EXAMTOPICS

- Expert Verified, Online, **Free**.

Custom View Settings

Question #501 *Topic 1*

A company runs a web application on a single Amazon EC2 instance. End users experience slow application performance during times of peak usage, when CPU utilization is consistently more than 95%.

A user data script installs required custom packages on the EC2 instance. The process of launching the instance takes several minutes.

The company is creating an Auto Scaling group that has mixed instance groups, varied CPUs, and a maximum capacity limit. The Auto Scaling group will use a launch template for various configuration options. The company needs to decrease application latency when new instances are launched during auto scaling.

Which solution will meet these requirements?

A. Use a predictive scaling policy. Use an instance maintenance policy to run the user data script. Set the default instance warmup time to 0 seconds.

B. Use a dynamic scaling policy. Use lifecycle hooks to run the user data script. Set the default instance warmup time to 0 seconds.

C. Use a predictive scaling policy. Enable warm pools for the Auto Scaling group. Use an instance maintenance policy to run the user data script.

D. Use a dynamic scaling policy. Enable warm pools for the Auto Scaling group. Use lifecycle hooks to run the user data script.

Question #502 *Topic 1*

A company needs to migrate its on-premises database fleet to Amazon RDS. The company is currently using a mixture of Microsoft SQL Server, MySQL, and Oracle databases. Some of the databases have custom schemas and stored procedures.

Which combination of steps should the company take for the migration? (Choose two.)

A. Use Migration Evaluator Quick Insights to analyze the source databases and to identify the stored procedures that need to be migrated.

B. Use AWS Application Migration Service to analyze the source databases and to identify the stored procedures that need to be migrated.

C. Use the AWS Schema Conversion Tool (AWS SCT) to analyze the source databases for changes that are required

D. Use AWS Database Migration Service (AWS DMS) to migrate the source databases to Amazon RDS.

E. Use AWS DataSync to migrate the data from the source databases to Amazon RDS.

Question #503 *Topic 1*

A company is migrating its blog platform to AWS. The company's on-premises servers connect to AWS through an AWS Site-to-Site VPN connection. The blog content is updated several times a day by multiple authors and is served from a file share on a network-attached storage (NAS) server.

The company needs to migrate the blog platform without delaying the content updates. The company has deployed Amazon EC2 instances across multiple Availability Zones to run the blog platform behind an Application Load Balancer. The company also needs to move 200 TB of archival data from its on-premises servers to Amazon S3 as soon as possible.

Which combination of stops will meet these requirements? (Choose two.)

A. Create a weekly cron job in Amazon EventBridge. Use the cron job to invoke an AWS Lambda function to update the EC2 instances from the NAS server.

B. Configure an Amazon Elastic Block Store (Amazon EBS) Multi-Attach volume for the EC2 instances to share for content access. Write code to synchronize the EBS volume with the NAS server weekly.

C. Mount an Amazon Elastic File System (Amazon EFS) file system to the on-premises servers to act as the NAS server. Copy the blog data to the EFS file system. Mount the EFS file system to the C2 instances to serve the content.

D. Order an AWS Snowball Edge Storage Optimized device. Copy the static data artifacts to the device. Ship the device to AWS.

E. Order an AWS Snowcons SSD device. Copy the static data artifacts to the device. Ship the device to AWS.

Question #504 *Topic 1*

A company plans to migrate a legacy on-premises application to AWS. The application is a Java web application that runs on Apache Tomcat with a PostgreSQL database.

The company does not have access to the source code but can deploy the application Java Archive (JAR) files. The application has increased traffic at the end of each month.

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

A. Launch Amazon EC2 instances in multiple Availability Zones. Deploy Tomcat and PostgreSQL to all the instances by using Amazon Elastic File System (Amazon EFS) mount points. Use AWS Step Functions to deploy additional EC2 instances to scale for increased traffic.

B. Provision Amazon Elastic Kubernetes Service (Amazon EKS) in an Auto Scaling group across multiple AWS Regions. Deploy Tomcat and PostgreSQL in the container images. Use a Network Load Balancer to scale for increased traffic.

C. Refactor the Java application into Python-based containers. Use AWS Lambda functions for the application logic. Store application data in Amazon DynamoDB global tables. Use AWS Storage Gateway and Lambda concurrency to scale for increased traffic.

D. Use AWS Elastic Beanstalk to deploy the Tomcat servers with auto scaling in multiple Availability Zones. Store application data in an Amazon RDS for PostgreSQL database. Deploy Amazon CloudFront and an Application Load Balancer to scale for increased traffic.

Question #505 *Topic 1*

A company is migrating its on-premises IoT platform to AWS. The platform consists of the following components:

- A MongoDB cluster as a data store for all collected and processed IoT data.
- An application that uses Message Queuing Telemetry Transport (MQTT) to connect to IoT devices every 5 minutes to collect data.
- An application that runs jobs periodically to generate reports from the IoT data. The jobs take 120-600 seconds to finish running.
- A web application that runs on a web server. End users use the web application to generate reports that are accessible to the general public.

