**QUESTION 2**

A company is developing a two-tier web application on AWS.

The company's developers have deployed the application on an Amazon EC2 instance that connects directly to a backend Amazon RDS database.

The company must not hardcode database credentials in the application.

The company must also implement a solution to automatically rotate the database credentials on a regular basis.

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

1. Store the database credentials in the instance metadata.

Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and instance metadata at the same time.

1. Store the database credentials in a configuration file in an encrypted Amazon S3 bucket.

Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and the credentials in the configuration file at the same time.

Use S3 Versioning to ensure the ability to fall back to previous values.

1. Store the database credentials as a secret in AWS Secrets Manager.

Turn on automatic rotation for the secret.

Attach the required permission to the EC2 role to grant access to the secret.

1. Store the database credentials as encrypted parameters in AWS Systems Manager Parameter Store.

Turn on automatic rotation for the encrypted parameters.

Attach the required permission to the EC2 role to grant access to the encrypted parameters.

**Answer:** C

**QUESTION 26**

A company has a production web application in which users upload documents through a web interlace or a mobile app.

According to a new regulatory requirement, new documents cannot be modified or deleted after they are stored.

What should a solutions architect do to meet this requirement?

1. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled.
2. Store the uploaded documents in an Amazon S3 bucket.

Configure an S3 Lifecycle policy to archive the documents periodically.

1. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning enabled. Configure an ACL to restrict all access to read-only.
2. Store the uploaded documents on an Amazon Elastic File System (Amazon EFS) volume. Access the data by mounting the volume in read-only mode.

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html>

**QUESTION 27**

A company has several web servers that need to frequently access a common Amazon RDS MySQL Multi-AZ DB instance.

The company wants a secure method for the web servers to connect to the database while meeting a security requirement to rotate user credentials frequently.

Which solution meets these requirements?

1. Store the database user credentials in AWS Secrets Manager.

Grant the necessary IAM permissions to allow the web servers to access AWS Secrets Manager.

1. Store the database user credentials in AWS Systems Manager OpsCenter.

Grant the necessary IAM permissions to allow the web servers to access OpsCenter.

1. Store the database user credentials in a secure Amazon S3 bucket.

Grant the necessary IAM permissions to allow the web servers to retrieve credentials and access the database.

1. Store the database user credentials in files encrypted with AWS Key Management Service (AWS KMS) on the web server file system. The web server should be able to decrypt the files and access the database.

**Answer:** A

**Explanation:**

AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html>

**QUESTION 48**

A global company is using Amazon API Gateway to design REST APIs for its loyalty club users in the us-east-1 Region and the ap-southeast-2 Region. A solutions architect must design a solution to protect these API Gateway managed REST APIs across multiple accounts from SQL injection and cross-site scripting attacks.

Which solution will meet these requirements with the LEAST amount of administrative effort?

1. Set up AWS WAF in both Regions.

Associate Regional web ACLs with an API stage.

1. Set up AWS Firewall Manager in both Regions.

Centrally configure AWS WAF rules.

1. Set up AWS Shield in bath Regions.

Associate Regional web ACLs with an API stage.

1. Set up AWS Shield in one of the Regions.

Associate Regional web ACLs with an API stage.

**Answer:** A

**QUESTION 45**

A company uses a popular content management system (CMS) for its corporate website. However, the required patching and maintenance are burdensome.

The company is redesigning its website and wants a new solution.

The website will be updated four times a year and does not need to have any dynamic content available.

The solution must provide high scalability and enhanced security.

Which combination of changes will meet these requirements with the LEAST operational overhead? (Choose TWO)

1. Deploy an AWS WAF web ACL in front of the website to provide HTTPS functionality.
2. Create and deploy an AWS Lambda function to manage and serve the website content.
3. Create the new website and an Amazon S3 bucket.

Deploy the website on the S3 bucket with static website hosting enabled.

1. Create the new website.

Deploy the website by using an Auto Scaling group of Amazon EC2 instances behind an Application Load Balancer.

**Answer:** AD

**QUESTION 119**

A company has an application that provides marketing services to stores.

The services are based on previous purchases by store customers.

The stores upload transaction data to the company through SFTP, and the data is processed and analyzed to generate new marketing offers.

Some of the files can exceed 200 GB in size.

Recently, the company discovered that some of the stores have uploaded files that contain personally identifiable information (PII) that should not have been included.

The company wants administrators to be alerted if PII is shared again.

The company also wants to automate remediation.

What should a solutions architect do to meet these requirements with the LEAST development effort?

1. Use an Amazon S3 bucket as a secure transfer point.

Use Amazon Inspector to scan me objects in the bucket.

If objects contain Pll, trigger an S3 Lifecycle policy to remove the objects that contain Pll.

