



Amazon-Web-Services

Exam Questions SAP-C02

AWS Certified Solutions Architect - Professional

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

- (Exam Topic 1)

A startup company recently migrated a large ecommerce website to AWS. The website has experienced a 70% increase in sales. Software engineers are using a private GitHub repository to manage code. The DevOps learn is using Jenkins for builds and unit testing. The engineers need to receive notifications for bad builds and zero downtime during deployments. The engineers also need to ensure any changes to production are seamless for users and can be rolled back in the event of a major issue.

The software engineers have decided to use AWS CodePipeline to manage their build and deployment process.

Which solution will meet these requirements?

- A. Use GitHub websockets to trigger the CodePipeline pipeline
- B. Use the Jenkins plugin for AWS CodeBuild to conduct unit testing
- C. Send alerts to an Amazon SNS topic for any bad build
- D. Deploy in an in-place
- E. all-at-once deployment configuration using AWS CodeDeploy.
- F. Use GitHub webhooks to trigger the CodePipeline pipeline
- G. Use the Jenkins plugin for AWS CodeBuild to conduct unit testing
- H. Send alerts to an Amazon SNS topic for any bad build
- I. Deploy in a blue/green deployment using AWS CodeDeploy.
- J. Use GitHub websockets to trigger the CodePipeline pipeline
- K. Use AWS X-Ray for unit testing and static code analysis
- L. Send alerts to an Amazon SNS topic for any bad build
- M. Deploy in a blue/green deployment using AWS CodeDeploy.
- N. Use GitHub webhooks to trigger the CodePipeline pipeline
- O. Use AWS X-Ray for unit testing and static code analysis
- P. Send alerts to an Amazon SNS topic for any bad build
- Q. Deploy in an in-place, all-at-once deployment configuration using AWS CodeDeploy.

Answer: B

NEW QUESTION 2

- (Exam Topic 1)

A company is running an application distributed over several Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer. The security team requires that all application access attempts be made available for analysis. Information about the client IP address, connection type, and user agent must be included.

Which solution will meet these requirements?

- A. Enable EC2 detailed monitoring, and include network logs. Send all logs through Amazon Kinesis Data Firehose to an Amazon Elasticsearch Service (Amazon ES) cluster that the security team uses for analysis.
- B. Enable VPC Flow Logs for all EC2 instance network interfaces. Publish VPC Flow Logs to an Amazon S3 bucket. Have the security team use Amazon Athena to query and analyze the logs.
- C. Enable access logs for the Application Load Balancer, and publish the logs to an Amazon S3 bucket. Have the security team use Amazon Athena to query and analyze the logs.
- D. Enable Traffic Mirroring and specify all EC2 instance network interfaces as the source.
- E. Send all traffic information through Amazon Kinesis Data Firehose to an Amazon Elasticsearch Service (Amazon ES) cluster that the security team uses for analysis.

Answer: C

Explanation:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html>

NEW QUESTION 3

- (Exam Topic 1)

A company wants to move a web application to AWS. The application stores session information locally on each web server, which will make auto scaling difficult. As part of the migration, the application will be rewritten to decouple the session data from the web servers. The company requires low latency, scalability, and availability.

Which service will meet the requirements for storing the session information in the MOST cost-effective way?

- A. Amazon ElastiCache with the Memcached engine
- B. Amazon S3
- C. Amazon RDS MySQL
- D. Amazon ElastiCache with the Redis engine

Answer: D

Explanation:

<https://aws.amazon.com/caching/session-management/>

Building real-time apps across versatile use cases like gaming, geospatial service, caching, session stores, or queuing, with advanced data structures, replication, and point-in-time snapshot support. Memcached: Building a simple, scalable caching layer for your data-intensive apps. <https://aws.amazon.com/elasticache/>

NEW QUESTION 4

- (Exam Topic 1)

A development team has created a new flight tracker application that provides near-real-time data to users. The application has a front end that consists of an Application Load Balancer (ALB) in front of two large Amazon EC2 instances in a single Availability Zone. Data is stored in a single Amazon RDS MySQL DB instance. An Amazon Route 53 DNS record points to the ALB.

Management wants the development team to improve the solution to achieve maximum reliability with the least amount of operational overhead.

Which set of actions should the team take?

- A. Create RDS MySQL read replica
- B. Deploy the application to multiple AWS Region
- C. Use a Route 53 latency-based routing policy to route to the application.
- D. Configure the DB instance as Multi-AZ
- E. Deploy the application to two additional EC2 instances in different Availability Zones behind an ALB.
- F. Replace the DB instance with Amazon DynamoDB global table
- G. Deploy the application in multiple AWS Region
- H. Use a Route 53 latency-based routing policy to route to the application.
- I. Replace the DB instance with Amazon Aurora with Aurora Replica
- J. Deploy the application to multiple smaller EC2 instances across multiple Availability Zones in an Auto Scaling group behind an ALB.

Answer: D

Explanation:

Multi AZ ASG + ALB + Aurora = Less overhead and automatic scaling

NEW QUESTION 5

- (Exam Topic 1)

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

VPC CIDR: 10.0.0.0/23

AZ1 subnet CIDR: 10.0.0.0/24 AZ2 subnet CIDR: 10.0.1.0/24

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

Which solution will meet these requirements?