The company needs to migrate the platform to AWS to reduce operational overhead while maintaining performance.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose three.)

A. Create AWS Step Functions state machines with AUS Lambda tasks to prepare the reports and to write the reports to Amazon S3. Configure an Amazon CloudFront distribution that has an S3 origin to serve the reports

B. Create an AWS Lambda function. Program the Lambda function to connect to the IoT devices. process the data, and write the data to the data store. Configure a Lambda layer to temporarily store messages for processing.

C. Configure an Amazon Elastic Kubernetes Service (Amazon EKS) cluster with Amazon EC2 instances to prepare the reports. Create an ingress controller on the EKS cluster to serve the reports.

D. Connect the IoT devices to AWS IoT Core to publish messages. Create an AWS IoT rule that runs when a message is received. Configure the rule to call an AWS Lambda function. Program the Lambda function to parse, transform, and store device message data to the data store.

E. Migrate the MongoDB cluster to Amazon DocumentDB (with MongoDB compatibility).

F. Migrate the MongoDB cluster to Amazon EC2 instances.

Question #506 *Topic 1*

A company creates an Amazon API Gateway API and shares the API with an external development team. The API uses AWS Lambda functions and is deployed to a stage that is named Production.

The external development team is the sole consumer of the API. The API experiences sudden increases of usage at specific times, leading to concerns about increased costs. The company needs to limit cost and usage without reworking the Lambda functions.

Which solution will meet these requirements MOST cost-effectively?

A. Configure the API to send requests to Amazon Simple Queue Service (Amazon SQS) queues instead of directly to the Lambda functions. Update the Lambda functions to consume messages from the queues and to process the requests. Set up the queues to invoke the Lambda functions when new messages arrive.

B. Configure provisioned concurrency for each Lambda function. Use AWS Application Auto Scaling to register the Lambda functions as targets. Set up scaling schedules to increase and decrease capacity to match changes in API usage.

C. Create an API Gateway API key and an AWS WAF Regional web ACL. Associate the web ACL with the Production stage. Add a rate-based rule to the web ACL. In the rule, specify the rate limit and a custom request aggregation that uses the X-API-Key header. Share the API key with the external development team.

D. Create an API Gateway API Key and usage plan. Define throttling limits and quotas in the usage plan. Associate the usage plan with the Production stage and the API key. Share the API key with the external development team.

Question #507 *Topic 1*

An entertainment company hosts a ticketing service on a fleet of Linux Amazon EC2 instances that are in an Auto Scaling group. The ticketing service uses a pricing file. The pricing file is stored in an Amazon S3 bucket that has S3 Standard storage. A central pricing solution that is hosted by a third party updates the pricing file.

The pricing file is updated every 1-15 minutes and has several thousand line items. The pricing file is downloaded to each EC2 instance when the instance launches.

The EC2 instances occasionally use outdated pricing information that can result in incorrect charges for customers.

Which solution will resolve this problem MOST cost-effectively?

A. Create an AWS Lambda function to update an Amazon DynamoDB table with new prices each time the pricing file is updated. Update the ticketing service to use DynramoDB to look up pricing

B. Create an AWS Lambda function to update an Amazon Elastic File System (Amazon EFS) file share with the pricing file each time the file is updated. Update the ticketing service to use Amazon EFS to access the pricing file.

C. Load Mountpoint for Amazon S3 onto the AMI of the EC2 instances. Configure Mountpoint for Amazon S3 to mount the S3 bucket that contains the pricing file. Update the ticketing service to point to the mount point and path to access the $3 object,

D. Create an Amazon Elastic Block Store (Amazon EBS) volume. Use EBS Multi-Attach to attach the volume to every EC2 instance. When a new EC2 instance launches, configure the new instance to update the pricing file on the EBS volume. Update the ticketing service to point to the new local source.

Question #508 *Topic 1*

A company has an application that uses Amazon EC2 instances in an Auto Scaling group. The quality assurance (QA) department needs to launch a large number of short-lived environments to test the application. The application environments are currently launched by the manager of the department using an AWS CloudFormation template. To launch the stack, the manager uses a role with permission to use CloudFormation, EC2, and Auto Scaling APIs. The manager wants to allow testers to launch their own environments, but does not want to grant broad permissions to each user.

Which set up would achieve these goals?

A. Upload the AWS CloudFormation template to Amazon S3. Give users in the QA department permission to assume the manager's role and add a policy that restricts the permissions to the template and the resources it creates. Train users to launch the template from the CloudFormation console.

B. Create an AWS Service Catalog product from the environment template. Add a launch constraint to the product with the existing role. Give users in the QA department permission to use AWS Service Catalog APIs only. Train users to launch the template from the AWS Service Catalog console.