1. Use an Amazon S3 bucket as a secure transfer point.

Use Amazon Macie to scan the objects in the bucket.

If objects contain Pll, use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects mat contain Pll.

1. Implement custom scanning algorithms in an AWS Lambda function.

Trigger the function when objects are loaded into the bucket.

If objects contain Rll, use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain Pll.

1. Implement custom scanning algorithms in an AWS Lambda function.

Trigger the function when objects are loaded into the bucket.

If objects contain Pll, use Amazon Simple Email Service (Amazon STS) to trigger a notification to the administrators and trigger on S3 Lifecycle policy to remove the objects mot contain PII.

**Answer:** B

**QUESTION 140**

A company recently migrated to AWS and wants to implement a solution to protect the traffic that flows in and out of the production VPC.

The company had an inspection server in its on-premises data center.

The inspection server performed specific operations such as traffic flow inspection and traffic filtering.

The company wants to have the same functionalities in the AWS Cloud.

Which solution will meet these requirements?

1. Use Amazon GuardDuty for traffic inspection and traffic filtering in the production VPC.

1. Use Traffic Mirroring to mirror traffic from the production VPC for traffic inspection and filtering.
2. Use AWS Network Firewall to create the required rules for traffic inspection and traffic filtering for the production VPC.

D. Use AWS Firewall Manager to create the required rules for traffic inspection and traffic filtering for the production VPC.

**Answer:** C

**QUESTION 164**

A solutions architect must design a highly available infrastructure for a website.

The website is powered by Windows web servers that run on Amazon EC2 instances.

The solutions architect must implement a solution that can mitigate a large-scale DDoS attack that originates from thousands of IP addresses.

Downtime is not acceptable for the website.

Which actions should the solutions architect take to protect the website from such an attack? (Select TWO)

1. Use AWS Shield Advanced to stop the DDoS attack.

1. Configure Amazon GuardDuty to automatically block the attackers.
2. Configure the website to use Amazon CloudFront for both static and dynamic content.
3. Use an AWS Lambda function to automatically add attacker IP addresses to VPC network ACLs.
4. Use EC2 Spot Instances in an Auto Scaling group with a target tracking scaling policy that is set to 80% CPU utilization

**Answer:** AC

**QUESTION 174**

A company needs to review its AWS Cloud deployment to ensure that its Amazon S3 buckets do not have unauthorized configuration changes.

What should a solutions architect do to accomplish this goal?

1. Turn on AWS Config with the appropriate rules.

1. Turn on AWS Trusted Advisor with the appropriate checks.
2. Turn on Amazon Inspector with the appropriate assessment template.
3. Turn on Amazon S3 server access logging.

Configure Amazon EventBridge (Amazon Cloud Watch Events).

**Answer:** A

**QUESTION 183**

A company is preparing to launch a public-facing web application in the AWS Cloud.

The architecture consists of Amazon EC2 instances within a VPC behind an Elastic Load Balancer (ELB).

A third-party service is used for the DNS.

The company's solutions architect must recommend a solution to detect and protect against large-scale DDoS attacks.

Which solution meets these requirements?

1. Enable Amazon GuardDuty on the account.

1. Enable Amazon Inspector on the EC2 instances.
2. Enable AWS Shield and assign Amazon Route 53 to it.
3. Enable AWS Shield Advanced and assign the ELB to it.

**Answer:** D

**Explanation:**

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

**QUESTION 190**

A company operates an ecommerce website on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group.

The site is experiencing performance issues related to a high request rate from illegitimate external systems with changing IP addresses.

The security team is worried about potential DDoS attacks against the website.

The company must block the illegitimate incoming requests in a way that has a minimal impact on legitimate users.

What should a solutions architect recommend?

1. Deploy Amazon Inspector and associate it with the ALB.

1. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.
2. Deploy rules to the network ACLs associated with the ALB to block the incoming traffic.
3. Deploy Amazon GuardDuty and enable rate-limiting protection when configuring GuardDuty.

**Answer:** B

**Explanation:** Rate limit

For a rate-based rule, enter the maximum number of requests to allow in any five-minute period from an IP address that matches the rule's conditions. The rate limit must be at least 100.

You can specify a rate limit alone, or a rate limit and conditions. If you specify only a rate limit, AWS WAF places the limit on all IP addresses. If you specify a rate limit and conditions, AWS WAF places the limit on IP addresses that match the conditions.

When an IP address reaches the rate limit threshold, AWS WAF applies the assigned action (block or count) as quickly as possible, usually within 30 seconds. Once the action is in place, if five minutes pass with no requests from the IP address, AWS WAF resets the counter to zero.

**QUESTION 113**

A company performs monthly maintenance on its AWS infrastructure.

