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

⚙ Custom View Settings

Question #251
Topic 1

A company is creating a REST API to share information with six of its partners based in the United States. The company has created an Amazon API Gateway Regional endpoint. Each of the six partners will access the API once per day to post daily sales figures.

After initial deployment, the company observes 1,000 requests per second originating from 500 different IP addresses around the world. The company believes this traffic is originating from a botnet and wants to secure its API while minimizing cost.

Which approach should the company take to secure its API?

A. Create an Amazon CloudFront distribution with the API as the origin. Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per day. Associate the web ACL with the CloudFront distribution. Configure CloudFront with an origin access identity (OAI) and associate it with the distribution. Configure API Gateway to ensure only the OAI can run the POST method.

B. Create an Amazon CloudFront distribution with the API as the origin. Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per day. Associate the web ACL with the CloudFront distribution. Add a custom header to the CloudFront distribution populated with an API key. Configure the API to require an API key on the POST method.

C. Create an AWS WAF web ACL with a rule to allow access to the IP addresses used by the six partners. Associate the web ACL with the API. Create a resource policy with a request limit and associate it with the API. Configure the API to require an API key on the POST method.

D. Create an AWS WAF web ACL with a rule to allow access to the IP addresses used by the six partners. Associate the web ACL with the API. Create a usage plan with a request limit and associate it with the API. Create an API key and add it to the usage plan. Most Voted

Correct Answer: *D*

Community vote distribution

D (97%)

Question #252   *Topic 1*

A company uses an Amazon Aurora PostgreSQL DB cluster for applications in a single AWS Region. The company's database team must monitor all data activity on all the databases.

Which solution will achieve this goal?

A. Set up an AWS Database Migration Service (AWS DMS) change data capture (CDC) task. Specify the Aurora DB cluster as the source. Specify Amazon Kinesis Data Firehose as the target. Use Kinesis Data Firehose to upload the data into an Amazon OpenSearch Service cluster for further analysis.

B. Start a database activity stream on the Aurora DB cluster to capture the activity stream in Amazon EventBridge. Define an AWS Lambda function as a target for EventBridge. Program the Lambda function to decrypt the messages from EventBridge and to publish all database activity to Amazon S3 for further analysis.

C. Start a database activity stream on the Aurora DB cluster to push the activity stream to an Amazon Kinesis data stream. Configure Amazon Kinesis Data Firehose to consume the Kinesis data stream and to deliver the data to Amazon S3 for further analysis. [Most Voted]

D. Set up an AWS Database Migration Service (AWS DMS) change data capture (CDC) task. Specify the Aurora DB cluster as the source. Specify Amazon Kinesis Data Firehose as the target. Use Kinesis Data Firehose to upload the data into an Amazon Redshift cluster. Run queries on the Amazon Redshift data to determine database activities on the Aurora database.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #253   *Topic 1*

An entertainment company recently launched a new game. To ensure a good experience for players during the launch period, the company deployed a static quantity of 12 r6g.16xlarge (memory optimized) Amazon EC2 instances behind a Network Load Balancer. The company's operations team used the Amazon CloudWatch agent and a custom metric to include memory utilization in its monitoring strategy.

Analysis of the CloudWatch metrics from the launch period showed consumption at about one quarter of the CPU and memory that the company expected. Initial demand for the game has subsided and has become more variable. The company decides to use an Auto Scaling group that monitors the CPU and memory consumption to dynamically scale the instance fleet. A solutions architect needs to configure the Auto Scaling group to meet demand in the most cost-effective way.

Which solution will meet these requirements?

A. Configure the Auto Scaling group to deploy c6g.4xlarge (compute optimized) instances. Configure a minimum capacity of 3, a desired capacity of 3, and a maximum capacity of 12.

B. Configure the Auto Scaling group to deploy m6g.4xlarge (general purpose) instances. Configure a minimum capacity of 3, a desired capacity of 3, and a maximum capacity of 12.

C. Configure the Auto Scaling group to deploy r6g.4xlarge (memory optimized) instances. Configure a minimum capacity of 3, a desired capacity of 3, and a maximum capacity of 12. [Most Voted]

D. Configure the Auto Scaling group to deploy r6g.8xlarge (memory optimized) instances. Configure a minimum capacity of 2, a desired capacity of 2, and a maximum capacity of 6.

Correct Answer: *C*

Community vote distribution

C (96%)   4%

Question #254   *Topic 1*

A financial services company loaded millions of historical stock trades into an Amazon DynamoDB table. The table uses on-demand capacity mode. Once each day at midnight, a few million new records are loaded into the table. Application read activity against the table happens in bursts throughout the day. and a limited set of keys are repeatedly looked up. The company needs to reduce costs associated with DynamoDB.

Which strategy should a solutions architect recommend to meet this requirement?

    A. Deploy an Amazon ElastiCache cluster in front of the DynamoDB table

    B. Deploy DynamoDB Accelerator (DAX). Configure DynamoDB auto scaling. Purchase Savings Plans in Cost Explorer.

    C. Use provisioned capacity mode. Purchase Savings Plans in Cost Explorer.

    D. Deploy DynamoDB Accelerator (DAX). Use provisioned capacity mode. Configure DynamoDB auto scaling. `Most Voted`

Correct Answer: *D*

Community vote distribution

                                        D (86%)   8%

Question #255   *Topic 1*

A company is creating a centralized logging service running on Amazon EC2 that will receive and analyze logs from hundreds of AWS accounts. AWS PrivateLink is being used to provide connectivity between the client services and the logging service.

In each AWS account with a client, an interface endpoint has been created for the logging service and is available. The logging service running on EC2 instances with a Network Load Balancer (NLB) are deployed in different subnets. The clients are unable to submit logs using the VPC endpoint.

Which combination of steps should a solutions architect take to resolve this issue? (Choose two.)

    A. Check that the NACL is attached to the logging service subnet to allow communications to and from the NLB subnets. Check that the NACL is attached to the NLB subnet to allow communications to and from the logging service subnets running on EC2 instances. `Most Voted`

    B. Check that the NACL is attached to the logging service subnets to allow communications to and from the interface endpoint subnets. Check that the NACL is attached to the interface endpoint subnet to allow communications to and from the logging service subnets running on EC2 instances.

    C. Check the security group for the logging service running on the EC2 instances to ensure it allows ingress from the NLB subnets. `Most Voted`

    D. Check the security group for the logging service running on EC2 instances to ensure it allows ingress from the clients.

    E. Check the security group for the NLB to ensure it allows ingress from the interface endpoint subnets.

Correct Answer: *AC*

Community vote distribution

                    AC (64%)   BD (22%)   7%

Question #256   *Topic 1*

A company has millions of objects in an Amazon S3 bucket. The objects are in the S3 Standard storage class. All the S3 objects are accessed frequently. The number of users and applications that access the objects is increasing rapidly. The objects are encrypted with server-side encryption with AWS KMS keys (SSE-KMS).

A solutions architect reviews the company's monthly AWS invoice and notices that AWS KMS costs are increasing because of the high number of requests from Amazon S3. The solutions architect needs to optimize costs with minimal changes to the application.

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

   A. Create a new S3 bucket that has server-side encryption with customer-provided keys (SSE-C) as the encryption type. Copy the existing objects to the new S3 bucket. Specify SSE-C.

   B. Create a new S3 bucket that has server-side encryption with Amazon S3 managed keys (SSE-S3) as the encryption type. Use S3 Batch Operations to copy the existing objects to the new S3 bucket. Specify SSE-S3. [Most Voted]

   C. Use AWS CloudHSM to store the encryption keys. Create a new S3 bucket. Use S3 Batch Operations to copy the existing objects to the new S3 bucket. Encrypt the objects by using the keys from CloudHSM.

   D. Use the S3 Intelligent-Tiering storage class for the S3 bucket. Create an S3 Intelligent-Tiering archive configuration to transition objects that are not accessed for 90 days to S3 Glacier Deep Archive.

   Correct Answer: *B*

   Community vote distribution
                              B (100%)

Question #257   *Topic 1*

A media storage application uploads user photos to Amazon S3 for processing by AWS Lambda functions. Application state is stored in Amazon DynamoDB tables. Users are reporting that some uploaded photos are not being processed properly. The application developers trace the logs and find that Lambda is experiencing photo processing issues when thousands of users upload photos simultaneously. The issues are the result of Lambda concurrency limits and the performance of DynamoDB when data is saved.

