SECTION 3

Compute: Amazon EC2 and AWS Lambda

Exam Scenarios

Exam Scenario	Solution
Administrator needs to check if any EC2 instances will be affected by scheduled hardware maintenance	Check the AWS Personal Health Dashboard
Scheduled hardware maintenance will affect a critical EC2 instance	Stop and start the instance to move it to different underlying hardware
When launching an EC2 instance the `InsufficientInstanceCapacity` error is experienced	This means AWS does not currently have enough capacity to service the request for that instance type. Try a different AZ or instance type
The error `InstanceLimitExceeded` is experienced when launching EC2 instances	EC2 instance limits have been reached, need to contact support to request an increased limit

Exam Scenarios

Exam Scenario	Solution
System status checks are failing for an EC2 instance	Stop and start again to move to a new host
For security and compliance reasons EC2 instances must not be able to access the internet	Launch them in a private subnet without a NAT gateway or NAT instance
EC2 instances must communicate with an internet-based service which whitelists a single source IP address	Place the instances behind a NAT gateway as the device will have a single elastic IP address that can be whitelisted
A distributed app is running on EC2 and can handle processing interruptions. Determine the best pricing model to use	Use Spot instances as the application can handle it if the instances are terminated

Exam Scenarios

Exam Scenario	Solution
Define AWS' responsibilities for EC2 hardware according to the AWS Shared Responsibility Model	AWS are responsible for managing the health of the underlying hosts
A nightly job runs on EC2 and stores results in S3. Takes 2 hours using multiple on-demand instances. If it fails, it must start again. Determine the best pricing model to use	Request a Spot block for time period required
An asynchronous process runs on EC2 and feeds data to a data warehouse for weekly/monthly reporting. Determine the best pricing model to use	Use Spot instances as the asynchronous nature of the reporting means the app can handle interruption if AWS need the capacity back
Need to track EC2 and on-premise computer memory utilization	Install the unified CloudWatch agent on both EC2 and on-premises servers

Exam Scenarios

Exam Scenario	Solution
Amazon EC2 Auto Scaling automatically terminates unhealthy instances but Administrator needs to keep the logs for subsequent analysis	Install the CloudWatch agent to stream logs to CloudWatch Logs
There is a suspected memory leak on an Amazon EC2 instance	Install the CloudWatch agent to monitor memory utilization
An AWS Lambda function is expected to see a large increase in traffic and must scale	Ensure the concurrency limit is higher than the expected simultaneous executions
Need to invoke an AWS Lambda function every 15 minutes	Create an event rule in Amazon CloudWatch events to execute the function periodically

SECTION 4

Scaling Compute: Elastic Load Balancing and Auto Scaling

Exam Scenarios

Exam Scenario	Solution
Design required for highly available and secure website on EC2 with ALB, and DB on EC2	Launch ALB in public subnets, web servers in private subnets and DB layer in private subnets – all layers across AZs
HealthyHostCount metrics for an ALB have dropped from 6 to 2. Need to determine the cause	The health checks on target EC2 instances are failing
An instance attached to an ALB exceeded the UnhealthyThresholdCount for consecutive health check failures. What will happen?	Health checks will continue and the ALB will take the instance out of service

Exam Scenarios

Exam Scenario	Solution
Requirement to track the source IP of clients and the instance that processes the request	Check the ALB access logs for this information
Requirement to trigger an alarm when all instances are unhealthy	Use Amazon CloudWatch with the condition: "AWS/ApplicationELB HealthyHostCount <= 0"
Need to check why users cannot connect to web server public IP and port (behind ALB)	Check the VPC Flow Logs

Exam Scenarios

Exam Scenario	Solution
HTTPCode_ELB_5XX_Count Amazon CloudWatch metrics are noticed for an ALB	The target group may not contain any healthy instances
CloudWatch shows 4XX errors for app with ALB but the Instances have already been terminated and need to analyze the root cause	Use ELB access logs to retrieve info from S3 bucket to find the originators of the requests
Need a load balancer where specific static public IP addresses can be whitelisted by clients	Use a Network Load Balancer (NLB)