- A. Update the Auto Scaling group to use the AZ2 subnet only
- B. Delete and re-create the AZ1 subnet using half the previous address space
- C. Adjust the Auto Scaling group to also use the new AZ1 subnet
- D. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only
- E. Remove the current AZ2 subnet
- F. Create a new AZ2 subnet using the second half of the address space from the original AZ1 subnet
- G. Create a new AZ3 subnet using half the original AZ2 subnet address space, then update the Auto Scaling group to target all three new subnets.
- H. Terminate the EC2 instances in the AZ1 subnet
- I. Delete and re-create the AZ1 subnet using half the address space
- J. Update the Auto Scaling group to use this new subnet
- K. Repeat this for the second AZ
- L. Define a new subnet in AZ3, then update the Auto Scaling group to target all three new subnets.
- M. Create a new VPC with the same IPv4 address space and define three subnets, with one for each AZ
- N. Update the existing Auto Scaling group to target the new subnets in the new VPC.
- O. Update the Auto Scaling group to use the AZ2 subnet only
- P. Update the AZ1 subnet to have half the previous address space
- Q. Adjust the Auto Scaling group to also use the AZ1 subnet again
- R. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only
- S. Update the current AZ2 subnet and assign the second half of the address space from the original AZ1 subnet
- T. Create a new AZ3 subnet using half the original AZ2 subnet address space, then update the Auto Scaling group to target all three new subnets.

Answer: A

Explanation:

https://aws.amazon.com/premiumsupport/knowledge-center/vpc-ip-address-range/?nc1=h_ls

It's not possible to modify the IP address range of an existing virtual private cloud (VPC) or subnet. You must delete the VPC or subnet, and then create a new VPC or subnet with your preferred CIDR block.

NEW QUESTION 6

- (Exam Topic 1)

A company that is developing a mobile game is making game assets available in two AWS Regions. Game assets are served from a set of Amazon EC2 instances behind an Application Load Balancer (ALB) in each Region. The company requires game assets to be fetched from the closest Region. If game assets become unavailable in the closest Region, they should be fetched from the other Region.

What should a solutions architect do to meet these requirements?

- A. Create an Amazon CloudFront distribution
- B. Create an origin group with one origin for each ALB
- C. Set one of the origins as primary.
- D. Create an Amazon Route 53 health check for each ALB
- E. Create a Route 53 failover routing record pointing to the two ALBs
- F. Set the Evaluate Target Health value to Yes.
- G. Create two Amazon CloudFront distributions, each with one ALB as the origin
- H. Create an Amazon Route 53 failover routing record pointing to the two CloudFront distributions
- I. Set the Evaluate Target Health value to Yes.
- J. Create an Amazon Route 53 health check for each ALB
- K. Create a Route 53 latency alias record pointing to the two ALBs
- L. Set the Evaluate Target Health value to Yes.

Answer: D

Explanation:

Failover routing policy – Use when you want to configure active-passive failover. Latency routing policy – Use when you have resources in multiple AWS Regions and you want to route traffic to the region that provides the best latency. <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

NEW QUESTION 7

- (Exam Topic 1)

A company wants to retire its Oracle Solaris NFS storage arrays. The company requires rapid data migration over its internet network connection to a combination of destinations for Amazon S3, Amazon Elastic File System (Amazon EFS), and Amazon FSx for Windows File Server. The company also requires a full initial copy, as well as incremental transfers of changes until the retirement of the storage arrays. All data must be encrypted and checked for integrity. What should a solutions architect recommend to meet these requirements?

- A. Configure CloudEndur
- B. Create a project and deploy the CloudEndure agent and token to the storage arra
- C. Run the migration plan to start the transfer.
- D. Configure AWS DataSyn
- E. Configure the DataSync agent and deploy it to the local networ
- F. Create a transfer task and start the transfer.
- G. Configure the aws S3 sync comman
- H. Configure the AWS client on the client side with credential
- I. Run the sync command to start the transfer.
- J. Configure AWS Transfer (or FT
- K. Configure the FTP client with credential
- L. Script the client to connect and sync to start the transfer.

Answer: B

NEW QUESTION 8

- (Exam Topic 1)

A group of research institutions and hospitals are in a partnership to study 2 PBs of genomic data. The institute that owns the data stores it in an Amazon S3 bucket and updates it regularly. The institute would like to give all of the organizations in the partnership read access to the data. All members of the partnership are extremely cost-conscious, and the institute that owns the account with the S3 bucket is concerned about covering the costs for requests and data transfers from Amazon S3.

Which solution allows for secure datasharing without causing the institute that owns the bucket to assume all the costs for S3 requests and data transfers'?

- A. Ensure that all organizations in the partnership have AWS account
- B. In the account with the S3 bucket, create a cross-account role for each account in the partnership that allows read access to the dat
- C. Have the organizations assume and use that read role when accessing the data.
- D. Ensure that all organizations in the partnership have AWS account
- E. Create a bucket policy on the bucket that owns the data The policy should allow the accounts in the partnership read access to the bucke
- F. Enable Requester Pays on the bucke
- G. Have the organizations use their AWS credentials when accessing the data.
- H. Ensure that all organizations in the partnership have AWS account
- I. Configure buckets in each of the accounts with a bucket policy that allows the institute that owns the data the ability to write to the bucket Periodically sync the data from the institute's account to the other organization
- J. Have the organizations use their AWS credentials when accessing the data using their accounts
- K. Ensure that all organizations in the partnership have AWS account
- L. In the account with the S3 bucket, create a cross-account role for each account in the partnership that allows read access to the dat
- M. Enable Requester Pays on the bucke
- N. Have the organizations assume and use that read role when accessing the data.