C. Upload the AWS CloudFormation template to Amazon S3. Give users in the QA department permission to use CloudFormation and S3 APIs, with conditions that restrict the permissions to the template and the resources it creates. Train users to launch the template from the CloudFormation console.

D. Create an AWS Elastic Beanstalk application from the environment template. Give users in the QA department permission to use Elastic Beanstalk permissions only. Train users to launch Elastic Beanstalk environments with the Elastic Beanstalk CLI, passing the existing role to the environment as a service role.

Question #509 *Topic 1*

A company is using a single AWS Region for its ecommerce website. The website includes a web application that runs on several Amazon EC2 instances behind an Application Load Balancer (ALB). The website also includes an Amazon DynamoDB table. A custom domain name in Amazon Route 53 is linked to the ALB. The company created an SSL/TLS certificate in AWS Certificate Manager (ACM) and attached the certificate to the ALB. The company is not using a content delivery network as part of its design.

The company wants to replicate its entire application stack in a second Region to provide disaster recovery, plan for future growth, and provide improved access time to users. A solutions architect needs to implement a solution that achieves these goals and minimizes administrative overhead.

Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)

A. Create an AWS CloudFormation template for the current infrastructure design. Use parameters for important system values, including Region. Use the CloudFormation template to create the new infrastructure in the second Region.

B. Use the AWS Management Console to document the existing infrastructure design in the first Region and to create the new infrastructure in the second Region.

C. Update the Route 53 hosted zone record for the application to use weighted routing. Send 50% of the traffic to the ALB in each Region.

D. Update the Route 53 hosted zone record for the application to use latency-based routing. Send traffic to the ALB in each Region.

E. Update the configuration of the existing DynamoDB table by enabling DynamoDB Streams. Add the second Region to create a global table.

F. Create a new DynamoDB table. Enable DynamoDB Streams for the new table. Add the second Region to create a global table. Copy the data from the existing DynamoDB table to the new table as a one-time operation.

Question #510 *Topic 1*

A company wants to create a single Amazon S3 bucket for its data scientists to store work-related documents. The company uses AWS IAM Identity Center to authenticate all users. A group for the data scientists was created.

The company wants to give the data scientists access to only their own work. The company also wants to create monthly reports that show which documents each user accessed.

Which combination of steps will meet these requirements? (Choose two.)

A. Create a custom IAM Identity Center permission set to grant the data scientists access to an S3 bucket prefix that matches their username tag. Use a policy to limit access to paths with the ${aws:PrincipalTag/userName}/* condition.

B. Create an IAM Identity Center role for the data scientists group that has Amazon S3 read access and write access. Add an S3 bucket policy that allows access to the IAM Identity Center role.

C. Configure AWS CloudTrail to log S3 data events and deliver the logs to an S3 bucket. Use Amazon Athena to run queries on the CloudTrail logs in Amazon S3 and generate reports.

D. Configure AWS CloudTrail to log S3 management events to CloudWatch. Use Amazon Athena's CloudWatch connector to query the logs and generate reports.

E. Enable S3 access logging to EMR File System (EMRFS). Use Amazon S3 Select to query logs and generate reports.

Question #511 *Topic 1*

A company hosts a data-processing application on Amazon EC2 instances. The application polls an Amazon Elastic File System (Amazon EFS) file system for newly uploaded files. When a new file is detected, the application extracts data from the file and runs logic to select a Docker container image to process the file. The application starts the appropriate container image and passes the file location as a parameter.

The data processing that the container performs can take up to 2 hours. When the processing is complete, the code that runs inside the container writes the file back to Amazon EFS and exits.

The company needs to refactor the application to eliminate the EC2 instances that are running the containers.

Which solution will meet these requirements?

A. Create an Amazon Elastic Container Service (Amazon ECS) cluster. Configure the processing to run as AWS Fargate tasks. Extract the container selection logic to run as an Amazon EventBridge rule that starts the appropriate Fargate task. Configure the EventBridge rule to run when files are added to the EFS file system.

B. Create an Amazon Elastic Container Service (Amazon ECS) cluster. Configure the processing to run as AWS Fargate tasks. Update and containerize the container selection logic to run as a Fargate service that starts the appropriate Fargate task. Configure an EFS event notification to invoke the Fargate service when files are added to the EFS file system.

C. Create an Amazon Elastic Container Service (Amazon ECS) cluster. Configure the processing to run as AWS Fargate tasks. Extract the container selection logic to run as an AWS Lambda function that starts the appropriate Fargate task. Migrate the storage of file uploads to an Amazon S3 bucket. Update the processing code to use Amazon S3. Configure an S3 event notification to invoke the Lambda function when objects are created.

D. Create AWS Lambda container images for the processing. Configure Lambda functions to use the container images. Extract the container selection logic to run as a decision Lambda function that invokes the appropriate Lambda processing function. Migrate the storage of file uploads to an Amazon S3 bucket. Update the processing code to use Amazon S3. Configure an S3 event notification to invoke the decision Lambda function when objects are created.

