EXAMTOPICS

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

⚙ Custom View Settings

Question #351   *Topic 1*

A company has a project that is launching Amazon EC2 instances that are larger than required. The project's account cannot be part of the company's organization in AWS Organizations due to policy restrictions to keep this activity outside of corporate IT. The company wants to allow only the launch of t3.small EC2 instances by developers in the project's account. These EC2 instances must be restricted to the us-east-2 Region.

What should a solutions architect do to meet these requirements?

A. Create a new developer account. Move all EC2 instances, users, and assets into us-east-2. Add the account to the company's organization in AWS Organizations. Enforce a tagging policy that denotes Region affinity.

B. Create an SCP that denies the launch of all EC2 instances except t3.small EC2 instances in us-east-2. Attach the SCP to the project's account.

C. Create and purchase a t3.small EC2 Reserved Instance for each developer in us-east-2. Assign each developer a specific EC2 instance with their name as the tag.

D. Create an IAM policy than allows the launch of only t3.small EC2 instances in us-east-2. Attach the policy to the roles and groups that the developers use in the project's account.

Question #352   *Topic 1*

A scientific company needs to process text and image data from an Amazon S3 bucket. The data is collected from several radar stations during a live, time-critical phase of a deep space mission. The radar stations upload the data to the source S3 bucket. The data is prefixed by radar station identification number.

The company created a destination S3 bucket in a second account. Data must be copied from the source S3 bucket to the destination S3 bucket to meet a compliance objective. This replication occurs through the use of an S3 replication rule to cover all objects in the source S3 bucket.

One specific radar station is identified as having the most accurate data. Data replication at this radar station must be monitored for completion within 30 minutes after the radar station uploads the objects to the source S3 bucket.

What should a solutions architect do to meet these requirements?

A. Setup an AWS DataSync agent to replicate the prefixed data from the source S3 bucket to the destination S3 bucket. Select to use all available bandwidth on the task, and monitor the task to ensure that itis in the TRANSFERRING status. Create an Amazon EventBridge rule to initiate an alert if this status changes.

B. In the second account, create another S3 bucket to receive data from the radar station with the most accurate data. Set up a new replication rule for this new S3 bucket to separate the replication from the other radar stations. Monitor the maximum replication time to the destination. Create an Amazon EventBridge rule to initiate an alert when the time exceeds the desired threshold.

C. Enable Amazon S3 Transfer Acceleration on the source S3 bucket, and configure the radar station with the most accurate data to use the new endpoint. Monitor the S3 destination bucket's TotalRequestLatency metric. Create an Amazon EventBridge rule to initiate an alert if this status changes.

D. Create a new S3 replication rule on the source S3 bucket that filters for the keys that use the prefix of the radar station with the most accurate data. Enable S3 Replication Time Control (S3 RTC). Monitor the maximum replication time to the destination. Create an Amazon EventBridge rule to initiate an alert when the time exceeds the desired threshold.

Question #353   *Topic 1*

A company wants to migrate its on-premises data center to the AWS Cloud. This includes thousands of virtualized Linux and Microsoft Windows servers, SAN storage, Java and PHP applications with MySQL, and Oracle databases. There are many dependent services hosted either in the same data center or externally. The technical documentation is incomplete and outdated. A solutions architect needs to understand the current environment and estimate the cloud resource costs after the migration.

Which tools or services should the solutions architect use to plan the cloud migration? (Choose three.)

A. AWS Application Discovery Service

B. AWS SMS

C. AWS X-Ray

D. AWS Cloud Adoption Readiness Tool (CART)

E. Amazon Inspector

F. AWS Migration Hub

Question #354   *Topic 1*

A solutions architect is reviewing an application's resilience before launch. The application runs on an Amazon EC2 instance that is deployed in a private subnet of a VPC. The EC2 instance is provisioned by an Auto Scaling group that has a minimum capacity of 1 and a maximum capacity of 1. The application stores data on an Amazon RDS for MySQL DB instance. The VPC has subnets configured in three Availability Zones and is configured with a single NAT gateway.

The solutions architect needs to recommend a solution to ensure that the application will operate across multiple Availability Zones.

Which solution will meet this requirement?

    A. Deploy an additional NAT gateway in the other Availability Zones. Update the route tables with appropriate routes. Modify the RDS for MySQL DB instance to a Multi-AZ configuration. Configure the Auto Scaling group to launch the instances across Availability Zones. Set the minimum capacity and maximum capacity of the Auto Scaling group to 3.

    B. Replace the NAT gateway with a virtual private gateway. Replace the RDS for MySQL DB instance with an Amazon Aurora MySQL DB cluster. Configure the Auto Scaling group to launch instances across all subnets in the VPC. Set the minimum capacity and maximum capacity of the Auto Scaling group to 3.

    C. Replace the NAT gateway with a NAT instance. Migrate the RDS for MySQL DB instance to an RDS for PostgreSQL DB instance. Launch a new EC2 instance in the other Availability Zones.

    D. Deploy an additional NAT gateway in the other Availability Zones. Update the route tables with appropriate routes. Modify the RDS for MySQL DB instance to turn on automatic backups and retain the backups for 7 days. Configure the Auto Scaling group to launch instances across all subnets in the VPC. Keep the minimum capacity and the maximum capacity of the Auto Scaling group at 1.

Question #355   *Topic 1*

A company is planning to migrate its on-premises transaction-processing application to AWS. The application runs inside Docker containers that are hosted on VMs in the company's data center. The Docker containers have shared storage where the application records transaction data.

The transactions are time sensitive. The volume of transactions inside the application is unpredictable. The company must implement a low-latency storage solution that will automatically scale throughput to meet increased demand. The company cannot develop the application further and cannot continue to administer the Docker hosting environment.

How should the company migrate the application to AWS to meet these requirements?

    A. Migrate the containers that run the application to Amazon Elastic Kubernetes Service (Amazon EKS). Use Amazon S3 to store the transaction data that the containers share.

    B. Migrate the containers that run the application to AWS Fargate for Amazon Elastic Container Service (Amazon ECS). Create an Amazon Elastic File System (Amazon EFS) file system. Create a Fargate task definition. Add a volume to the task definition to point to the EFS file system.

    C. Migrate the containers that run the application to AWS Fargate for Amazon Elastic Container Service (Amazon ECS). Create an Amazon Elastic Block Store (Amazon EBS) volume. Create a Fargate task definition. Attach the EBS volume to each running task.

    D. Launch Amazon EC2 instances. Install Docker on the EC2 instances. Migrate the containers to the EC2 instances. Create an Amazon Elastic File System (Amazon EFS) file system. Add a mount point to the EC2 instances for the EFS file system.

Question #356   *Topic 1*

A company is planning to migrate to the AWS Cloud. The company hosts many applications on Windows servers and Linux servers. Some of the servers are physical, and some of the servers are virtual. The company uses several types of databases in its on-premises environment. The company does not have an accurate inventory of its on-premises servers and applications.

The company wants to rightsize its resources during migration. A solutions architect needs to obtain information about the network connections and the application relationships. The solutions architect must assess the company's current environment and develop a migration plan.

Which solution will provide the solutions architect with the required information to develop the migration plan?

   A. Use Migration Evaluator to request an evaluation of the environment from AWS. Use the AWS Application Discovery Service Agentless Collector to import the details into a Migration Evaluator Quick Insights report.

   B. Use AWS Migration Hub and install the AWS Application Discovery Agent on the servers. Deploy the Migration Hub Strategy Recommendations application data collector. Generate a report by using Migration Hub Strategy Recommendations.

   C. Use AWS Migration Hub and run the AWS Application Discovery Service Agentless Collector on the servers. Group the servers and databases by using AWS Application Migration Service. Generate a report by using Migration Hub Strategy Recommendations.