Answer: B

Explanation:

In general, bucket owners pay for all Amazon S3 storage and data transfer costs associated with their bucket. A bucket owner, however, can configure a bucket to be a Requester Pays bucket. With Requester Pays buckets, the requester instead of the bucket owner pays the cost of the request and the data download from the bucket. The bucket owner always pays the cost of storing data. If you enable Requester Pays on a bucket, anonymous access to that bucket is not allowed. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/RequesterPaysExamples.html>

NEW QUESTION 9

- (Exam Topic 1)

A company has a three-tier application running on AWS with a web server, an application server, and an Amazon RDS MySQL DB instance. A solutions architect is designing a disaster recovery (DR) solution with an RPO of 5 minutes.

Which solution will meet the company's requirements?

- A. Configure AWS Backup to perform cross-Region backups of all servers every 5 minute
- B. Reprovision the three tiers in the DR Region from the backups using AWS CloudFormation in the event of a disaster.
- C. Maintain another running copy of the web and application server stack in the DR Region using AWS CloudFormation drill detectio
- D. Configure cross-Region snapshots of the DB instance to the DR Region every 5 minute
- E. In the event of a disaster, restore the DB instance using the snapshot in the DR Region.
- F. Use Amazon EC2 Image Builder to create and copy AMIs of the web and application server to both the primary and DR Region
- G. Create a cross-Region read replica of the DB instance in the DR Regio
- H. In the event of a disaster, promote the read replica to become the master and reprovision the servers with AWS CloudFormation using the AMIs.
- I. Create AMTs of the web and application servers in the DR Regio
- J. Use scheduled AWS Glue jobs to synchronize the DB instance with another DB instance in the DR Regio
- K. In the event of a disaster, switch to the DB instance in the DR Region and reprovision the servers with AWS CloudFormation using the AMIs.

Answer: C

Explanation:

deploying a brand new RDS instance will take >30 minutes. You will use EC2 Image builder to put the AMIs into the new region, but not use image builder to LAUNCH them.

NEW QUESTION 10

- (Exam Topic 1)

A company has 50 AWS accounts that are members of an organization in AWS Organizations. Each account contains multiple VPCs. The company wants to use AWS Transit Gateway to establish connectivity between the VPCs in each member account. Each time a new member account is created, the company wants to automate the process of creating a new VPC and a transit gateway attachment.

Which combination of steps will meet these requirements? (Select TWO)

- A. From the management account, share the transit gateway with member accounts by using AWS Resource Access Manager
- B. From the management account, share the transit gateway with member accounts by using an AWS Organizations SCP
- C. Launch an AWS CloudFormation stack set from the management account that automatically creates a new VPC and a VPC transit gateway attachment in a member account
- D. Associate the attachment with the transit gateway in the management account by using the transit gateway ID.
- E. Launch an AWS CloudFormation stack set from the management account that automatically creates a new VPC and a peering transit gateway attachment in a member account
- F. Share the attachment with the transit gateway in the management account by using a transit gateway service-linked role.
- G. From the management account, share the transit gateway with member accounts by using AWS Service Catalog

Answer: AC

NEW QUESTION 10

- (Exam 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
- B. Include the necessary IAM roles for each administrator.
- C. Create the OrganizationAccountAccessPolicy IAM policy in each member account
- D. Connect the member accounts to the management account by using cross-account access.
- E. Create the OrganizationAccountAccessRole IAM role in each member account
- F. Grant permission to the management account to assume the IAM role.
- G. Create the OrganizationAccountAccessRole IAM role in the management account. Attach the Administrator Access AWS managed policy to the IAM role
- H. Assign the IAM role to the administrators in each member account.

Answer: C

NEW QUESTION 14

- (Exam Topic 1)

A solutions architect needs to advise a company on how to migrate its on-premises data processing application to the AWS Cloud. Currently, users upload input files through a web portal. The web server then stores the uploaded files on NAS and messages the processing server over a message queue. Each media file can take up to 1 hour to process. The company has determined that the number of media files awaiting processing is significantly higher during business hours, with the number of files rapidly declining after business hours.

What is the MOST cost-effective migration recommendation?

- A. Create a queue using Amazon SQS
- B. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the file
- C. Store the processed files in an Amazon S3 bucket.
- D. Create a queue using Amazon MQ
- E. Configure the existing web server to publish to the new queue. When there are messages in the queue, create a new Amazon EC2 instance to pull requests from the queue and process the file
- F. Store the processed files in Amazon EFS
- G. Shut down the EC2 instance after the task is complete.
- H. Create a queue using Amazon SNS
- I. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the file
- J. Store the processed files in Amazon EFS.
- K. Create a queue using Amazon SNS
- L. Configure the existing web server to publish to the new queue
- M. Use Amazon EC2 instances in an EC2 Auto Scaling group to pull requests from the queue and process the file
- N. Scale the EC2 instances based on the SQS queue length
- O. Store the processed files in an Amazon S3 bucket.

Answer: D

Explanation:

<https://aws.amazon.com/blogs/compute/operating-lambda-performance-optimization-part-1/>

NEW QUESTION 19

- (Exam Topic 1)

A company standardized its method of deploying applications to AWS using AWS CodePipeline and AWS CloudFormation. The applications are in Typescript and Python. The company has recently acquired another business that deploys applications to AWS using Python scripts.

Developers from the newly acquired company are hesitant to move their applications under CloudFormation because it would require them to learn a new domain-specific language and eliminate their access to language features, such as looping.

How can the acquired applications quickly be brought up to deployment standards while addressing the developers' concerns?

