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

Custom View Settings

Question #301 *Topic 1*

A company is building an application that will run on an AWS Lambda function. Hundreds of customers will use the application. The company wants to give each customer a quota of requests for a specific time period. The quotas must match customer usage patterns. Some customers must receive a higher quota for a shorter time period.

Which solution will meet these requirements?

A. Create an Amazon API Gateway REST API with a proxy integration to invoke the Lambda function. For each customer, configure an API Gateway usage plan that includes an appropriate request quota. Create an API key from the usage plan for each user that the customer needs.
Most Voted

B. Create an Amazon API Gateway HTTP API with a proxy integration to invoke the Lambda function. For each customer configure an API Gateway usage plan that includes an appropriate request quota Configure route-level throttling for each usage plan. Create an API Key from the usage plan for each user that the customer needs.

C. Create a Lambda function alias for each customer. Include a concurrency limit with an appropriate request quota. Create a Lambda function URL for each function alias. Share the Lambda function URL for each alias with the relevant customer.

D. Create an Application Load Balancer (ALB) in a VPC. Configure the Lambda function as a target for the ALB. Configure an AWS WAF web ACL for the ALB. For each customer configure a rale-based rule that includes an appropriate request quota.

Correct Answer: *A*

Community vote distribution

A (88%) 12%

Question #302 *Topic 1*

A company is planning to migrate its on-premises VMware cluster of 120 VMs to AWS. The VMs have many different operating systems and many custom software packages installed. The company also has an on-premises NFS server that is 10 TB in size. The company has set up a 10 Gbps AWS Direct Connect connection to AWS for the migration.

Which solution will complete the migration to AWS in the LEAST amount of time?

A. Export the on-premises VMs and copy them to an Amazon S3 bucket. Use VM Import/Export to create AMIs from the VM images that are stored in Amazon S3. Order an AWS Snowball Edge device. Copy the NFS server data to the device. Restore the NFS server data to an Amazon EC2 instance that has NFS configured.

B. Configure AWS Application Migration Service with a connection to the VMware cluster. Create a replication job for the VMS. Create an Amazon Elastic File System (Amazon EFS) file system. Configure AWS DataSync to copy the NFS server data to the EFS file system over the Direct Connect connection. Most Voted

C. Recreate the VMs on AWS as Amazon EC2 instances. Install all the required software packages. Create an Amazon FSx for Lustre file system. Configure AWS DataSync to copy the NFS server data to the FSx for Lustre file system over the Direct Connect connection.

D. Order two AWS Snowball Edge devices. Copy the VMs and the NFS server data to the devices. Run VM Import/Export after the data from the devices is loaded to an Amazon S3 bucket. Create an Amazon Elastic File System (Amazon EFS) file system. Copy the NFS server data from Amazon S3 to the EFS file system.

Correct Answer: *B*

Community vote distribution

B (94%) 6%

Question #303 *Topic 1*

An online survey company runs its application in the AWS Cloud. The application is distributed and consists of microservices that run in an automatically scaled Amazon Elastic Container Service (Amazon ECS) cluster. The ECS cluster is a target for an Application Load Balancer (ALB). The ALB is a custom origin for an Amazon CloudFront distribution.

The company has a survey that contains sensitive data. The sensitive data must be encrypted when it moves through the application. The application's data-handling microservice is the only microservice that should be able to decrypt the data

Which solution will meet these requirements?

A. Create a symmetric AWS Key Management Service (AWS KMS) key that is dedicated to the data-handling microservice. Create a field-level encryption profile and a configuration. Associate the KMS key and the configuration with the CloudFront cache behavior.

B. Create an RSA key pair that is dedicated to the data-handing microservice. Upload the public key to the CloudFront distribution. Create a field-level encryption profile and a configuration. Add the configuration to the CloudFront cache behavior. Most Voted

C. Create a symmetric AWS Key Management Service (AWS KMS) key that is dedicated to the data-handling microservice. Create a Lambda@Edge function. Program the function to use the KMS key to encrypt the sensitive data.

D. Create an RSA key pair that is dedicated to the data-handling microservice. Create a Lambda@Edge function. Program the function to use the private key of the RSA key pair to encrypt the sensitive data.

Correct Answer: *B*

Community vote distribution

B (87%) 13%

Question #304 *Topic 1*

A solutions architect is determining the DNS strategy for an existing VPC. The VPC is provisioned to use the 10.24.34.0/24 CIDR block. The VPC also uses Amazon Route 53 Resolver for DNS. New requirements mandate that DNS queries must use private hosted zones. Additionally instances that have public IP addresses must receive corresponding public hostnames

Which solution will meet these requirements to ensure that the domain names are correctly resolved within the VPC?

A. Create a private hosted zone. Activate the enableDnsSupport attribute and the enableDnsHostnames attribute for the VPC. Update the VPC DHCP options set to include domain-name-servers=10.24.34.2.

B. Create a private hosted zone Associate the private hosted zone with the VPC. Activate the enableDnsSupport attribute and the enableDnsHostnames attribute for the VPC. Create a new VPC DHCP options set, and configure domain-name-servers=AmazonProvidedDNS. Associate the new DHCP options set with the VPC. Most Voted

C. Deactivate the enableDnsSupport attribute for the VPActivate the enableDnsHostnames attribute for the VPCreate a new VPC DHCP options set, and configure doman-name-servers=10.24.34.2. Associate the new DHCP options set with the VPC.

D. Create a private hosted zone. Associate the private hosted zone with the VPC. Activate the enableDnsSupport attribute for the VPC. Deactivate the enableDnsHostnames attribute for the VPC. Update the VPC DHCP options set to include domain-name-servers=AmazonProvidedDNS.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #305 *Topic 1*

A data analytics company has an Amazon Redshift cluster that consists of several reserved nodes. The cluster is experiencing unexpected bursts of usage because a team of employees is compiling a deep audit analysis report. The queries to generate the report are complex read queries and are CPU intensive.

Business requirements dictate that the cluster must be able to service read and write queries at all times. A solutions architect must devise a solution that accommodates the bursts of usage.

Which solution meets these requirements MOST cost-effectively?

A. Provision an Amazon EMR cluster Offload the complex data processing tasks.

B. Deploy an AWS Lambda function to add capacity to the Amazon Redshift cluster by using a classic resize operation when the cluster's CPU metrics in Amazon CloudWatch reach 80%.

C. Deploy an AWS Lambda function to add capacity to the Amazon Redshift cluster by using an elastic resize operation when the cluster's CPU metrics in Amazon CloudWatch reach 80%.

D. Turn on the Concurrency Scaling feature for the Amazon Redshift cluster. Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #306 *Topic 1*

A research center is migrating to the AWS Cloud and has moved its on-premises 1 PB object storage to an Amazon S3 bucket. One hundred scientists are using this object storage to store their work-related documents. Each scientist has a personal folder on the object store. All the scientists are members of a single IAM user group.

The research center's compliance officer is worried that scientists will be able to access each other's work. The research center has a strict obligation to report on which scientist accesses which documents. The team that is responsible for these reports has little AWS experience and wants a ready-to-use solution that minimizes operational overhead.

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

A. Create an identity policy that grants the user read and write access. Add a condition that specifies that the S3 paths must be prefixed with $(aws:username). Apply the policy on the scientists' IAM user group. Most Voted

B. Configure a trail with AWS CloudTrail to capture all object-level events in the S3 bucket. Store the trail output in another S3 bucket. Use Amazon Athena to query the logs and generate reports. Most Voted

C. Enable S3 server access logging. Configure another S3 bucket as the target for log delivery. Use Amazon Athena to query the logs and generate reports.

D. Create an S3 bucket policy that grants read and write access to users in the scientists' IAM user group.

E. Configure a trail with AWS CloudTrail to capture all object-level events in the S3 bucket and write the events to Amazon CloudWatch. Use the Amazon Athena CloudWatch connector to query the logs and generate reports.