Question #512 *Topic 1*

A media company has a 30-T8 repository of digital news videos. These videos are stored on tape in an on-premises tape library and referenced by a Media Asset Management (MAM) system. The company wants to enrich the metadata for these videos in an automated fashion and put them into a searchable catalog by using a MAM feature. The company must be able to search based on information in the video, such as objects, scenery items, or people's faces. A catalog is available that contains faces of people who have appeared in the videos that include an image of each person. The company would like to migrate these videos to AWS.

The company has a high-speed AWS Direct Connect connection with AWS and would like to move the MAM solution video content directly from its current file system.

How can these requirements be met by using the LEAST amount of ongoing management overhead and causing MINIMAL disruption to the existing system?

A. Set up an AWS Storage Gateway, file gateway appliance on-premises. Use the MAM solution to extract the videos from the current archive and push them into the file gateway. Use the catalog of faces to build a collection in Amazon Rekognition. Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Rekognition pull the video from the Amazon S3 files backing the file gateway, retrieve the required metadata, and push the metadata into the MAM solution.

B. Set up an AWS Storage Gateway, tape gateway appliance on-premises. Use the MAM solution to extract the videos from the current archive and push them into the tape gateway. Use the catalog of faces to build a collection in Amazon Rekognition. Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Amazon Rekognition process the video in the tape gateway, retrieve the required metadata, and push the metadata into the MAM solution.

C. Configure a video ingestion stream by using Amazon Kinesis Video Streams. Use the catalog of faces to build a collection in Amazon Rekognition. Stream the videos from the MAM solution into Kinesis Video Streams. Configure Amazon Rekognition to process the streamed videos. Then, use a stream consumer to retrieve the required metadata, and push the metadata into the MAM solution. Configure the stream to store the videos in Amazon S3.

D. Set up an Amazon EC2 instance that runs the OpenCV libraries. Copy the videos, images, and face catalog from the on-premises library into an Amazon EBS volume mounted on this EC2 instance. Process the videos to retrieve the required metadata, and push the metadata into the MAM solution, while also copying the video files to an Amazon S3 bucket.

Question #513 *Topic 1*

A company needs to optimize the cost of an AWS environment that contains multiple accounts in an organization in AWS Organizations. The company conducted cost optimization activities 3 years ago and purchased Amazon EC2 Standard Reserved Instances that recently expired.

The company needs EC2 instances for 3 more years. Additionally, the company has deployed a new serverless workload.

Which strategy will provide the company with the MOST cost savings?

A. Purchase the same Reserved Instances for an additional 3-year term with All Upfront payment. Purchase a 3-year Compute Savings Plan with All Upfront payment in the management account to cover any additional compute costs

B. Purchase a 1-year Compute Savings Plan with No Upfront payment in each member account. Use the Savings Plans recommendations in the AWS Cost Management console to choose the Compute Savings Plan.

C. Purchase a 3-year EC2 Instance Savings Plan with No Upfront payment in the management account to cover EC2 costs in each AWS Region. Purchase a 3-year Compute Savings Plan with No Upfront payment in the management account to cover any additional compute costs.

D. Purchase a 3-year EC2 Instance Savings Plan with All Upfront payment in each member account. Use the Savings Plans recommendations in the AWS Cost Management console to choose the EC2 Instance Savings Plan.

Question #514 *Topic 1*

A company operates a static content distribution platform that serves customers globally. The customers consume content from their own AWS accounts.

The company serves its content from an Amazon S3 bucket. The company uploads the content from its on-premises environment to the S3 bucket by using an S3 File Gateway.

The company wants to improve the platform's performance and reliability by serving content from the AWS Region that is geographically closest to customers. The company must route the on-premises data to Amazon S3 with minimal latency and without public internet exposure.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

A. Implement S3 Multi-Region Access Points

B. Use S3 Cross-Region Replication (CRR) to copy content to different Regions

C. Create an AWS Lambda function that tracks the routing of clients to Regions

D. Use an AWS Site-to-Site VPN connection to connect to a Multi-Region Access Point.

E. Use AWS PrivateLink and AWS Direct Connect to connect to a Multi-Region Access Point.

Question #515 *Topic 1*

A company is migrating its data center to the AWS Cloud and needs to complete the migration as quickly as possible. The company has many applications that are running on hundreds of VMware VMs in the data center. Each VM is configured with a shared Windows folder that contains common shared files. The file share is larger than 100 GB in size.

The company's compliance team requires a change request to be fled and approved for every software installation and modification to each VM. The company has an AWS Direct Connect connection with 10 GB of bandwidth between AWS and the data center.

Which set of steps should the company take to complete the migration in the LEAST amount of time?

A. Use VM ImporvExport to create images of each VM. Use AWS Application Migration Service to manage and view the images. Copy the Windows file share data to an Amazon Elastic File System (Amazon EFS) file system. After migration, remap the file share to the EFS file system.