Exam Scenarios

Exam Scenario	Solution
Poor performance has been experienced for an application running on Amazon EC2	Use EC2 Auto Scaling to dynamically scale
503 and 504 errors experienced and instances have high CPU utilization	Use EC2 Auto Scaling to dynamically scale
ASG does not launch instances during busy periods despite max capacity not being reached	Could be due to service limits (check Trusted Advisor) or check for RunInstances requests in CloudTrail in case they are failing
Need to analyze instances before they are terminated	Use Auto Scaling lifecycle hooks to pause termination

Exam Scenarios

Exam Scenario	Solution
Auto Scaling scales based on queue depth but at beginning of day app slows down	Create a scheduled scaling policy
Create highly available EC2 Auto Scaling group for a single instance app	Use at least 3 AZs, min size of 2, desired capacity of 2, and max of 2
Elastic Beanstalk worker node reads messages from SQS queue. Auto Scaling scales instances. App slows down when number of messages in queue increases	Update ASG to scale on queue depth
ALB is expecting a large spike in traffic and the application is memory heavy	Use the RequestCountPerTarget metric to control scaling

Exam Scenarios

Exam Scenario	Solution
New instances in an Auto Scaling group are not showing up in the aggregated metrics. Step scaling is used	Likely due to the warm-up period having not yet expired

SECTION 5

Storage: Amazon EBS, EFS, and AWS Storage Gateway

Exam Scenarios

Exam Scenario	Solution
User deleted some data in an Amazon EBS volume and there's a recent snapshot	Can create a new EBS volume from the snapshot and attach it to an instance and copy the delete file across
EBS volume runs out of space and need to prevent it happening again	Use CloudWatch agent on EC2 and monitor disk metrics with CloudWatch alarm
Most cost-effective option for big data app that stores sequentially and infrequent access	Cold HDD (sc1)
EBS volume capacity is increased but cannot see the space	Need to extend the volume's file system to gain access to extra space

Exam Scenarios

Exam Scenario	Solution
Need to replace user-shared drives. Must support POSIX permissions and NFS protocols and be accessible from on-premise servers and EC2	Use Amazon EFS
Low latency access required for image files in an office location with synchronized backup to offsite location. Local access required and disaster recovery	Use an AWS Storage Gateway volume gateway configured as a stored volume
Performance issues with iSCSI drives in volume gateway. CacheHitPercent metric is below 55% and CachePerecentUsed is above 95%	Create a larger disk for cached volume and select it in management console
Tape archival system needs replacement	Use an AWS Storage Gateway tape gateway

SECTION 6

Operations: AWS Systems Manager and OpsWorks

Exam Scenarios

Exam Scenario	Solution
Application running on EC2 needs login credentials for a DB that are stored as secure strings in SSM Parameter Store	Create an IAM role for the instance and grant permission to read the parameters
Linux instances are patched with Systems Manager Patch Manager. Application slows down whilst updates are happening	Change maintenance window to patch 10% of instances in the patch group at a time
Custom Linux AMI used with AWS Systems Manager. Can't find instances in Session Manager console	Need to add permissions to instance profile and install the SSM agent on the instances

Exam Scenarios

Exam Scenario	Solution
Multiple environments require authentication credentials for external service. Deployed using CloudFormation	Store credentials in SSM Parameter Store and pass an environment tag as a parameter in CloudFormation template
IAM access keys used to manage EC2 instances using the CLI. Company policy mandates that access keys are automatically disabled after 60 days	Use an AWS Config rule to identify noncompliant keys. Create a custom AWS Systems Manager Automation document for remediation

