) messages to the company. Add the Lambda functions as the target of the Eventbridge (CloudWatch Events) rule.

Create an Amazon EventBridge (Amazon CloudWath Events) rule to look for API calls of DisableKey and ScheduleKeyDeletion. Create an AWS Lambda function to generate the alarm and send the notification to the company. Add the lambda function as the target of the SNS policy.

- A. Use inbound rule 100 to allow traffic on TCP port 443.  
Use inbound rule 200 to deny traffic on TCP port 3306.  
Use outbound rule 100 to allow traffic on TCP port 443
- B. Use inbound rule 100 to deny traffic on TCP port 3306.  
Use inbound rule 200 to allow traffic on TCP port range 1024-65535.

- Use outbound rule 100 to allow traffic on TCP port 443
- C. Use inbound rule 100 to allow traffic on TCP port range 1024-65535.  
Use inbound rule 200 to deny traffic on TCP port 3306.  
Use outbound rule 100 to allow traffic on TCP port 443
- D. Use inbound rule 100 to deny traffic on TCP port 3306.  
Use inbound rule 200 to allow traffic on TCP port 443.  
Use outbound rule 100 to allow traffic on TCP port 443

**Answer:** A

#### QUESTION 574

A company is hosting a static website on Amazon S3. The company has configured an Amazon CloudFront distribution to serve the website contents. The company has associated an AWS WAF web ACL with the CloudFront distribution. The web ACL ensures that requests originate from the United States to address compliance restrictions.

The company is worried that the S3 URL might still be accessible directly and that requests can bypass the CloudFront distribution.

Which combination of steps should the company take to remove direct access to the S3 URL?  
(Select TWO.)

- A. Select "Restrict Bucket Access" in the origin settings of the CloudFront distribution
- B. Create an origin access identity (OAI) for the S3 origin
- C. Update the S3 bucket policy to allow s3 GetObject with a condition that the aws Referer key matches the secret value Deny all other requests
- D. Configure the S3 bucket policy so that only the origin access identity (OAI) has read permission for objects in the bucket
- E. Add an origin custom header that has the name Referer to the CloudFront distribution. Give the header a secret value.

**Answer:** AD

#### QUESTION 575

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

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

What must the security team do to enable Detective?

- A. Enable Amazon Macie so that Security Hub will allow Detective to process findings from Macie.
- B. Disable AWS Key Management Service (AWS KMS) encryption on CloudTrail logs in every member account of the organization
- C. Enable Amazon GuardDuty on all member accounts. Try to enable Detective in 48 hours
- D. Ensure that the principal that launches Detective has the organization's ListAccounts permission

**Answer:** D

#### QUESTION 576

An application team wants to use AWS Certificate Manager (ACM) to request public certificates to

ensure that data is secured in transit. The domains that are being used are not currently hosted on Amazon Route 53

The application team wants to use an AWS managed distribution and caching solution to optimize requests to its systems and provide better points of presence to customers. The distribution solution will use a primary domain name that is customized. The distribution solution also will use several alternative domain names. The certificates must renew automatically over an indefinite period of time.

Which combination of steps should the application team take to deploy this architecture? (Select THREE.)

- A. Request a certificate (from ACM in the us-west-2 Region)  
Add the domain names that the certificate will secure
- B. Send an email message to the domain administrators to request vacation of the domains for ACM
- C. Request validation of the domains for ACM through DNS  
Insert CNAME records into each domain's DNS zone
- D. Create an Application Load Balancer for the caching solution  
Select the newly requested certificate from ACM to be used for secure connections
- E. Create an Amazon CloudFront distribution for the caching solution  
Enter the main CNAME record as the Origin Name Enter the subdomain names or alternate names in the Alternate Domain Names Distribution Settings  
Select the newly requested certificate from ACM to be used for secure connections
- F. Request a certificate from ACM in the us-east-1 Region  
Add the domain names that the certificate will secure

**Answer:** CDF

#### QUESTION 577

A security engineer needs to create an AWS Key Management Service (AWS KMS) key that will be used to encrypt all data stored in a company's Amazon S3 Buckets in the us-west-1 Region. The key will use server-side encryption. Usage of the key must be limited to requests coming from Amazon S3 within the company's account.

Which statement in the KMS key policy will meet these requirements?