B. Deploy the AWS Application Discovery Service agentless appliance to VMware vCenter. Review the portfolio of discovered VMs in AWS Migration Hub.

C. Deploy the AWS Application Migration Service agentless appliance to VMware vCenter. Copy the Windows file share data to a new Amazon FSx for Windows File Server file system. After migration, remap the file share on each VM to the FSx for Windows File Server file system.
C. Create and review a portfolio in AWS Migration Hub. Order an AWS Snowcone device. Deploy AWS Application Migration Service to VMware vCenter and export all the VMs to the Snowcone device. Copy all Windows file share data to the Snowcone device. Ship the Snowcone device to AWS. Use Application Migration Service to deploy all the migrated instances.

D. Deploy the AWS Application Discovery Service Agent and the AWS Application Migration Service Agent onto each VMware hypervisor directly. Review the portfolio in AWS Migration Hub. Copy each VM's file share data to a new Amazon FSx for Windows File Server file system. After migration, remap the file share on each VM to the FSx for Windows File Server file system.

Question #516 *Topic 1*

A company has multiple AWS accounts that are in an organization in AWS Organizations. The company needs to store AWS account activity and query the data from a central location by using SQL.

Which solution will meet these requirements?

A. Create an AWS CloudTraii trail in each account. Specify CloudTrail management events for the trail. Configure CloudTrail to send the events to Amazon CloudWatch Logs. Configure CloudWatch cross-account observability. Query the data in CloudWatch Logs Insights.

B. Use a delegated administrator account to create an AWS CloudTrail Lake data store. Specify CloudTrail management events for the data store. Enable the data store for all accounts in the organization. Query the data in CloudTrail Lake.

C. Use a delegated administrator account to create an AWS CloudTral trail. Specify CloudTrail management events for the trail. Enable the trail for all accounts in the organization. Keep all other settings as default. Query the CloudTrail data from the CloudTrail event history page.

D. Use AWS CloudFormation StackSets to deploy AWS CloudTrail Lake data stores in each account. Specify CloudTrail management events for the data stores. Keep all other settings as default, Query the data in CloudTrail Lake.

Question #517 *Topic 1*

A company is using AWS to develop and manage its production web application. The application includes an Amazon API Gateway HTTP API that invokes an AWS Lambda function. The Lambda function processes and then stores data in a database.

The company wants to implement user authorization for the web application in an integrated way. The company already uses a third-party identity provider that issues OAuth tokens for the company's other applications.

Which solution will meet these requirements?

A. Integrate the company's third-party identity provider with API Gateway. Configure an API Gateway Lambda authorizer to validate tokens from the identity provider. Require the Lambda authorizer on all API routes. Update the web application to get tokens from the identity provider and include the tokens in the Authorization header when calling the API Gateway HTTP API.

B. Integrate the company's third-party identity provider with AWS Directory Service. Configure Directory Service as an API Gateway authorizer to validate tokens from the identity provider. Require the Directory Service authorizer on all API routes. Configure AWS IAM Identity Center as a SAML 2.0 identity Provider. Configure the web application as a custom SAML 2.0 application.

C. Integrate the company's third-party identity provider with AWS IAM Identity Center. Configure API Gateway to use IAM Identity Center for zero-configuration authentication and authorization. Update the web application to retrieve AWS Security Token Service (AWS STS) tokens from IAM Identity Center and include the tokens in the Authorization header when calling the API Gateway HTTP API.

D. Integrate the company's third-party identity provider with AWS IAM Identity Center. Configure IAM users with permissions to call the API Gateway HTTP API. Update the web application to extract request parameters from the IAM users and include the parameters in the Authorization header when calling the API Gateway HTTP API.

Question #518 *Topic 1*

A company has deployed applications to thousands of Amazon EC2 instances in an AWS account. A security audit discovers that several unencrypted Amazon Elastic Block Store (Amazon EBS) volumes are attached to the EC2 instances. The company's security policy requires the EBS volumes to be encrypted.

The company needs to implement an automated solution to encrypt the EBS volumes. The solution also must prevent development teams from creating unencrypted EBS volumes.

Which solution will meet these requirements?

A. Configure the AWS Config managed rule that identifies unencrypted EBS volumes. Configure an automatic remediation action. Associate an AWS Systems Manager Automation runbook that includes the steps to create a new encrypted EBS volume. Create an AWS Key Management Service (AWS KMS) customer managed key. In the key policy, include a statement to deny the creation of unencrypted EBS volumes.

B. Use AWS Systems Manager Fleet Manager to create a list of unencrypted EBS volumes, Create a Systems Manager Automation runbook that includes the steps to create a new encrypted EBS volume. Create an SCP to deny the creation of unencrypted EBS volumes.

C. Use AWS Systems Manager Fleet Manager to create a list of unencrypted EBS volumes. Create a Systems Manager Automation runbook that includes the steps to create a new encrypted EBS volume. Modify the AWS account setting for EBS encryption to always encrypt new EBS volumes.