SECTION 8

Infrastructure Automation: AWS CloudFormation

Exam Scenarios

Exam Scenario	Solution
Need to review updates to a CloudFormation stack before deploying them in production	Use change sets
Stack deployed and manual changes were made. Need to capture changes and update template	Use drift detection and use output to update template and redeploy the stack
Need to update new version of app on EC2 and ALB. Must avoid DNS changes and be able to rollback	Update template with AutoScalingReplacingUpdate policy and perform an update
Need to write a single template that can be deployed across several environments / Region	Use parameters to enter custom values and use Ref intrinsic function to reference the parameter
Tried to launch instance in a different region from a working template and it fails	Probably due to incorrect AMI ID

Exam Scenarios

Exam Scenario	Solution
CloudFormation stack created for first time and fails with ROLLBACK_COMPLETE status	To continue administrator must relaunch the template to create a new stack
Template for infrastructure in one region used to deploy in another and fails	Template likely referenced an AMI that doesn't exist in the new region and/or services that don't exist
CloudFormation stack fails and returns UPDATE_ROLLBACK_FAILED	Fix the error that caused the rollback to fail and then select "Continue update rollback" in the console
Need to deploy a single CloudFormation template across multiple accounts	Use StackSets
CloudFormation deploys stack with separate VPC for each app. Fails to deploy	May have reached the default limit for VPCs in the account

Exam Scenarios

Exam Scenario	Solution
Would like to manually address any issues with CloudFormation stack creation	Set the OnFailure parameter to "DO_NOTHING”
CloudFormation fails with "The image id ‘[ami-2a69aa47]’ does not exist"	Most likely the template is being run in a different region where the AMI does not exist
When creating Stack a wait condition error is experienced: ""received 0 signals out of the 1 expected from the EC2 instance"."	Check instance has a route through NAT device and in the cfn logs confirm that the cfn-signal command ran successfully

SECTION 9

Networking: Amazon Virtual Private Cloud (VPC)

Exam Scenarios

Exam Scenario	Solution
Need to identify the instances that are generating the most traffic using a NAT gateway	Use VPC flow logs on the NAT gateway ENI and use CloudWatch insights to filter based on source IP address
Latency on a NAT instance has increased, need a solution that scales with demand cost-efficiently	Swap with a NAT gateway
NAT gateway is NOT highly available across AZs, only within an AZ	Use multiple NAT gateways for HA across AZs
NAT instance deployed but not working	Make sure to disable source/destination checks
Need to enable access to S3 without the instances using public IP addresses	Use a NAT gateway or VPC endpoint

Exam Scenarios

Exam Scenario	Solution
EC2 instance in private subnet cannot reach the Internet. Route table has a route to a NAT gateway with a status of "Blackhole"	Indicates the NAT gateway has been deleted
Need to connect to S3 from EC2 using private network only. Must also ensure that only the instances can access the bucket	Create a VPC endpoint and a bucket policy with a Condition that limits S3 actions to the VPC endpoint as the source
VPC endpoint setup to allow private IP address connectivity to S3 bucket, permissions configured, but instances still can't connect	Make sure the subnet has a target in the route table for the VPC endpoint

Exam Scenarios

Exam Scenario	Solution
Need to manage EC2 instances in a private subnet from an office using SSH but instances cannot have internet access	Add a VGW and configure routing in the VPC and establish a VPN to the office
Need encryption in-transit and at-rest for hybrid environment	Use an AWS VPN and use KMS keys for data encryption
Network change was made that resulted in application to DB connection issues	Analyze using VPC Flow Logs
Inbound and outbound internet connectivity required for EC2 instances	Need to attach an internet gateway to the VPC and add an entry in the route table for the subnet that points to the internet gateway

Exam Scenarios

Exam Scenario	Solution
Web application has EC2 with public IPs behind an ALB. EC2 instances cannot connect to external service	Need to create an attach an IGW to the VPC and update the route table
VPC peering connection setup between two different VPCs. Instances in private subnets still can't communicate	Make sure the route tables are updated
A company has configured a VPC peering connection between two VPCs and needs to set up connectivity between instances in private subnets	Configure the VPC route tables with routes pointing to the address range of the other VPC
Company backing up one VPC to another in different region. All data must be private and encrypted	Use inter-region VPC peering which encrypts across the AWS global network