   D. Use the AWS Migration Hub import tool to load the details of the company's on-premises environment. Generate a report by using Migration Hub Strategy Recommendations.

Question #357   *Topic 1*

A financial services company sells its software-as-a-service (SaaS) platform for application compliance to large global banks. The SaaS platform runs on AWS and uses multiple AWS accounts that are managed in an organization in AWS Organizations. The SaaS platform uses many AWS resources globally.

For regulatory compliance, all API calls to AWS resources must be audited, tracked for changes, and stored in a durable and secure data store.

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

   A. Create a new AWS CloudTrail trail. Use an existing Amazon S3 bucket in the organization's management account to store the logs. Deploy the trail to all AWS Regions. Enable MFA delete and encryption on the S3 bucket.

   B. Create a new AWS CloudTrail trail in each member account of the organization. Create new Amazon S3 buckets to store the logs. Deploy the trail to all AWS Regions. Enable MFA delete and encryption on the S3 buckets.

   C. Create a new AWS CloudTrail trail in the organization's management account. Create a new Amazon S3 bucket with versioning turned on to store the logs. Deploy the trail for all accounts in the organization. Enable MFA delete and encryption on the S3 bucket.

   D. Create a new AWS CloudTrail trail in the organization's management account. Create a new Amazon S3 bucket to store the logs. Configure Amazon Simple Notification Service (Amazon SNS) to send log-file delivery notifications to an external management system that will track the logs. Enable MFA delete and encryption on the S3 bucket.

Question #358   *Topic 1*

A company is deploying a distributed in-memory database on a fleet of Amazon EC2 instances. The fleet consists of a primary node and eight worker nodes. The primary node is responsible for monitoring cluster health, accepting user requests, distributing user requests to worker nodes, and sending an aggregate response back to a client. Worker nodes communicate with each other to replicate data partitions.

The company requires the lowest possible networking latency to achieve maximum performance.

Which solution will meet these requirements?

    A. Launch memory optimized EC2 instances in a partition placement group.

    B. Launch compute optimized EC2 instances in a partition placement group.

    C. Launch memory optimized EC2 instances in a cluster placement group.

    D. Launch compute optimized EC2 instances in a spread placement group.

Question #359   *Topic 1*

A company maintains information on premises in approximately 1 million.csv files that are hosted on a VM. The data initially is 10 TB in size and grows at a rate of 1 TB each week. The company needs to automate backups of the data to the AWS Cloud.

Backups of the data must occur daily. The company needs a solution that applies custom filters to back up only a subset of the data that is located in designated source directories. The company has set up an AWS Direct Connect connection.

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

    A. Use the Amazon S3 CopyObject API operation with multipart upload to copy the existing data to Amazon S3. Use the CopyObject API operation to replicate new data to Amazon S3 daily.

    B. Create a backup plan in AWS Backup to back up the data to Amazon S3. Schedule the backup plan to run daily.

    C. Install the AWS DataSync agent as a VM that runs on the on-premises hypervisor. Configure a DataSync task to replicate the data to Amazon S3 daily.

    D. Use an AWS Snowball Edge device for the initial backup. Use AWS DataSync for incremental backups to Amazon S3 daily.

Question #360   Topic 1

A financial services company has an asset management product that thousands of customers use around the world. The customers provide feedback about the product through surveys. The company is building a new analytical solution that runs on Amazon EMR to analyze the data from these surveys. The following user personas need to access the analytical solution to perform different actions:

• Administrator: Provisions the EMR cluster for the analytics team based on the team's requirements
• Data engineer: Runs ETL scripts to process, transform, and enrich the datasets
• Data analyst: Runs SQL and Hive queries on the data

A solutions architect must ensure that all the user personas have least privilege access to only the resources that they need. The user personas must be able to launch only applications that are approved and authorized. The solution also must ensure tagging for all resources that the user personas create.

Which solution will meet these requirements?

A. Create IAM roles for each user persona. Attach identity-based policies to define which actions the user who assumes the role can perform. Create an AWS Config rule to check for noncompliant resources. Configure the rule to notify the administrator to remediate the noncompliant resources.

B. Setup Kerberos-based authentication for EMR clusters upon launch. Specify a Kerberos security configuration along with cluster-specific Kerberos options.

C. Use AWS Service Catalog to control the Amazon EMR versions available for deployment, the cluster configuration, and the permissions for each user persona.

D. Launch the EMR cluster by using AWS CloudFormation, Attach resource-based policies to the EMR cluster during cluster creation. Create an AWS. Config rule to check for noncompliant clusters and noncompliant Amazon S3 buckets. Configure the rule to notify the administrator to remediate the noncompliant resources.

Question #361   *Topic 1*

A software as a service (SaaS) company uses AWS to host a service that is powered by AWS PrivateLink. The service consists of proprietary software that runs on three Amazon EC2 instances behind a Network Load Balancer (NLB). The instances are in private subnets in multiple Availability Zones in the eu-west-2 Region. All the company's customers are in eu-west-2.

However, the company now acquires a new customer in the us-east-1 Region. The company creates a new VPC and new subnets in us-east-1. The company establishes inter-Region VPC peering between the VPCs in the two Regions.

The company wants to give the new customer access to the SaaS service, but the company does not want to immediately deploy new EC2 resources in us-east-1.

Which solution will meet these requirements?

   A. Configure a PrivateLink endpoint service in us-east-1 to use the existing NLB that is in eu-west-2. Grant specific AWS accounts access to connect to the SaaS service.

   B. Create an NLB in us-east-1. Create an IP target group that uses the IP addresses of the company's instances in eu-west-2 that host the SaaS service. Configure a PrivateLink endpoint service that uses the NLB that is in us-east-1. Grant specific AWS accounts access to connect to the SaaS service.

   C. Create an Application Load Balancer (ALB) in front of the EC2 instances in eu-west-2. Create an NLB in us-east-1. Associate the NLB that is in us-east-1 with an ALB target group that uses the ALB that is in eu-west-2. Configure a PrivateLink endpoint service that uses the NLB that is in us-east-1. Grant specific AWS accounts access to connect to the SaaS service.

   D. Use AWS Resource Access Manager (AWS RAM) to share the EC2 instances that are in eu-west-2. In us-east-1, create an NLB and an instance target group that includes the shared EC2 instances from eu-west-2. Configure a PrivateLink endpoint service that uses the NLB that is in us-east-1. Grant specific AWS accounts access to connect to the SaaS service.

Question #362   *Topic 1*

A company needs to monitor a growing number of Amazon S3 buckets across two AWS Regions. The company also needs to track the percentage of objects that are encrypted in Amazon S3. The company needs a dashboard to display this information for internal compliance teams.

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

   A. Create a new 3 Storage Lens dashboard in each Region to track bucket and encryption metrics. Aggregate data from both Region dashboards into a single dashboard in Amazon QuickSight for the compliance teams.

   B. Deploy an AWS Lambda function in each Region to list the number of buckets and the encryption status of objects. Store this data in Amazon S3. Use Amazon Athena queries to display the data on a custom dashboard in Amazon QuickSight for the compliance teams.

   C. Use the S3 Storage Lens default dashboard to track bucket and encryption metrics. Give the compliance teams access to the dashboard directly in the S3 console.

   D. Create an Amazon EventBridge rule to detect AWS CloudTrail events for S3 object creation. Configure the rule to invoke an AWS Lambda function to record encryption metrics in Amazon DynamoDB. Use Amazon QuickSight to display the metrics in a dashboard for the compliance teams.