- A. Create CloudFormation templates and re-use parts of the Python scripts as instance user data
- B. Use the AWS Cloud Development Kit (AWS CDK) to deploy the application using these templates
- C. Incorporate the AWS CDK into CodePipeline and deploy the application to AWS using these templates.
- D. Use a third-party resource provisioning engine inside AWS CodeBuild to standardize the deployment processes of the existing and acquired company

- E. Orchestrate the CodeBuild job using CodePipeline.
- F. Standardize on AWS OpsWork
- G. Integrate OpsWorks with CodePipeline
- H. Have the developers create Chef recipes to deploy their applications on AWS.
- I. Define the AWS resources using Typescript or Python
- J. Use the AWS Cloud Development Kit (AWS CDK) to create CloudFormation templates from the developers' code, and use the AWS CDK to create CloudFormation stack
- K. Incorporate the AWS CDK as a CodeBuild job in CodePipeline.

Answer: D

NEW QUESTION 21

- (Exam Topic 1)

A company has many services running in its on-premises data center. The data center is connected to AWS using AWS Direct Connect (DX) and an IPSec VPN. The service data is sensitive and connectivity cannot traverse the internet. The company wants to expand into a new market segment and begin offering its services to other companies that are using AWS.

Which solution will meet these requirements?

- A. Create a VPC Endpoint Service that accepts TCP traffic, host it behind a Network Load Balancer, and make the service available over DX.
- B. Create a VPC Endpoint Service that accepts HTTP or HTTPS traffic, host it behind an Application Load Balancer, and make the service available over DX.
- C. Attach an internet gateway to the VPC
- D. and ensure that network access control and security group rules allow the relevant inbound and outbound traffic.
- E. Attach a NAT gateway to the VPC
- F. and ensure that network access control and security group rules allow the relevant inbound and outbound traffic.

Answer: A

NEW QUESTION 23

- (Exam Topic 1)

To abide by industry regulations, a solutions architect must design a solution that will store a company's critical data in multiple public AWS Regions, including in the United States, where the company's headquarters is located. The solutions architect is required to provide access to the data stored in AWS to the company's global WAN network. The security team mandates that no traffic accessing this data should traverse the public internet.

How should the solutions architect design a highly available solution that meets the requirements and is cost-effective?

- A. Establish AWS Direct Connect connections from the company headquarters to all AWS Regions in use. Use the company WAN to send traffic over to the headquarters and then to the respective DX connection to access the data.
- B. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection
- C. Use inter-region VPC peering to access the data in other AWS Regions.
- D. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection
- E. Use an AWS transit VPC solution to access data in other AWS Regions.
- F. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection
- G. Use Direct Connect Gateway to access data in other AWS Regions.

Answer: D

Explanation:

This feature also allows you to connect to any of the participating VPCs from any Direct Connect location, further reducing your costs for making using AWS services on a cross-region basis. <https://aws.amazon.com/blogs/aws/new-aws-direct-connect-gateway-inter-region-vpc-access/>
<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-g>

NEW QUESTION 25

- (Exam Topic 1)

A company is running a containerized application in the AWS Cloud. The application is running by using Amazon Elastic Container Service (Amazon ECS) on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group.

The company uses Amazon Elastic Container Registry (Amazon ECR) to store its container images. When a new image version is uploaded, the new image version receives a unique tag.

The company needs a solution that inspects new image versions for common vulnerabilities and exposures. The solution must automatically delete new image tags that have Critical or High severity findings. The solution also must notify the development team when such a deletion occurs.

Which solution meets these requirements?

- A. Configure scan on push on the repository
- B. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke an AWS Step Functions state machine when a scan is complete for images that have Critical or High severity findings. Use the Step Functions state machine to delete the image tag for those images and to notify the development team through Amazon Simple Notification Service (Amazon SNS)
- C. Configure scan on push on the repository. Configure scan results to be pushed to an Amazon Simple Queue Service (Amazon SQS) queue. Invoke an AWS Lambda function when a new message is added to the SQS queue. Use the Lambda function to delete the image tag for images that have Critical or High severity findings.
- D. Notify the development team by using Amazon Simple Email Service (Amazon SES).
- E. Schedule an AWS Lambda function to start a manual image scan every hour. Configure Amazon EventBridge (Amazon CloudWatch Events) to invoke another Lambda function when a scan is complete.
- F. Use the second Lambda function to delete the image tag for images that have Critical or High severity findings.
- G. Notify the development team by using Amazon Simple Notification Service (Amazon SNS)
- H. Configure periodic image scan on the repository. Configure scan results to be added to an Amazon Simple Queue Service (Amazon SQS) queue. Invoke an AWS Step Functions state machine when a new message is added to the SQS queue. Use the Step Functions state machine to delete the image tag for images that have Critical or High severity findings.
- I. Notify the development team by using Amazon Simple Email Service (Amazon SES).

Answer: C

NEW QUESTION 26

- (Exam Topic 1)

A company is building a hybrid solution between its existing on-premises systems and a new backend in AWS. The company has a management application to monitor the state of its current IT infrastructure and automate responses to issues. The company wants to incorporate the status of its consumed AWS services into the application. The application uses an HTTPS endpoint to receive updates.

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

- A. Configure AWS Systems Manager OpsCenter to ingest operational events from the on-premises systems. Retire the on-premises management application and adopt OpsCenter as the hub.
- B. Configure Amazon EventBridge (Amazon CloudWatch Events) to detect and react to changes for AWS Health events from the AWS Personal Health Dashboard. Configure the EventBridge (CloudWatch Events) event to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic and subscribe the topic to the HTTPS endpoint of the management application.
- C. Modify the on-premises management application to call the AWS Health API to poll for status events of AWS services.
- D. Configure Amazon EventBridge (Amazon CloudWatch Events) to detect and react to changes for AWS Health events from the AWS Service Health Dashboard. Configure the EventBridge (CloudWatch Events) event to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic and subscribe the topic to an HTTPS endpoint for the management application with a topic filter corresponding to the services being used.