Exam Scenarios

Exam Scenario	Solution
Malicious IP identified and must be blocked from all ingress and egress connectivity	Add a rule to a network ACL for all affected subnets
VPC connected to data center by VPN. User pings private subnet instance from on-prem computer and fails. VPC Flow Logs show accept for inbound but reject for outbound traffic	Modify the network ACL to allow outbound traffic
Malicious traffic coming from a single IP address	Use a NACL for the web server subnet to deny IP address
Admin has setup instance for remote access and can SSH from internet but cannot ping	Most likely reason is that the instance's security group does not have a rule allowing ICMP

Exam Scenarios

Exam Scenario	Solution
Admin connecting to EC2 instance using SSH from office but gets connection timeout from home	Most likely doesn't have the home network IP range in the security group allow rule for SSH

SECTION 10

DNS: Amazon Route 53

Exam Scenarios

Exam Scenario	Solution
Use Route 53 to direct based on health checks with (2xx) traffic to primary and other responses to secondary	Need to create an A record for each server and a HTTP (not TCP) health check
Route 53 health check uses string matching for "/html". Alert shows health check fails	The search string must appear entirely within the first 5,120 bytes of the response body
Need to make a website promotion visible to users from a specific country only	Use Route 53 geolocation routing policy

Exam Scenarios

Exam Scenario	Solution
New website runs on EC2 behind ALB. Need to create record in Route 53 to point to the domain apex (e.g. example.com)	Use an alias record
Hosted zone in Account A and ALB in Account B. Need the most cost-effective and efficient solution for pointing to the ALB	Create an Alias record in Account A that points to ALB in Account B

SECTION 11

Object Storage and Content Delivery: S3 and CloudFront

Exam Scenarios

Exam Scenario	Solution
Static website on Amazon S3 with custom domain name	Requires that the bucket name matches the DNS name / record set name in Route 53
503 errors experienced with new site and thousands of user	Request rate is too high
Discrepancy with number of objects in bucket console vs CloudWatch	Use Amazon S3 Inventory to properly determine the number of objects in a bucket
Need to enforce encryption on all objects uploaded to bucket	Use a bucket policy with a "Condition": { "Bool": { "aws:SecureTransport": "false" statement for PutObject and with the resource set to the bucket

Exam Scenarios

Exam Scenario	Solution
Unauthorized users tried to connect to S3 buckets. Need to know which buckets are targeted and who is trying to get access	Use S3 server access logs and Athena to query for HTTP 403 errors and look for IAM user or role making requests
Need to provide access to third-party to S3 bucket and must limit amount of access. List of users changes a lot	Use a pre-signed URL allowing access to the specific files
Need to protect S3 data from ransomware attacks that encrypt data	Enable S3 versioning
After enabling MFA on a bucket, what operations will require MFA authentication?	Permanently removing object versions and suspending versioning on the bucket

Exam Scenarios

Exam Scenario	Solution
Files are downloaded from S3, edited and uploaded with same file name. Sometimes they are accidentally modified or deleted	To allow recovery enable versioning on the bucket
Existing application uses EC2, RDS, EFS and S3. Need to enable encryption	Can enable encryption only on S3 (as already deployed)
Static website deployed but "HTTP 403 Forbidden" message received	Add bucket policy granting everyone read access to objects
Application on EC2 must save files to Amazon S3 and needs access	Create an IAM role for S3 access and attach to EC2 instance

Exam Scenarios

Exam Scenario	Solution
History of revisions to files stored in an S3 bucket must be maintained	Implement S3 versioning
Large volume of log files stored in S3 bucket and processed daily	Most cost-effective option is S3 standard
Need to restrict S3 bucket access to same account after previously shared with other account	Change ACL to restrict only to bucket owner
Static content is served from Amazon S3 with long loading times	Use CloudFront to cache for better performance
Need to use custom domain name with CloudFront	Create an alias record in Route 53 pointing to the distribution URL