Question #363   Topic 1

A company's CISO has asked a solutions architect to re-engineer the company's current CI/CD practices to make sure patch deployments to its application can happen as quickly as possible with minimal downtime if vulnerabilities are discovered. The company must also be able to quickly roll back a change in case of errors.

The web application is deployed in a fleet of Amazon EC2 instances behind an Application Load Balancer. The company is currently using GitHub to host the application source code, and has configured an AWS CodeBuild project to build the application. The company also intends to use AWS CodePipeline to trigger builds from GitHub commits using the existing CodeBuild project.

What CI/CD configuration meets all of the requirements?

A. Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for in-place deployment. Monitor the newly deployed code, and, if there are any issues, push another code update

B. Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for blue/green deployments. Monitor the newly deployed code, and, if there are any issues, trigger a manual rollback using CodeDeploy.

C. Configure CodePipeline with a deploy stage using AWS CloudFormation to create a pipeline for test and production stacks. Monitor the newly deployed code, and, if there are any issues, push another code update.

D. Configure the CodePipeline with a deploy stage using AWS OpsWorks and in-place deployments. Monitor the newly deployed code, and, if there are any issues, push another code update.

Question #363   Topic 1

Question #364   Topic 1

A company is managing many AWS accounts by using an organization in AWS Organizations. Different business units in the company run applications on Amazon EC2 instances. All the EC2 instances must have a BusinessUnit tag so that the company can track the cost for each business unit.

A recent audit revealed that some instances were missing this tag. The company manually added the missing tag to the instances.

What should a solutions architect do to enforce the tagging requirement in the future?

A. Enable tag policies in the organization. Create a tag policy for the BusinessUnit tag. Ensure that compliance with tag key capitalization is turned off. Implement the tag policy for the ec2:instance resource type. Attach the tag policy to the root of the organization.

B. Enable tag policies in the organization. Create a tag policy for the BusinessUnit tag. Ensure that compliance with tag key capitalization is turned on. Implement the tag policy for the ec2:instance resource type. Attach the tag policy to the organization's management account.

C. Create an SCP and attach the SCP to the root of the organization. Include the following statement in the SCP:

```
{
    "Sid": "DenyEC2Creation",
    "Effect": "Deny",
     "Action": [
            "ec2:RunInstances"
    ],
    "Resource": [
            "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition":      {
            "Null": {
                    "aw:RequestTag/BusinessUnit": "true"
            }
        }
}
```

D. Create an SCP and attach the SCP to the organization's management account. Include the following statement in the SCP:

```
{
    "Sid": "DenyEC2Creation",
     "Effect": "Deny",
     "Action": [
            "e2:RunInstances"
    ],
    "Resource": [
          "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition": {
            "Null": {
                    "aws:RequestTag/BusinessUnit": "false"
            }
        }
}
```

Question #365   *Topic 1*

A company is running a workload that consists of thousands of Amazon EC2 instances. The workload is running in a VPC that contains several public subnets and private subnets. The public subnets have a route for 0.0.0.0/0 to an existing internet gateway. The private subnets have a route for 0.0.0.0/0 to an existing NAT gateway.

A solutions architect needs to migrate the entire fleet of EC2 instances to use IPv6. The EC2 instances that are in private subnets must not be accessible from the public internet.

What should the solutions architect do to meet these requirements?

A. Update the existing VPC, and associate a custom IPv6 CIDR block with the VPC and all subnets. Update all the VPC route tables, and add a route for ::/0 to the internet gateway.

B. Update the existing VPC, and associate an Amazon-provided IPv6 CIDR block with the VPC and all subnets. Update the VPC route tables for all private subnets, and add a route for ::/0 to the NAT gateway.

C. Update the existing VPC, and associate an Amazon-provided IPv6 CIDR block with the VPC and all subnets. Create an egress-only internet gateway. Update the VPC route tables for all private subnets, and add a route for ::/0 to the egress-only internet gateway.

D. Update the existing VPC, and associate a custom IPV6 CIDR block with the VPC and all subnets. Create a new NAT gateway, and enable IPV6 support. Update the VPC route tables for all private subnets, and add a route for ::/0 to the IPv6-enabled NAT gateway.

Question #366   *Topic 1*

A company is using Amazon API Gateway to deploy a private REST API that will provide access to sensitive data. The API must be accessible only from an application that is deployed in a VPC. The company deploys the API successfully. However, the API is not accessible from an Amazon EC2 instance that is deployed in the VPC.

Which solution will provide connectivity between the EC2 instance and the API?

A. Create an interface VPC endpoint for API Gateway. Attach an endpoint policy that allows apigateway:* actions. Disable private DNS naming for the VPC endpoint. Configure an API resource policy that allows access from the VPC. Use the VPC endpoint's DNS name to access the API.

B. Create an interface VPC endpoint for API Gateway. Attach an endpoint policy that allows the execute-api:Invoke action. Enable private DNS naming for the VPC endpoint. Configure an API resource policy that allows access from the VPC endpoint. Use the API endpoint's DNS names to access the API.

C. Create a Network Load Balancer (NLB) and a VPC link. Configure private integration between API Gateway and the NLB. Use the API endpoint's DNS names to access the API.

D. Create an Application Load Balancer (ALB) and a VPC Link. Configure private integration between API Gateway and the ALB. Use the ALB endpoint's DNS name to access the API.

Question #367
Topic 1

A large payroll company recently merged with a small staffing company. The unified company now has multiple business units, each with its own existing AWS account.

A solutions architect must ensure that the company can centrally manage the billing and access policies for all the AWS accounts. The solutions architect configures AWS Organizations by sending an invitation to all member accounts of the company from a centralized management account.

What should the solutions architect do next to meet these requirements?

A. Create the OrganizationAccountAccess IAM group in each member account. Include the necessary IAM roles for each administrator.

B. Create the OrganizationAccountAccessPolicy IAM policy in each member account. Connect the member accounts to the management account by using cross-account access.

C. Create the OrganizationAccountAccessRole IAM role in each member account. Grant permission to the management account to assume the IAM role.

D. Create the OrganizationAccountAccessRole IAM role in the management account. Attach the AdministratorAccess AWS managed policy to the IAM role. Assign the IAM role to the administrators in each member account.

Question #368
Topic 1

A company has application services that have been containerized and deployed on multiple Amazon EC2 instances with public IPs. An Apache Kafka cluster has been deployed to the EC2 instances. A PostgreSQL database has been migrated to Amazon RDS for PostgreSQL. The company expects a significant increase of orders on its platform when a new version of its flagship product is released.

What changes to the current architecture will reduce operational overhead and support the product release?

A. Create an EC2 Auto Scaling group behind an Application Load Balancer. Create additional read replicas for the DB instance. Create Amazon Kinesis data streams and configure the application services to use the data streams. Store and serve static content directly from Amazon S3.

B. Create an EC2 Auto Scaling group behind an Application Load Balancer. Deploy the DB instance in Multi-AZ mode and enable storage auto scaling. Create Amazon Kinesis data streams and configure the application services to use the data streams. Store and serve static content directly from Amazon S3.

C. Deploy the application on a Kubernetes cluster created on the EC2 instances behind an Application Load Balancer. Deploy the DB instance in Multi-AZ mode and enable storage auto scaling. Create an Amazon Managed Streaming for Apache Kafka cluster and configure the application services to use the cluster. Store static content in Amazon S3 behind an Amazon CloudFront distribution.

D. Deploy the application on Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate and enable auto scaling behind an Application Load Balancer. Create additional read replicas for the DB instance. Create an Amazon Managed Streaming for Apache Kafka cluster and configure the application services to use the cluster. Store static content in Amazon S3 behind an Amazon CloudFront distribution.