A.

```
{
 "Effect": "Allow",
 "Principal": {
 "AWS": "*"
 },
 "Action": [
 "kms:Encrypt",
 "kms:Decrypt",
 "kms:ReEncrypt*",
 "kms:GenerateDataKey*",
 "kms:DescribeKey"
],
 "Resource": "*",
 "Condition": {
 "StringEquals": {
 "kms:ViaService": "s3.us-west-1.amazonaws.com",
 "kms:CallerAccount": "<CustomerAccountID>"
 }
 }
}
```

B.

```
{
 "Effect": "Allow",
 "Principal": {
 "AWS": "s3.us-west-1.amazonaws.com"
 },
 "Action": [
 "kms:Encrypt",
 "kms:Decrypt",
 "kms:ReEncrypt*",
 "kms:GenerateDataKey*",
 "kms:DescribeKey"
],
 "Resource": "*",
 "Condition": {
 "StringEquals": {
 "kms:CallerAccount": "<CustomerAccountID>"
 }
 }
}
```

C.

```
i
 "Effect": "Allow",
 "Principal": [
 "AWS": "*"
],
 "Action": [
 "kms:Encrypt",
 "kms:Decrypt",
 "kms:ReEncrypt*",
 "kms:GenerateDataKey*",
 "kms:DescribeKey"
],
 "Resource": "*",
 "Condition": [
 "StringEquals": [
 "kms:EncryptionContext:aws:s3:arn": [
 "arn:aws:s3:::/*"
]
]
]
},
```

---

**Answer:** C**QUESTION 578**

A business requires a forensic logging solution for hundreds of Docker-based apps running on Amazon EC2. The solution must analyze logs in real time, provide message replay, and persist logs.

Which Amazon Web Offerings (AWS) services should be employed to satisfy these requirements? (Select two.)

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

**Answer:** BD**QUESTION 579**

Within a VPC, a corporation runs an Amazon RDS Multi-AZ DB instance. The database instance is connected to the internet through a NAT gateway via two subnets. Additionally, the organization has application servers that are hosted on Amazon EC2 instances and use the RDS database. These EC2 instances have been deployed onto two more private subnets inside the same VPC. These EC2 instances connect to the internet through a default route via the same NAT gateway. Each VPC subnet has its own route table. The organization implemented a new security requirement after a recent security examination. Never allow the database instance to connect to the internet. A security engineer must perform this update promptly without interfering with the network traffic of the application servers.

How will the security engineer be able to comply with these requirements?

- A. Remove the existing NAT gateway. Create a new NAT gateway that only the application server subnets can use.
- B. Configure the DB instance TMs inbound network ACL to deny traffic from the security group ID of the NAT gateway.
- C. Modify the route tables of the DB instance subnets to remove the default route to the NAT gateway.
- D. Configure the route table of the NAT gateway to deny connections to the DB instance subnets.

**Answer:** C

**Explanation:**

Each subnet has a route table, so modify the routing associated with DB instance subnets to prevent internet access.

#### QUESTION 580

A development team is attempting to encrypt and decode a secure string parameter from the AWS Systems Manager Parameter Store using an AWS Key Management Service (AWS KMS) CMK. However, each attempt results in an error message being sent to the development team.

Which CMK-related problems possibly account for the error? (Select two.)

- A. The CMK is used in the attempt does not exist.
- B. The CMK is used in the attempt needs to be rotated.
- C. The CMK is used in the attempt is using the CMK TMs key ID instead of the CMK ARN.
- D. The CMK is used in the attempt is not enabled.
- E. The CMK is used in the attempt is using an alias.

**Answer:** AD

**Explanation:**

<https://docs.aws.amazon.com/kms/latest/developerguide/services-parameter-store.html#parameter-store-cmk-fail>

#### QUESTION 581

A business stores website images in an Amazon S3 bucket. The firm serves the photos to end users through Amazon CloudFront. The firm learned lately that the photographs are being accessible from nations in which it does not have a distribution license.

Which steps should the business take to safeguard the photographs and restrict their distribution? (Select two.)

- A. Update the S3 bucket policy to restrict access to a CloudFront origin access identity (OAI).
- 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:**

For Enable Geo-Restriction, choose Yes. For Restriction Type, choose Whitelist to allow access to certain countries, or choose Blacklist to block access from certain countries.