During these maintenance activities, the company needs to rotate the credentials tor its Amazon RDS tor MySQL databases across multiple AWS Regions.

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

1. Store the credentials as secrets in AWS Secrets Manager.

Use multi-Region secret replication for the required Regions.

Configure Secrets Manager to rotate the secrets on a schedule.

1. Store the credentials as secrets in AWS Systems Manager by creating a secure string parameter.

Use multi-Region secret replication for the required Regions.

Configure Systems Manager to rotate the secrets on a schedule.

1. Store the credentials in an Amazon S3 bucket that has server-side encryption (SSE) enabled. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke an AWS Lambda function to rotate the credentials.

1. Encrypt the credentials as secrets by using AWS Key Management Service (AWS KMS) multiRegion customer managed keys.

Store the secrets in an Amazon DynamoDB global table.

Use an AWS Lambda function to retrieve the secrets from DynamoDB.

Use the RDS API to rotate the secrets.

**Answer:** D

**QUESTION 211**

A company's web application is running on Amazon EC2 instances behind an Application Load Balancer.

The company recently changed its policy, which now requires the application to be accessed from one specific country only.

Which configuration will meet this requirement?

1. Configure the security group for the EC2 instances.

1. Configure the security group on the Application Load Balancer.
2. Configure AWS WAF on the Application Load Balancer in a VPC.
3. Configure the network ACL for the subnet that contains the EC2 instances.

**Answer:** C

**Explanation:**

<https://aws.amazon.com/about-aws/whats-new/2017/10/aws-waf-now-supports-geographicmatch/>

**QUESTION 217**

A security team wants to limit access to specific services or actions in all of the team's AWS accounts.

All accounts belong to a large organization in AWS Organizations.

The solution must be scalable and there must be a single point where permissions can be maintained.

What should a solutions architect do to accomplish this?

1. Create an ACL to provide access to the services or actions.

1. Create a security group to allow accounts and attach it to user groups.
2. Create cross-account roles in each account to deny access to the services or actions.
3. Create a service control policy in the root organizational unit to deny access to the services or actions.

**Answer:** D

**Explanation:**

Service control policies (SCPs) are one type of policy that you can use to manage your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines. <https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html>

**QUESTION 218**

A company is concerned about the security of its public web application due to recent web attacks.

The application uses an Application Load Balancer (ALB).

A solutions architect must reduce the risk of DDoS attacks against the application.

What should the solutions architect do to meet this requirement?

1. Add an Amazon Inspector agent to the ALB.

1. Configure Amazon Macie to prevent attacks.
2. Enable AWS Shield Advanced to prevent attacks.
3. Configure Amazon GuardDuty to monitor the ALB.

**Answer:** C

**QUESTION 236**

An application runs on Amazon EC2 instances in private subnets.

The application needs to access an Amazon DynamoDB table.

What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

1. Use a VPC endpoint for DynamoDB.

1. Use a NAT gateway in a public subnet.
2. Use a NAT instance in a private subnet.
3. Use the internet gateway attached to the VPC.

**Answer:** A

**Explanation:** <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpointsdynamodb.html>

A VPC endpoint for DynamoDB enables Amazon EC2 instances in your VPC to use their private IP addresses to access DynamoDB with no exposure to the public internet. Your EC2 instances do not require public IP addresses, and you don't need an internet gateway, a NAT device, or a virtual private gateway in your VPC. You use endpoint policies to control access to DynamoDB. Traffic between your VPC and the AWS service does not leave the Amazon network.

**QUESTION 242**

A company is designing a cloud communications platform that is driven by APIs.

The application is hosted on Amazon EC2 instances behind a Network Load Balancer (NLB).

The company uses Amazon API Gateway to provide external users with access to the application through APIs.

The company wants to protect the platform against web exploits like SQL injection and also wants to detect and mitigate large, sophisticated DDoS attacks.

Which combination of solutions provides the MOST protection? (Select TWO)

1. Use AWS WAF to protect the NLB.

1. Use AWS Shield Advanced with the NLB.
2. Use AWS WAF to protect Amazon API Gateway.
3. Use Amazon GuardDuty with AWS Shield Standard.
4. Use AWS Shield Standard with Amazon API Gateway.

**Answer:** CE

**QUESTION 220**

A solutions architect must design a solution that uses Amazon CloudFront with an Amazon S3 origin to store a static website.

The company's security policy requires that all website traffic be inspected by AWS WAF.

How should the solutions architect comply with these requirements?

1. Configure an S3 bucket policy lo accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.
2. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.
3. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only.

Associate AWS WAF to CloudFront.

1. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket.

Enable AWS WAF on the distribution.

**Answer:** D

**Explanation:** <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-contentrestricting-access-to-s3.html>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-webawswaf.html>