Exam Scenarios

Exam Scenario	Solution
CloudFront in front of ALB and EC2 and logging enabled. Need to view logs for HTTP layer 7 status codes	Check ALB access logs and CloudFront access logs
App running on EC2 with RDS multi-AZ has static content on S3. Need to improve performance as load testing slowed it down	Use CloudFront to cache the content
Need to secure S3 bucket that is used with CloudFront	Use an OAI and grant permissions to read objects in the bucket
Website with dynamic content and need to restrict access from certain countries and regions	Use Amazon CloudFront geo-restriction and Amazon Route 53 geolocation routing

SECTION 12

Databases: Amazon RDS and ElastiCache

Exam Scenarios

Exam Scenario	Solution
Automated failover of a multi-AZ DB occurred	This may be due to storage failure on primary DB or the instance type could have been changed
Need to encrypt unencrypted RDS database	Take a snapshot, encrypt it, then restore a new encrypted instance from the snapshot
RDS DB query latency is high and CPU utilization is at 100%	Scale up with larger instance type
Need to share RDS DB snapshots across different accounts. Data must be encrypted	Use an AWS KMS key for encryption and update key policy to grant accounts with access then share snapshot

Exam Scenarios

Exam Scenario	Solution
DB needs to be made HA to protect against failure and updates cannot impact users in business hours	Change to Multi-AZ outside of business hours
Need to protect RDS databases against table corruption within a 30 day window of protection	Enable automated backups and set the appropriate retention period
Shared Responsibility Model	AWS is responsible for maintenance, patches and other updates for Aurora DB
AuroraReplicaLagMaximum is high for DB on eCommerce site. What affect could this have?	may result in cart not updating correctly (inconsistency)

Exam Scenarios

Exam Scenario	Solution
EC2 connects to RDS instance and fails with: "Error Establishing a Database Connection"	Web server may be using certificate validation and RDS does not trust the certificate. Or, the DB security group does not have the correct ingress rule
Aurora DB is hitting 100% CPU. Read-heavy app with many lookups	Add Aurora Replicas and use a Reader Endpoint for product table lookups
Database is running MySQL on Amazon EC2. Need to increase availability and durability without changing application	Use Aurora MySQL and configure an Aurora Replica in another AZ
Reporting job runs against RDS instance and is causing performance issues	Create a read replica and point the reporting job to the read replica endpoint

Exam Scenarios

Exam Scenario	Solution
Backup of RDS instance must be copied regularly to another account for testing	Create a snapshot with create-db-snapshot CLI, share with other account, then create a copy in that account
MySQL database on RDS must be patched due to a security vulnerability. Who is responsible?	AWS is responsible for patching Amazon RDS database instances
Reporting job runs against RDS instance and is causing performance issues	Create a read replica and point the reporting job to the read replica endpoint

Exam Scenarios

Exam Scenario	Solution
How can a Redis cluster be scaled to improve read times	Scale horizontally by adding shards
High CPU on a Memcached cluster	Options are to add additional nodes to cluster or vertically scale the node types
ElastiCache Memcached storing session state. Performance poor, eviction count metrics are high	Scale the cluster by adding additional nodes
A Memcached cluster is experiencing increased traffic, need to change to larger node type	Create a new cache cluster with the new node type using the CreateCacheCluster API

SECTION 13

Management, Governance and Billing

Exam Scenarios

Exam Scenario	Solution
Audit requests to AWS Organizations for creating new accounts by federated users	use CloudTrail and look for the federated identity user name
Employees have created individual AWS accounts not under control. Security team need them in AWS Organizations	Send each account an invitation from the central organization
Need to restrict ability to launch specific instance types for a specific team/account	Use an organizations SCP to deny launches unless the instance type is T2, create an IAM group in the account granting access to T2 instances to the relevant users