Question #369   *Topic 1*

A company hosts a VPN in an on-premises data center. Employees currently connect to the VPN to access files in their Windows home directories. Recently, there has been a large growth in the number of employees who work remotely. As a result, bandwidth usage for connections into the data center has begun to reach 100% during business hours.

The company must design a solution on AWS that will support the growth of the company's remote workforce, reduce the bandwidth usage for connections into the data center, and reduce operational overhead.

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

 A. Create an AWS Storage Gateway Volume Gateway. Mount a volume from the Volume Gateway to the on-premises file server.

 B. Migrate the home directories to Amazon FSx for Windows File Server.

 C. Migrate the home directories to Amazon FSx for Lustre.

 D. Migrate remote users to AWS Client VPN.

 E. Create an AWS Direct Connect connection from the on-premises data center to AWS.

Question #370   *Topic 1*

A company has multiple AWS accounts. The company recently had a security audit that revealed many unencrypted Amazon Elastic Block Store (Amazon EBS) volumes attached to Amazon EC2 instances.

A solutions architect must encrypt the unencrypted volumes and ensure that unencrypted volumes will be detected automatically in the future. Additionally, the company wants a solution that can centrally manage multiple AWS accounts with a focus on compliance and security.

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

 A. Create an organization in AWS Organizations. Set up AWS Control Tower, and turn on the strongly recommended controls (guardrails). Join all accounts to the organization. Categorize the AWS accounts into OUs.

 B. Use the AWS CLI to list all the unencrypted volumes in all the AWS accounts. Run a script to encrypt all the unencrypted volumes in place.

 C. Create a snapshot of each unencrypted volume. Create a new encrypted volume from the unencrypted snapshot. Detach the existing volume, and replace it with the encrypted volume.

 D. Create an organization in AWS Organizations. Set up AWS Control Tower, and turn on the mandatory controls (guardrails). Join all accounts to the organization. Categorize the AWS accounts into OUs.

 E. Turn on AWS CloudTrail. Configure an Amazon EventBridge rule to detect and automatically encrypt unencrypted volumes.

Question #371   *Topic 1*

A company hosts an intranet web application on Amazon EC2 instances behind an Application Load Balancer (ALB). Currently, users authenticate to the application against an internal user database.

The company needs to authenticate users to the application by using an existing AWS Directory Service for Microsoft Active Directory directory. All users with accounts in the directory must have access to the application.

Which solution will meet these requirements?

    A. Create a new app client in the directory. Create a listener rule for the ALB. Specify the authenticate-oidc action for the listener rule. Configure the listener rule with the appropriate issuer, client ID and secret, and endpoint details for the Active Directory service. Configure the new app client with the callback URL that the ALB provides.

    B. Configure an Amazon Cognito user pool. Configure the user pool with a federated identity provider (IdP) that has metadata from the directory. Create an app client. Associate the app client with the user pool. Create a listener rule for the ALSpecify the authenticate-cognito action for the listener rule. Configure the listener rule to use the user pool and app client.

    C. Add the directory as a new IAM identity provider (IdP). Create a new IAM role that has an entity type of SAML 2.0 federation. Configure a role policy that allows access to the ALB. Configure the new role as the default authenticated user role for the IdP. Create a listener rule for the ALB. Specify the authenticate-oidc action for the listener rule.

    D. Enable AWS IAM Identity Center (AWS Single Sign-On). Configure the directory as an external identity provider (IdP) that uses SAML. Use the automatic provisioning method. Create a new IAM role that has an entity type of SAML 2.0 federation. Configure a role policy that allows access to the ALB. Attach the new role to all groups. Create a listener rule for the ALB. Specify the authenticate-cognito action for the listener rule.

Question #372   *Topic 1*

A company has a website that serves many visitors. The company deploys a backend service for the website in a primary AWS Region and a disaster recovery (DR) Region.

A single Amazon CloudFront distribution is deployed for the website. The company creates an Amazon Route 53 record set with health checks and a failover routing policy for the primary Region's backend service. The company configures the Route 53 record set as an origin for the CloudFront distribution. The company configures another record set that points to the backend service's endpoint in the DR Region as a secondary failover record type. The TTL for both record sets is 60 seconds.

Currently, failover takes more than 1 minute. A solutions architect must design a solution that will provide the fastest failover time.

Which solution will achieve this goal?

    A. Deploy an additional CloudFront distribution. Create a new Route 53 failover record set with health checks for both CloudFront distributions.

    B. Set the TTL to 4 second for the existing Route 53 record sets that are used for the backend service in each Region.

    C. Create new record sets for the backend services by using a latency routing policy. Use the record sets as an origin in the CloudFront distribution.

    D. Create a CloudFront origin group that includes two origins, one for each backend service Region. Configure origin failover as a cache behavior for the CloudFront distribution.

Question #373
Topic 1

A company is using multiple AWS accounts and has multiple DevOps teams running production and non-production workloads in these accounts. The company would like to centrally-restrict access to some of the AWS services that the DevOps teams do not use. The company decided to use AWS Organizations and successfully invited all AWS accounts into the Organization. They would like to allow access to services that are currently in-use and deny a few specific services. Also they would like to administer multiple accounts together as a single unit.

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

A. Use a Deny list strategy.

B. Review the Access Advisor in AWS IAM to determine services recently used

C. Review the AWS Trusted Advisor report to determine services recently used.

D. Remove the default FullAWSAccess SCP.

E. Define organizational units (OUs) and place the member accounts in the OUs.

F. Remove the default DenyAWSAccess SCP.

Question #374
Topic 1

A live-events company is designing a scaling solution for its ticket application on AWS. The application has high peaks of utilization during sale events. Each sale event is a one-time event that is scheduled. The application runs on Amazon EC2 instances that are in an Auto Scaling group. The application uses PostgreSQL for the database layer.

The company needs a scaling solution to maximize availability during the sale events.

Which solution will meet these requirements?

A. Use a predictive scaling policy for the EC2 instances. Host the database on an Amazon Aurora PostgreSQL Serverless v2 Multi-AZ DB instance with automatically scaling read replicas. Create an AWS Step Functions state machine to run parallel AWS Lambda functions to pre-warm the database before a sale event. Create an Amazon EventBridge rule to invoke the state machine.

B. Use a scheduled scaling policy for the EC2 instances. Host the database on an Amazon RDS for PostgreSQL Mulli-AZ DB instance with automatically scaling read replicas. Create an Amazon EventBridge rule that invokes an AWS Lambda function to create a larger read replica before a sale event. Fail over to the larger read replica. Create another EventBridge rule that invokes another Lambda function to scale down the read replica after the sale event.

C. Use a predictive scaling policy for the EC2 instances. Host the database on an Amazon RDS for PostgreSQL MultiAZ DB instance with automatically scaling read replicas. Create an AWS Step Functions state machine to run parallel AWS Lambda functions to pre-warm the database before a sale event. Create an Amazon EventBridge rule to invoke the state machine.

D. Use a scheduled scaling policy for the EC2 instances. Host the database on an Amazon Aurora PostgreSQL Multi-AZ DB cluster. Create an Amazon EventBridge rule that invokes an AWS Lambda function to create a larger Aurora Replica before a sale event. Fail over to the larger Aurora Replica. Create another EventBridge rule that invokes another Lambda function to scale down the Aurora Replica after the sale event.

Question #375   *Topic 1*

A company runs an intranet application on premises. The company wants to configure a cloud backup of the application. The company has selected AWS Elastic Disaster Recovery for this solution.

The company requires that replication traffic does not travel through the public internet. The application also must not be accessible from the internet. The company does not want this solution to consume all available network bandwidth because other applications require bandwidth.