Correct Answer: *AB*

Community vote distribution

AB (76%) 14% 10%

Question #307 *Topic 1*

A company uses AWS Organizations to manage a multi-account structure. The company has hundreds of AWS accounts and expects the number of accounts to increase. The company is building a new application that uses Docker images. The company will push the Docker images to Amazon Elastic Container Registry (Amazon ECR). Only accounts that are within the company's organization should have access to the images.

The company has a CI/CD process that runs frequently. The company wants to retain all the tagged images. However, the company wants to retain only the five most recent untagged images.

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

A. Create a private repository in Amazon ECR. Create a permissions policy for the repository that allows only required ECR operations. Include a condition to allow the ECR operations if the value of the aws:PrincipalOrgID condition key is equal to the ID of the company's organization. Add a lifecycle rule to the ECR repository that deletes all untagged images over the count of five Most Voted

B. Create a public repository in Amazon ECR. Create an IAM role in the ECR account. Set permissions so that any account can assume the role if the value of the aws:PrincipalOrgID condition key is equal to the ID of the company's organization. Add a lifecycle rule to the ECR repository that deletes all untagged images over the count of five.

C. Create a private repository in Amazon ECR. Create a permissions policy for the repository that includes only required ECR operations. Include a condition to allow the ECR operations for all account IDs in the organization Schedule a daily Amazon EventBridge rule to invoke an AWS Lambda function that deletes all untagged images over the count of five.

D. Create a public repository in Amazon ECR. Configure Amazon ECR to use an interface VPC endpoint with an endpoint policy that includes the required permissions for images that the company needs to pull. Include a condition to allow the ECR operations for all account IDs in the company's organization. Schedule a daily Amazon EventBridge rule to invoke an AWS Lambda function that deletes all untagged images over the count of five.

Correct Answer: *A*

Community vote distribution

A (100%)

Question #308 *Topic 1*

A solutions architect is reviewing a company's process for taking snapshots of Amazon RDS DB instances. The company takes automatic snapshots every day and retains the snapshots for 7 days.

The solutions architect needs to recommend a solution that takes snapshots every 6 hours and retains the snapshots for 30 days. The company uses AWS Organizations to manage all of its AWS accounts. The company needs a consolidated view of the health of the RDS snapshots.

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

A. Turn on the cross-account management feature in AWS Backup. Create a backup plan that specifies the frequency and retention requirements. Add a tag to the DB instances. Apply the backup plan by using tags. Use AWS Backup to monitor the status of the backups. Most Voted

B. Turn on the cross-account management feature in Amazon RDS. Create a snapshot global policy that specifies the frequency and retention requirements. Use the RDS console in the management account to monitor the status of the backups.

C. Turn on the cross-account management feature in AWS CloudFormation. From the management account, deploy a CloudFormation stack set that contains a backup plan from AWS Backup that specifies the frequency and retention requirements. Create an AWS Lambda function in the management account to monitor the status of the backups. Create an Amazon EventBridge rule in each account to run the Lambda function on a schedule.

D. Configure AWS Backup in each account. Create an Amazon Data Lifecycle Manager lifecycle policy that specifies the frequency and retention requirements. Specify the DB instances as the target resource Use the Amazon Data Lifecycle Manager console in each member account to monitor the status of the backups.

Correct Answer: *A*

Community vote distribution

A (100%)

Question #309 *Topic 1*

A company is using AWS Organizations with a multi-account architecture. The company's current security configuration for the account architecture includes SCPs, resource-based policies, identity-based policies, trust policies, and session policies.

A solutions architect needs to allow an IAM user in Account A to assume a role in Account B.

Which combination of steps must the solutions architect take to meet this requirement? (Choose three.)

A. Configure the SCP for Account A to allow the action. Most Voted

B. Configure the resource-based policies to allow the action.

C. Configure the identity-based policy on the user in Account A to allow the action. Most Voted

D. Configure the identity-based policy on the user in Account B to allow the action.

E. Configure the trust policy on the target role in Account B to allow the action. Most Voted

F. Configure the session policy to allow the action and to be passed programmatically by the GetSessionToken API operation.

Correct Answer: *ACE*

Community vote distribution

ACE (57%) BCE (26%) Other

Question #310 *Topic 1*

A company wants to use Amazon S3 to back up its on-premises file storage solution. The company's on-premises file storage solution supports NFS, and the company wants its new solution to support NFS. The company wants to archive the backup files after 5 days. If the company needs archived files for disaster recovery, the company is willing to wait a few days for the retrieval of those files.

Which solution meets these requirements MOST cost-effectively?

A. Deploy an AWS Storage Gateway file gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the file gateway. Create an S3 Lifecycle rule to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) after 5 days.

B. Deploy an AWS Storage Gateway volume gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the volume gateway. Create an S3 Lifecycle rule to move the files to S3 Glacier Deep Archive after 5 days.

C. Deploy an AWS Storage Gateway tape gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the tape gateway. Create an S3 Lifecycle rule to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) after 5 days.

D. Deploy an AWS Storage Gateway file gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the file gateway. Create an S3 Lifecycle rule to move the files to S3 Glacier Deep Archive after 5 days. Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #311 *Topic 1*

A company runs its application on Amazon EC2 instances and AWS Lambda functions. The EC2 instances experience a continuous and stable load. The Lambda functions experience a varied and unpredictable load. The application includes a caching layer that uses an Amazon MemoryDB for Redis cluster.

A solutions architect must recommend a solution to minimize the company's overall monthly costs.

Which solution will meet these requirements?

A. Purchase an EC2 instance Savings Plan to cover the EC2 instances. Purchase a Compute Savings Plan for Lambda to cover the minimum expected consumption of the Lambda functions. Purchase reserved nodes to cover the MemoryDB cache nodes. Most Voted

B. Purchase a Compute Savings Plan to cover the EC2 instances. Purchase Lambda reserved concurrency to cover the expected Lambda usage. Purchase reserved nodes to cover the MemoryDB cache nodes.

C. Purchase a Compute Savings Plan to cover the entire expected cost of the EC2 instances, Lambda functions, and MemoryDB cache nodes.

D. Purchase a Compute Savings Plan to cover the EC2 instances and the MemoryDB cache nodes. Purchase Lambda reserved concurrency to cover the expected Lambda usage.

Correct Answer: *A*

Community vote distribution

A (88%) 12%

Question #312 *Topic 1*

A company is launching a new online game on Amazon EC2 instances. The game must be available globally. The company plans to run the game in three AWS Regions us-east-1, eu-west-1, and ap-southeast-1. The game's leaderboards, player inventory and event status must be available across Regions.

A solutions architect must design a solution that will give any Region the ability to scale to handle the load of all Regions. Additionally, users must automatically connect to the Region that provides the least latency.

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

A. Create an EC2 Spot Fleet. Attach the Spot Fleet to a Network Load Balancer (NLB) in each Region. Create an AWS Global Accelerator IP address that points to the NLB. Create an Amazon Route 53 latency-based routing entry for the Global Accelerator IP address. Save the game metadata to an Amazon RDS for MySQL DB instance in each Region. Set up a read replica in the other Regions.

B. Create an Auto Scaling group for the EC2 instances Attach the Auto Scaling group to a Network Load Balancer (NLB) in each Region. For each Region, create an Amazon Route 53 entry that uses geoproximity routing and points to the NLB in that Region. Save the game metadata to MySQL databases on EC2 instances in each Region. Set up replication between the database EC2 instances in each Region.

C. Create an Auto Scaling group for the EC2 instances. Attach the Auto Scaling group to a Network Load Balancer (NLB) in each Region. For each Region, create an Amazon Route 53 entry that uses latency-based routing and points to the NLB in that Region. Save the game metadata to an Amazon DynamoDB global table. Most Voted

D. Use EC2 Global View. Deploy the EC2 instances to each Region. Attach the instances to a Network Load Balancer (NLB). Deploy a DNS server on an EC2 instance in each Region. Set up custom logic on each DNS server to redirect the user to the Region that provides the lowest latency. Save the game metadata to an Amazon Aurora global database.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #313 *Topic 1*

A company is deploying a third-party firewall appliance solution from AWS Marketplace to monitor and protect traffic that leaves the company's AWS environments. The company wants to deploy this appliance into a shared services VPC and route all outbound internet-bound traffic through the appliances.