Which combination of actions should a solutions architect take to increase the performance and reliability of the application? (Choose two.)

   A. Evaluate and adjust the RCUs for the DynamoDB tables.

   B. Evaluate and adjust the WCUs for the DynamoDB tables. [Most Voted]

   C. Add an Amazon ElastiCache layer to increase the performance of Lambda functions.

   D. Add an Amazon Simple Queue Service (Amazon SQS) queue and reprocessing logic between Amazon S3 and the Lambda functions. [Most Voted]

   E. Use S3 Transfer Acceleration to provide lower latency to users.

   Correct Answer: *BD*

   Community vote distribution
                              BD (100%)

Question #258   *Topic 1*

A company runs an application in an on-premises data center. The application gives users the ability to upload media files. The files persist in a file server. The web application has many users. The application server is overutilized, which causes data uploads to fail occasionally. The company frequently adds new storage to the file server. The company wants to resolve these challenges by migrating the application to AWS.

Users from across the United States and Canada access the application. Only authenticated users should have the ability to access the application to upload files. The company will consider a solution that refactors the application, and the company needs to accelerate application development.

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

  A. Use AWS Application Migration Service to migrate the application server to Amazon EC2 instances. Create an Auto Scaling group for the EC2 instances. Use an Application Load Balancer to distribute the requests. Modify the application to use Amazon S3 to persist the files. Use Amazon Cognito to authenticate users.

  B. Use AWS Application Migration Service to migrate the application server to Amazon EC2 instances. Create an Auto Scaling group for the EC2 instances. Use an Application Load Balancer to distribute the requests. Set up AWS IAM Identity Center (AWS Single Sign-On) to give users the ability to sign in to the application. Modify the application to use Amazon S3 to persist the files.

  C. Create a static website for uploads of media files. Store the static assets in Amazon S3. Use AWS AppSync to create an API. Use AWS Lambda resolvers to upload the media files to Amazon S3. Use Amazon Cognito to authenticate users.

  D. Use AWS Amplify to create a static website for uploads of media files. Use Amplify Hosting to serve the website through Amazon CloudFront. Use Amazon S3 to store the uploaded media files. Use Amazon Cognito to authenticate users. `Most Voted`

Correct Answer: *D*

Community vote distribution
                          D (91%)   9%

Question #259   *Topic 1*

A company has an application that is deployed on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are part of an Auto Scaling group. The application has unpredictable workloads and frequently scales out and in. The company's development team wants to analyze application logs to find ways to improve the application's performance. However, the logs are no longer available after instances scale in.

Which solution will give the development team the ability to view the application logs after a scale-in event?

  A. Enable access logs for the ALB. Store the logs in an Amazon S3 bucket.

  B. Configure the EC2 instances to publish logs to Amazon CloudWatch Logs by using the unified CloudWatch agent. `Most Voted`

  C. Modify the Auto Scaling group to use a step scaling policy.

  D. Instrument the application with AWS X-Ray tracing.

Correct Answer: *B*

Community vote distribution
                          B (100%)

Question #260   *Topic 1*

A company runs an unauthenticated static website (www.example.com) that includes a registration form for users. The website uses Amazon S3 for hosting and uses Amazon CloudFront as the content delivery network with AWS WAF configured. When the registration form is submitted, the website calls an Amazon API Gateway API endpoint that invokes an AWS Lambda function to process the payload and forward the payload to an external API call.

During testing, a solutions architect encounters a cross-origin resource sharing (CORS) error. The solutions architect confirms that the CloudFront distribution origin has the Access-Control-Allow-Origin header set to www.example.com.

What should the solutions architect do to resolve the error?

   A. Change the CORS configuration on the S3 bucket. Add rules for CORS to the AllowedOrigin element for www.example.com.

   B. Enable the CORS setting in AWS WAF. Create a web ACL rule in which the Access-Control-Allow-Origin header is set to www.example.com.

   C. Enable the CORS setting on the API Gateway API endpoint. Ensure that the API endpoint is configured to return all responses that have the Access-Control-Allow-Origin header set to www.example.com. `Most Voted`

   D. Enable the CORS setting on the Lambda function. Ensure that the return code of the function has the Access-Control-Allow-Origin header set to www.example.com.

   Correct Answer: *C*

   Community vote distribution
                              C (95%)   5%

Question #261   *Topic 1*

A company has many separate AWS accounts and uses no central billing or management. Each AWS account hosts services for different departments in the company. The company has a Microsoft Azure Active Directory that is deployed.

A solutions architect needs to centralize billing and management of the company's AWS accounts. The company wants to start using identity federation instead of manual user management. The company also wants to use temporary credentials instead of long-lived access keys.

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

   A. Create a new AWS account to serve as a management account. Deploy an organization in AWS Organizations. Invite each existing AWS account to join the organization. Ensure that each account accepts the invitation. `Most Voted`

   B. Configure each AWS account's email address to be aws+@example.com so that account management email messages and invoices are sent to the same place.

   C. Deploy AWS IAM Identity Center (AWS Single Sign-On) in the management account. Connect IAM Identity Center to the Azure Active Directory. Configure IAM Identity Center for automatic synchronization of users and groups. `Most Voted`

   D. Deploy an AWS Managed Microsoft AD directory in the management account. Share the directory with all other accounts in the organization by using AWS Resource Access Manager (AWS RAM).

   E. Create AWS IAM Identity Center (AWS Single Sign-On) permission sets. Attach the permission sets to the appropriate IAM Identity Center groups and AWS accounts. `Most Voted`

   F. Configure AWS Identity and Access Management (IAM) in each AWS account to use AWS Managed Microsoft AD for authentication and authorization.

   Correct Answer: *ACE*

   Community vote distribution
                              ACE (100%)

Question #262

Topic 1

A company wants to manage the costs associated with a group of 20 applications that are infrequently used, but are still business-critical, by migrating to AWS. The applications are a mix of Java and Node.js spread across different instance clusters. The company wants to minimize costs while standardizing by using a single deployment methodology.

Most of the applications are part of month-end processing routines with a small number of concurrent users, but they are occasionally run at other times. Average application memory consumption is less than 1 GB. though some applications use as much as 2.5 GB of memory during peak processing. The most important application in the group is a billing report written in Java that accesses multiple data sources and often runs for several hours.

Which is the MOST cost-effective solution?

A. Deploy a separate AWS Lambda function for each application. Use AWS CloudTrail logs and Amazon CloudWatch alarms to verify completion of critical jobs.

B. Deploy Amazon ECS containers on Amazon EC2 with Auto Scaling configured for memory utilization of 75%. Deploy an ECS task for each application being migrated with ECS task scaling. Monitor services and hosts by using Amazon CloudWatch. Most Voted

C. Deploy AWS Elastic Beanstalk for each application with Auto Scaling to ensure that all requests have sufficient resources. Monitor each AWS Elastic Beanstalk deployment by using CloudWatch alarms.

D. Deploy a new Amazon EC2 instance cluster that co-hosts all applications by using EC2 Auto Scaling and Application Load Balancers. Scale cluster size based on a custom metric set on instance memory utilization. Purchase 3-year Reserved Instance reservations equal to the GroupMaxSize parameter of the Auto Scaling group.

Correct Answer: *B*

Community vote distribution

B (86%)   14%

Question #263

Topic 1

A solutions architect needs to review the design of an Amazon EMR cluster that is using the EMR File System (EMRFS). The cluster performs tasks that are critical to business needs. The cluster is running Amazon EC2 On-Demand Instances at all times for all task, primary, and core nodes. The EMR tasks run each morning, starting at 1:00 AM. and take 6 hours to finish running. The amount of time to complete the processing is not a priority because the data is not referenced until late in the day.

The solutions architect must review the architecture and suggest a solution to minimize the compute costs.

Which solution should the solutions architect recommend to meet these requirements?

A. Launch all task, primary, and core nodes on Spot Instances in an instance fleet. Terminate the cluster, including all instances, when the processing is completed.