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

    A. Create a VPC that has at least two private subnets, two NAT gateways, and a virtual private gateway.

    B. Create a VPC that has at least two public subnets, a virtual private gateway, and an internet gateway.

    C. Create an AWS Site-to-Site VPN connection between the on-premises network and the target AWS network.

    D. Create an AWS Direct Connect connection and a Direct Connect gateway between the on-premises network and the target AWS network.

    E. During configuration of the replication servers, select the option to use private IP addresses for data replication.

    F. During configuration of the launch settings for the target servers, select the option to ensure that the Recovery instance's private IP address matches the source server's private IP address.

Question #376   *Topic 1*

A company that provides image storage services wants to deploy a customer-facing solution to AWS. Millions of individual customers will use the solution. The solution will receive batches of large image files, resize the files, and store the files in an Amazon S3 bucket for up to 6 months.

The solution must handle significant variance in demand. The solution must also be reliable at enterprise scale and have the ability to rerun processing jobs in the event of failure.

Which solution will meet these requirements MOST cost-effectively?

    A. Use AWS Step Functions to process the S3 event that occurs when a user stores an image. Run an AWS Lambda function that resizes the image in place and replaces the original file in the S3 bucket. Create an S3 Lifecycle expiration policy to expire all stored images after 6 months.

    B. Use Amazon EventBridge to process the S3 event that occurs when a user uploads an image. Run an AWS Lambda function that resizes the image in place and replaces the original file in the S3 bucket. Create an S3 Lifecycle expiration policy to expire all stored images after 6 months.

    C. Use S3 Event Notifications to invoke an AWS Lambda function when a user stores an image. Use the Lambda function to resize the image in place and to store the original file in the S3 bucket. Create an S3 Lifecycle policy to move all stored images to S3 Standard-Infrequent Access (S3 Standard-IA) after 6 months.

    D. Use Amazon Simple Queue Service (Amazon SQS) to process the S3 event that occurs when a user stores an image. Run an AWS Lambda function that resizes the image and stores the resized file in an S3 bucket that uses S3 Standard-Infrequent Access (S3 Standard-IA). Create an S3 Lifecycle policy to move all stored images to S3 Glacier Deep Archive after 6 months.

Question #377   *Topic 1*

A company has an organization in AWS Organizations that includes a separate AWS account for each of the company's departments. Application teams from different departments develop and deploy solutions independently.

The company wants to reduce compute costs and manage costs appropriately across departments. The company also wants to improve visibility into billing for individual departments. The company does not want to lose operational flexibility when the company selects compute resources.

Which solution will meet these requirements?

A. Use AWS Budgets for each department. Use Tag Editor to apply tags to appropriate resources. Purchase EC2 Instance Savings Plans.

B. Configure AWS Organizations to use consolidated billing. Implement a tagging strategy that identifies departments. Use SCPs to apply tags to appropriate resources. Purchase EC2 Instance Savings Plans.

C. Configure AWS Organizations to use consolidated billing. Implement a tagging strategy that identifies departments. Use Tag Editor to apply tags to appropriate resources. Purchase Compute Savings Plans.

D. Use AWS Budgets for each department. Use SCPs to apply tags to appropriate resources. Purchase Compute Savings Plans.

Question #378   *Topic 1*

A company has a web application that securely uploads pictures and videos to an Amazon S3 bucket. The company requires that only authenticated users are allowed to post content. The application generates a presigned URL that is used to upload objects through a browser interface. Most users are reporting slow upload times for objects larger than 100 MB.

What can a solutions architect do to improve the performance of these uploads while ensuring only authenticated users are allowed to post content?

A. Set up an Amazon API Gateway with an edge-optimized API endpoint that has a resource as an S3 service proxy. Configure the PUT method for this resource to expose the S3 PutObject operation. Secure the API Gateway using a COGNITO_USER_POOLS authorizer. Have the browser interface use API Gateway instead of the presigned URL to upload objects.

B. Set up an Amazon API Gateway with a regional API endpoint that has a resource as an S3 service proxy. Configure the PUT method for this resource to expose the S3 PutObject operation. Secure the API Gateway using an AWS Lambda authorizer. Have the browser interface use API Gateway instead of the presigned URL to upload objects.

C. Enable an S3 Transfer Acceleration endpoint on the S3 bucket. Use the endpoint when generating the presigned URL. Have the browser interface upload the objects to this URL using the S3 multipart upload API.

D. Configure an Amazon CloudFront distribution for the destination S3 bucket. Enable PUT and POST methods for the CloudFront cache behavior. Update the CloudFront origin to use an origin access identity (OAI). Give the OAI user 3: PutObject permissions in the bucket policy. Have the browser interface upload objects using the CloudFront distribution.

Question #379   *Topic 1*

A large company is migrating its entire IT portfolio to AWS. Each business unit in the company has a standalone AWS account that supports both development and test environments. New accounts to support production workloads will be needed soon.

The finance department requires a centralized method for payment but must maintain visibility into each group's spending to allocate costs.

The security team requires a centralized mechanism to control IAM usage in all the company's accounts.

What combination of the following options meets the company's needs with the LEAST effort? (Choose two.)

A. Use a collection of parameterized AWS CloudFormation templates defining common IAM permissions that are launched into each account. Require all new and existing accounts to launch the appropriate stacks to enforce the least privilege model.

B. Use AWS Organizations to create a new organization from a chosen payer account and define an organizational unit hierarchy. Invite the existing accounts to join the organization and create new accounts using Organizations.

C. Require each business unit to use its own AWS accounts. Tag each AWS account appropriately and enable Cost Explorer to administer chargebacks.

D. Enable all features of AWS Organizations and establish appropriate service control policies that filter IAM permissions for sub-accounts.

E. Consolidate all of the company's AWS accounts into a single AWS account. Use tags for billing purposes and the IAM's Access Advisor feature to enforce the least privilege model.

Question #380   *Topic 1*

A company has a solution that analyzes weather data from thousands of weather stations. The weather stations send the data over an Amazon API Gateway REST API that has an AWS Lambda function integration. The Lambda function calls a third-party service for data pre-processing. The third-party service gets overloaded and fails the pre-processing, causing a loss of data.

A solutions architect must improve the resiliency of the solution. The solutions architect must ensure that no data is lost and that data can be processed later if failures occur.

What should the solutions architect do to meet these requirements?

A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the queue as the dead-letter queue for the API.

B. Create two Amazon Simple Queue Service (Amazon SQS) queues: a primary queue and a secondary queue. Configure the secondary queue as the dead-letter queue for the primary queue. Update the API to use a new integration to the primary queue. Configure the Lambda function as the invocation target for the primary queue.

C. Create two Amazon EventBridge event buses: a primary event bus and a secondary event bus. Update the API to use a new integration to the primary event bus. Configure an EventBridge rule to react to all events on the primary event bus. Specify the Lambda function as the target of the rule. Configure the secondary event bus as the failure destination for the Lambda function.

D. Create a custom Amazon EventBridge event bus. Configure the event bus as the failure destination for the Lambda function.

Question #381   *Topic 1*

A company built an ecommerce website on AWS using a three-tier web architecture. The application is Java-based and composed of an Amazon CloudFront distribution, an Apache web server layer of Amazon EC2 instances in an Auto Scaling group, and a backend Amazon Aurora MySQL database.

Last month, during a promotional sales event, users reported errors and timeouts while adding items to their shopping carts. The operations team recovered the logs created by the web servers and reviewed Aurora DB cluster performance metrics. Some of the web servers were terminated before logs could be collected and the Aurora metrics were not sufficient for query performance analysis.

Which combination of steps must the solutions architect take to improve application performance visibility during peak traffic events? (Choose three.)

A. Configure the Aurora MySQL DB cluster to publish slow query and error logs to Amazon CloudWatch Logs.

B. Implement the AWS X-Ray SDK to trace incoming HTTP requests on the EC2 instances and implement tracing of SQL queries with the X-Ray SDK for Java.