A solutions architect needs to recommend a deployment method that prioritizes reliability and minimizes failover time between firewall appliances within a single AWS Region. The company has set up routing from the shared services VPC to other VPCs.

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

A. Deploy two firewall appliances into the shared services VPC, each in a separate Availability Zone. Most Voted

B. Create a new Network Load Balancer in the shared services VPC. Create a new target group, and attach it to the new Network Load Balancer. Add each of the firewall appliance instances to the target group.

C. Create a new Gateway Load Balancer in the shared services VPCreate a new target group, and attach it to the new Gateway Load Balancer Add each of the firewall appliance instances to the target group. Most Voted

D. Create a VPC interface endpoint. Add a route to the route table in the shared services VPC. Designate the new endpoint as the next hop for traffic that enters the shared services VPC from other VPCs.

E. Deploy two firewall appliances into the shared services VPC, each in the same Availability Zone.

F. Create a VPC Gateway Load Balancer endpoint. Add a route to the route table in the shared services VPC. Designate the new endpoint as the next hop for traffic that enters the shared services VPC from other VPCs. Most Voted

Correct Answer: *ACF*

Community vote distribution

ACF (90%) 7%

Question #314 *Topic 1*

A solutions architect needs to migrate an on-premises legacy application to AWS. The application runs on two servers behind a load balancer. The application requires a license file that is associated with the MAC address of the server's network adapter It takes the software vendor 12 hours to send new license files. The application also uses configuration files with a static IP address to access a database server, host names are not supported.

Given these requirements, which combination of steps should be taken to implement highly available architecture for the application servers in AWS? (Choose two.)

A. Create a pool of ENIs. Request license files from the vendor for the pool, and store the license files in Amazon S3. Create a bootstrap automation script to download a license file and attach the corresponding ENI to an Amazon EC2 instance. Most Voted

B. Create a pool of ENIs. Request license files from the vendor for the pool, store the license files on an Amazon EC2 instance. Create an AMI from the instance and use this AMI for all future EC2 instances.

C. Create a bootstrap automation script to request a new license file from the vendor .When the response is received, apply the license file to an Amazon EC2 instance.

D. Edit the bootstrap automation script to read the database server IP address from the AWS Systems Manager Parameter Store, and inject the value into the local configuration files. Most Voted

E. Edit an Amazon EC2 instance to include the database server IP address in the configuration files and re-create the AMI to use for all future EC2 stances.

Correct Answer: *AD*

Community vote distribution

AD (100%)

Question #315 *Topic 1*

A company runs its sales reporting application in an AWS Region in the United States. The application uses an Amazon API Gateway Regional API and AWS Lambda functions to generate on-demand reports from data in an Amazon RDS for MySQL database. The frontend of the application is hosted on Amazon S3 and is accessed by users through an Amazon CloudFront distribution. The company is using Amazon Route 53 as the DNS service for the domain. Route 53 is configured with a simple routing policy to route traffic to the API Gateway API.

In the next 6 months, the company plans to expand operations to Europe. More than 90% of the database traffic is read-only traffic. The company has already deployed an API Gateway API and Lambda functions in the new Region.

A solutions architect must design a solution that minimizes latency for users who download reports.

Which solution will meet these requirements?

A. Use an AWS Database Migration Service (AWS DMS) task with full load to replicate the primary database in the original Region to the database in the new Region. Change the Route 53 record to latency-based routing to connect to the API Gateway API.

B. Use an AWS Database Migration Service (AWS DMS) task with full load plus change data capture (CDC) to replicate the primary database in the original Region to the database in the new Region. Change the Route 53 record to geolocation routing to connect to the API Gateway API.

C. Configure a cross-Region read replica for the RDS database in the new Region Change the Route 53 record to latency-based routing to connect to the API Gateway API. Most Voted

D. Configure a cross-Region read replica for the RDS database in the new Region. Change the Route 53 record to geolocation routing to connect to the API Gateway API.

Correct Answer: *C*

Community vote distribution

C (96%) 4%

Question #316 *Topic 1*

A software company needs to create short-lived test environments to test pull requests as part of its development process. Each test environment consists of a single Amazon EC2 instance that is in an Auto Scaling group.

The test environments must be able to communicate with a central server to report test results. The central server is located in an on-premises data center. A solutions architect must implement a solution so that the company can create and delete test environments without any manual intervention. The company has created a transit gateway with a VPN attachment to the on-premises network.

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

A. Create an AWS CloudFormation template that contains a transit gateway attachment and related routing configurations. Create a CloudFormation stack set that includes this template. Use CloudFormation StackSets to deploy a new stack for each VPC in the account. Deploy a new VPC for each test environment.

B. Create a single VPC for the test environments. Include a transit gateway attachment and related routing configurations. Use AWS CloudFormation to deploy all test environments into the VPC. Most Voted

C. Create a new OU in AWS Organizations for testing. Create an AWS CioudFormation template that contains a VPC, necessary networking resources, a transit gateway attachment, and related routing configurations. Create a CloudFormation stack set that includes this template. Use CloudFormation StackSets for deployments into each account under the testing OU. Create a new account for each test environment.

D. Convert the test environment EC2 instances into Docker images. Use AWS CloudFormation to configure an Amazon Elastic Kubernetes Service (Amazon EKS) cluster in a new VPC, create a transit gateway attachment, and create related routing configurations. Use Kubernetes to manage the deployment and lifecycle of the test environments.

Correct Answer: *B*

Community vote distribution

B (85%) A (15%)

Question #317 *Topic 1*

A company is deploying a new API to AWS. The API uses Amazon API Gateway with a Regional API endpoint and an AWS Lambda function for hosting. The API retrieves data from an external vendor API, stores data in an Amazon DynamoDB global table, and retrieves data from the DynamoDB global table The API key for the vendor's API is stored in AWS Secrets Manager and is encrypted with a customer managed key in AWS Key Management Service (AWS KMS). The company has deployed its own API into a single AWS Region.

A solutions architect needs to change the API components of the company's API to ensure that the components can run across multiple Regions in an active-active configuration.

Which combination of changes will meet this requirement with the LEAST operational overhead? (Choose three.)

A. Deploy the API to multiple Regions. Configure Amazon Route 53 with custom domain names that route traffic to each Regional API endpoint. Implement a Route 53 multivalue answer routing policy. Most Voted

B. Create a new KMS multi-Region customer managed key. Create a new KMS customer managed replica key in each in-scope Region. Most Voted

C. Replicate the existing Secrets Manager secret to other Regions. For each in-scope Region's replicated secret, select the appropriate KMS key. Most Voted

D. Create a new AWS managed KMS key in each in-scope Region. Convert an existing key to a multiRegion key. Use the multi-Region key in other Regions.

E. Create a new Secrets Manager secret in each in-scope Region. Copy the secret value from the existing Region to the new secret in each in-scope Region.

F. Modify the deployment process for the Lambda function to repeat the deployment across in-scope Regions. Turn on the multi-Region option for the existing API. Select the Lambda function that is deployed in each Region as the backend for the multi-Region API.

Correct Answer: *ABC*

Community vote distribution

ABC (76%) BCF (24%)

Question #318 *Topic 1*

An online retail company hosts its stateful web-based application and MySQL database in an on-premises data center on a single server. The company wants to increase its customer base by conducting more marketing campaigns and promotions. In preparation, the company wants to migrate its application and database to AWS to increase the reliability of its architecture.

Which solution should provide the HIGHEST level of reliability?

A. Migrate the database to an Amazon RDS MySQL Multi-AZ DB instance. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in Amazon Neptune

B. Migrate the database to Amazon Aurora MySQL. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in an Amazon ElastiCache for Redis replication group. Most Voted

C. Migrate the database to Amazon DocumentDB (with MongoDB compatibility). Deploy the application in an Auto Scaling group on Amazon EC2 instances behind a Network Load Balancer Store sessions in Amazon Kinesis Data Firehose.