B. Launch the primary and core nodes on On-Demand Instances. Launch the task nodes on Spot Instances in an instance fleet. Terminate the cluster, including all instances, when the processing is completed. Purchase Compute Savings Plans to cover the On-Demand Instance usage.

C. Continue to launch all nodes on On-Demand Instances. Terminate the cluster, including all instances, when the processing is completed. Purchase Compute Savings Plans to cover the On-Demand Instance usage.

D. Launch the primary and core nodes on On-Demand Instances. Launch the task nodes on Spot Instances in an instance fleet. Terminate only the task node instances when the processing is completed. Purchase Compute Savings Plans to cover the On-Demand Instance usage. Most Voted

Correct Answer: *D*

Community vote distribution

D (58%)   B (41%)

Question #264   Topic 1

A company has migrated a legacy application to the AWS Cloud. The application runs on three Amazon EC2 instances that are spread across three Availability Zones. One EC2 instance is in each Availability Zone. The EC2 instances are running in three private subnets of the VPC and are set up as targets for an Application Load Balancer (ALB) that is associated with three public subnets.

The application needs to communicate with on-premises systems. Only traffic from IP addresses in the company's IP address range are allowed to access the on-premises systems. The company's security team is bringing only one IP address from its internal IP address range to the cloud. The company has added this IP address to the allow list for the company firewall. The company also has created an Elastic IP address for this IP address.

A solutions architect needs to create a solution that gives the application the ability to communicate with the on-premises systems. The solution also must be able to mitigate failures automatically.

Which solution will meet these requirements?

A. Deploy three NAT gateways, one in each public subnet. Assign the Elastic IP address to the NAT gateways. Turn on health checks for the NAT gateways. If a NAT gateway fails a health check, recreate the NAT gateway and assign the Elastic IP address to the new NAT gateway.

B. Replace the ALB with a Network Load Balancer (NLB). Assign the Elastic IP address to the NLTurn on health checks for the NLIn the case of a failed health check, redeploy the NLB in different subnets.

C. Deploy a single NAT gateway in a public subnet. Assign the Elastic IP address to the NAT gateway. Use Amazon CloudWatch with a custom metric to monitor the NAT gateway. If the NAT gateway is unhealthy, invoke an AWS Lambda function to create a new NAT gateway in a different subnet. Assign the Elastic IP address to the new NAT gateway. Most Voted

D. Assign the Elastic IP address to the ALB. Create an Amazon Route 53 simple record with the Elastic IP address as the value. Create a Route 53 health check. In the case of a failed health check, recreate the ALB in different subnets.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #265   *Topic 1*

A company uses AWS Organizations to manage more than 1,000 AWS accounts. The company has created a new developer organization. There are 540 developer member accounts that must be moved to the new developer organization. All accounts are set up with all the required information so that each account can be operated as a standalone account.

Which combination of steps should a solutions architect take to move all of the developer accounts to the new developer organization? (Choose three.)

    A. Call the MoveAccount operation in the Organizations API from the old organization's management account to migrate the developer accounts to the new developer organization.

    B. From the management account, remove each developer account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API. `Most Voted`

    C. From each developer account, remove the account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API.

    D. Sign in to the new developer organization's management account and create a placeholder member account that acts as a target for the developer account migration.

    E. Call the InviteAccountToOrganization operation in the Organizations API from the new developer organization's management account to send invitations to the developer accounts. `Most Voted`

    F. Have each developer sign in to their account and confirm to join the new developer organization. `Most Voted`

Correct Answer: *BEF*

Community vote distribution

                    BEF (89%)   6%

Question #266   *Topic 1*

A company's interactive web application uses an Amazon CloudFront distribution to serve images from an Amazon S3 bucket. Occasionally, third-party tools ingest corrupted images into the S3 bucket. This image corruption causes a poor user experience in the application later. The company has successfully implemented and tested Python logic to detect corrupt images.

A solutions architect must recommend a solution to integrate the detection logic with minimal latency between the ingestion and serving.

Which solution will meet these requirements?

    A. Use a Lambda@Edge function that is invoked by a viewer-response event.

    B. Use a Lambda@Edge function that is invoked by an origin-response event.

    C. Use an S3 event notification that invokes an AWS Lambda function. `Most Voted`

    D. Use an S3 event notification that invokes an AWS Step Functions state machine.

Correct Answer: *C*

Community vote distribution

                    C (96%)   4%

Question #267   *Topic 1*

A company has an application that runs on Amazon EC2 instances in an Amazon EC2 Auto Scaling group. The company uses AWS CodePipeline to deploy the application. The instances that run in the Auto Scaling group are constantly changing because of scaling events.

When the company deploys new application code versions, the company installs the AWS CodeDeploy agent on any new target EC2 instances and associates the instances with the CodeDeploy deployment group. The application is set to go live within the next 24 hours.

What should a solutions architect recommend to automate the application deployment process with the LEAST amount of operational overhead?

A. Configure Amazon EventBridge to invoke an AWS Lambda function when a new EC2 instance is launched into the Auto Scaling group. Code the Lambda function to associate the EC2 instances with the CodeDeploy deployment group.

B. Write a script to suspend Amazon EC2 Auto Scaling operations before the deployment of new code. When the deployment is complete, create a new AMI and configure the Auto Scaling group's launch template to use the new AMI for new launches. Resume Amazon EC2 Auto Scaling operations.

C. Create a new AWS CodeBuild project that creates a new AMI that contains the new code. Configure CodeBuild to update the Auto Scaling group's launch template to the new AMI. Run an Amazon EC2 Auto Scaling instance refresh operation.

D. Create a new AMI that has the CodeDeploy agent installed. Configure the Auto Scaling group's launch template to use the new AMI. Associate the CodeDeploy deployment group with the Auto Scaling group instead of the EC2 instances. Most Voted

Correct Answer: *D*

Community vote distribution

D (95%)   5%

Question #268   *Topic 1*

A company has a website that runs on four Amazon EC2 instances that are behind an Application Load Balancer (ALB). When the ALB detects that an EC2 instance is no longer available, an Amazon CloudWatch alarm enters the ALARM state. A member of the company's operations team then manually adds a new EC2 instance behind the ALB.

A solutions architect needs to design a highly available solution that automatically handles the replacement of EC2 instances. The company needs to minimize downtime during the switch to the new solution.

Which set of steps should the solutions architect take to meet these requirements?

A. Delete the existing ALB. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Create a new ALB. Attach the Auto Scaling group to the new ALB. Attach the existing EC2 instances to the Auto Scaling group.

B. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Attach the Auto Scaling group to the existing ALAttach the existing EC2 instances to the Auto Scaling group. Most Voted

C. Delete the existing ALB and the EC2 instances. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Create a new ALB. Attach the Auto Scaling group to the new ALB. Wait for the Auto Scaling group to launch the minimum number of EC2 instances.

D. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Attach the Auto Scaling group to the existing ALB. Wait for the existing ALB to register the existing EC2 instances with the Auto Scaling group.

Correct Answer: *B*

Community vote distribution

B (91%)   9%

Question #269   *Topic 1*

A company wants to optimize AWS data-transfer costs and compute costs across developer accounts within the company's organization in AWS Organizations. Developers can configure VPCs and launch Amazon EC2 instances in a single AWS Region. The EC2 instances retrieve approximately 1 TB of data each day from Amazon S3.

The developer activity leads to excessive monthly data-transfer charges and NAT gateway processing charges between EC2 instances and S3 buckets, along with high compute costs. The company wants to proactively enforce approved architectural patterns for any EC2 instance and VPC infrastructure that developers deploy within the AWS accounts. The company does not want this enforcement to negatively affect the speed at which the developers can perform their tasks.

Which solution will meet these requirements MOST cost-effectively?

   A. Create SCPs to prevent developers from launching unapproved EC2 instance types. Provide the developers with an AWS CloudFormation template to deploy an approved VPC configuration with S3 interface endpoints. Scope the developers' IAM permissions so that the developers can launch VPC resources only with CloudFormation.

   B. Create a daily forecasted budget with AWS Budgets to monitor EC2 compute costs and S3 data-transfer costs across the developer accounts. When the forecasted cost is 75% of the actual budget cost, send an alert to the developer teams. If the actual budget cost is 100%, create a budget action to terminate the developers' EC2 instances and VPC infrastructure.