C. Configure the Aurora MySQL DB cluster to stream slow query and error logs to Amazon Kinesis.

D. Install and configure an Amazon CloudWatch Logs agent on the EC2 instances to send the Apache logs to CloudWatch Logs.

E. Enable and configure AWS CloudTrail to collect and analyze application activity from Amazon EC2 and Aurora

F. Enable Aurora MySQL DB cluster performance benchmarking and publish the stream to AWS X-Ray.

Question #382   *Topic 1*

A company that provisions job boards for a seasonal workforce is seeing an increase in traffic and usage. The backend services run on a pair of Amazon EC2 instances behind an Application Load Balancer with Amazon DynamoDB as the datastore. Application read and write traffic is slow during peak seasons.

Which option provides a scalable application architecture to handle peak seasons with the LEAST development effort?

A. Migrate the backend services to AWS Lambda. Increase the read and write capacity of DynamoDB.

B. Migrate the backend services to AWS Lambda. Configure DynamoDB to use global tables.

C. Use Auto Scaling groups for the backend services. Use DynamoDB auto scaling.

D. Use Auto Scaling groups for the backend services. Use Amazon Simple Queue Service (Amazon SQS) and an AWS Lambda function to write to DynamoDB.

Question #383
Topic 1

A company is migrating to the cloud. It wants to evaluate the configurations of virtual machines in its existing data center environment to ensure that it can size new Amazon EC2 instances accurately. The company wants to collect metrics, such as CPU, memory, and disk utilization, and it needs an inventory of what processes are running on each instance. The company would also like to monitor network connections to map communications between servers.

Which would enable the collection of this data MOST cost effectively?

A. Use AWS Application Discovery Service and deploy the data collection agent to each virtual machine in the data center.

B. Configure the Amazon CloudWatch agent on all servers within the local environment and publish metrics to Amazon CloudWatch Logs.

C. Use AWS Application Discovery Service and enable agentless discovery in the existing virtualization environment.

D. Enable AWS Application Discovery Service in the AWS Management Console and configure the corporate firewall to allow scans over a VPN.

Question #384
Topic 1

A company provides a software as a service (SaaS) application that runs in the AWS Cloud. The application runs on Amazon EC2 instances behind a Network Load Balancer (NLB). The instances are in an Auto Scaling group and are distributed across three Availability Zones in a single AWS Region.

The company is deploying the application into additional Regions. The company must provide static IP addresses for the application to customers so that the customers can add the IP addresses to allow lists. The solution must automatically route customers to the Region that is geographically closest to them.

Which solution will meet these requirements?

A. Create an Amazon CloudFront distribution. Create a CloudFront origin group. Add the NLB for each additional Region to the origin group. Provide customers with the IP address ranges of the distribution's edge locations.

B. Create an AWS Global Accelerator standard accelerator. Create a standard accelerator endpoint for the NLB in each additional Region. Provide customers with the Global Accelerator IP address.

C. Create an Amazon CloudFront distribution. Create a custom origin for the NLB in each additional Region. Provide customers with the IP address ranges of the distribution's edge locations.

D. Create an AWS Global Accelerator custom routing accelerator. Create a listener for the custom routing accelerator. Add the IP address and ports for the NLB in each additional Region. Provide customers with the Global Accelerator IP address.

Question #385   *Topic 1*

A company is running multiple workloads in the AWS Cloud. The company has separate units for software development. The company uses AWS Organizations and federation with SAML to give permissions to developers to manage resources in their AWS accounts. The development units each deploy their production workloads into a common production account.

Recently, an incident occurred in the production account in which members of a development unit terminated an EC2 instance that belonged to a different development unit. A solutions architect must create a solution that prevents a similar incident from happening in the future. The solution also must allow developers the possibility to manage the instances used for their workloads.

Which strategy will meet these requirements?

   A. Create separate OUs in AWS Organizations for each development unit. Assign the created OUs to the company AWS accounts. Create separate SCP with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag that matches the development unit name. Assign the SCP to the corresponding OU.

   B. Pass an attribute for DevelopmentUnit as an AWS Security Token Service (AWS STS) session tag during SAML federation. Update the IAM policy for the developers' assumed IAM role with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag and aws:PrincipalTag/DevelopmentUnit.

   C. Pass an attribute for DevelopmentUnit as an AWS Security Token Service (AWS STS) session tag during SAML federation. Create an SCP with an allow action and a StringEquals condition for the DevelopmentUnit resource tag and aws:PrincipalTag/DevelopmentUnit. Assign the SCP to the root OU.

   D. Create separate IAM policies for each development unit. For every IAM policy, add an allow action and a StringEquals condition for the DevelopmentUnit resource tag and the development unit name. During SAML federation, use AWS Security Token Service (AWS STS) to assign the IAM policy and match the development unit name to the assumed IAM role.

Question #386   *Topic 1*

An enterprise company is building an infrastructure services platform for its users. The company has the following requirements:

• Provide least privilege access to users when launching AWS infrastructure so users cannot provision unapproved services.
• Use a central account to manage the creation of infrastructure services.
• Provide the ability to distribute infrastructure services to multiple accounts in AWS Organizations.
• Provide the ability to enforce tags on any infrastructure that is started by users.

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

   A. Develop infrastructure services using AWS CloudFormation templates. Add the templates to a central Amazon S3 bucket and add the IAM roles or users that require access to the S3 bucket policy.

   B. Develop infrastructure services using AWS CloudFormation templates. Upload each template as an AWS Service Catalog product to portfolios created in a central AWS account. Share these portfolios with the Organizations structure created for the company.

   C. Allow user IAM roles to have AWSCloudFormationFullAccess and AmazonS3ReadOnlyAccess permissions. Add an Organizations SCP at the AWS account root user level to deny all services except AWS CloudFormation and Amazon S3.

   D. Allow user IAM roles to have ServiceCatalogEndUserAccess permissions only. Use an automation script to import the central portfolios to local AWS accounts, copy the TagOption, assign users access, and apply launch constraints.

   E. Use the AWS Service Catalog TagOption Library to maintain a list of tags required by the company. Apply the TagOption to AWS Service Catalog products or portfolios.

   F. Use the AWS CloudFormation Resource Tags property to enforce the application of tags to any CloudFormation templates that will be created for users.

Question #387   *Topic 1*

A company deploys a new web application. As part of the setup, the company configures AWS WAF to log to Amazon S3 through Amazon Kinesis Data Firehose. The company develops an Amazon Athena query that runs once daily to return AWS WAF log data from the previous 24 hours. The volume of daily logs is constant. However, over time, the same query is taking more time to run.

A solutions architect needs to design a solution to prevent the query time from continuing to increase. The solution must minimize operational overhead.

Which solution will meet these requirements?

A. Create an AWS Lambda function that consolidates each day's AWS WAF logs into one log file.

B. Reduce the amount of data scanned by configuring AWS WAF to send logs to a different S3 bucket each day.

C. Update the Kinesis Data Firehose configuration to partition the data in Amazon S3 by date and time. Create external tables for Amazon Redshift. Configure Amazon Redshift Spectrum to query the data source.

D. Modify the Kinesis Data Firehose configuration and Athena table definition to partition the data by date and time. Change the Athena query to view the relevant partitions.

Question #388   *Topic 1*

A company is developing a web application that runs on Amazon EC2 instances in an Auto Scaling group behind a public-facing Application Load Balancer (ALB). Only users from a specific country are allowed to access the application. The company needs the ability to log the access requests that have been blocked. The solution should require the least possible maintenance.

Which solution meets these requirements?