D. Migrate the database to an Amazon RDS MariaDB Multi-AZ DB instance. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in Amazon ElastiCache for Memcached.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #319 *Topic 1*

A company's solutions architect needs to provide secure Remote Desktop connectivity to users for Amazon EC2 Windows instances that are hosted in a VPC. The solution must integrate centralized user management with the company's on-premises Active Directory. Connectivity to the VPC is through the internet. The company has hardware that can be used to establish an AWS Site-to-Site VPN connection.

Which solution will meet these requirements MOST cost-effectively?

A. Deploy a managed Active Directory by using AWS Directory Service for Microsoft Active Directory. Establish a trust with the on-premises Active Directory. Deploy an EC2 instance as a bastion host in the VPC. Ensure that the EC2 instance is joined to the domain. Use the bastion host to access the target instances through RDP.

B. Configure AWS IAM Identity Center (AWS Single Sign-On) to integrate with the on-premises Active Directory by using the AWS Directory Service for Microsoft Active Directory AD Connector. Configure permission sets against user groups for access to AWS Systems Manager. Use Systems Manager Fleet Manager to access the target instances through RDP. Most Voted

C. Implement a VPN between the on-premises environment and the target VPEnsure that the target instances are joined to the on-premises Active Directory domain over the VPN connection. Configure RDP access through the VPN. Connect from the company's network to the target instances.

D. Deploy a managed Active Directory by using AWS Directory Service for Microsoft Active Directory. Establish a trust with the on-premises Active Directory. Deploy a Remote Desktop Gateway on AWS by using an AWS Quick Start. Ensure that the Remote Desktop Gateway is joined to the domain. Use the Remote Desktop Gateway to access the target instances through RDP.

Correct Answer: *B*

Community vote distribution

B (51%) C (46%)

Question #320 *Topic 1*

A company's compliance audit reveals that some Amazon Elastic Block Store (Amazon EBS) volumes that were created in an AWS account were not encrypted. A solutions architect must implement a solution to encrypt all new EBS volumes at rest.

Which solution will meet this requirement with the LEAST effort?

A. Create an Amazon EventBridge rule to detect the creation of unencrypted EBS volumes. Invoke an AWS Lambda function to delete noncompliant volumes.

B. Use AWS Audit Manager with data encryption.

C. Create an AWS Config rule to detect the creation of a new EBS volume. Encrypt the volume by using AWS Systems Manager Automation.

D. Turn on EBS encryption by default in all AWS Regions. Most Voted

Correct Answer: *D*

Community vote distribution

D (79%) C (21%)

Question #321 *Topic 1*

A research company is running daily simulations in the AWS Cloud to meet high demand. The simulations run on several hundred Amazon EC2 instances that are based on Amazon Linux 2. Occasionally, a simulation gets stuck and requires a cloud operations engineer to solve the problem by connecting to an EC2 instance through SSH.

Company policy states that no EC2 instance can use the same SSH key and that all connections must be logged in AWS CloudTrail.

How can a solutions architect meet these requirements?

A. Launch new EC2 instances, and generate an individual SSH key for each instance. Store the SSH key in AWS Secrets Manager. Create a new IAM policy, and attach it to the engineers' IAM role with an Allow statement for the GetSecretValue action. Instruct the engineers to fetch the SSH key from Secrets Manager when they connect through any SSH client.

B. Create an AWS Systems Manager document to run commands on EC2 instances to set a new unique SSH key. Create a new IAM policy, and attach it to the engineers' IAM role with an Allow statement to run Systems Manager documents. Instruct the engineers to run the document to set an SSH key and to connect through any SSH client.

C. Launch new EC2 instances without setting up any SSH key for the instances. Set up EC2 Instance Connect on each instance. Create a new IAM policy, and attach it to the engineers' IAM role with an Allow statement for the SendSSHPublicKey action. Instruct the engineers to connect to the instance by using a browser-based SSH client from the EC2 console. Most Voted

D. Set up AWS Secrets Manager to store the EC2 SSH key. Create a new AWS Lambda function to create a new SSH key and to call AWS Systems Manager Session Manager to set the SSH key on the EC2 instance. Configure Secrets Manager to use the Lambda function for automatic rotation once daily. Instruct the engineers to fetch the SSH key from Secrets Manager when they connect through any SSH client.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #322 *Topic 1*

A company is migrating mobile banking applications to run on Amazon EC2 instances in a VPC. Backend service applications run in an on-premises data center. The data center has an AWS Direct Connect connection into AWS. The applications that run in the VPC need to resolve DNS requests to an on-premises Active Directory domain that runs in the data center.

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

A. Provision a set of EC2 instances across two Availability Zones in the VPC as caching DNS servers to resolve DNS queries from the application servers within the VPC.

B. Provision an Amazon Route 53 private hosted zone. Configure NS records that point to on-premises DNS servers.

C. Create DNS endpoints by using Amazon Route 53 Resolver. Add conditional forwarding rules to resolve DNS namespaces between the on-premises data center and the VPC. Most Voted

D. Provision a new Active Directory domain controller in the VPC with a bidirectional trust between this new domain and the on-premises Active Directory domain.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #323 *Topic 1*

A company processes environmental data. The company has set up sensors to provide a continuous stream of data from different areas in a city. The data is available in JSON format.

The company wants to use an AWS solution to send the data to a database that does not require fixed schemas for storage. The data must be sent in real time.

Which solution will meet these requirements?

A. Use Amazon Kinesis Data Firehose to send the data to Amazon Redshift.

B. Use Amazon Kinesis Data Streams to send the data to Amazon DynamoDB. Most Voted

C. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to send the data to Amazon Aurora.

D. Use Amazon Kinesis Data Firehose to send the data to Amazon Keyspaces (for Apache Cassandra).

Correct Answer: *B*

Community vote distribution

B (94%) 6%

Question #324 *Topic 1*

A company is migrating a legacy application from an on-premises data center to AWS. The application uses MongoDB as a key-value database. According to the company's technical guidelines, all Amazon EC2 instances must be hosted in a private subnet without an internet connection. In addition, all connectivity between applications and databases must be encrypted. The database must be able to scale based on demand.

Which solution will meet these requirements?

A. Create new Amazon DocumentDB (with MongoDB compatibility) tables for the application with Provisioned IOPS volumes. Use the instance endpoint to connect to Amazon DocumentDB.

B. Create new Amazon DynamoDB tables for the application with on-demand capacity. Use a gateway VPC endpoint for DynamoDB to connect to the DynamoDB tables. Most Voted

C. Create new Amazon DynamoDB tables for the application with on-demand capacity. Use an interface VPC endpoint for DynamoDB to connect to the DynamoDB tables.

D. Create new Amazon DocumentDB (with MongoDB compatibility) tables for the application with Provisioned IOPS volumes. Use the cluster endpoint to connect to Amazon DocumentDB.

Correct Answer: *B*

Community vote distribution

B (53%) D (40%) 7%

Question #325 *Topic 1*

A company is running an application on Amazon EC2 instances in the AWS Cloud. The application is using a MongoDB database with a replica set as its data tier. The MongoDB database is installed on systems in the company's on-premises data center and is accessible through an AWS Direct Connect connection to the data center environment.

A solutions architect must migrate the on-premises MongoDB database to Amazon DocumentDB (with MongoDB compatibility).

Which strategy should the solutions architect choose to perform this migration?

A. Create a fleet of EC2 instances. Install MongoDB Community Edition on the EC2 instances, and create a database. Configure continuous synchronous replication with the database that is running in the on-premises data center.

B. Create an AWS Database Migration Service (AWS DMS) replication instance. Create a source endpoint for the on-premises MongoDB database by using change data capture (CDC). Create a target endpoint for the Amazon DocumentDB database. Create and run a DMS migration task. Most Voted

C. Create a data migration pipeline by using AWS Data Pipeline. Define data nodes for the on-premises MongoDB database and the Amazon DocumentDB database. Create a scheduled task to run the data pipeline.