   C. Create an AWS Service Catalog portfolio that users can use to create an approved VPC configuration with S3 gateway endpoints and approved EC2 instances. Share the portfolio with the developer accounts. Configure an AWS Service Catalog launch constraint to use an approved IAM role. Scope the developers' IAM permissions to allow access only to AWS Service Catalog. Most Voted

   D. Create and deploy AWS Config rules to monitor the compliance of EC2 and VPC resources in the developer AWS accounts. If developers launch unapproved EC2 instances or if developers create VPCs without S3 gateway endpoints, perform a remediation action to terminate the unapproved resources.

   Correct Answer: *C*

   Community vote distribution
               C (94%)   6%

Question #270   *Topic 1*

A company is expanding. The company plans to separate its resources into hundreds of different AWS accounts in multiple AWS Regions. A solutions architect must recommend a solution that denies access to any operations outside of specifically designated Regions.

Which solution will meet these requirements?

   A. Create IAM roles for each account. Create IAM policies with conditional allow permissions that include only approved Regions for the accounts.

   B. Create an organization in AWS Organizations. Create IAM users for each account. Attach a policy to each user to block access to Regions where an account cannot deploy infrastructure.

   C. Launch an AWS Control Tower landing zone. Create OUs and attach SCPs that deny access to run services outside of the approved Regions. Most Voted

   D. Enable AWS Security Hub in each account. Create controls to specify the Regions where an account can deploy infrastructure.

   Correct Answer: *C*

   Community vote distribution
                                  C (100%)

Question #271   *Topic 1*

A company wants to refactor its retail ordering web application that currently has a load-balanced Amazon EC2 instance fleet for web hosting, database API services, and business logic. The company needs to create a decoupled, scalable architecture with a mechanism for retaining failed orders while also minimizing operational costs.

Which solution will meet these requirements?

    A. Use Amazon S3 for web hosting with Amazon API Gateway for database API services. Use Amazon Simple Queue Service (Amazon SQS) for order queuing. Use Amazon Elastic Container Service (Amazon ECS) for business logic with Amazon SQS long polling for retaining failed orders.

    B. Use AWS Elastic Beanstalk for web hosting with Amazon API Gateway for database API services. Use Amazon MQ for order queuing. Use AWS Step Functions for business logic with Amazon S3 Glacier Deep Archive for retaining failed orders.

    C. Use Amazon S3 for web hosting with AWS AppSync for database API services. Use Amazon Simple Queue Service (Amazon SQS) for order queuing. Use AWS Lambda for business logic with an Amazon SQS dead-letter queue for retaining failed orders. [Most Voted]

    D. Use Amazon Lightsail for web hosting with AWS AppSync for database API services. Use Amazon Simple Email Service (Amazon SES) for order queuing. Use Amazon Elastic Kubernetes Service (Amazon EKS) for business logic with Amazon OpenSearch Service for retaining failed orders.

Correct Answer: *C*

Community vote distribution

                        C (85%)   A (15%)

Question #272   *Topic 1*

A company hosts a web application on AWS in the us-east-1 Region. The application servers are distributed across three Availability Zones behind an Application Load Balancer. The database is hosted in a MySQL database on an Amazon EC2 instance. A solutions architect needs to design a cross-Region data recovery solution using AWS services with an RTO of less than 5 minutes and an RPO of less than 1 minute. The solutions architect is deploying application servers in us-west-2, and has configured Amazon Route 53 health checks and DNS failover to us-west-2.

Which additional step should the solutions architect take?

    A. Migrate the database to an Amazon RDS for MySQL instance with a cross-Region read replica in us-west-2.

    B. Migrate the database to an Amazon Aurora global database with the primary in us-east-1 and the secondary in us-west-2. [Most Voted]

    C. Migrate the database to an Amazon RDS for MySQL instance with a Multi-AZ deployment.

    D. Create a MySQL standby database on an Amazon EC2 instance in us-west-2.

Correct Answer: *B*

Community vote distribution

                        B (94%)   6%

Question #273   *Topic 1*

A company is using AWS Organizations to manage multiple accounts. Due to regulatory requirements, the company wants to restrict specific member accounts to certain AWS Regions, where they are permitted to deploy resources. The resources in the accounts must be tagged, enforced based on a group standard, and centrally managed with minimal configuration.

What should a solutions architect do to meet these requirements?

    A. Create an AWS Config rule in the specific member accounts to limit Regions and apply a tag policy.

    B. From the AWS Billing and Cost Management console, in the management account, disable Regions for the specific member accounts and apply a tag policy on the root.

    C. Associate the specific member accounts with the root. Apply a tag policy and an SCP using conditions to limit Regions.

    D. Associate the specific member accounts with a new OU. Apply a tag policy and an SCP using conditions to limit Regions. [Most Voted]

    Correct Answer: *D*

    Community vote distribution
                                            D (100%)

Question #274   *Topic 1*

A company has an application that generates reports and stores them in an Amazon S3 bucket. When a user accesses their report, the application generates a signed URL to allow the user to download the report. The company's security team has discovered that the files are public and that anyone can download them without authentication. The company has suspended the generation of new reports until the problem is resolved.

Which set of actions will immediately remediate the security issue without impacting the application's normal workflow?

    A. Create an AWS Lambda function that applies a deny all policy for users who are not authenticated. Create a scheduled event to invoke the Lambda function.

    B. Review the AWS Trusted Advisor bucket permissions check and implement the recommended actions.

    C. Run a script that puts a private ACL on all of the objects in the bucket.

    D. Use the Block Public Access feature in Amazon S3 to set the IgnorePublicAcls option to TRUE on the bucket. [Most Voted]

    Correct Answer: *D*

    Community vote distribution
                        D (79%)   14%   7%

Question #275 | Topic 1

A company is planning to migrate an Amazon RDS for Oracle database to an RDS for PostgreSQL DB instance in another AWS account. A solutions architect needs to design a migration strategy that will require no downtime and that will minimize the amount of time necessary to complete the migration. The migration strategy must replicate all existing data and any new data that is created during the migration. The target database must be identical to the source database at completion of the migration process.

All applications currently use an Amazon Route 53 CNAME record as their endpoint for communication with the RDS for Oracle DB instance. The RDS for Oracle DB instance is in a private subnet.

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

A. Create a new RDS for PostgreSQL DB instance in the target account. Use the AWS Schema Conversion Tool (AWS SCT) to migrate the database schema from the source database to the target database. Most Voted

B. Use the AWS Schema Conversion Tool (AWS SCT) to create a new RDS for PostgreSQL DB instance in the target account with the schema and initial data from the source database.

C. Configure VPC peering between the VPCs in the two AWS accounts to provide connectivity to both DB instances from the target account. Configure the security groups that are attached to each DB instance to allow traffic on the database port from the VPC in the target account. Most Voted

D. Temporarily allow the source DB instance to be publicly accessible to provide connectivity from the VPC in the target account. Configure the security groups that are attached to each DB instance to allow traffic on the database port from the VPC in the target account.

E. Use AWS Database Migration Service (AWS DMS) in the target account to perform a full load plus change data capture (CDC) migration from the source database to the target database. When the migration is complete, change the CNAME record to point to the target DB instance endpoint. Most Voted

F. Use AWS Database Migration Service (AWS DMS) in the target account to perform a change data capture (CDC) migration from the source database to the target database. When the migration is complete, change the CNAME record to point to the target DB instance endpoint.

Correct Answer: *ACE*

Community vote distribution

ACE (97%)

Question #276 | Topic 1

A company has implemented an ordering system using an event-driven architecture. During initial testing, the system stopped processing orders. Further log analysis revealed that one order message in an Amazon Simple Queue Service (Amazon SQS) standard queue was causing an error on the backend and blocking all subsequent order messages. The visibility timeout of the queue is set to 30 seconds, and the backend processing timeout is set to 10 seconds. A solutions architect needs to analyze faulty order messages and ensure that the system continues to process subsequent messages.

Which step should the solutions architect take to meet these requirements?