Answer: A

Explanation:

ALB & NLB both supports IPs as targets. Questions is based on TCP traffic over VPN to on-premise. TCP is layer 4 and the , load balancer should be NLB. Then next questions does NLB supports loadbalancing traffic over VPN. And answer is YEs based on below URL.

<https://aws.amazon.com/about-aws/whats-new/2018/09/network-load-balancer-now-supports-aws-vpn/>

Target as IPs for NLB & ALB: <https://aws.amazon.com/elasticloadbalancing/faqs/?nc=sn&loc=5> <https://aws.amazon.com/elasticloadbalancing/application-load-balancer/>

NEW QUESTION 27

- (Exam Topic 1)

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

Which design should a solutions architect implement?

- A. Store the uploaded images in Amazon Elastic File System (Amazon EFS). Send application log information about each image to Amazon CloudWatch Log.
- B. Create a fleet of Amazon EC2 instances that use CloudWatch Logs to determine which images need to be processed.
- C. Place processed images in another directory in Amazon EFS.
- D. Enable Amazon CloudFront and configure the origin to be the one of the EC2 instances in the fleet.
- E. Store the uploaded images in an Amazon S3 bucket and configure an S3 bucket event notification to send a message to Amazon Simple Notification Service (Amazon SNS). Create a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) to pull messages from Amazon SNS to process the images and place them in Amazon Elastic File System (Amazon EFS). Use Amazon CloudWatch metrics for the SNS message volume to scale out EC2 instances.
- F. Enable Amazon CloudFront and configure the origin to be the ALB in front of the EC2 instances.
- G. Store the uploaded images in an Amazon S3 bucket and configure an S3 bucket event notification to send a message to the Amazon Simple Queue Service (Amazon SQS) queue.
- H. Create a fleet of Amazon EC2 instances to pull messages from the SQS queue to process the images and place them in another S3 bucket.
- I. Use Amazon CloudWatch metrics for queue depth to scale out EC2 instances.
- J. Enable Amazon CloudFront and configure the origin to be the S3 bucket that contains the processed images.
- K. Store the uploaded images on a shared Amazon Elastic Block Store (Amazon EBS) volume mounted to a fleet of Amazon EC2 Spot instances.
- L. Create an Amazon DynamoDB table that contains information about each uploaded image and whether it has been processed.
- M. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to scale out EC2 instances.
- N. Enable Amazon CloudFront and configure the origin to reference an Elastic Load Balancer in front of the fleet of EC2 instances.

Answer: C

NEW QUESTION 28

- (Exam Topic 1)

A company plans to migrate to AWS. A solutions architect uses AWS Application Discovery Service over the fleet and discovers that there is an Oracle data warehouse and several PostgreSQL databases. Which combination of migration patterns will reduce licensing costs and operational overhead? (Select TWO.)

- A. Lift and shift the Oracle data warehouse to Amazon EC2 using AWS DMS.
- B. Migrate the Oracle data warehouse to Amazon Redshift using AWS SCT and AWS QMS.
- C. Lift and shift the PostgreSQL databases to Amazon EC2 using AWS DMS.
- D. Migrate the PostgreSQL databases to Amazon RDS for PostgreSQL using AWS DMS.
- E. Migrate the Oracle data warehouse to an Amazon EMR managed cluster using AWS DMS.

Answer: BD

Explanation:

<https://aws.amazon.com/getting-started/hands-on/migrate-oracle-to-amazon-redshift/> <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-postgresql-database>

NEW QUESTION 31

- (Exam Topic 1)

A solutions architect is evaluating the reliability of a recently migrated application running on AWS. The front end is hosted on Amazon S3 and accelerated by Amazon CloudFront. The application layer is running in a stateless Docker container on an Amazon EC2 On-Demand Instance with an Elastic IP address. The storage layer is a MongoDB database running on an EC2 Reserved Instance in the same Availability Zone as the application layer.

Which combination of steps should the solutions architect take to eliminate single points of failure with minimal application code changes? (Select TWO.)

- A. Create a REST API in Amazon API Gateway and use AWS Lambda functions as the application layer.
- B. Create an Application Load Balancer and migrate the Docker container to AWS Fargate.
- C. Migrate the storage layer to Amazon DynamoDB.
- D. Migrate the storage layer to Amazon DocumentDB (with MongoDB compatibility).

E. Create an Application Load Balancer and move the storage layer to an EC2 Auto Scaling group.

Answer: BD

Explanation:

https://aws.amazon.com/documentdb/?nc1=h_ls

<https://aws.amazon.com/blogs/containers/using-alb-ingress-controller-with-amazon-eks-on-fargate/>

NEW QUESTION 33

- (Exam 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.
- B. Use Amazon EventBridge (Amazon CloudWatch Events) to schedule an AWS Lambda function to copy the EBS snapshots to the additional Regions.
- C. Set up AWS Backup to create the EBS snapshot.
- D. Configure Amazon S3 cross-Region replication to copy the EBS snapshots to the additional Regions.
- E. Schedule Amazon EC2 Image Builder to run once daily to create an AMI and copy the AMI to the additional Regions.

Answer: B

NEW QUESTION 34

- (Exam Topic 1)

A company with global offices has a single 1 Gbps AWS Direct Connect connection to a single AWS Region. The company's on-premises network uses the connection to communicate with the company's resources in the AWS Cloud. The connection has a single private virtual interface that connects to a single VPC. A solutions architect must implement a solution that adds a redundant Direct Connect connection in the same Region. The solution also must provide connectivity to other Regions through the same pair of Direct Connect connections as the company expands into other Regions.