D. Create a source endpoint for the on-premises MongoDB database by using AWS Glue crawlers. Configure continuous asynchronous replication between the MongoDB database and the Amazon DocumentDB database.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #326 *Topic 1*

A company is rearchitecting its applications to run on AWS. The company's infrastructure includes multiple Amazon EC2 instances. The company's development team needs different levels of access. The company wants to implement a policy that requires all Windows EC2 instances to be joined to an Active Directory domain on AWS. The company also wants to implement enhanced security processes such as multi-factor authentication (MFA). The company wants to use managed AWS services wherever possible.

Which solution will meet these requirements?

A. Create an AWS Directory Service for Microsoft Active Directory implementation. Launch an Amazon Workspace. Connect to and use the Workspace for domain security configuration tasks.

B. Create an AWS Directory Service for Microsoft Active Directory implementation. Launch an EC2 instance. Connect to and use the EC2 instance for domain security configuration tasks. Most Voted

C. Create an AWS Directory Service Simple AD implementation. Launch an EC2 instance. Connect to and use the EC2 instance for domain security configuration tasks.

D. Create an AWS Directory Service Simple AD implementation. Launch an Amazon Workspace. Connect to and use the Workspace for domain security configuration tasks.

Correct Answer: *B*

Community vote distribution

B (55%) A (45%)

Question #327 *Topic 1*

A company wants to migrate its on-premises application to AWS. The database for the application stores structured product data and temporary user session data. The company needs to decouple the product data from the user session data. The company also needs to implement replication in another AWS Region for disaster recovery.

Which solution will meet these requirements with the HIGHEST performance?

A. Create an Amazon RDS DB instance with separate schemas to host the product data and the user session data. Configure a read replica for the DB instance in another Region.

B. Create an Amazon RDS DB instance to host the product data. Configure a read replica for the DB instance in another Region. Create a global datastore in Amazon ElastiCache for Memcached to host the user session data.

C. Create two Amazon DynamoDB global tables. Use one global table to host the product data. Use the other global table to host the user session data. Use DynamoDB Accelerator (DAX) for caching.

D. Create an Amazon RDS DB instance to host the product data. Configure a read replica for the DB instance in another Region. Create an Amazon DynamoDB global table to host the user session data. Most Voted

Correct Answer: *D*

Community vote distribution

D (50%) C (35%) B (15%)

Question #328 *Topic 1*

A company orchestrates a multi-account structure on AWS by using AWS Control Tower. The company is using AWS Organizations, AWS Config, and AWS Trusted Advisor. The company has a specific OU for development accounts that developers use to experiment on AWS. The company has hundreds of developers, and each developer has an individual development account.

The company wants to optimize costs in these development accounts. Amazon EC2 instances and Amazon RDS instances in these accounts must be burstable. The company wants to disallow the use of other services that are not relevant.

What should a solutions architect recommend to meet these requirements?

A. Create a custom SCP in AWS Organizations to allow the deployment of only burstable instances and to disallow services that are not relevant. Apply the SCP to the development OU.

B. Create a custom detective control (guardrail) in AWS Control Tower. Configure the control (guardrail) to allow the deployment of only burstable instances and to disallow services that are not relevant. Apply the control (guardrail) to the development OU.

C. Create a custom preventive control (guardrail) in AWS Control Tower. Configure the control (guardrail) to allow the deployment of only burstable instances and to disallow services that are not relevant. Apply the control (guardrail) to the development OU. Most Voted

D. Create an AWS Config rule in the AWS Control Tower account. Configure the AWS Config rule to allow the deployment of only burstable instances and to disallow services that are not relevant. Deploy the AWS Config rule to the development OU by using AWS CloudFormation StackSets.

Correct Answer: *C*

Community vote distribution

C (61%) A (39%)

Question #329 *Topic 1*

A financial services company runs a complex, multi-tier application on Amazon EC2 instances and AWS Lambda functions. The application stores temporary data in Amazon S3. The S3 objects are valid for only 45 minutes and are deleted after 24 hours.

The company deploys each version of the application by launching an AWS CloudFormation stack. The stack creates all resources that are required to run the application. When the company deploys and validates a new application version, the company deletes the CloudFormation stack of the old version.

The company recently tried to delete the CloudFormation stack of an old application version, but the operation failed. An analysis shows that CloudFormation failed to delete an existing S3 bucket. A solutions architect needs to resolve this issue without making major changes to the application's architecture.

Which solution meets these requirements?

A. Implement a Lambda function that deletes all files from a given S3 bucket. Integrate this Lambda function as a custom resource into the CloudFormation stack. Ensure that the custom resource has a DependsOn attribute that points to the S3 bucket's resource. Most Voted

B. Modify the CloudFormation template to provision an Amazon Elastic File System (Amazon EFS) file system to store the temporary files there instead of in Amazon S3. Configure the Lambda functions to run in the same VPC as the file system. Mount the file system to the EC2 instances and Lambda functions.

C. Modify the CloudF ormation stack to create an S3 Lifecycle rule that expires all objects 45 minutes after creation. Add a DependsOn attribute that points to the S3 bucket's resource.

D. Modify the CloudFormation stack to attach a DeletionPolicy attribute with a value of Delete to the S3 bucket.

Correct Answer: *A*

Community vote distribution

A (94%) 6%

Question #330 *Topic 1*

A company has developed a mobile game. The backend for the game runs on several virtual machines located in an on-premises data center. The business logic is exposed using a REST API with multiple functions. Player session data is stored in central file storage. Backend services use different API keys for throttling and to distinguish between live and test traffic.

The load on the game backend varies throughout the day. During peak hours, the server capacity is not sufficient. There are also latency issues when fetching player session data. Management has asked a solutions architect to present a cloud architecture that can handle the game's varying load and provide low-latency data access. The API model should not be changed.

Which solution meets these requirements?

A. Implement the REST API using a Network Load Balancer (NLB). Run the business logic on an Amazon EC2 instance behind the NLB. Store player session data in Amazon Aurora Serverless.

B. Implement the REST API using an Application Load Balancer (ALB). Run the business logic in AWS Lambda. Store player session data in Amazon DynamoDB with on-demand capacity.

C. Implement the REST API using Amazon API Gateway. Run the business logic in AWS Lambda. Store player session data in Amazon DynamoDB with on-demand capacity. Most Voted

D. Implement the REST API using AWS AppSync. Run the business logic in AWS Lambda. Store player session data in Amazon Aurora Serverless.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #331 *Topic 1*

A company is migrating an application to the AWS Cloud. The application runs in an on-premises data center and writes thousands of images into a mounted NFS file system each night. After the company migrates the application, the company will host the application on an Amazon EC2 instance with a mounted Amazon Elastic File System (Amazon EFS) file system.

The company has established an AWS Direct Connect connection to AWS. Before the migration cutover, a solutions architect must build a process that will replicate the newly created on-premises images to the EFS file system.

What is the MOST operationally efficient way to replicate the images?

A. Configure a periodic process to run the aws s3 sync command from the on-premises file system to Amazon S3. Configure an AWS Lambda function to process event notifications from Amazon S3 and copy the images from Amazon S3 to the EFS file system.

B. Deploy an AWS Storage Gateway file gateway with an NFS mount point. Mount the file gateway file system on the on-premises server. Configure a process to periodically copy the images to the mount point.

C. Deploy an AWS DataSync agent to an on-premises server that has access to the NFS file system. Send data over the Direct Connect connection to an S3 bucket by using a public VIF. Configure an AWS Lambda function to process event notifications from Amazon S3 and copy the images from Amazon S3 to the EFS file system.

D. Deploy an AWS DataSync agent to an on-premises server that has access to the NFS file system. Send data over the Direct Connect connection to an AWS PrivateLink interface VPC endpoint for Amazon EFS by using a private VIF. Configure a DataSync scheduled task to send the images to the EFS file system every 24 hours. Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #332 *Topic 1*

A company recently migrated a web application from an on-premises data center to the AWS Cloud. The web application infrastructure consists of an Amazon CloudFront distribution that routes to an Application Load Balancer (ALB), with Amazon Elastic Container Service (Amazon ECS) to process requests. A recent security audit revealed that the web application is accessible by using both CloudFront and ALB endpoints. However, the company requires that the web application must be accessible only by using the CloudFront endpoint.