A. Increase the backend processing timeout to 30 seconds to match the visibility timeout.

B. Reduce the visibility timeout of the queue to automatically remove the faulty message.

C. Configure a new SQS FIFO queue as a dead-letter queue to isolate the faulty messages.

D. Configure a new SQS standard queue as a dead-letter queue to isolate the faulty messages. Most Voted

Correct Answer: *D*

Community vote distribution

D (88%) | 12%

Question #277   *Topic 1*

A company has automated the nightly retraining of its machine learning models by using AWS Step Functions. The workflow consists of multiple steps that use AWS Lambda. Each step can fail for various reasons, and any failure causes a failure of the overall workflow.

A review reveals that the retraining has failed multiple nights in a row without the company noticing the failure. A solutions architect needs to improve the workflow so that notifications are sent for all types of failures in the retraining process.

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

A. Create an Amazon Simple Notification Service (Amazon SNS) topic with a subscription of type "Email" that targets the team's mailing list.
`Most Voted`

B. Create a task named "Email" that forwards the input arguments to the SNS topic. `Most Voted`

C. Add a Catch field to all Task, Map, and Parallel states that have a statement of "ErrorEquals": ["States.ALL"] and "Next": "Email".
`Most Voted`

D. Add a new email address to Amazon Simple Email Service (Amazon SES). Verify the email address.

E. Create a task named "Email" that forwards the input arguments to the SES email address.

F. Add a Catch field to all Task, Map, and Parallel states that have a statement of "ErrorEquals": ["States.Runtime"] and "Next": "Email".

Correct Answer: *ABC*

Community vote distribution

ABC (88%)   4%

Question #278   *Topic 1*

A company plans to deploy a new private intranet service on Amazon EC2 instances inside a VPC. An AWS Site-to-Site VPN connects the VPC to the company's on-premises network. The new service must communicate with existing on-premises services. The on-premises services are accessible through the use of hostnames that reside in the company.example DNS zone. This DNS zone is wholly hosted on premises and is available only on the company's private network.

A solutions architect must ensure that the new service can resolve hostnames on the company.example domain to integrate with existing services.

Which solution meets these requirements?

A. Create an empty private zone in Amazon Route 53 for company.example. Add an additional NS record to the company's on-premises company.example zone that points to the authoritative name servers for the new private zone in Route 53.

B. Turn on DNS hostnames for the VPC. Configure a new outbound endpoint with Amazon Route 53 Resolver. Create a Resolver rule to forward requests for company.example to the on-premises name servers. `Most Voted`

C. Turn on DNS hostnames for the VPConfigure a new inbound resolver endpoint with Amazon Route 53 Resolver. Configur&the on-premises DNS server to forward requests for company.example to the new resolver.

D. Use AWS Systems Manager to configure a run document that will install a hosts file that contains any required hostnames. Use an Amazon EventBridge rule to run the document when an instance is entering the running state.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #279   *Topic 1*

A company uses AWS CloudFormation to deploy applications within multiple VPCs that are all attached to a transit gateway. Each VPC that sends traffic to the public internet must send the traffic through a shared services VPC. Each subnet within a VPC uses the default VPC route table, and the traffic is routed to the transit gateway. The transit gateway uses its default route table for any VPC attachment.

A security audit reveals that an Amazon EC2 instance that is deployed within a VPC can communicate with an EC2 instance that is deployed in any of the company's other VPCs. A solutions architect needs to limit the traffic between the VPCs. Each VPC must be able to communicate only with a predefined, limited set of authorized VPCs.

What should the solutions architect do to meet these requirements?

A. Update the network ACL of each subnet within a VPC to allow outbound traffic only to the authorized VPCs. Remove all deny rules except the default deny rule.

B. Update all the security groups that are used within a VPC to deny outbound traffic to security groups that are used within the unauthorized VPCs.

C. Create a dedicated transit gateway route table for each VPC attachment. Route traffic only to the authorized VPCs. `Most Voted`

D. Update the main route table of each VPC to route traffic only to the authorized VPCs through the transit gateway.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #280   *Topic 1*

A company has a Windows-based desktop application that is packaged and deployed to the users' Windows machines. The company recently acquired another company that has employees who primarily use machines with a Linux operating system. The acquiring company has decided to migrate and rehost the Windows-based desktop application to AWS.

All employees must be authenticated before they use the application. The acquiring company uses Active Directory on premises but wants a simplified way to manage access to the application on AWS for all the employees.

Which solution will rehost the application on AWS with the LEAST development effort?

A. Set up and provision an Amazon Workspaces virtual desktop for every employee. Implement authentication by using Amazon Cognito identity pools. Instruct employees to run the application from their provisioned Workspaces virtual desktops.

B. Create an Auto Scaling group of Windows-based Amazon EC2 instances. Join each EC2 instance to the company's Active Directory domain. Implement authentication by using the Active Directory that is running on premises. Instruct employees to run the application by using a Windows remote desktop.

C. Use an Amazon AppStream 2.0 image builder to create an image that includes the application and the required configurations. Provision an AppStream 2.0 On-Demand fleet with dynamic Fleet Auto Scaling policies for running the image. Implement authentication by using AppStream 2.0 user pools. Instruct the employees to access the application by starting browser-based AppStream 2.0 streaming sessions. `Most Voted`

D. Refactor and containerize the application to run as a web-based application. Run the application in Amazon Elastic Container Service (Amazon ECS) on AWS Fargate with step scaling policies. Implement authentication by using Amazon Cognito user pools. Instruct the employees to run the application from their browsers.

Correct Answer: *C*

Community vote distribution

C (95%)   5%

Question #281   *Topic 1*

A company is collecting a large amount of data from a fleet of IoT devices. Data is stored as Optimized Row Columnar (ORC) files in the Hadoop Distributed File System (HDFS) on a persistent Amazon EMR cluster. The company's data analytics team queries the data by using SQL in Apache Presto deployed on the same EMR cluster. Queries scan large amounts of data, always run for less than 15 minutes, and run only between 5 PM and 10 PM.

The company is concerned about the high cost associated with the current solution. A solutions architect must propose the most cost-effective solution that will allow SQL data queries.

Which solution will meet these requirements?

    A. Store data in Amazon S3. Use Amazon Redshift Spectrum to query data.

    B. Store data in Amazon S3. Use the AWS Glue Data Catalog and Amazon Athena to query data. `Most Voted`

    C. Store data in EMR File System (EMRFS). Use Presto in Amazon EMR to query data.

    D. Store data in Amazon Redshift. Use Amazon Redshift to query data.

Correct Answer: *B*

Community vote distribution

                   B (96%)   4%

Question #282   *Topic 1*

A large company recently experienced an unexpected increase in Amazon RDS and Amazon DynamoDB costs. The company needs to increase visibility into details of AWS Billing and Cost Management. There are various accounts associated with AWS Organizations, including many development and production accounts. There is no consistent tagging strategy across the organization, but there are guidelines in place that require all infrastructure to be deployed using AWS CloudFormation with consistent tagging. Management requires cost center numbers and project ID numbers for all existing and future DynamoDB tables and RDS instances.

Which strategy should the solutions architect provide to meet these requirements?

    A. Use Tag Editor to tag existing resources. Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources.

    B. Use an AWS Config rule to alert the finance team of untagged resources. Create a centralized AWS Lambda based solution to tag untagged RDS databases and DynamoDB resources every hour using a cross-account role.

    C. Use Tag Editor to tag existing resources. Create cost allocation tags to define the cost center and project ID. Use SCPs to restrict resource creation that do not have the cost center and project ID on the resource. `Most Voted`

    D. Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources. Update existing federated roles to restrict privileges to provision resources that do not include the cost center and project ID on the resource.

Correct Answer: *C*

Community vote distribution

                   C (89%)   11%

Question #283   *Topic 1*

A company wants to send data from its on-premises systems to Amazon S3 buckets. The company created the S3 buckets in three different accounts. The company must send the data privately without the data traveling across the internet. The company has no existing dedicated connectivity to AWS.

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

A. Establish a networking account in the AWS Cloud. Create a private VPC in the networking account. Set up an AWS Direct Connect connection with a private VIF between the on-premises environment and the private VPC. Most Voted

B. Establish a networking account in the AWS Cloud. Create a private VPC in the networking account. Set up an AWS Direct Connect connection with a public VIF between the on-premises environment and the private VPC.

