**QUESTION 3**

A company is deploying a new public web application to AWS.

The application will run behind an Application Load Balancer (ALB).

The application needs to be encrypted at the edge with an SSL/TLS certificate that is issued by an external certificate authority (CA).

The certificate must be rotated each year before the certificate expires.

What should a solutions architect do to meet these requirements?

1. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate.

Apply the certificate to the ALB.

Use the managed renewal feature to automatically rotate the certificate.

1. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate.

Import the key material from the certificate.

Apply the certificate to the ALB.

Use the managed renewal feature to automatically rotate the certificate.

1. Use AWS Certificate Manager (ACM) Private Certificate Authority to issue an SSL/TLS certificate from the root CA.

Apply the certificate to the ALB.

Use the managed renewal feature to automatically rotate the certificate.

1. Use AWS Certificate Manager (ACM) to import an SSL/TLS certificate.

Apply the certificate to the ALB.

Use Amazon EventBridge (Amazon CloudWatch Events) to send a notification when the certificate is nearing expiration. Rotate the certificate manually.

**Answer:** D

**QUESTION 21**

A company recently signed a contract with an AWS Managed Service Provider (MSP) Partner for help with an application migration initiative.

A solutions architect needs to share an Amazon Machine Image (AMI) from an existing AWS account with the MSP Partner's AWS account.

The AMI is backed by Amazon Elastic Block Store (Amazon EBS) and uses a customer managed customer master key (CMK) to encrypt EBS volume snapshots.

What is the MOST secure way for the solutions architect to share the AMI with the MSP Partner's AWS account?

1. Make the encrypted AMI and snapshots publicly available.

Modify the CMK's key policy to allow the MSP Partner's AWS account to use the key.

1. Modify the launchPermission property of the AMI.

Share the AMI with the MSP Partner's AWS account only.

Modify the CMK's key policy to allow the MSP Partner's AWS account to use the key.

1. Modify the launchPermission property of the AMI.

Share the AMI with the MSP Partner's AWS account only.

Modify the CMK's key policy to trust a new CMK that is owned by the MSP Partner for encryption.

1. Export the AMI from the source account to an Amazon S3 bucket in the MSP Partner's AWS account.

Encrypt the S3 bucket with a CMK that is owned by the MSP Partner.

Copy and launch the AMI in the MSP Partner's AWS account.

**Answer:** B

**QUESTION 23**

A company hosts its web applications in the AWS Cloud.

The company configures Elastic Load Balancers to use certificate that are imported into AWS Certificate Manager (ACM).

The company's security team must be notified 30 days before the expiration of each certificate.

What should a solutions architect recommend to meet the requirement?

1. Add a rule m ACM to publish a custom message to an Amazon Simple Notification Service (Amazon SNS) topic every day beginning 30 days before any certificate will expire.

1. Create an AWS Config rule that checks for certificates that will expire within 30 days. Configure Amazon EventBridge (Amazon CloudWatch Events) to invoke a custom alert by way of Amazon Simple Notification Service (Amazon SNS) when AWS Config reports a noncompliant resource.
2. Use AWS trusted Advisor to check for certificates that will expire within to days.

Create an Amazon CloudWatch alarm that is based on Trusted Advisor metrics for check status changes.

Configure the alarm to send a custom alert by way of Amazon Simple rectification Service (Amazon SNS).

1. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to detect any certificates that will expire within 30 days.

Configure the rule to invoke an AWS Lambda function.

Configure the Lambda function to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS).

**Answer:** B

**Explanation:**

<https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-expiration/>

**QUESTION 35**

A company is preparing to store confidential data in Amazon S3.

For compliance reasons the data must be encrypted at rest Encryption key usage must be logged tor auditing purposes.

Keys must be rotated every year.

Which solution meets these requirements and the MOST operationally efferent?

1. Server-side encryption with customer-provided keys (SSE-C).
2. Server-side encryption with Amazon S3 managed keys (SSE-S3).
3. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with manual rotation.
4. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with automate rotation.

**Answer:** D

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

When you enable automatic key rotation for a customer managed key, AWS KMS generates new cryptographic material for the KMS key every year.

AWS KMS also saves the KMS key's older cryptographic material in perpetuity so it can be used to decrypt data that the KMS key encrypted.

Key rotation in AWS KMS is a cryptographic best practice that is designed to be transparent and easy to use.

AWS KMS supports optional automatic key rotation only for customer managed CMKs.

Enable and disable key rotation. Automatic key rotation is disabled by default on customer managed CMKs.

When you enable (or re-enable) key rotation, AWS KMS automatically rotates the CMK 365 days after the enable date and every 365 days thereafter.

**QUESTION 50**

A company is running an online transaction processing (OLTP) workload on AWS.

This workload uses an unencrypted Amazon RDS DB instance in a Multi-AZ deployment.

Daily database snapshots are taken from this instance.

What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?

1. Encrypt a copy of the latest DB snapshot.

Replace existing DB instance by restoring the encrypted snapshot.

1. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it.

Enable encryption on the DB instance.

1. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS). Restore encrypted snapshot to an existing DB instance.
2. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS)

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_RestoreFromSnapshot.html>

#US

ER\_RestoreFromSnapshot.CON

Under "Encrypt unencrypted resources"

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

**QUESTION 51**

A company wants to build a scalable key management Infrastructure to support developers who need to encrypt data in their applications.

What should a solutions architect do to reduce the operational burden?

1. Use multifactor authentication (MFA) to protect the encryption keys.

1. Use AWS Key Management Service (AWS KMS) to protect the encryption keys.
2. Use AWS Certificate Manager (ACM) to create, store, and assign the encryption keys.
3. Use an IAM policy to limit the scope of users who have access permissions to protect the encryption keys.

**Answer:** B

**QUESTION 52**

A company has a dynamic web application hosted on two Amazon EC2 instances.

The company has its own SSL certificate, which is on each instance to perform SSL termination.

There has been an increase in traffic recently, and the operations team determined that SSL encryption and decryption is causing the compute capacity of the web servers to reach their maximum limit.

What should a solutions architect do to increase the application's performance?

1. Create a new SSL certificate using AWS Certificate Manager (ACM) install the ACM certificate on each instance.

1. Create an Amazon S3 bucket Migrate the SSL certificate to the S3 bucket. Configure the EC2 instances to reference the bucket for SSL termination.
2. Create another EC2 instance as a proxy server Migrate the SSL certificate to the new instance and configure it to direct connections to the existing EC2 instances.
3. Import the SSL certificate into AWS Certificate Manager (ACM).

Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.

**Answer:** D

**Explanation:**

<https://aws.amazon.com/certificate-manager/>

"With AWS Certificate Manager, you can quickly request a certificate, deploy it on ACMintegrated AWS resources, such as Elastic Load Balancers, Amazon CloudFront distributions, and APIs on API Gateway, and let AWS Certificate Manager handle certificate renewals. It also enables you to create private certificates for your internal resources and manage the certificate lifecycle centrally."

**QUESTION 160**

A company's containerized application runs on an Amazon EC2 instance.

The application needs to download security certificates before it can communicate with other business applications.

The company wants a highly secure solution to encrypt and decrypt the certificates in near real time.

The solution also needs to store data in highly available storage after the data is encrypted.

Which solution will meet these requirements with the LEAST operational overhead?

1. Create AWS Secrets Manager secrets for encrypted certificates.

Manually update the certificates as needed.

Control access to the data by using fine-grained IAM access.

1. Create an AWS Lambda function that uses the Python cryptography library to receive and perform encryption operations.

Store the function in an Amazon S3 bucket.

1. Create an AWS Key Management Service (AWS KMS) customer managed key.

Allow the EC2 role to use the KMS key for encryption operations.

Store the encrypted data on Amazon S3.

1. Create an AWS Key Management Service (AWS KMS) customer managed key.

Allow the EC2 role to use the KMS key for encryption operations.

Store the encrypted data on Amazon Elastic Block Store (Amazon EBS) volumes.

**Answer:** D

**QUESTION 170**

A solutions architect needs to ensure that all Amazon Elastic Block Store (Amazon EBS) volumes restored from unencrypted EBS snapshots are encrypted.

What should the solutions architect do to accomplish this?

1. Enable EBS encryption by default for the AWS Region.
2. Enable EBS encryption by default for the specific volumes.
3. Create a new volume and specify the symmetric customer master key (CMK) to use for encryption
4. Create a new volume and specify the asymmetric customer master key (CMK) to use for encryption.

**Answer:** A

**Explanation:**

Question asked is to ensure that all volumes restored are encrypted. So have to be "Enable encryption by default".

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#encryption-bydefault>

**QUESTION 184**

A company is building an application in the AWS Cloud.

The application will store data in Amazon S3 buckets in two AWS Regions.

The company must use an AWS Key Management Service (AWS KMS) customer managed key to encrypt all data that is stored in the S3 buckets.

The data in both S3 buckets must be encrypted and decrypted with the same KMS key.

The data and the key must be stored in each of the two Regions.

Which solution will meet these requirements with the LEAST operational overhead?

1. Create an S3 bucket in each Region.

Configure the S3 buckets to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3).

Configure replication between the S3 buckets.

1. Create a customer managed multi-Region KMS key.

Create an S3 bucket in each Region.

Configure replication between the S3 buckets.

Configure the application to use the KMS key with client-side encryption.

1. Create a customer managed KMS key and an S3 bucket in each Region.

Configure the S3 buckets to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3).

Configure replication between the S3 buckets.

1. Create a customer managed KMS key and an S3 bucket m each Region.

Configure the S3 buckets to use server-side encryption with AWS KMS keys (SSE-KMS). Configure replication between the S3 buckets.

**Answer:** C

**Explanation:**

From https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.html For most users, the default AWS KMS key store, which is protected by FIPS 140-2 validated cryptographic modules, fulfills their security requirements. There is no need to add an extra layer of maintenance responsibility or a dependency on an additional service. However, you might consider creating a custom key store if your organization has any of the following requirements: Key material cannot be stored in a shared environment. Key material must be subject to a secondary, independent audit path. The HSMs that generate and store key material must be certified at FIPS 140-2 Level 3.

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