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-geo-restriction/>

**QUESTION 582**

A company has multiple departments. Each department has its own AWS account. All these accounts belong to the same organization in AWS Organizations. A large .csv file is stored in an Amazon S3 bucket in the sales department's AWS account. The company wants to allow users from the other accounts to access the .csv file's content through the combination of AWS Glue and Amazon Athena. However, the company does not want to allow users from the other accounts to access other files in the same folder.

Which solution will meet these requirements?

- A. Apply a user policy in the other accounts to allow AWS Glue and Athena to access the .csv file.
- B. Use S3 Select to restrict access to the .csv file. In AWS Glue Data Catalog, use S3 Select as the source of the AWS Glue database.
- C. Define an AWS Glue Data Catalog resource policy in AWS Glue to grant cross-account S3 object access to the .csv file.
- D. Grant AWS Glue access to Amazon S3 in a resource-based policy that specifies the organization as the principal.

**Answer:** A

**QUESTION 583**

A company's security information events management (SIEM) tool receives new AWS CloudTrail logs from an Amazon S3 bucket that is configured to send all object created event notification to an Amazon SNS topic. An Amazon SQS queue is subscribed to this SNS topic. The company's SEM tool then polls this SQS queue for new messages using an IAM role and fetches new log events from the S3 bucket based on the SQS messages.

After a recent security review that resulted in restricted permissions, the SEM tool has stopped receiving new CloudTrail logs.

Which of the following are possible causes of this issue? (Select THREE)

- A. The SQS queue does not allow the SQS SendMessage action from the SNS topic
- B. The SNS topic does not allow the SNS Publish action from Amazon S3
- C. The SNS topic is not delivering raw messages to the SQS queue
- D. The S3 bucket policy does not allow CloudTrail to perform the PutObject action
- E. The IAM role used by the SEM tool does not have permission to subscribe to the SNS topic
- F. The IAM role used by the SEM tool does not allow the SQS DeleteMessage action.

**Answer:** ADF

**QUESTION 584**

A company recently deployed a new AWS account and wants to be notified immediately if a specific number of unauthorized AWS API requests are detected. A security engineer has turned on AWS CloudTrail for the account and is sending CloudTrail logs to Amazon CloudWatch.

Which other action must the security engineer perform to receive automated alerts about unauthorized AWS API calls?

- A. Create a CloudWatch metric filter that looks for API call error codes. Configure an alarm that is based on that metric's rate to send an Amazon Simple Notification Service (Amazon SNS) notification when the threshold is exceeded.
- B. Configure CloudTrail to stream event data to Amazon Kinesis Data Streams. Configure an AWS

- Lambda function on the stream to initiate an alarm when the threshold is exceeded.
- C. Run an Amazon Athena SQL query against CloudTrail log files for unauthorized API requests. Use Amazon QuickSight to create an operational dashboard.
  - D. Use the AWS Personal Health Dashboard to monitor the account's use of AWS services and to provide an alert if service error rates increase.

**Answer:** C

**Explanation:**

<https://docs.aws.amazon.com/athena/latest/ug/cloudtrail-logs.html>

### QUESTION 585

A company is using Amazon GuardDuty in its AWS environment. The company asks a security engineer to suspend GuardDuty.

Which combination of steps must the security engineer perform to meet this requirement?  
(Choose two.)

- A. Disable all optional data sources from all detectors in all regions.
- B. Disassociate or delete all member accounts.
- C. Disable all associated monitoring services.
- D. Delete all existing findings.
- E. Export all existing findings.

**Answer:** AB

**Explanation:**

[https://docs.aws.amazon.com/guardduty/latest/ug/guardduty\\_suspend-disable.html](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_suspend-disable.html)

### QUESTION 586

A company has a PHP-based web application that uses Amazon S3 as an object store for user files. The S3 bucket that stores the files is configured for server-side encryption with S3 managed encryption keys (SSE-S3).

According to new security requirements, the company must control all encryption keys.  
Additionally, all objects in the S3 bucket must be encrypted by a key that the company controls.

Which combination of steps must a security engineer take to meet these requirements? (Choose three.)

- A. Create a new-customer managed CMK in AWS Key Management Service (AWS KMS).
- B. Change the SSE-S3 configuration on the S3 bucket to server-side encryption with customer-provided encryption keys (SSE-C).
- C. Configure the PHP SDK to use the SSE-S3 key to encrypt the data before the data is uploaded to Amazon S3.
- D. Create an AWS managed CMK for Amazon S3 in AWS Key Management Service (AWS KMS).
- E. Change the SSE-S3 configuration on the S3 bucket to server-side encryption with AWS KMS managed encryption keys (SSE-KMS).
- F. Change all the S3 objects in the bucket to use the new encryption key.