Which solution will meet this requirement with the LEAST amount of effort?

A. Create a new security group and attach it to the CloudFront distribution. Update the ALB security group ingress to allow access only from the CloudFront security group.

B. Update ALB security group ingress to allow access only from the com.amazonaws.global.cloudfront.origin-facing CloudFront managed prefix list. Most Voted

C. Create a com.amazonaws.region.elasticloadbalancing VPC interface endpoint for Elastic Load Balancing. Update the ALB scheme from internet-facing to internal.

D. Extract CloudFront IPs from the AWS provided ip-ranges.json document. Update ALB security group ingress to allow access only from CloudFront IPs.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #333 *Topic 1*

A company hosts a community forum site using an Application Load Balancer (ALB) and a Docker application hosted in an Amazon ECS cluster. The site data is stored in Amazon RDS for MySQL and the container image is stored in ECR. The company needs to provide their customers with a disaster recovery SLA with an RTO of no more than 24 hours and RPO of no more than 8 hours.

Which of the following solutions is the MOST cost-effective way to meet the requirements?

A. Use AWS CloudFormation to deploy identical ALB, EC2, ECS and RDS resources in two regions. Schedule RDS snapshots every 8 hours. Use RDS multi-region replication to update the secondary region's copy of the database. In the event of a failure, restore from the latest snapshot, and use an Amazon Route 53 DNS failover policy to automatically redirect customers to the ALB in the secondary region.

B. Store the Docker image in ECR in two regions. Schedule RDS snapshots every 8 hours with snapshots copied to the secondary region. In the event of a failure, use AWS CloudFormation to deploy the ALB, EC2, ECS and RDS resources in the secondary region, restore from the latest snapshot, and update the DNS record to point to the ALB in the secondary region. Most Voted

C. Use AWS CloudFormation to deploy identical ALB, EC2, ECS, and RDS resources in a secondary region. Schedule hourly RDS MySQL backups to Amazon S3 and use cross-region replication to replicate data to a bucket in the secondary region. In the event of a failure, import the latest Docker image to Amazon ECR in the secondary region, deploy to the EC2 instance, restore the latest MySQL backup, and update the DNS record to point to the ALB in the secondary region.

D. Deploy a pilot light environment in a secondary region with an ALB and a minimal resource EC2 deployment for Docker in an AWS Auto Scaling group with a scaling policy to increase instance size and number of nodes. Create a cross-region read replica of the RDS data. In the event of a failure, promote the replica to primary, and update the DNS record to point to the ALB in the secondary region.

Correct Answer: *B*

Community vote distribution

B (92%) 8%

Question #334 *Topic 1*

A company is migrating its infrastructure to the AWS Cloud. The company must comply with a variety of regulatory standards for different projects. The company needs a multi-account environment.

A solutions architect needs to prepare the baseline infrastructure. The solution must provide a consistent baseline of management and security, but it must allow flexibility for different compliance requirements within various AWS accounts. The solution also needs to integrate with the existing on-premises Active Directory Federation Services (AD FS) server.

Which solution meets these requirements with the LEAST amount of operational overhead?

A. Create an organization in AWS Organizations. Create a single SCP for least privilege access across all accounts. Create a single OU for all accounts. Configure an IAM identity provider for federation with the on-premises AD FS server. Configure a central logging account with a defined process for log generating services to send log events to the central account. Enable AWS Config in the central account with conformance packs for all accounts.

B. Create an organization in AWS Organizations. Enable AWS Control Tower on the organization. Review included controls (guardrails) for SCPs. Check AWS Config for areas that require additions. Add OUs as necessary. Connect AWS IAM Identity Center (AWS Single Sign-On) to the on-premises AD FS server. Most Voted

C. Create an organization in AWS Organizations. Create SCPs for least privilege access. Create an OU structure, and use it to group AWS accounts. Connect AWS IAM Identity Center (AWS Single Sign-On) to the on-premises AD FS server. Configure a central logging account with a defined process for log generating services to send log events to the central account. Enable AWS Config in the central account with aggregators and conformance packs.

D. Create an organization in AWS Organizations. Enable AWS Control Tower on the organization. Review included controls (guardrails) for SCPs. Check AWS Config for areas that require additions. Configure an IAM identity provider for federation with the on-premises AD FS server.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #335 *Topic 1*

An online magazine will launch its latest edition this month. This edition will be the first to be distributed globally. The magazine's dynamic website currently uses an Application Load Balancer in front of the web tier, a fleet of Amazon EC2 instances for web and application servers, and Amazon Aurora MySQL. Portions of the website include static content and almost all traffic is read-only.

The magazine is expecting a significant spike in internet traffic when the new edition is launched. Optimal performance is a top priority for the week following the launch.

Which combination of steps should a solutions architect take to reduce system response times for a global audience? (Choose two.)

A. Use logical cross-Region replication to replicate the Aurora MySQL database to a secondary Region. Replace the web servers with Amazon S3. Deploy S3 buckets in cross-Region replication mode.

B. Ensure the web and application tiers are each in Auto Scaling groups. Introduce an AWS Direct Connect connection. Deploy the web and application tiers in Regions across the world.

C. Migrate the database from Amazon Aurora to Amazon RDS for MySQL. Ensure all three of the application tiers – web, application, and database – are in private subnets.

D. Use an Aurora global database for physical cross-Region replication. Use Amazon S3 with cross-Region replication for static content and resources. Deploy the web and application tiers in Regions across the world. Most Voted

E. Introduce Amazon Route 53 with latency-based routing and Amazon CloudFront distributions. Ensure the web and application tiers are each in Auto Scaling groups. Most Voted

Correct Answer: *DE*

Community vote distribution

DE (100%)

Question #336 *Topic 1*

An online gaming company needs to optimize the cost of its workloads on AWS. The company uses a dedicated account to host the production environment for its online gaming application and an analytics application.

Amazon EC2 instances host the gaming application and must always be available. The EC2 instances run all year. The analytics application uses data that is stored in Amazon S3. The analytics application can be interrupted and resumed without issue.

Which solution will meet these requirements MOST cost-effectively?

A. Purchase an EC2 Instance Savings Plan for the online gaming application instances. Use On-Demand Instances for the analytics application.

B. Purchase an EC2 Instance Savings Plan for the online gaming application instances. Use Spot Instances for the analytics application. Most Voted

C. Use Spot Instances for the online gaming application and the analytics application. Set up a catalog in AWS Service Catalog to provision services at a discount.

D. Use On-Demand Instances for the online gaming application. Use Spot Instances for the analytics application. Set up a catalog in AWS Service Catalog to provision services at a discount.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #337 *Topic 1*

A company runs applications in hundreds of production AWS accounts. The company uses AWS Organizations with all features enabled and has a centralized backup operation that uses AWS Backup.

The company is concerned about ransomware attacks. To address this concern, the company has created a new policy that all backups must be resilient to breaches of privileged-user credentials in any production account.

Which combination of steps will meet this new requirement? (Choose three.)

A. Implement cross-account backup with AWS Backup vaults in designated non-production accounts. Most Voted

B. Add an SCP that restricts the modification of AWS Backup vaults. Most Voted

C. Implement AWS Backup Vault Lock in compliance mode.

C. Implement least privilege access for the IAM service role that is assigned to AWS Backup. Most Voted

D. Configure the backup frequency, lifecycle, and retention period to ensure that at least one backup always exists in the cold tier.

E. Configure AWS Backup to write all backups to an Amazon S3 bucket in a designated non-production account. Ensure that the S3 bucket has S3 Object Lock enabled.