D. Configure the AWS Config managed rule that identifies unencrypted EBS volumes. Configure an automatic remediation action. Associate an AWS Systems Manager Automation runbook that includes the steps to create a new encrypted EBS volume. Modify the AWS account setting for EBS encryption to always encrypt new EBS volumes.

Question #519 *Topic 1*

A company is running a large containerized workload in the AWS Cloud. The workload consists of approximately 100 different services. The company uses Amazon Elastic Container Service (Amazon ECS) to orchestrate the workload.

Recently the company's development team started using AWS Fargate instead of Amazon EC2 instances in the ECS cluster. In the past, the workload has come close to running the maximum number of EC2 instances that are available in the account.

The company is worried that the workload could reach the maximum number of ECS tasks that are allowed. A solutions architect must implement a solution that will notify the development team when Fargate reaches 80% of the maximum number of tasks.

What should the solutions architect do to meet this requirement?

A. Use Amazon CloudWatch to monitor the Sample Count statistic for each service in the ECS cluster. Set an alarm for when the math expression sample count/SERVICE_QUOTA(service)*100 is greater than 80. Notify the development team by using Amazon Simple Notification Service (Amazon SNS).

B. Use Amazon CloudWatch to monitor service quotas that are published under the AWS/Usage metric namespace. Set an alarm for when the math expression metric/SERVICE_QUOTA(metric)*100 is greater than 80. Notify the development team by using Amazon Simple Notification Service (Amazon SNS).

C. Create an AWS Lambda function to poll detailed metrics from the ECS cluster. When the number of running Fargate tasks is greater than 80, invoke Amazon Simple Email Service (Amazon SES) to notify the development team.

D. Create an AWS Config rule to evaluate whether the Fargate SERVICE_QUOTA is greater than 80. Use Amazon Simple Email Service (Amazon SES) to notify the development team when the AWS Config rule is not compliant.

Question #520 *Topic 1*

A company has several AWS Lambda functions written in Python. The functions are deployed with the .zip package deployment type. The functions use a Lambda layer that contains common libraries and packages in a .zip file. The Lambda .zip packages and Lambda layer .zip file are stored in an Amazon S3 bucket.

The company must implement automatic scanning of the Lambda functions and the Lambda layer to identify CVEs. A subset of the Lambda functions must receive automated code scans to detect potential data leaks and other vulnerabilities. The code scans must occur only for selected Lambda functions, not all the Lambda functions.

Which combination of actions will meet these requirements? (Choose three.)

A. Activate Amazon Inspector. Start automated CVE scans.

B. Activate Lambda standard scanning and Lambda code scanning in Amazon Inspector.

C. Enable Amazon GuardDuty. Enable the Lambda Protection feature in GuardDuty.

D. Enable scanning in the Monitor settings of the Lambda functions that need code scans.

E. Tag Lambda functions that do not need code scans. In the tag, include a key of InspectorCodeExclusion and a value of LambdaCodeScanning.

F. Use Amazon Inspector to scan the 3 bucket that contains the Lambda .zip packages and the Lambda layer .zip file for code scans.

Question #521 *Topic 1*

A company is changing the way that it handles patching of Amazon EC2 instances in its application account. The company currently patches instances over the internet by using a NAT gateway in a VPC in the application account.

The company has EC2 instances set up as a patch source repository in a dedicated private VPC in a core account. The company wants to use AWS Systems Manager Patch Manager and the patch source repository in the core account to patch the EC2 instances in the application account. The company must prevent all EC2 instances in the application account from accessing the internet.

The EC2 instances in the application account need to access Amazon S3, where the application data is stored. These EC2 instances need connectivity to Systems Manager and to the patch source repository in the private VPC in the core account.

Which solution will meet these requirements?

A. Create a network ACL that blocks outbound traffic on port 80. Associate the network ACL with all subnets in the application account. In the application account and the core account, deploy one EC2 instance that runs a custom VPN server. Create a VPN tunnel to access the private VPC. Update the route table in the application account.

B. Create private VIFs for Systems Manager and Amazon S3. Delete the NAT gateway from the VPC in the application account. Create a transit gateway to access the patch source repository EC2 instances in the core account. Update the route table in the core account.

C. Create VPC endpoints for Systems Manager and Amazon S3. Delete the NAT gateway from the VPC in the application account. Create a VPC peering connection to access the patch source repository EC2 instances in the core account. Update the route tables in both accounts.

D. Create a network ACL that blocks inbound traffic on port 80. Associate the network ACL with all subnets in the application account. Create a transit gateway to access the patch source repository EC2 instances in the core account. Update the route tables in both accounts.

Question #522 *Topic 1*

A company in the United States (US) has acquired a company in Europe. Both companies use the AWS Cloud. The US company has built a new application with a microservices architecture. The US company is hosting the application across five VPCs in the us-east-2 Region. The application must be able to access resources in one VPC in the eu-west-1 Region.
However, the application must not be able to access any other VPCs.