**Answer:** BCE

**Explanation:**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/s3-userguide.pdf#specifying-s3-encryption>

**QUESTION 587**

A company wants to establish separate AWS Key Management Service (AWS KMS) keys to use for different AWS services. The company's security engineer created the following key policy to allow the infrastructure deployment team to create encrypted Amazon Elastic Block Store (Amazon EBS) volumes by assuming the InfrastructureDeployment IAM role:

```
{
 "Version": "2012-10-17",
 "Id": "key-policy-ebs",
 "Statement": [
 {
 "Sid": "Enable IAM User Permissions",
 "Effect": "Allow",
 "Principal": {
 "AWS": "arn:aws:iam::123456789012:root"
 },
 "Action": "kms:*",
 "Resource": "*"
 },
 {
 "Sid": "Allow use of the key",
 "Effect": "Allow",
 "Principal": {
 "AWS": "arn:aws:iam::123456789012:role/aws-
reserved/sso.amazonaws.com/InfrastructureDeployment"
 },
 "Action": [
 "kms:Encrypt",
 "kms:Decrypt",
 "kms:ReEncrypt*",
 "kms:GenerateDataKey*",
 "kms:DescribeKey",
 "kms>CreateGrant",
 "kms>ListGrants",
 "kms:RevokeGrant"
],
 "Resource": "*",
 "Condition": {
 "StringEquals": {
 "kms:ViaService": "ec2.us-west-2.amazonaws.com"
 }
 }
 }
]
}
```

abs51793

The security engineer recently discovered that IAM roles other than the InfrastructureDeployment role used this key for other services.

Which change to the policy should the security engineer make to resolve these issues?

- In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change StringEquals to StringLike.
- In the policy document, remove the statement block that contains the Sid "Enable IAM User Permissions". Add key management policies to the KMS policy.
- In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change the kms:ViaService value to ec2.us-east-1.amazonaws.com.
- In the policy document, add a new statement block that grants the kms:Disable\* permission to the

security engineer's IAM role.

**Answer:** C

**Explanation:**

<https://docs.aws.amazon.com/kms/latest/developerguide/kms-dg.pdf>

**QUESTION 588**

A company has a new AWS account that does not have AWS CloudTrail configured. The account has an IAM access key that was issued by AWS Security Token Service (AWS STS). A security engineer discovers that the IAM access key has been compromised within the last 24 hours.

The security engineer must stop the compromised IAM access key from being used. The security engineer also must determine which activities the key has been used for so far.

What should the security engineer do to meet these requirements?

- A. In the CloudTrail console, under CloudTrail event history, search by access key for the compromised key, with the correlated events, and identify which IAM user the key belongs to. In the IAM console, revoke all active sessions for that IAM user.
- B. Create a new CloudTrail trail. In the CloudTrail console, under CloudTrail event history, search by access key for the compromised key, view the correlated events, and identify which IAM user the key belongs to. In the IAM console, revoke all active sessions for that IAM user.
- C. Create a new CloudTrail trail. In the CloudTrail console, under CloudTrail event history, search by access key for the compromised key, view the correlated events, and identify which IAM role the key belongs to. In the IAM console, delete that IAM role.
- D. In the CloudTrail console, under CloudTrail event history, search by access key for the compromised key, view the correlated events, and identify which IAM role the key belongs to. In the IAM console, revoke all active sessions for that IAM role.

**Answer:** A

**Explanation:**

<https://aws.amazon.com/premiumsupport/knowledge-center/troubleshoot-iam-account-activity/>

**QUESTION 589**

A company has a strict policy against using root credentials. The company's security team wants to be alerted as soon as possible when root credentials are used to sign in to the AWS Management Console.

How should the security team achieve this goal?

- A. Use AWS Lambda to periodically query AWS CloudTrail for console login events and send alerts using Amazon Simple Notification Service (Amazon SNS).
- B. Use Amazon EventBridge (Amazon CloudWatch Events) to monitor console logins and direct them to Amazon Simple Notification Service (Amazon SNS).
- C. Use Amazon Athena to query AWS SSO logs and send alerts using Amazon Simple Notification Service (Amazon SNS) for root login events.
- D. Configure AWS Resource Access Manager to review the access logs and send alerts using Amazon Simple Notification Service (Amazon SNS).