C. Create an Amazon S3 interface endpoint in the networking account. Most Voted

D. Create an Amazon S3 gateway endpoint in the networking account.

E. Establish a networking account in the AWS Cloud. Create a private VPC in the networking account. Peer VPCs from the accounts that host the S3 buckets with the VPC in the network account.

Correct Answer: *AC*

Community vote distribution

AC (87%)   7%

Question #284   *Topic 1*

A company operates quick-service restaurants. The restaurants follow a predictable model with high sales traffic for 4 hours daily. Sales traffic is lower outside of those peak hours.

The point of sale and management platform is deployed in the AWS Cloud and has a backend that is based on Amazon DynamoDB. The database table uses provisioned throughput mode with 100,000 RCUs and 80,000 WCUs to match known peak resource consumption.

The company wants to reduce its DynamoDB cost and minimize the operational overhead for the IT staff.

Which solution meets these requirements MOST cost-effectively?

A. Reduce the provisioned RCUs and WCUs.

B. Change the DynamoDB table to use on-demand capacity.

C. Enable Dynamo DB auto scaling for the table. Most Voted

D. Purchase 1-year reserved capacity that is sufficient to cover the peak load for 4 hours each day.

Correct Answer: *C*

Community vote distribution

C (68%)   B (23%)   9%

Question #285   *Topic 1*

A company hosts a blog post application on AWS using Amazon API Gateway, Amazon DynamoDB, and AWS Lambda. The application currently does not use API keys to authorize requests. The API model is as follows:

GET /posts/{postId}: to get post details
GET /users/{userId}: to get user details
GET /comments/{commentId}: to get comments details

The company has noticed users are actively discussing topics in the comments section, and the company wants to increase user engagement by making the comments appear in real time.

Which design should be used to reduce comment latency and improve user experience?

A. Use edge-optimized API with Amazon CloudFront to cache API responses.

B. Modify the blog application code to request GET/comments/{commentId} every 10 seconds.

C. Use AWS AppSync and leverage WebSockets to deliver comments. Most Voted

D. Change the concurrency limit of the Lambda functions to lower the API response time.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #286   *Topic 1*

A company manages hundreds of AWS accounts centrally in an organization in AWS Organizations. The company recently started to allow product teams to create and manage their own S3 access points in their accounts. The S3 access points can be accessed only within VPCs, not on the internet.

What is the MOST operationally efficient way to enforce this requirement?

A. Set the S3 access point resource policy to deny the s3:CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.

B. Create an SCP at the root level in the organization to deny the s3:CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC. Most Voted

C. Use AWS CloudFormation StackSets to create a new IAM policy in each AWS account that allows the s3:CreateAccessPoint action only if the s3:AccessPointNetworkOrigin condition key evaluates to VPC.

D. Set the S3 bucket policy to deny the s3:CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.

Correct Answer: *B*

Community vote distribution

B (95%)   5%

Question #287
Topic 1

A solutions architect must update an application environment within AWS Elastic Beanstalk using a blue/green deployment methodology. The solutions architect creates an environment that is identical to the existing application environment and deploys the application to the new environment.

What should be done next to complete the update?

A. Redirect to the new environment using Amazon Route 53.

B. Select the Swap Environment URLs option. Most Voted

C. Replace the Auto Scaling launch configuration.

D. Update the DNS records to point to the green environment.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #288
Topic 1

A company is building an image service on the web that will allow users to upload and search random photos. At peak usage, up to 10,000 users worldwide will upload their images. The will then overlay text on the uploaded images, which will then be published on the company website.

Which design should a solutions architect implement?

A. Store the uploaded images in Amazon Elastic File System (Amazon EFS). Send application log information about each image to Amazon CloudWatch Logs. Create a fleet of Amazon EC2 instances that use CloudWatch Logs to determine which images need to be processed. Place processed images in another directory in Amazon EFS. Enable Amazon CloudFront and configure the origin to be the one of the EC2 instances in the fleet.

B. Store the uploaded images in an Amazon S3 bucket and configure an S3 bucket event notification to send a message to Amazon Simple Notification Service (Amazon SNS). Create a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) to pull messages from Amazon SNS to process the images and place them in Amazon Elastic File System (Amazon EFS). Use Amazon CloudWatch metrics for the SNS message volume to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to be the ALB in front of the EC2 instances.

C. Store the uploaded images in an Amazon S3 bucket and configure an S3 bucket event notification to send a message to the Amazon Simple Queue Service (Amazon SQS) queue. Create a fleet of Amazon EC2 instances to pull messages from the SQS queue to process the images and place them in another S3 bucket. Use Amazon CloudWatch metrics for queue depth to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to be the S3 bucket that contains the processed images. Most Voted

D. Store the uploaded images on a shared Amazon Elastic Block Store (Amazon EBS) volume mounted to a fleet of Amazon EC2 Spot instances. Create an Amazon DynamoDB table that contains information about each uploaded image and whether it has been processed. Use an Amazon EventBridge rule to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to reference an Elastic Load Balancer in front of the fleet of EC2 instances.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #289   Topic 1

A company has deployed its database on an Amazon RDS for MySQL DB instance in the us-east-1 Region. The company needs to make its data available to customers in Europe. The customers in Europe must have access to the same data as customers in the United States (US) and will not tolerate high application latency or stale data. The customers in Europe and the customers in the US need to write to the database. Both groups of customers need to see updates from the other group in real time.

Which solution will meet these requirements?

A. Create an Amazon Aurora MySQL replica of the RDS for MySQL DB instance. Pause application writes to the RDS DB instance. Promote the Aurora Replica to a standalone DB cluster. Reconfigure the application to use the Aurora database and resume writes. Add eu-west-1 as a secondary Region to the DB cluster. Enable write forwarding on the DB cluster. Deploy the application in eu-west-1. Configure the application to use the Aurora MySQL endpoint in eu-west-1. [Most Voted]

B. Add a cross-Region replica in eu-west-1 for the RDS for MySQL DB instance. Configure the replica to replicate write queries back to the primary DB instance. Deploy the application in eu-west-1. Configure the application to use the RDS for MySQL endpoint in eu-west-1.

C. Copy the most recent snapshot from the RDS for MySQL DB instance to eu-west-1. Create a new RDS for MySQL DB instance in eu-west-1 from the snapshot. Configure MySQL logical replication from us-east-1 to eu-west-1. Enable write forwarding on the DB cluster. Deploy the application in eu-wes&1. Configure the application to use the RDS for MySQL endpoint in eu-west-1.

D. Convert the RDS for MySQL DB instance to an Amazon Aurora MySQL DB cluster. Add eu-west-1 as a secondary Region to the DB cluster. Enable write forwarding on the DB cluster. Deploy the application in eu-west-1. Configure the application to use the Aurora MySQL endpoint in eu-west-1.

Correct Answer: *A*

Community vote distribution

A (66%)   D (34%)

Question #290
Topic 1

A company is serving files to its customers through an SFTP server that is accessible over the internet. The SFTP server is running on a single Amazon EC2 instance with an Elastic IP address attached. Customers connect to the SFTP server through its Elastic IP address and use SSH for authentication. The EC2 instance also has an attached security group that allows access from all customer IP addresses.

A solutions architect must implement a solution to improve availability, minimize the complexity of infrastructure management, and minimize the disruption to customers who access files. The solution must not change the way customers connect.

Which solution will meet these requirements?

A. Disassociate the Elastic IP address from the EC2 instance. Create an Amazon S3 bucket to be used for SFTP file hosting. Create an AWS Transfer Family server. Configure the Transfer Family server with a publicly accessible endpoint. Associate the SFTP Elastic IP address with the new endpoint. Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to the S3 bucket.

B. Disassociate the Elastic IP address from the EC2 instance. Create an Amazon S3 bucket to be used for SFTP file hosting. Create an AWS Transfer Family server. Configure the Transfer Family server with a VPC-hosted, internet-facing endpoint. Associate the SFTP Elastic IP address with the new endpoint. Attach the security group with customer IP addresses to the new endpoint. Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to the S3 bucket. [Most Voted]

C. Disassociate the Elastic IP address from the EC2 instance. Create a new Amazon Elastic File System (Amazon EFS) file system to be used for SFTP file hosting. Create an AWS Fargate task definition to run an SFTP server. Specify the EFS file system as a mount in the task definition. Create a Fargate service by using the task definition, and place a Network Load Balancer (NLB) in front of the service. When configuring the service, attach the security group with customer IP addresses to the tasks that run the SFTP server. Associate the Elastic IP address with the NLB. Sync all files from the SFTP server to the S3 bucket.