Correct Answer: *ABC*

Community vote distribution

ABC (56%) ACD (29%) Other

Question #338 *Topic 1*

A company needs to aggregate Amazon CloudWatch logs from its AWS accounts into one central logging account. The collected logs must remain in the AWS Region of creation. The central logging account will then process the logs, normalize the logs into standard output format, and stream the output logs to a security tool for more processing.

A solutions architect must design a solution that can handle a large volume of logging data that needs to be ingested. Less logging will occur outside normal business hours than during normal business hours. The logging solution must scale with the anticipated load. The solutions architect has decided to use an AWS Control Tower design to handle the multi-account logging process.

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

A. Create a destination Amazon Kinesis data stream in the central logging account. Most Voted

B. Create a destination Amazon Simple Queue Service (Amazon SQS) queue in the central logging account.

C. Create an IAM role that grants Amazon CloudWatch Logs the permission to add data to the Amazon Kinesis data stream. Create a trust policy. Specify the trust policy in the IAM role. In each member account, create a subscription filter for each log group to send data to the Kinesis data stream. Most Voted

D. Create an IAM role that grants Amazon CloudWatch Logs the permission to add data to the Amazon Simple Queue Service (Amazon SQS) queue. Create a trust policy. Specify the trust policy in the IAM role. In each member account, create a single subscription filter for all log groups to send data to the SQS queue.

E. Create an AWS Lambda function. Program the Lambda function to normalize the logs in the central logging account and to write the logs to the security tool. Most Voted

F. Create an AWS Lambda function. Program the Lambda function to normalize the logs in the member accounts and to write the logs to the security tool.

Correct Answer: *ACE*

Community vote distribution

ACE (100%)

Question #339 *Topic 1*

A company is migrating a legacy application from an on-premises data center to AWS. The application consists of a single application server and a Microsoft SQL Server database server. Each server is deployed on a VMware VM that consumes 500 TB of data across multiple attached volumes.

The company has established a 10 Gbps AWS Direct Connect connection from the closest AWS Region to its on-premises data center. The Direct Connect connection is not currently in use by other services.

Which combination of steps should a solutions architect take to migrate the application with the LEAST amount of downtime? (Choose two.)

A. Use an AWS Server Migration Service (AWS SMS) replication job to migrate the database server VM to AWS.

B. Use VM Import/Export to import the application server VM.

C. Export the VM images to an AWS Snowball Edge Storage Optimized device.

D. Use an AWS Server Migration Service (AWS SMS) replication job to migrate the application server VM to AWS. Most Voted

E. Use an AWS Database Migration Service (AWS DMS) replication instance to migrate the database to an Amazon RDS DB instance. Most Voted

Correct Answer: *DE*

Community vote distribution

DE (58%) AD (30%) 9%

Question #340 *Topic 1*

A company operates a fleet of servers on premises and operates a fleet of Amazon EC2 instances in its organization in AWS Organizations. The company's AWS accounts contain hundreds of VPCs. The company wants to connect its AWS accounts to its on-premises network. AWS Site-to-Site VPN connections are already established to a single AWS account. The company wants to control which VPCs can communicate with other VPCs.

Which combination of steps will achieve this level of control with the LEAST operational effort? (Choose three.)

A. Create a transit gateway in an AWS account. Share the transit gateway across accounts by using AWS Resource Access Manager (AWS RAM). Most Voted

B. Configure attachments to all VPCs and VPNs. Most Voted

C. Setup transit gateway route tables. Associate the VPCs and VPNs with the route tables. Most Voted

D. Configure VPC peering between the VPCs.

E. Configure attachments between the VPCs and VPNs.

F. Setup route tables on the VPCs and VPNs.

Correct Answer: *ABC*

Community vote distribution

ABC (73%) ACE (27%)

Question #341 *Topic 1*

A company needs to optimize the cost of its application on AWS. The application uses AWS Lambda functions and Amazon Elastic Container Service (Amazon ECS) containers that run on AWS Fargate. The application is write-heavy and stores data in an Amazon Aurora MySQL database.

The load on the application is not consistent. The application experiences long periods of no usage, followed by sudden and significant increases and decreases in traffic. The database runs on a memory optimized DB instance that cannot handle the load.

A solutions architect must design a solution that can scale to handle the changes in traffic.

Which solution will meet these requirements MOST cost-effectively?

A. Add additional read replicas to the database. Purchase Instance Savings Plans and RDS Reserved Instances.

B. Migrate the database to an Aurora DB cluster that has multiple writer instances. Purchase Instance Savings Plans.

C. Migrate the database to an Aurora global database. Purchase Compute Savings Plans and RDS Reserved instances.

D. Migrate the database to Aurora Serverless v1. Purchase Compute Savings Plans. Most Voted

Correct Answer: *D*

Community vote distribution

D (95%) 5%

Question #342 *Topic 1*

A company migrated an application to the AWS Cloud. The application runs on two Amazon EC2 instances behind an Application Load Balancer (ALB).
Application data is stored in a MySQL database that runs on an additional EC2 instance. The application's use of the database is read-heavy.

The application loads static content from Amazon Elastic Block Store (Amazon EBS) volumes that are attached to each EC2 instance. The static content is updated frequently and must be copied to each EBS volume.

The load on the application changes throughout the day. During peak hours, the application cannot handle all the incoming requests. Trace data shows that the database cannot handle the read load during peak hours.

Which solution will improve the reliability of the application?

A. Migrate the application to a set of AWS Lambda functions. Set the Lambda functions as targets for the ALB. Create a new single EBS volume for the static content. Configure the Lambda functions to read from the new EBS volume. Migrate the database to an Amazon RDS for MySQL Multi-AZ DB cluster.

B. Migrate the application to a set of AWS Step Functions state machines. Set the state machines as targets for the ALCreate an Amazon Elastic File System (Amazon EFS) file system for the static content. Configure the state machines to read from the EFS file system. Migrate the database to Amazon Aurora MySQL Serverless v2 with a reader DB instance.

C. Containerize the application. Migrate the application to an Amazon Elastic Container Service (Amazon ECS) cluster. Use the AWS Fargate launch type for the tasks that host the application. Create a new single EBS volume for the static content. Mount the new EBS volume on the ECS cluster. Configure AWS Application Auto Scaling on the ECS cluster. Set the ECS service as a target for the ALB. Migrate the database to an Amazon RDS for MySQL Multi-AZ DB cluster.

D. Containerize the application. Migrate the application to an Amazon Elastic Container Service (Amazon ECS) cluster. Use the AWS Fargate launch type for the tasks that host the application. Create an Amazon Elastic File System (Amazon EFS) file system for the static content. Mount the EFS file system to each container. Configure AWS Application Auto Scaling on the ECS cluster. Set the ECS service as a target for the ALB. Migrate the database to Amazon Aurora MySQL Serverless v2 with a reader DB instance. Most Voted

Correct Answer: *D*

Community vote distribution

D (90%) 10%

Question #343 *Topic 1*

A solutions architect wants to make sure that only AWS users or roles with suitable permissions can access a new Amazon API Gateway endpoint. The solutions architect wants an end-to-end view of each request to analyze the latency of the request and create service maps.

How can the solutions architect design the API Gateway access control and perform request inspections?

A. For the API Gateway method, set the authorization to AWS_IAM. Then, give the IAM user or role execute-api:Invoke permission on the REST API resource. Enable the API caller to sign requests with AWS Signature when accessing the endpoint. Use AWS X-Ray to trace and analyze user requests to API Gateway. Most Voted

B. For the API Gateway resource, set CORS to enabled and only return the company's domain in Access-Control-Allow-Origin headers. Then, give the IAM user or role execute-api:Invoke permission on the REST API resource. Use Amazon CloudWatch to trace and analyze user requests to API Gateway.

C. Create an AWS Lambda function as the custom authorizer, ask the API client to pass the key and secret when making the call, and then use Lambda to validate the key/secret pair against the IAM system. Use AWS X-Ray to trace and analyze user requests to API Gateway.

D. Create a client certificate for API Gateway. Distribute the certificate to the AWS users and roles that need to access the endpoint. Enable the API caller to pass the client certificate when accessing the endpoint. Use Amazon CloudWatch to trace and analyze user requests to API Gateway.