**Answer:** D

**Explanation:**

<https://aws.amazon.com/blogs/security/how-to-receive-notifications-when-your-aws-accounts->

root-access-keys-are-used/

**QUESTION 590**

A security engineer recently rotated all IAM access keys in an AWS account. The security engineer then configured AWS Config and enabled the following AWS Config managed rules; mfa-enabled-for-iam-console-access, iam-user-mfa-enabled, access-key-rotated, and iam-user-unused-credentials-check.

The security engineer notices that all resources are displaying as noncompliant after the IAM GenerateCredentialReport API operation is invoked.

What could be the reason for the noncompliant status?

- A. The IAM credential report was generated within the past 4 hours.
- B. The security engineer does not have the GenerateCredentialReport permission.
- C. The security engineer does not have the GetCredentialReport permission.
- D. The AWS Config rules have a MaximumExecutionFrequency value of 24 hours.

**Answer:** D

**Explanation:**

<https://aws.amazon.com/blogs/mt/managing-aged-access-keys-through-aws-config-remediations/>

**QUESTION 591**

A company wants to gain better control of its large number of AWS accounts by establishing a centralized location where the accounts can be managed. The company also wants to prevent any users outside the company-owned AWS accounts from accessing a company Amazon S3 bucket.

Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Implement an organization in AWS Organizations. Build a detective control by monitoring AWS CloudTrail logs for attempts to access the S3 bucket from IP addresses outside the company.
- B. Deploy an AWS Control Tower landing zone, and migrate the accounts. Create an S3 bucket policy that restricts access to only a principal list of accounts that have been manually entered.
- C. Create an organization in AWS Organizations. Invite the AWS accounts to join the organization. Create a resource policy that includes a PrincipalOrgID condition key for the S3 bucket.
- D. Invite all of the company's AWS accounts into AWS Control Tower. Use AWS Control Tower's automatic protection for the AWS accounts to deny access from external users.

**Answer:** C

**Explanation:**

<https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-aws-organization-of-iam-principals/>

**QUESTION 592**

A company uses Amazon GuardDuty to detect threats and malicious activities in AWS accounts. The company has subscribed to a third-party threat intelligence list uploaded to an Amazon S3 bucket.

How should the security engineer efficiently use the threat list across all company AWS accounts?

- A. Ensure the S3 bucket policy allows all company AWS accounts access to the threat list. Use an AWS Lambda function to automatically add the threat list to all company AWS accounts.
- B. Ensure GuardDuty is in master-member configuration. Add the threat list to the master account referencing the S3 object that contains the threat list.
- C. Ensure all accounts are part of the same organization in AWS Organizations. Add the threat list to any company account within AWS Organizations.
- D. Ensure the threat list in the S3 bucket is publicly accessible. Use an Amazon CloudWatch Events event on GuardDuty findings to match IPs against the threat list.

**Answer:** C

**Explanation:**

<https://aws.amazon.com/blogs/aws/new-using-amazon-guardduty-to-protect-your-s3-buckets/>

#### QUESTION 593

A security engineer needs to create an AWS Key Management Service (AWS KMS) key that will be used to encrypt all data stored in a company's Amazon S3 buckets in the us-west-1 Region. The key will use server-side encryption. Usage of the key must be limited to requests coming from Amazon S3 within the company's account.

Which statement in the KMS key policy will meet these requirements?

A. {  
    "Effect": "Allow",  
    "Principal": {  
        "AWS": "\*"  
    },  
    "Action": [  
        "kms: Encrypt",  
        "kms: Decrypt",  
        "kms: ReEncrypt\*",  
        "kms: GenerateDataKey\*",  
        "kms: DescribeKey"  
    ],  
    "Resource": "\*",  
    "Condition": {  
        "StringEquals": {  
            "kms:ViaService": "s3.us-west-1.amazonaws.com",  
            "kms:CallerAccount": "<CustomerAccountID>"  
        }  
    }  
}

B. {  
    "Effect": "Allow",  
    "Principal": [  
        "AWS": "s3.us-west-1.amazonaws.com"  
    ],  
    "Resource": "\*",  
    "Condition": {  
        "StringEquals": {  
            "kms:CallerAccount": "<CustomerAccountID>"  
        }  
    }  
}  
  