D. Disassociate the Elastic IP address from the EC2 instance. Create a multi-attach Amazon Elastic Block Store (Amazon EBS) volume to be used for SFTP file hosting. Create a Network Load Balancer (NLB) with the Elastic IP address attached. Create an Auto Scaling group with EC2 instances that run an SFTP server. Define in the Auto Scaling group that instances that are launched should attach the new multi-attach EBS volume. Configure the Auto Scaling group to automatically add instances behind the NLB. Configure the Auto Scaling group to use the security group that allows customer IP addresses for the EC2 instances that the Auto Scaling group launches. Sync all files from the SFTP server to the new multi-attach EBS volume.

Correct Answer: *B*

Community vote distribution

B (85%)   A (15%)

Question #291
Topic 1

A company ingests and processes streaming market data. The data rate is constant. A nightly process that calculates aggregate statistics takes 4 hours to complete. The statistical analysis is not critical to the business, and data points are processed during the next iteration if a particular run fails.

The current architecture uses a pool of Amazon EC2 Reserved Instances with 1-year reservations. These EC2 instances run full time to ingest and store the streaming data in attached Amazon Elastic Block Store (Amazon EBS) volumes. A scheduled script launches EC2 On-Demand Instances each night to perform the nightly processing. The instances access the stored data from NFS shares on the ingestion servers. The script terminates the instances when the processing is complete.

The Reserved Instance reservations are expiring. The company needs to determine whether to purchase new reservations or implement a new design.

Which solution will meet these requirements MOST cost-effectively?

A. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon S3. Use a scheduled script to launch a fleet of EC2 On-Demand Instances each night to perform the batch processing of the S3 data. Configure the script to terminate the instances when the processing is complete.

B. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon S3. Use AWS Batch with Spot Instances to perform nightly processing with a maximum Spot price that is 50% of the On-Demand price. Most Voted

C. Update the ingestion process to use a fleet of EC2 Reserved Instances with 3-year reservations behind a Network LoadBalancer. Use AWS Batch with Spot Instances to perform nightly processing with a maximum Spot price that is 50% of the On-Demand price.

D. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon Redshift. Use Amazon EventBridge to schedule an AWS Lambda function to run nightly to query Amazon Redshift to generate the daily statistics.

Correct Answer: *B*

Community vote distribution

B (95%)   5%

Question #292
Topic 1

A company needs to migrate an on-premises SFTP site to AWS. The SFTP site currently runs on a Linux VM. Uploaded files are made available to downstream applications through an NFS share.

As part of the migration to AWS, a solutions architect must implement high availability. The solution must provide external vendors with a set of static public IP addresses that the vendors can allow. The company has set up an AWS Direct Connect connection between its on-premises data center and its VPC.

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

A. Create an AWS Transfer Family server. Configure an internet-facing VPC endpoint for the Transfer Family server. Specify an Elastic IP address for each subnet. Configure the Transfer Family server to place files into an Amazon Elastic File System (Amazon EFS) file system that is deployed across multiple Availability Zones. Modify the configuration on the downstream applications that access the existing NFS share to mount the EFS endpoint instead. Most Voted

B. Create an AWS Transfer Family server. Configure a publicly accessible endpoint for the Transfer Family server. Configure the Transfer Family server to place files into an Amazon Elastic File System (Amazon EFS) file system that is deployed across multiple Availability Zones. Modify the configuration on the downstream applications that access the existing NFS share to mount the EFS endpoint instead.

C. Use AWS Application Migration Service to migrate the existing Linux VM to an Amazon EC2 instance. Assign an Elastic IP address to the EC2 instance. Mount an Amazon Elastic File System (Amazon EFS) file system to the EC2 instance. Configure the SFTP server to place files in the EFS file system. Modify the configuration on the downstream applications that access the existing NFS share to mount the EFS endpoint instead.

D. Use AWS Application Migration Service to migrate the existing Linux VM to an AWS Transfer Family server. Configure a publicly accessible endpoint for the Transfer Family server. Configure the Transfer Family server to place files into an Amazon FSx for Lustre file system that is deployed across multiple Availability Zones. Modify the configuration on the downstream applications that access the existing NFS share to mount the FSx for Lustre endpoint instead.

Correct Answer: A

Community vote distribution

A (96%)   4%

Question #293
Topic 1

A solutions architect has an operational workload deployed on Amazon EC2 instances in an Auto Scaling group. The VPC architecture spans two Availability Zones (AZ) with a subnet in each that the Auto Scaling group is targeting. The VPC is connected to an on-premises environment and connectivity cannot be interrupted. The maximum size of the Auto Scaling group is 20 instances in service. The VPC IPv4 addressing is as follows:

VPC CIDR: 10.0.0.0/23 -

AZ1 subnet CIDR: 10.0.0.0/24 -

AZ2 subnet CIDR: 10.0.1.0/24 -

Since deployment, a third AZ has become available in the Region. The solutions architect wants to adopt the new AZ without adding additional IPv4 address space and without service downtime. Which solution will meet these requirements?

A. Update the Auto Scaling group to use the AZ2 subnet only. Delete and re-create the AZ1 subnet using half the previous address space. Adjust the Auto Scaling group to also use the new AZ1 subnet. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only. Remove the current AZ2 subnet. Create a new AZ2 subnet using the second half of the address space from the original AZ1 subnet. Create a new AZ3 subnet using half the original AZ2 subnet address space, then update the Auto Scaling group to target all three new subnets. Most Voted

B. Terminate the EC2 instances in the AZ1 subnet. Delete and re-create the AZ1 subnet using half the address space. Update the Auto Scaling group to use this new subnet. Repeat this for the second AZ. Define a new subnet in AZ3, then update the Auto Scaling group to target all three new subnets.

C. Create a new VPC with the same IPv4 address space and define three subnets, with one for each AZ. Update the existing Auto Scaling group to target the new subnets in the new VPC.

D. Update the Auto Scaling group to use the AZ2 subnet only. Update the AZ1 subnet to have half the previous address space. Adjust the Auto Scaling group to also use the AZ1 subnet again. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only. Update the current AZ2 subnet and assign the second half of the address space from the original AZ1 subnet. Create a new AZ3 subnet using half the original AZ2 subnet address space, then update the Auto Scaling group to target all three new subnets.

Correct Answer: A

Community vote distribution

A (91%)   9%

Question #294   *Topic 1*

A company uses an organization in AWS Organizations to manage the company's AWS accounts. The company uses AWS CloudFormation to deploy all infrastructure. A finance team wants to build a chargeback model. The finance team asked each business unit to tag resources by using a predefined list of project values.

When the finance team used the AWS Cost and Usage Report in AWS Cost Explorer and filtered based on project, the team noticed noncompliant project values. The company wants to enforce the use of project tags for new resources.

Which solution will meet these requirements with the LEAST effort?

A. Create a tag policy that contains the allowed project tag values in the organization's management account. Create an SCP that denies the cloudformation:CreateStack API operation unless a project tag is added. Attach the SCP to each OU. `Most Voted`

B. Create a tag policy that contains the allowed project tag values in each OU. Create an SCP that denies the cloudformation:CreateStack API operation unless a project tag is added. Attach the SCP to each OU.

C. Create a tag policy that contains the allowed project tag values in the AWS management account. Create an IAM policy that denies the cloudformation:CreateStack API operation unless a project tag is added. Assign the policy to each user.

D. Use AWS Service Catalog to manage the CloudFormation stacks as products. Use a TagOptions library to control project tag values. Share the portfolio with all OUs that are in the organization.

Correct Answer: *A*

Community vote distribution
A (100%)

Question #295   *Topic 1*

An application is deployed on Amazon EC2 instances that run in an Auto Scaling group. The Auto Scaling group configuration uses only one type of instance.

CPU and memory utilization metrics show that the instances are underutilized. A solutions architect needs to implement a solution to permanently reduce the EC2 cost and increase the utilization.

