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"
                    ]
                }
            }
        }
    ]
}
```

B. Apply the following SCP:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRRESTRICTROOTUSER",
            "Effect": "Deny",
            "Principal" : "arn:aws:iam::*:root"
            "Action": "*",
            "Resource": [
                "*"

            ]
        }
    ]
}
```

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"
                    ]
                }
            }
        }
    ]
}
```

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:*:*:*"
            ]
        }
    ]
}
```

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"
                    ]
                }
            }
        }
    ]
}
```

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

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/*"
        }
    ]
}
```

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

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 form 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:EncrytionContext: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

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