The VPCs in both Regions have no overlapping CIDR ranges. All accounts are already consolidated in one organization in AWS Organizations.

Which solution will meet these requirements MOST cost-effectively?

A. Create one transit gateway in eu-west-1. Attach the VPCs in us-east-2 and the VPC in eu-west-1 to the transit gateway. Create the necessary route entries in each VPC so that the traffic is routed through the transit gateway.

B. Create one transit gateway in each Region. Attach the involved subnets to the regional transit gateway. Create the necessary route entries in the associated route tables for each subnet so that the traffic is routed through the regional transit gateway. Peer the two transit gateways.

C. Create a full mesh VPC peering connection configuration between all the VPCs. Create the necessary route entries in each VPC so that the traffic is routed through the VPC peering connection.

D. Create one VPC peering connection for each VPC in us-east-2 to the VPC in eu-west-1. Create the necessary route entries in each VPC so that the traffic is routed through the VPC peering connection.

Question #523 *Topic 1*

A travel company built a web application that uses Amazon Simple Email Service (Amazon SES) to send email notifications to users. The company needs to enable logging to help troubleshoot email delivery issues. The company also needs the ability to do searches that are based on recipient, subject, and time sent.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

A. Create an Amazon SES configuration set with Amazon Data Firehose as the destination. Choose to send logs to an Amazon S3 bucket.

B. Enable AWS CloudTrail logging. Specify an Amazon S3 bucket as the destination for the logs.

C. Use Amazon Athena to query the logs in the Amazon S3 bucket for recipient, subject, and time sent.

D. Create an Amazon CloudWatch log group. Configure Amazon SES to send logs to the log group.

E. Use Amazon Athena to query the logs in Amazon CloudWatch for recipient, subject, and time sent.

Question #524 *Topic 1*

A company migrated to AWS and uses AWS Business Support. The company wants to monitor the cost-effectiveness of Amazon EC2 instances across AWS accounts. The EC2 instances have tags for department, business unit, and environment. Development EC2 instances have high cost but low utilization.

The company needs to detect and stop any underutilized development EC2 instances. Instances are underutilized if they had 10% or less average daily CPU utilization and 5 MB or less network I/O for at least 4 of the past 14 days.

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

A. Configure Amazon CloudWatch dashboards to monitor EC2 instance utilization based on tags for department, business unit, and environment. Create an Amazon EventBridge rule that invokes an AWS Lambda function to stop underutilized development EC2 instances.

B. Configure AWS Systems Manager to track EC2 instance utilization and report underutilized instances to Amazon CloudWatch. Filter the CloudWatch data by tags for department, business unit, and environment. Create an Amazon EventBridge rule that invokes an AWS Lambda function to stop underutilized development EC2 instances.

C. Create an Amazon EventBridge rule to detect low utilization of EC2 instances reported by AWS Trusted Advisor. Configure the rule to invoke an AWS Lambda function that filters the data by tags for department, business unit, and environment and stops underutilized development EC2 instances.

D. Create an AWS Lambda function to run daily to retrieve utilization data for all EC2 instances. Save the data to an Amazon DynamoDB table. Create an Amazon QuickSight dashboard that uses the DynamoDB table as a data source to identify and stop underutilized development EC2 instances.

Question #525 *Topic 1*

A company is hosting an application on AWS for a project that will run for the next 3 years. The application consists of 20 Amazon EC2 On-Demand Instances that are registered in a target group for a Network Load Balancer (NLB). The instances are spread across two Availability Zones. The application is stateless and runs 24 hours a day, 7 days a week.

The company receives reports from users who are experiencing slow responses from the application. Performance metrics show that the instances are at 10% CPU utilization during normal application use. However, the CPU utilization increases to 100% at busy times, which typically last for a few hours.

The company needs a new architecture to resolve the problem of slow responses from the application.

Which solution will meet these requirements MOST cost-effectively?

A. Create an Auto Scaling group. Attach the Auto Scaling group to the target group of the NLB. Set the minimum capacity to 20 and the desired capacity to 28. Purchase Reserved Instances for 20 instances.

B. Create a Spot Fleet that has a request type of request. Set the TotalTargetCapacity parameter to 20. Set the DefaultTargetCapacityType parameter to On-Demand. Specify the NLB when creating the Spot Fleet.

C. Create a Spot Fleet that has a request type of maintain. Set the TotalTargetCapacity parameter to 20. Set the DefaultTargetCapacityType parameter to Spot. Replace the NLB with an Application Load Balancer.

D. Create an Auto Scaling group. Attach the Auto Scaling group to the target group of the NLB. Set the minimum capacity to 4 and the maximum capacity to 28. Purchase Reserved Instances for four instances.

Question #526 *Topic 1*

Accompany is building an application to collect and transmit sensor data from a factory. The application will use AWS IoT Core to send data from hundreds of devices to an Amazon S3 data lake. The company must enrich the data before loading the data into Amazon S3.