Which solution will meet these requirements with the LEAST number of configuration changes in the future?

A. List instance types that have properties that are similar to the properties that the current instances have. Modify the Auto Scaling group's launch template configuration to use multiple instance types from the list.

B. Use the information about the application's CPU and memory utilization to select an instance type that matches the requirements. Modify the Auto Scaling group's configuration by adding the new instance type. Remove the current instance type from the configuration.

C. Use the information about the application's CPU and memory utilization to specify CPU and memory requirements in a new revision of the Auto Scaling group's launch template. Remove the current instance type from the configuration. `Most Voted`

D. Create a script that selects the appropriate instance types from the AWS Price List Bulk API. Use the selected instance types to create a new revision of the Auto Scaling group's launch template.

Correct Answer: *C*

Community vote distribution
C (62%)   B (34%)   4%

Question #296   Topic 1

A company implements a containerized application by using Amazon Elastic Container Service (Amazon ECS) and Amazon API Gateway The application data is stored in Amazon Aurora databases and Amazon DynamoDB databases. The company automates infrastructure provisioning by using AWS CloudFormation. The company automates application deployment by using AWS CodePipeline.

A solutions architect needs to implement a disaster recovery (DR) strategy that meets an RPO of 2 hours and an RTO of 4 hours.

Which solution will meet these requirements MOST cost-effectively?

A. Set up an Aurora global database and DynamoDB global tables to replicate the databases to a secondary AWS Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon CloudFront with origin failover to route traffic to the secondary Region during a DR scenario.

B. Use AWS Database Migration Service (AWS DMS), Amazon EventBridge, and AWS Lambda to replicate the Aurora databases to a secondary AWS Region. Use DynamoDB Streams, EventBridge. and Lambda to replicate the DynamoDB databases to the secondary Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon Route 53 failover routing to switch traffic from the primary Region to the secondary Region.

C. Use AWS Backup to create backups of the Aurora databases and the DynamoDB databases in a secondary AWS Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon Route 53 failover routing to switch traffic from the primary Region to the secondary Region. Most Voted

D. Set up an Aurora global database and DynamoDB global tables to replicate the databases to a secondary AWS Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon Route 53 failover routing to switch traffic from the primary Region to the secondary Region.

Correct Answer: *C*

Community vote distribution

                    C (58%)   D (37%)   5%

Question #297   Topic 1

A company has a complex web application that leverages Amazon CloudFront for global scalability and performance. Over time, users report that the web application is slowing down.

The company's operations team reports that the CloudFront cache hit ratio has been dropping steadily. The cache metrics report indicates that query strings on some URLs are inconsistently ordered and are specified sometimes in mixed-case letters and sometimes in lowercase letters.

Which set of actions should the solutions architect take to increase the cache hit ratio as quickly as possible?

A. Deploy a Lambda@Edge function to sort parameters by name and force them to be lowercase. Select the CloudFront viewer request trigger to invoke the function. Most Voted

B. Update the CloudFront distribution to disable caching based on query string parameters.

C. Deploy a reverse proxy after the load balancer to post-process the emitted URLs in the application to force the URL strings to be lowercase.

D. Update the CloudFront distribution to specify casing-insensitive query string processing.

Correct Answer: *A*

Community vote distribution

                    A (92%)   8%

Question #298   *Topic 1*

A company runs an ecommerce application in a single AWS Region. The application uses a five-node Amazon Aurora MySQL DB cluster to store information about customers and their recent orders. The DB cluster experiences a large number of write transactions throughout the day.

The company needs to replicate the data in the Aurora database to another Region to meet disaster recovery requirements. The company has an RPO of 1 hour.

Which solution will meet these requirements with the LOWEST cost?

    A. Modify the Aurora database to be an Aurora global database. Create a second Aurora database in another Region.

    B. Enable the Backtrack feature for the Aurora database. Create an AWS Lambda function that runs daily to copy the snapshots of the database to a backup Region.

    C. Use AWS Database Migration Service (AWS DMS). Create a DMS change data capture (CDC) task that replicates the ongoing changes from the Aurora database to an Amazon S3 bucket in another Region. Most Voted

    D. Turn off automated Aurora backups. Configure Aurora backups with a backup frequency of 1 hour. Specify another Region as the destination Region. Select the Aurora database as the resource assignment.

    Correct Answer: *C*

    Community vote distribution
                        C (63%)   A (28%)   9%

Question #299   *Topic 1*

A company's solutions architect is evaluating an AWS workload that was deployed several years ago. The application tier is stateless and runs on a single large Amazon EC2 instance that was launched from an AMI. The application stores data in a MySQL database that runs on a single EC2 instance.

The CPU utilization on the application server EC2 instance often reaches 100% and causes the application to stop responding. The company manually installs patches on the instances. Patching has caused downtime in the past. The company needs to make the application highly available.

Which solution will meet these requirements with the LEAST development me?

    A. Move the application tier to AWS Lambda functions in the existing VPC. Create an Application Load Balancer to distribute traffic across the Lambda functions. Use Amazon GuardDuty to scan the Lambda functions. Migrate the database to Amazon DocumentDB (with MongoDB compatibility).

    B. Change the EC2 instance type to a smaller Graviton powered instance type. Use the existing AMI to create a launch template for an Auto Scaling group. Create an Application Load Balancer to distribute traffic across the instances in the Auto Scaling group. Set the Auto Scaling group to scale based on CPU utilization. Migrate the database to Amazon DynamoDB.

    C. Move the application tier to containers by using Docker. Run the containers on Amazon Elastic Container Service (Amazon ECS) with EC2 instances. Create an Application Load Balancer to distribute traffic across the ECS cluster. Configure the ECS cluster to scale based on CPU utilization. Migrate the database to Amazon Neptune.

    D. Create a now AMI that is configured with AWS Systems Manager Agent (SSM Agent). Use the new AMI to create a launch template for an Auto Scaling group. Use smaller instances in the Auto Scaling group. Create an Application Load Balancer to distribute traffic across the instances in the Auto Scaling group. Set the Auto Scaling group to scale based on CPU utilization. Migrate the database to Amazon Aurora MySQL. Most Voted

    Correct Answer: *D*

    Community vote distribution
                                        D (100%)

Question #300
Topic 1

A company is planning to migrate several applications to AWS. The company does not have a good understanding of its entire application estate. The estate consists of a mixture of physical machines and VMs.

One application that the company will migrate has many dependencies that are sensitive to latency. The company is unsure what all the dependencies are. However the company knows that the low-latency communications use a custom IP-based protocol that runs on port 1000. The company wants to migrate the application and these dependencies together to move all the low-latency interfaces to AWS at the same time.

The company has installed the AWS Application Discovery Agent and has been collecting data for several months.

What should the company do to identify the dependencies that need to be migrated in the same phase as the application?

A. Use AWS Migration Hub and select the servers that host the application. Visualize the network graph to find servers that interact with the application. Turn on data exploration in Amazon Athena. Query the data that is transferred between the servers to identify the servers that communicate on port 1000. Return to Migration Hub. Create a move group that is based on the findings from the Athena queries. Most Voted

B. Use AWS Application Migration Service and select the servers that host the application. Visualize the network graph to find servers that interact with the application. Configure Application Migration Service to launch test instances for all the servers that interact with the application. Perform acceptance tests on the test instances. If no issues are identified, create a move group that is based on the tested servers.

C. Use AWS Migration Hub and select the servers that host the application. Turn on data exploration in Network Access Analyzer. Use the Network Access Analyzer console to select the servers that host the application. Select a Network Access Scope of port 1000 and note the matching servers. Return to Migration Hub. Create a move group that is based on the findings from Network Access Analyzer.

D. Use AWS Migration Hub and select the servers that host the application. Push the Amazon CloudWalch agent to the identified servers by using the AWS Application Discovery Agent. Export the CloudWatch logs that the agents collect to Amazon S3. Use Amazon Athena to query the logs to find servers that communicate on port 1000. Return to Migration Hub Create a move group that is based on the findings from the Athena queries.

Correct Answer: *A*

Community vote distribution

A (92%)   8%

[← Previous Questions]   [Next Questions →]

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

Start Learning for free