A. Create an IPSet containing a list of IP ranges that belong to the specified country. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from an IP range in the IPSet. Associate the rule with the web ACL. Associate the web ACL with the ALB.

B. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from the specified country. Associate the rule with the web ACL. Associate the web ACL with the ALB.

C. Configure AWS Shield to block any requests that do not originate from the specified country. Associate AWS Shield with the ALB.

D. Create a security group rule that allows ports 80 and 443 from IP ranges that belong to the specified country. Associate the security group with the ALB.

Question #389   *Topic 1*

A company is migrating an application from on-premises infrastructure to the AWS Cloud. During migration design meetings, the company expressed concerns about the availability and recovery options for its legacy Windows file server. The file server contains sensitive business-critical data that cannot be recreated in the event of data corruption or data loss. According to compliance requirements, the data must not travel across the public internet. The company wants to move to AWS managed services where possible.

The company decides to store the data in an Amazon FSx for Windows File Server file system. A solutions architect must design a solution that copies the data to another AWS Region for disaster recovery (DR) purposes.

Which solution will meet these requirements?

   A. Create a destination Amazon S3 bucket in the DR Region. Establish connectivity between the FSx for Windows File Server file system in the primary Region and the S3 bucket in the DR Region by using Amazon FSx File Gateway. Configure the S3 bucket as a continuous backup source in FSx File Gateway.

   B. Create an FSx for Windows File Server file system in the DR Region. Establish connectivity between the VPC the primary Region and the VPC in the DR Region by using AWS Site-to-Site VPN. Configure AWS DataSync to communicate by using VPN endpoints.

   C. Create an FSx for Windows File Server file system in the DR Region. Establish connectivity between the VPC in the primary Region and the VPC in the DR Region by using VPC peering. Configure AWS DataSync to communicate by using interface VPC endpoints with AWS PrivateLink.

   D. Create an FSx for Windows File Server file system in the DR Region. Establish connectivity between the VPC in the primary Region and the VPC in the DR Region by using AWS Transit Gateway in each Region. Use AWS Transfer Family to copy files between the FSx for Windows File Server file system in the primary Region and the FSx for Windows File Server file system in the DR Region over the private AWS backbone network.

Question #390   *Topic 1*

A company is currently in the design phase of an application that will need an RPO of less than 5 minutes and an RTO of less than 10 minutes. The solutions architecture team is forecasting that the database will store approximately 10 TB of data. As part of the design, they are looking for a database solution that will provide the company with the ability to fail over to a secondary Region.

Which solution will meet these business requirements at the LOWEST cost?

   A. Deploy an Amazon Aurora DB cluster and take snapshots of the cluster every 5 minutes. Once a snapshot is complete, copy the snapshot to a secondary Region to serve as a backup in the event of a failure.

   B. Deploy an Amazon RDS instance with a cross-Region read replica in a secondary Region. In the event of a failure, promote the read replica to become the primary.

   C. Deploy an Amazon Aurora DB cluster in the primary Region and another in a secondary Region. Use AWS DMS to keep the secondary Region in sync.

   D. Deploy an Amazon RDS instance with a read replica in the same Region. In the event of a failure, promote the read replica to become the primary.

Question #391   *Topic 1*

A financial company needs to create a separate AWS account for a new digital wallet application. The company uses AWS Organizations to manage its accounts. A solutions architect uses the IAM user Support1 from the management account to create a new member account with finance1@example.com as the email address.

What should the solutions architect do to create IAM users in the new member account?

    A. Sign in to the AWS Management Console with AWS account root user credentials by using the 64-character password from the initial AWS Organizations email sent to finance1@example.com. Set up the IAM users as required.

    B. From the management account, switch roles to assume the OrganizationAccountAccessRole role with the account ID of the new member account. Set up the IAM users as required.

    C. Go to the AWS Management Console sign-in page. Choose "Sign in using root account credentials." Sign in in by using the email address finance 1@example.com and the management account's root password. Set up the IAM users as required.

    D. Go to the AWS Management Console sign-in page. Sign in by using the account ID of the new member account and the Support1 IAM credentials. Set up the IAM users as required.

Question #392   *Topic 1*

A car rental company has built a serverless REST API to provide data to its mobile app. The app consists of an Amazon API Gateway API with a Regional endpoint, AWS Lambda functions, and an Amazon Aurora MySQL Serverless DB cluster. The company recently opened the API to mobile apps of partners. A significant increase in the number of requests resulted, causing sporadic database memory errors.

Analysis of the API traffic indicates that clients are making multiple HTTP GET requests for the same queries in a short period of time. Traffic is concentrated during business hours, with spikes around holidays and other events.

The company needs to improve its ability to support the additional usage while minimizing the increase in costs associated with the solution.

Which strategy meets these requirements?

    A. Convert the API Gateway Regional endpoint to an edge-optimized endpoint. Enable caching in the production stage.

    B. Implement an Amazon ElastiCache for Redis cache to store the results of the database calls. Modify the Lambda functions to use the cache.

    C. Modify the Aurora Serverless DB cluster configuration to increase the maximum amount of available memory.

    D. Enable throttling in the API Gateway production stage. Set the rate and burst values to limit the incoming calls.

Question #393
Topic 1

A company is migrating an on-premises application and a MySQL database to AWS. The application processes highly sensitive data, and new data is constantly updated in the database. The data must not be transferred over the internet. The company also must encrypt the data in transit and at rest.

The database is 5 TB in size. The company already has created the database schema in an Amazon RDS for MySQL DB instance. The company has set up a 1 Gbps AWS Direct Connect connection to AWS. The company also has set up a public VIF and a private VIF. A solutions architect needs to design a solution that will migrate the data to AWS with the least possible downtime.

Which solution will meet these requirements?

A. Perform a database backup. Copy the backup files to an AWS Snowball Edge Storage Optimized device. Import the backup to Amazon S3. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) for encryption at rest. Use TLS for encryption in transit. Import the data from Amazon S3 to the DB instance.

B. Use AWS Database Migration Service (AWS DMS) to migrate the data to AWS. Create a DMS replication instance in a private subnet. Create VPC endpoints for AWS DMS. Configure a DMS task to copy data from the on-premises database to the DB instance by using full load plus change data capture (CDC). Use the AWS Key Management Service (AWS KMS) default key for encryption at rest. Use TLS for encryption in transit.

C. Perform a database backup. Use AWS DataSync to transfer the backup files to Amazon S3. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) for encryption at rest. Use TLS for encryption in transit. Import the data from Amazon S3 to the DB instance.

D. Use Amazon S3 File Gateway. Set up a private connection to Amazon S3 by using AWS PrivateLink. Perform a database backup. Copy the backup files to Amazon S3. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) for encryption at rest. Use TLS for encryption in transit. Import the data from Amazon S3 to the DB instance.

Question #394
Topic 1

Accompany is deploying a new cluster for big data analytics on AWS. The cluster will run across many Linux Amazon EC2 instances that are spread across multiple Availability Zones.

All of the nodes in the cluster must have read and write access to common underlying file storage. The file storage must be highly available, must be resilient, must be compatible with the Portable Operating System Interface (POSIX), and must accommodate high levels of throughput.

Which storage solution will meet these requirements?

A. Provision an AWS Storage Gateway file gateway NFS file share that is attached to an Amazon S3 bucket. Mount the NFS file share on each EC2 instance in the cluster.

B. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses General Purpose performance mode. Mount the EFS file system on each EC2 instance in the cluster.

C. Provision a new Amazon Elastic Block Store (Amazon EBS) volume that uses the io2 volume type. Attach the EBS volume to all of the EC2 instances in the cluster.

D. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses Max I/O performance mode. Mount the EFS file system on each EC2 instance in the cluster.