Which solution meets these requirements?

- A. Provision a Direct Connect gateway.
- B. Delete the existing private virtual interface from the existing connection.
- C. Create the second Direct Connect connection.
- D. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the Direct Connect gateway.
- E. Connect the Direct Connect gateway to the single VPC.
- F. Keep the existing private virtual interface.
- G. Create the second Direct Connect connection.
- H. Create a new private virtual interface on the new connection, and connect the new private virtual interface to the single VPC.
- I. Keep the existing private virtual interface.
- J. Create the second Direct Connect connection.
- K. Create a new public virtual interface on the new connection, and connect the new public virtual interface to the single VPC.
- L. Provision a transit gateway.
- M. Delete the existing private virtual interface from the existing connection. Create the second Direct Connect connection.
- N. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the transit gateway.
- O. Associate the transit gateway with the single VPC.

Answer: A

Explanation:

A Direct Connect gateway is a globally available resource. You can create the Direct Connect gateway in any Region and access it from all other Regions. The following describe scenarios where you can use a Direct Connect gateway.

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html>

NEW QUESTION 39

- (Exam Topic 1)

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

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

Which solution will meet these requirements?

- A. Disassociate the Elastic IP address from the EC2 instance.
- B. Create an Amazon S3 bucket to be used for SFTP file hosting.
- C. Create an AWS Transfer Family server. Configure the Transfer Family server with a publicly accessible endpoint. Associate the SFTP Elastic IP address with the new endpoint. Point the Transfer Family server to the S3 bucket.
- D. Sync all files from the SFTP server to the S3 bucket.
- E. Disassociate the Elastic IP address from the EC2 instance.
- F. Create an Amazon S3 bucket to be used for SFTP file hosting.
- G. Create an AWS Transfer Family server.
- H. Configure the Transfer Family server with a VPC-hosted, internet-facing endpoint.
- I. Associate the SFTP Elastic IP address with the new endpoint.
- K. Attach the security group with customer IP addresses to the new endpoint.
- L. Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to the S3 bucket.
- M. Disassociate the Elastic IP address from the EC2 instance.
- N. Create a new Amazon Elastic File System (Amazon EFS) file system to be used for SFTP file hosting.
- O. Create an AWS Fargate task definition to run an SFTP server.
- P. Specify the EFS file system as a mount in the task definition.
- Q. Create a Fargate service by using the task definition, and place a Network Load Balancer (NLB) in front of the service. When configuring the service, attach the

- security group with customer IP addresses to the tasks that run the SFTP server
- R. Associate the Elastic IP address with the NLB
 - S. Sync all files from the SFTP server to the S3 bucket.
 - T. Disassociate the Elastic IP address from the EC2 instance
 - . Create a multi-attach Amazon Elastic Block Store (Amazon EBS) volume to be used for SFTP file hosting
 - . Create a Network Load Balancer (NLB) with the Elastic IP address attached
 - . Create an Auto Scaling group with EC2 instances that run an SFTP server. Define in the Auto Scaling group that instances that are launched should attach the new multi-attach EBS volume. Configure the Auto Scaling group to automatically add instances behind the NLB. Configure the Auto Scaling group to use the security group that allows customer IP addresses for the EC2 instances that the Auto Scaling group launches
 - . Sync all files from the SFTP server to the new multi-attach EBS volume.

Answer: B

Explanation:

<https://docs.aws.amazon.com/transfer/latest/userguide/create-server-in-vpc.html> <https://aws.amazon.com/premiumsupport/knowledge-center/aws-sftp-endpoint-type/>

NEW QUESTION 43

- (Exam Topic 1)

A company wants to migrate an application to Amazon EC2 from VMware Infrastructure that runs in an on-premises data center. A solutions architect must preserve the software and configuration settings during the migration. What should the solutions architect do to meet these requirements?

- A. Configure the AWS DataSync agent to start replicating the data store to Amazon FSx for Windows File Server. Use the SMB share to host the VMware data store
- B. Use VM Import/Export to move the VMs to Amazon EC2.
- C. Use the VMware vSphere client to export the application as an image in Open Virtualization Format (OVF) format. Create an Amazon S3 bucket to store the image in the destination AWS Region
- D. Create and apply an IAM role for VM Import. Use the AWS CLI to run the EC2 import command.
- E. Configure AWS Storage Gateway for files service to export a Common Internet File System (CIFS) share
- F. Create a backup copy to the shared folder
- G. Sign in to the AWS Management Console and create an AMI from the backup copy. Launch an EC2 instance that is based on the AMI.
- H. Create a managed-instance activation for a hybrid environment in AWS Systems Manager
- I. Download and install Systems Manager Agent on the on-premises VM. Register the VM with Systems Manager to be a managed instance. Use AWS Backup to create a snapshot of the VM and create an AMI
- J. Launch an EC2 instance that is based on the AMI

Answer: B

Explanation:

<https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html>

- Export an OVF Template
- Create / use an Amazon S3 bucket for storing the exported images. The bucket must be in the Region where you want to import your VMs.
- Create an IAM role named vmimport.
- You'll use AWS CLI to run the import commands. <https://aws.amazon.com/premiumsupport/knowledge-center/import-instances/>

NEW QUESTION 45

- (Exam Topic 1)

A company's AWS architecture currently uses access keys and secret access keys stored on each instance to access AWS services. Database credentials are hard-coded on each instance. SSH keys for command-line remote access are stored in a secured Amazon S3 bucket. The company has asked its solutions architect to improve the security posture of the architecture without adding operational complexity. Which combination of steps should the solutions architect take to accomplish this? (Select THREE.)