Correct Answer: *A*

Community vote distribution

A (100%)

Question #344 *Topic 1*

A company is using AWS CodePipeline for the CI/CD of an application to an Amazon EC2 Auto Scaling group. All AWS resources are defined in AWS CloudFormation templates. The application artifacts are stored in an Amazon S3 bucket and deployed to the Auto Scaling group using instance user data scripts. As the application has become more complex, recent resource changes in the CloudFormation templates have caused unplanned downtime.

How should a solutions architect improve the CI/CD pipeline to reduce the likelihood that changes in the templates will cause downtime?

A. Adapt the deployment scripts to detect and report CloudFormation error conditions when performing deployments. Write test plans for a testing team to run in a non-production environment before approving the change for production.

B. Implement automated testing using AWS CodeBuild in a test environment. Use CloudFormation change sets to evaluate changes before deployment. Use AWS CodeDeploy to leverage blue/green deployment patterns to allow evaluations and the ability to revert changes, if needed. Most Voted

C. Use plugins for the integrated development environment (IDE) to check the templates for errors, and use the AWS CLI to validate that the templates are correct. Adapt the deployment code to check for error conditions and generate notifications on errors. Deploy to a test environment and run a manual test plan before approving the change for production.

D. Use AWS CodeDeploy and a blue/green deployment pattern with CloudFormation to replace the user data deployment scripts. Have the operators log in to running instances and go through a manual test plan to verify the application is running as expected.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #345 *Topic 1*

A North American company with headquarters on the East Coast is deploying a new web application running on Amazon EC2 in the us-east-1 Region. The application should dynamically scale to meet user demand and maintain resiliency. Additionally, the application must have disaster recovery capabilities in an active-passive configuration with the us-west-1 Region.

Which steps should a solutions architect take after creating a VPC in the us-east-1 Region?

A. Create a VPC in the us-west-1 Region. Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs in each Region as part of an Auto Scaling group spanning both VPCs and served by the ALB.

B. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALDeploy the same solution to the us-west-1 Region. Create an Amazon Route 53 record set with a failover routing policy and health checks enabled to provide high availability across both Regions.

Most Voted

C. Create a VPC in the us-west-1 Region. Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer (ALB) that spans both VPCs. Deploy EC2 instances across multiple Availability Zones as part of an Auto Scaling group in each VPC served by the ALB. Create an Amazon Route 53 record that points to the ALB.

D. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. Deploy the same solution to the us-west-1 Region. Create separate Amazon Route 53 records in each Region that point to the ALB in the Region. Use Route 53 health checks to provide high availability across both Regions.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #346 *Topic 1*

A company has a legacy application that runs on multiple NET Framework components. The components share the same Microsoft SQL Server database and communicate with each other asynchronously by using Microsoft Message Queueing (MSMQ).

The company is starting a migration to containerized .NET Core components and wants to refactor the application to run on AWS. The .NET Core components require complex orchestration. The company must have full control over networking and host configuration. The application's database model is strongly relational.

Which solution will meet these requirements?

A. Host the INET Core components on AWS App Runner. Host the database on Amazon RDS for SQL Server. Use Amazon EventBiridge for asynchronous messaging.

B. Host the .NET Core components on Amazon Elastic Container Service (Amazon ECS) with the AWS Fargate launch type. Host the database on Amazon DynamoDUse Amazon Simple Notification Service (Amazon SNS) for asynchronous messaging.

C. Host the .NET Core components on AWS Elastic Beanstalk. Host the database on Amazon Aurora PostgreSQL Serverless v2. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) for asynchronous messaging.

D. Host the NET Core components on Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type. Host the database on Amazon Aurora MySQL Serverless v2. Use Amazon Simple Queue Service (Amazon SQS) for asynchronous messaging. Most Voted

Correct Answer: *D*

Community vote distribution

D (96%) 4%

Question #347 *Topic 1*

A solutions architect has launched multiple Amazon EC2 instances in a placement group within a single Availability Zone. Because of additional load on the system, the solutions architect attempts to add new instances to the placement group. However, the solutions architect receives an insufficient capacity error.

What should the solutions architect do to troubleshoot this issue?

A. Use a spread placement group. Set a minimum of eight instances for each Availability Zone.

B. Stop and start all the instances in the placement group. Try the launch again. Most Voted

C. Create a new placement group. Merge the new placement group with the original placement group.

D. Launch the additional instances as Dedicated Hosts in the placement groups.

Correct Answer: *B*

Community vote distribution

B (88%) 13%

Question #348 *Topic 1*

A company has used infrastructure as code (IaC) to provision a set of two Amazon EC2 instances. The instances have remained the same for several years.

The company's business has grown rapidly in the past few months. In response, the company's operations team has implemented an Auto Scaling group to manage the sudden increases in traffic. Company policy requires a monthly installation of security updates on all operating systems that are running.

The most recent security update required a reboot. As a result, the Auto Scaling group terminated the instances and replaced them with new, unpatched instances.

Which combination of steps should a solutions architect recommend to avoid a recurrence of this issue? (Choose two.)

A. Modify the Auto Scaling group by setting the Update policy to target the oldest launch configuration for replacement.

B. Create a new Auto Scaling group before the next patch maintenance. During the maintenance window, patch both groups and reboot the instances.

C. Create an Elastic Load Balancer in front of the Auto Scaling group. Configure monitoring to ensure that target group health checks return healthy after the Auto Scaling group replaces the terminated instances. Most Voted

D. Create automation scripts to patch an AMI, update the launch configuration, and invoke an Auto Scaling instance refresh. Most Voted

E. Create an Elastic Load Balancer in front of the Auto Scaling group. Configure termination protection on the instances.

Correct Answer: *CD*

Community vote distribution

CD (44%) AD (36%) AC (18%)

Question #349 *Topic 1*

A team of data scientists is using Amazon SageMaker instances and SageMaker APIs to train machine learning (ML) models. The SageMaker instances are deployed in a VPC that does not have access to or from the internet. Datasets for ML model training are stored in an Amazon S3 bucket. Interface VPC endpoints provide access to Amazon S3 and the SageMaker APIs.

Occasionally, the data scientists require access to the Python Package Index (PyPI) repository to update Python packages that they use as part of their workflow. A solutions architect must provide access to the PyPI repository while ensuring that the SageMaker instances remain isolated from the internet.

Which solution will meet these requirements?

A. Create an AWS CodeCommit repository for each package that the data scientists need to access. Configure code synchronization between the PyPI repository and the CodeCommit repository. Create a VPC endpoint for CodeCommit.

B. Create a NAT gateway in the VPC. Configure VPC routes to allow access to the internet with a network ACL that allows access to only the PyPI repository endpoint.

C. Create a NAT instance in the VPConfigure VPC routes to allow access to the internet. Configure SageMaker notebook instance firewall rules that allow access to only the PyPI repository endpoint.

D. Create an AWS CodeArtifact domain and repository. Add an external connection for public:pypi to the CodeArtifact repository. Configure the Python client to use the CodeArtifact repository. Create a VPC endpoint for CodeArtifact. Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #350 *Topic 1*

A solutions architect works for a government agency that has strict disaster recovery requirements. All Amazon Elastic Block Store (Amazon EBS) snapshots are required to be saved in at least two additional AWS Regions. The agency also is required to maintain the lowest possible operational overhead.

Which solution meets these requirements?

A. Configure a policy in Amazon Data Lifecycle Manager (Amazon DLM) to run once daily to copy the EBS snapshots to the additional Regions. Most Voted

B. Use Amazon EventBridge to schedule an AWS Lambda function to copy the EBS snapshots to the additional Regions.

C. Setup AWS Backup to create the EBS snapshots. Configure Amazon S3 Cross-Region Replication to copy the EBS snapshots to the additional Regions.

D. Schedule Amazon EC2 Image Builder to run once daily to create an AMI and copy the AMI to the additional Regions.

Correct Answer: *A*

Community vote distribution

A (89%) 11%

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