Exam Scenarios

Exam Scenario	Solution
Need to ensure that S3 buckets are NEVER deleted in a production account	Use an SCP to deny the s3:DeleteBucket API action
Need to create user-defined cost allocation tags for new account	Use Tag Editor in new account to create user-defined tags and then use the billing and cost management console in the payer account to mark them as cost allocation tags
Separate departments must operate in isolation and only use pre-approved services	Use AWS Organizations to create accounts (Organizations API) and SCPs to control the services available for use

Exam Scenarios

Exam Scenario	Solution
Developers can manipulate IAM policies/roles and need to block them from some services	Use an SCP to block those services
AWS bill is increasing and unauthorized services are being used across accounts	Use AWS Organizations with an SCP to restrict the unauthorized services
Configuring AWS SSO for an Organizations master account. Directory created and full access enabled	Next step is to create a permission set and associate with directory users and groups
Process to create a custom dashboard in CloudWatch for custom metrics after installing agent on EC2	Create metric filters and select custom metrics

Exam Scenarios

Exam Scenario	Solution
Need to test notification settings for CloudWatch alarm with SNS	Use the set-alarm-state CLI command to test
App with EC2 and RDS is running slowly and suspected high CPU	Use CloudWatch metrics to examine resource usage
Site uses CloudFront and S3. Users accessing content that does not exist or they don't have access to	Check the 4XXErrorRate metric in CloudWatch to understand the extent of the issue
Script generates custom CloudWatch metrics from EC2 instance and clock is configured incorrectly by 30 mins	CloudWatch will accept the custom metric data and record it

Exam Scenarios

Exam Scenario	Solution
Need to collect logs from many EC2 instances	Use the unified CloudWatch Agent
External auditor needs to check for unauthorized changes to AWS account	Create an IAM user, assign an IAM policy with read access to CloudTrail logs on Amazon S3
Need to identify who is creating EIPs and not using them	Use CloudTrail and query logs using Athena to search for EIP address events
S3 bucket holds sensitive data. Must monitor object upload / download activity including AWS account and IAM user account of caller and time of API call	Use AWS CloudTrail and enable data event logging

Exam Scenarios

Exam Scenario	Solution
Need to record any modifications or deletions of CloudTrail logs in an S3 bucket	Enable CloudTrail log file integrity validation and enabled MFA delete on the bucket
Large increase in requests to SQS. Need to determine the source of the calls	Use CloudTrail to audit API calls
Need to ensure that S3 buckets have logging enabled without stopping users creating them	Auto remediate with AWS Config managed rule S3_BUCKET_LOGGING_ENABLE
Need to provide real-time compliance reporting for security groups to check that port 80 is not being used	Use the AWS Config restricted-common-ports rule and add port 80

Exam Scenarios

Exam Scenario	Solution
Company wants to limit the AMIs that are used. Need to review compliance with the policy	Create an AWS Config rule to check that only approved AMIs are used
Need to automatically disable access keys that are greater than 90 days old	Use Config rule to identify noncompliant keys and use Systems Manager Automation to remediate
Need to address concerns about exposing sensitive data in buckets without restricting ability to create them	Use AWS Config rules to identify public buckets and send SNS notification to security team
Need to ensure CloudFormation deployment changes are tracked for governance	Use AWS Config

Exam Scenarios

Exam Scenario	Solution
Company needs to verify that specific KMS CMK is used to encrypted EBS volumes	Use AWS Config with the encrypted-volumes managed rule and specify the key ID of the CMK
Need to create replica of existing infrastructure in new account. AWS Service Catalog is used	Most efficient option is to share the portfolio with the new accounts and import into those other accounts
Users have a specialized EC2 instance config and don't want to configure EC2 settings but need to launch/terminate instances. Special instance must only be available to them	Use CloudFormation template with AWS Service Catalog portfolio and grant permissions to users
Shared portfolio is imported into a second AWS account controlled by a different administrator	Admin can add products from the imported portfolio to a local portfolio