- A. Use Amazon EC2 instance profiles with an IAM role.
- B. Use AWS Secrets Manager to store access keys and secret access keys.
- C. Use AWS Systems Manager Parameter Store to store database credentials.
- D. Use a secure fleet of Amazon EC2 bastion hosts (or remote access).
- E. Use AWS KMS to store database credentials.
- F. Use AWS Systems Manager Session Manager for remote access

Answer: ACF

Explanation:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html>

NEW QUESTION 47

- (Exam Topic 1)

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

- A. Increase the backend processing timeout to 30 seconds to match the visibility timeout
- B. Reduce the visibility timeout of the queue to automatically remove the faulty message
- C. Configure a new SQS FIFO queue as a dead-letter queue to isolate the faulty messages
- D. Configure a new SQS standard queue as a dead-letter queue to isolate the faulty messages.

Answer: D

NEW QUESTION 52

- (Exam Topic 1)

A company has a policy that all Amazon EC2 instances that are running a database must exist within the same subnets in a shared VPC. Administrators must follow security compliance requirements and are not allowed to directly log in to the shared account. All company accounts are members of the same organization in AWS Organizations. The number of accounts will rapidly increase as the company grows.

A solutions architect uses AWS Resource Access Manager to create a resource share in the shared account. What is the MOST operationally efficient configuration to meet these requirements?

- A. Add the VPC to the resource share
- B. Add the account IDs as principals
- C. Add all subnets within the VPC to the resource share
- D. Add the account IDs as principals
- E. Add all subnets within the VPC to the resource share
- F. Add the organization as a principal.
- G. Add the VPC to the resource share
- H. Add the organization as a principal

Answer: C

Explanation:

<https://docs.aws.amazon.com/ram/latest/userguide/getting-started-sharing.html#getting-started-sharing-create> To restrict resource sharing to only principals in your organization, choose Allow sharing with principals in your organization only.

<https://docs.aws.amazon.com/ram/latest/userguide/ram-ug.pdf>

NEW QUESTION 56

- (Exam Topic 2)

A company is in the process of implementing AWS Organizations to constrain its developers to use only Amazon EC2, Amazon S3, and Amazon DynamoDB. The developers' account resides in a dedicated organizational unit (OU). The solutions architect has implemented the following SCP on the developers' account:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowEC2",
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    },
    {
      "Sid": "AllowDynamoDB",
      "Effect": "Allow",
      "Action": "dynamodb:*",
      "Resource": "*"
    },
    {
      "Sid": "AllowS3",
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

When this policy is deployed, IAM users in the developers' account are still able to use AWS services that are not listed in the policy. What should the solutions architect do to eliminate the developers' ability to use services outside the scope of this policy?

- A. Create an explicit deny statement for each AWS service that should be constrained
- B. Remove the Full AWS Access SCP from the developer account's OU
- C. Modify the Full AWS Access SCP to explicitly deny all services
- D. Add an explicit deny statement using a wildcard to the end of the SCP

Answer: B

NEW QUESTION 57

- (Exam Topic 2)

A company is migrating its marketing website and content management system from an on-premises data center to AWS. The company wants the AWS application to be deployed in a VPC with Amazon EC2 instances used for the web servers and an Amazon RDS instance for the database.

The company has a runbook document that describes the installation process of the on-premises system. The company would like to base the AWS system on the processes referenced in the runbook document. The runbook document describes the installation and configuration of the operating systems, network settings, the website, and content management system software on the servers. After the migration is complete, the company wants to be able to make changes quickly to take advantage of other AWS features.

How can the application and environment be deployed and automated in AWS, while allowing for future changes?

- A. Update the runbook to describe how to create the VPC
- B. Deploy the EC2 instances and the RDS instance for the application by using the AWS Console. Make sure that the rest of the steps in the runbook are updated to reflect any changes that may come from the AWS migration.
- C. Write a Python script that uses the AWS API to create the VPC
- D. Deploy the EC2 instances and the RDS instance for the application. Write shell scripts that implement the rest of the steps in the runbook. Have the Python script copy and run the shell scripts on the newly created instances to complete the installation.
- E. Write an AWS CloudFormation template that creates the VPC, the EC2 instances, and the RDS instance for the application. Ensure that the rest of the steps in the runbook are updated to reflect any changes that may come from the AWS migration.

F. Write an AWS CloudFormation template that creates the VPC the EC2 instances, and the RDS instance for the application Include EC2 user data in the AWS Cloud Formation template to install and configure the software.

Answer: D

NEW QUESTION 62

- (Exam Topic 2)

A company's solution architect is designing a disaster recovery (DR) solution for an application that runs on AWS. The application uses PostgreSQL 11.7 as its database. The company has an RPO of 30 seconds. The solution architect must design a DR solution with the primary database in the us-east-1 Region and the database in the us-west-2 Region.

What should the solution architect do to meet these requirements with minimum application change?

- A. Migrate the database to Amazon RDS for PostgreSQL in us-east-1. Set up a read replica in us-west-2. Set the managed RPO for the RDS database to 30 seconds.
- B. Migrate the database to Amazon RDS for PostgreSQL in us-east-1. Set up a standby replica in an Availability Zone in us-west-2, Set the managed RPO for the RDS database to 30 seconds.
- C. Migrate the database to an Amazon Aurora PostgreSQL global database with the primary Region as us-east-1 and the secondary Region as us-west-2. Set the managed RPO for the Aurora database to 30 seconds.
- D. Migrate the database to Amazon DynamoDB in us-east-1. Set up global tables with replica tables that are created in us-west-2.