Question #395   *Topic 1*

A company hosts a software as a service (SaaS) solution on AWS. The solution has an Amazon API Gateway API that serves an HTTPS endpoint. The API uses AWS Lambda functions for compute. The Lambda functions store data in an Amazon Aurora Serverless v1 database.

The company used the AWS Serverless Application Model (AWS SAM) to deploy the solution. The solution extends across multiple Availability Zones and has no disaster recovery (DR) plan.

A solutions architect must design a DR strategy that can recover the solution in another AWS Region. The solution has an RTO of 5 minutes and an RPO of 1 minute.

What should the solutions architect do to meet these requirements?

   A. Create a read replica of the Aurora Serverless v1 database in the target Region. Use AWS SAM to create a runbook to deploy the solution to the target Region. Promote the read replica to primary in case of disaster.

   B. Change the Aurora Serverless v1 database to a standard Aurora MySQL global database that extends across the source Region and the target Region. Use AWS SAM to create a runbook to deploy the solution to the target Region.

   C. Create an Aurora Serverless v1 DB cluster that has multiple writer instances in the target Region. Launch the solution in the target Region. Configure the two Regional solutions to work in an active-passive configuration.

   D. Change the Aurora Serverless v1 database to a standard Aurora MySQL global database that extends across the source Region and the target Region. Launch the solution in the target Region. Configure the two Regional solutions to work in an active-passive configuration.

Question #396   *Topic 1*

A company owns a chain of travel agencies and is running an application in the AWS Cloud. Company employees use the application to search for information about travel destinations. Destination content is updated four times each year.

Two fixed Amazon EC2 instances serve the application. The company uses an Amazon Route 53 public hosted zone with a multivalue record of travel.example.com that returns the Elastic IP addresses for the EC2 instances. The application uses Amazon DynamoDB as its primary data store. The company uses a self-hosted Redis instance as a caching solution.

During content updates, the load on the EC2 instances and the caching solution increases drastically. This increased load has led to downtime on several occasions. A solutions architect must update the application so that the application is highly available and can handle the load that is generated by the content updates.

Which solution will meet these requirements?

   A. Set up DynamoDB Accelerator (DAX) as in-memory cache. Update the application to use DAX. Create an Auto Scaling group for the EC2 instances. Create an Application Load Balancer (ALB). Set the Auto Scaling group as a target for the ALB. Update the Route 53 record to use a simple routing policy that targets the ALB's DNS alias. Configure scheduled scaling for the EC2 instances before the content updates.

   B. Set up Amazon ElastiCache for Redis. Update the application to use ElastiCache. Create an Auto Scaling group for the EC2 instances. Create an Amazon CloudFront distribution, and set the Auto Scaling group as an origin for the distribution. Update the Route 53 record to use a simple routing policy that targets the CloudFront distribution's DNS alias. Manually scale up EC2 instances before the content updates.

   C. Set up Amazon ElastiCache for Memcached. Update the application to use ElastiCache. Create an Auto Scaling group for the EC2 instances. Create an Application Load Balancer (ALB). Set the Auto Scaling group as a target for the ALB. Update the Route 53 record to use a simple routing policy that targets the ALB's DNS alias. Configure scheduled scaling for the application before the content updates.

   D. Set up DynamoDB Accelerator (DAX) as in-memory cache. Update the application to use DAX. Create an Auto Scaling group for the EC2 instances. Create an Amazon CloudFront distribution, and set the Auto Scaling group as an origin for the distribution. Update the Route 53 record to use a simple routing policy that targets the CloudFront distribution's DNS alias. Manually scale up EC2 instances before the content updates.

Question #397   *Topic 1*

A company needs to store and process image data that will be uploaded from mobile devices using a custom mobile app. Usage peaks between 8 AM and 5 PM on weekdays, with thousands of uploads per minute. The app is rarely used at any other time. A user is notified when image processing is complete.

Which combination of actions should a solutions architect take to ensure image processing can scale to handle the load? (Choose three.)

    A. Upload files from the mobile software directly to Amazon S3. Use S3 event notifications to create a message in an Amazon MQ queue.

    B. Upload files from the mobile software directly to Amazon S3. Use S3 event notifications to create a message in an Amazon Simple Queue Service (Amazon SQS) standard queue.

    C. Invoke an AWS Lambda function to perform image processing when a message is available in the queue.

    D. Invoke an S3 Batch Operations job to perform image processing when a message is available in the queue.

    E. Send a push notification to the mobile app by using Amazon Simple Notification Service (Amazon SNS) when processing is complete.

    F. Send a push notification to the mobile app by using Amazon Simple Email Service (Amazon SES) when processing is complete.

Question #398   *Topic 1*

A company is building an application on AWS. The application sends logs to an Amazon OpenSearch Service cluster for analysis. All data must be stored within a VPC.

Some of the company's developers work from home. Other developers work from three different company office locations. The developers need to access OpenSearch Service to analyze and visualize logs directly from their local development machines.

Which solution will meet these requirements?

    A. Configure and set up an AWS Client VPN endpoint. Associate the Client VPN endpoint with a subnet in the VPC. Configure a Client VPN self-service portal. Instruct the developers to connect by using the client for Client VPN.

    B. Create a transit gateway, and connect it to the VPC. Create an AWS Site-to-Site VPN. Create an attachment to the transit gateway. Instruct the developers to connect by using an OpenVPN client.

    C. Create a transit gateway, and connect it to the VPOrder an AWS Direct Connect connection. Set up a public VIF on the Direct Connect connection. Associate the public VIF with the transit gateway. Instruct the developers to connect to the Direct Connect connection.

    D. Create and configure a bastion host in a public subnet of the VPC. Configure the bastion host security group to allow SSH access from the company CIDR ranges. Instruct the developers to connect by using SSH.

Question #399	Topic 1

A company wants to migrate its website from an on-premises data center onto AWS. At the same time, it wants to migrate the website to a containerized microservice-based architecture to improve the availability and cost efficiency. The company's security policy states that privileges and network permissions must be configured according to best practice, using least privilege.

A solutions architect must create a containerized architecture that meets the security requirements and has deployed the application to an Amazon ECS cluster.

What steps are required after the deployment to meet the requirements? (Choose two.)

    A. Create tasks using the bridge network mode.

    B. Create tasks using the awsvpc network mode.

    C. Apply security groups to Amazon EC2 instances, and use IAM roles for EC2 instances to access other resources.

    D. Apply security groups to the tasks, and pass IAM credentials into the container at launch time to access other resources.

    E. Apply security groups to the tasks, and use IAM roles for tasks to access other resources.

Question #400	Topic 1

A company is running a serverless application that consists of several AWS Lambda functions and Amazon DynamoDB tables. The company has created new functionality that requires the Lambda functions to access an Amazon Neptune DB cluster. The Neptune DB cluster is located in three subnets in a VPC.

Which of the possible solutions will allow the Lambda functions to access the Neptune DB cluster and DynamoDB tables? (Choose two.)

    A. Create three public subnets in the Neptune VPC, and route traffic through an internet gateway. Host the Lambda functions in the three new public subnets.

    B. Create three private subnets in the Neptune VPC, and route internet traffic through a NAT gateway. Host the Lambda functions in the three new private subnets.

    C. Host the Lambda functions outside the VPUpdate the Neptune security group to allow access from the IP ranges of the Lambda functions.

    D. Host the Lambda functions outside the VPC. Create a VPC endpoint for the Neptune database, and have the Lambda functions access Neptune over the VPC endpoint.

    E. Create three private subnets in the Neptune VPC. Host the Lambda functions in the three new isolated subnets. Create a VPC endpoint for DynamoDB, and route DynamoDB traffic to the VPC endpoint.

← 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