Exam Scenarios

Exam Scenario	Solution
Need to monitor costs per user in an account	Activate the createdBy tag and analyze with AWS Cost Explorer
How to check for underutilized EC2 instances?	Use AWS Cost Explorer to generate resource optimization recommendations
Bill is increasing over time, need to determine the cause of increased cost	Use AWS Cost Explorer
Need breakdown of costs per project in a single account using Cost Explorer	Do this by activating cost allocation tags and creating and applying resource tags

Exam Scenarios

Exam Scenario	Solution
Need to check that security best practices are being followed for the AWS account root user	Use AWS Trusted Advisor security checks to review configuration of root user
Costs rising and need to be alerted when a specific spending limit is forecast to be exceeded	Use AWS Budgets
Company needs to track the allocation of reserved instances in consolidated bill	Use the AWS Cost and Usage report
Company needs to integrate AWS maintenance events that may affect their resources into an operations dashboard	Use the AWS Health API

SECTION 14

Security and Compliance

Exam Scenarios

Exam Scenario	Solution
Company wishes to force users to change their passwords regularly	Create an IAM password policy and enabled password expiration
Need to restrict access to a bucket based on source IP range	Use bucket policy with "Condition": "NotIpAddress": statement
Need to control access to group of EC2 instances with specific tags	Use an IAM policy with a condition element granting access based on the tag and attach an IAM policy to the user or groups that require access
IAM policy for SQS queue allows too much access. Who is responsible for correcting the issue?	According the AWS shared responsibility mode, this is a customer responsibility

Exam Scenarios

Exam Scenario	Solution
Data is encrypted with AWS KMS customer-managed CMKs. Need to enable rotation ensuring the data remains readable	Just enable key rotation in AWS KMS for the CMK (backing key is rotated, data key is not changed)
Company must rotate encryption keys once a year with least effort	Use customer-managed CMK and enabled automatic key rotation
App uses KMS CMK with imported key material and references the CMK by alias in the application. Must be rotated every 6 months	To rotate, create a new CMK with new imported material and update the key alias to point to new CMK

Exam Scenarios

Exam Scenario	Solution
Certificate request rejected by ACM	Submit a request for a certificate using the correct domain name NOT the ALB FQDN
Security findings are missing in Amazon Inspector	Verify agent installed on affected instances and restart agent
Security team need to verify vulnerabilities and exposures are addressed for EC2 instances regularly	Use Amazon Inspector and perform regular assessments
There may be a vulnerable version of software installed on EC2 instances and need to check	Create and run an Amazon Inspector assessment template

Exam Scenarios

Exam Scenario	Solution
Need to use information in request header to count requests from each front-end server	Use a string match statement
Large amount of suspicious HTTP requests hitting an ALB from various source IPs	Block the traffic using AWS WAF with a rate-based rule and a defined threshold
Many 404 errors being sent to one IP address every minute. Bot may be collecting info	Use AWS WAF to block the activity
Website has been deployed and penetration testing shows its vulnerable to cross-site scripting	Use AWS WAF to mitigate cross-site scripting attacks

Exam Scenarios

Exam Scenario	Solution
Application is under repeated DDoS attacks. Need to minimize downtime and require 24/7 support	Setup AWS Shield Advanced
Company needs to understand the PCI status of the AWS infrastructure	Use AWS Artifact to locate this information

Exam Scenarios

Exam Scenario	Solution
Company uses LDAP and needs to implement access control in AWS as part of an integration between internal and cloud	Need to configure SAM federation of IAM users and groups with the LDAP DB and map LDAP user and groups to IAM roles
Permissions policy for cross-account access must be created and attached. Who is responsible for doing this?	According to the AWS shared responsibility model, this is a customer responsibility
Company wishes to move from IAM user accounts to using on-premises Active Directory accounts for AWS management console access	Configure a VPN tunnel and use Active Directory Connector