The application will transmit the sensor data every 5 seconds. New sensor data must be available in Amazon S3 less than 30 minutes after the application collects the data. No other applications are processing the sensor data from AWS IoT Core.

Which solution will meet these requirements MOST cost-effectively?

A. Create a topic in AWS IoT Core to ingest the sensor data. Create an AWS Lambda function to enrich the data and to write the data to Amazon S3. Configure an AWS IoT rule action to invoke the Lambda function.

B. Use AWS IoT Core Basic Ingest to ingest the sensor data. Configure an AWS IoT rule action to write the data to Amazon Kinesis Data Firehose. Set the Kinesis Data Firehose buffering interval to 900 seconds. Use Kinesis Data Firehose to invoke an AWS Lambda function to enrich the data, Configure Kinesis Data Firehose to deliver the data to Amazon S3.

C. Create a topic in AWS IoT Core to ingest the sensor data. Configure an AWS IoT rule action to send the data to an Amazon Timestream table. Create an AWS Lambda, function to read the data from Timestream. Configure the Lambda function to enrich the data and to write the data to Amazon S3.

D. Use AWS IoT Core Basic Ingest to ingest the sensor data. Configure an AWS IoT rule action to write the data to Amazon Kinesis Data Streams. Create a consumer AWS Lambda function to process the data from Kinesis Data Streams and to enrich the data. Call the S3 PutObject API operation from the Lambda function to write the data to Amazon S3.

Question #527 *Topic 1*

A company is collecting data from a large set of IoT devices. The data is stored in an Amazon S3 data lake. Data scientists perform analytics on Amazon EC2 instances that run in two public subnets in a VPC in a separate AWS account.

The data scientists need access to the data lake from the EC2 instances. The EC2 instances already have an assigned role with permissions to access Amazon S3.
According to company policies, only authorized networks are allowed to have access to the IoT data.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

A. Create a gateway VPC endpoint for Amazon S3 in the data scientists' VPC.

B. Create an S3 access point in the data scientists' AWS account for the data lake.

C. Update the EC2 instance role. Add a policy with a condition that allows the s3:GetObject action when the value for the s3:DataAccessPointArn condition key is a valid access point ARN.

D. Update the VPC route table to route S3 traffic to an S3 access point.

E. Add an S3 bucket policy with a condition that allows the s3:GetObject action when the value for the s3:DataAccessPointArn condition key is a valid access point ARN.

Question #528 *Topic 1*

A company wants to migrate its website to AWS. The website uses containers that are deployed in an on-premises, self-managed Kubernetes cluster. All data for the website is stored in an on-premises PostgreSQL database.

The company has decided to migrate the on-premises Kubernetes cluster to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The EKS cluster will use EKS managed node groups with a static number of nodes. The company will also migrate the on-premises database to an Amazon RDS for PostgreSQL database.

A solutions architect needs to estimate the total cost of ownership (TCO) for this workload before the migration.

Which solution will provide the required TCO information?

A. Request access to Migration Evaluator. Run the Migration Evaluator Collector and import the data. Configure a scenario. Export a Quick Insights report from Migration Evaluator.

B. Launch AWS Database Migration Service (AWS DMS) for the on-premises database. Generate an assessment report. Create an estimate in AWS Pricing Calculator for the costs of the EKS migration.

C. Initialize AWS Application Migration Service. Add the on-premises servers as source servers. Launch a test instance. Output a TCO report from Application Migration Service.

D. Access the AWS Cloud Economics Center webpage to assess the AWS Cloud Value Framework. Create an AWS Cost and Usage report from the Cloud Value Framework.

Question #529 *Topic 1*

An events company runs a ticketing platform on AWS. The company's customers configure and schedule their events on the platform. The events result in large increases of traffic to the platform. The company knows the date and time of each customer's events.

The company runs the platform on an Amazon Elastic Container Service (Amazon ECS) cluster. The ECS cluster consists of Amazon EC2 On-Demand Instances that are in an Auto Scaling group. The Auto Scaling group uses a predictive scaling policy.

The ECS cluster makes frequent requests to an Amazon S3 bucket to download ticket assets. The ECS cluster and the S3 bucket are in the same AWS Region and the same AWS account. Traffic between the ECS cluster and the S3 bucket flows across a NAT gateway.

The company needs to optimize the cost of the platform without decreasing the platform's availability.

Which combination of steps will meet these requirements? (Choose two.)

A. Create a gateway VPC endpoint for the S3 bucket.

B. Add another ECS capacity provider that uses an Auto Scaling group of Spot Instances. Configure the new capacity provider strategy to have the same weight as the existing capacity provider strategy.

C. Create On-Demand Capacity Reservations for the applicable instance type for the time period of the scheduled scaling policies.

D. Enable S3 Transfer Acceleration on the S3 bucket.

E. Replace the predictive scaling policy with scheduled scaling policies for the scheduled events.

← Previous Questions