C. {  
    "Effect": "Allow",  
    "Principal": [  
        "AWS": "s3.us-west-1.amazonaws.com"  
    ],  
    "Action": [  
        "kms: Encrypt",  
        "kms: Decrypt",  
        "kms: ReEncrypt\*",  
        "kms: GenerateDataKey\*",  
        "kms: DescribeKey"  
    ],  
    "Resource": "\*",  
    "Condition": {  
        "StringEquals": {  
            "kms:CallerAccount": "<AWSAccountID>"  
        }  
    }  
}

```
D. {
 "Effect": "Allow",
 "Principal": {
 "AWS": "*"
 },
 "Action": [
 "kms: Encrypt",
 "kms: Decrypt",
 "kms: ReEncrypt*",
 "kms: GenerateDataKey*",
 "kms: DescribeKey"
],
 "Resource": "*",
 "Condition": {
 "StringEquals": {
 "kms:EncryptionContext:aws:s3:arn": [
 "arn:aws:s3:::*"
],
 "kms:CallerAccount": "<CustomerAccountID>"
 }
 }
}
```

**Answer:** D

**QUESTION 594**

A company recently set up Amazon GuardDuty and is receiving a high number of findings from IP addresses within the company. A security engineer has verified that these IP addresses are trusted and allowed.

Which combination of steps should the security engineer take to configure GuardDuty so that it does not produce findings for these IP addresses? (Choose two.)

- A. Create a plaintext configuration file that contains the trusted IP addresses.
- B. Create a JSON configuration file that contains the trusted IP addresses.
- C. Upload the configuration file directly to GuardDuty.
- D. Upload the configuration file to Amazon S3. Add a new trusted IP list to GuardDuty that points to the file.
- E. Manually copy and paste the configuration file data into the trusted IP list in GuardDuty.

**Answer:** DE

**QUESTION 595**

A security engineer is analyzing Amazon GuardDuty findings. The security engineer observes an Impact value for ThreatPurpose in a GuardDuty finding.

What does this value indicate?

- A. An adversary has compromised an AWS resource so that the resource is capable of contacting its

- home command and control (C&C) server to receive further instructions for malicious activity.
- B. GuardDuty is detecting activity or activity patterns that are different from the established baseline for a particular AWS resource.
  - C. GuardDuty is detecting activity or activity patterns that suggest that an adversary is attempting to manipulate, interrupt, or destroy the company's systems and data.
  - D. GuardDuty is detecting activity or activity patterns that an adversary might use to expand its knowledge of the company's systems and internal networks.

**Answer:** A

**Explanation:**

[https://docs.aws.amazon.com/guardduty/latest/ug/guardduty\\_finding-format.html](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-format.html)

### QUESTION 596

A company has recently recovered from a security incident that required the restoration of Amazon EC2 instances from snapshots.

After performing a gap analysis of its disaster recovery procedures and backup strategies, the company is concerned that, next time, it will not be able to recover the EC2 instances if the AWS account was compromised and Amazon EBS snapshots were deleted.

All EBS snapshots are encrypted using an AWS KMS CMK.

Which solution would solve this problem?

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

**Answer:** C

**Explanation:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-modifying-snapshot-permissions.html>

### QUESTION 597

A software-as-a-service (SaaS) company hosts an application on AWS in a VPC. External customers will use the application on their own Amazon EC2 instances. To access the application, the customers need to install a client application on an EC2 instance in a VPC in their AWS accounts.

A security engineer is designing a solution to allow communication between the client software and the SaaS application. The solution must maximize scalability and security.

Which combination of actions will meet these requirements? (Choose two.)

- A. Create a Network Load Balancer (NLB) in the VPC in the SaaS company account. Use the NLB for TLS termination and load balancing. Use EC2 instances as targets for the NLB.

- B. Create a Network Load Balancer (NLB) in the VPCs in the customer accounts. Use the NLB for TLS termination and load balancing. Use EC2 instances as targets for the NLB.
- C. Create an AWS PrivateLink endpoint service in the VPCs in the customer accounts. Create a PrivateLink interface endpoint in the VPC in the SaaS company account.
- D. Create an AWS PrivateLink endpoint service in the VPC in the SaaS company account. Create a PrivateLink interface endpoint in the VPCs in the customer accounts.
- E. Create a VPC peering connection between the VPC in the SaaS company account and the VPCs in the customer accounts. Create the required routes for a VPC peering connection.

**Answer:** BE