Answer: A

NEW QUESTION 67

- (Exam Topic 2)

A company wants to migrate its workloads from on-premises to AWS. The workloads run on Linux and Windows. The company has a large on-premises infrastructure that consists of physical machines and VMs that host numerous applications.

The company must capture details about the system configuration, system performance, running processes and network connections of its on-premises servers. The company also must divide the on-premises applications into groups for AWS migrations. The company needs recommendations for Amazon EC2 instance types so that the company can run its workloads on AWS in the most cost-effective manner.

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

- A. Assess the existing applications by installing AWS Application Discovery Agent on the physical machines and VMs.
- B. Assess the existing applications by installing AWS Systems Manager Agent on the physical machines and VMs
- C. Group servers into applications for migration by using AWS Systems Manager Application Manager.
- D. Group servers into applications for migration by using AWS Migration Hub.
- E. Generate recommended instance types and associated costs by using AWS Migration Hub.
- F. Import data about server sizes into AWS Trusted Advisor
- G. Follow the recommendations for cost optimization.

Answer: BDF

NEW QUESTION 70

- (Exam Topic 2)

A company is running a three-tier web application in an on-premises data center. The frontend is served by an Apache web server, the middle tier is a monolithic Java application, and the storage tier is a PostgreSQL database.

During a recent marketing promotion, customers could not place orders through the application because the application crashed. An analysis showed that all three tiers were overloaded. The application became unresponsive, and the database reached its capacity limit because of read operations. The company already has several similar promotions scheduled in the near future.

A solutions architect must develop a plan for migration to AWS to resolve these issues. The solution must maximize scalability and must minimize operational effort.

Which combination of steps will meet these requirements? (Select THREE.)

- A. Refactor the frontend so that static assets can be hosted on Amazon S3. Use Amazon CloudFront to serve the frontend to customer
- B. Connect the frontend to the Java application.
- C. Rehost the Apache web server of the frontend on Amazon EC2 instances that are in an Auto Scaling group
- D. Use a load balancer in front of the Auto Scaling group
- E. Use Amazon Elastic File System (Amazon EFS) to host the static assets that the Apache web server needs.
- F. Rehost the Java application in an AWS Elastic Beanstalk environment that includes auto scaling.
- G. Refactor the Java application
- H. Develop a Docker container to run the Java application
- I. Use AWS Fargate to host the container.
- J. Use AWS Database Migration Service (AWS DMS) to replatform the PostgreSQL database to an Amazon Aurora PostgreSQL database
- K. Use Aurora Auto Scaling for read replicas.
- L. Rehost the PostgreSQL database on an Amazon EC2 instance that has twice as much memory as the on-premises server.

Answer: BCF

NEW QUESTION 72

- (Exam Topic 2)

A company has a new security policy. The policy requires the company to log any event that retrieves data from Amazon S3 buckets. The company must save these audit logs in a dedicated S3 bucket. The company created the audit logs S3 bucket in an AWS account that is designated for centralized logging. The S3 bucket has a bucket policy that allows write-only cross-account access. A solutions architect must ensure that all S3 object-level access is being logged for current S3 buckets and future S3 buckets. Which solution will meet these requirements?

- A. Enable server access logging for all current S3 buckets
- B. Use the audit logs S3 bucket as a destination for audit logs
- C. Enable replication between all current S3 buckets and the audit logs S3 bucket. Enable S3 Versioning in the audit logs S3 bucket
- D. Configure S3 Event Notifications for all current S3 buckets to invoke an AWS Lambda function every time objects are accessed. Store Lambda logs in the audit logs S3 bucket.

- E. Enable AWS CloudTrail
- F. and use the audit logs S3 bucket to store logs Enable data event logging for S3 event sources, current S3 buckets, and future S3 buckets.

Answer: D

NEW QUESTION 73

- (Exam Topic 2)

A company uses multiple AWS accounts in a single AWS Region A solutions architect is designing a solution to consolidate logs generated by Elastic Load Balancers (ELBs) in the AppDev, AppTest and AppProd accounts. The logs should be stored in an existing Amazon S3 bucket named s3-elb-logs in the central AWS account. The central account is used for log consolidation only and does not have ELBs deployed ELB logs must be encrypted at rest Which combination of steps should the solutions architect take to build the solution" (Select TWO)

- A. Update the S3 bucket policy for the s3-elb-logs bucket to allow the s3 PutBucketLogging action for the central AWS account ID
- B. Update the S3 bucket policy for the s3-elb-logs bucket to allow the s3 PutObject and s3 DeleteObject actions for the AppDev AppTest and AppProd account IDs
- C. Update the S3 bucket policy for the s3-elb-logs bucket to allow the s3 PutObject action for the AppDev AppTest and AppProd account IDs
- D. Enable access logging for the ELB
- E. Set the S3 location to the s3-elb-logs bucket
- F. Enable Amazon S3 default encryption using server-side encryption with S3 managed encryption keys (SSE-S3) for the s3-elb-logs S3 bucket

Answer: AE

NEW QUESTION 74

- (Exam Topic 2)

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
- C. 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
- D. Update the existing VPC
- E. 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
- F. 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.

Answer: C

NEW QUESTION 76

- (Exam Topic 2)

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

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

- A. Use Tag Editor to tag existing resources Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources
- B. Use an AWS Config rule to alert the finance team of untagged resources Create a centralized AWS Lambda based solution to tag untagged RDS databases and DynamoDB resources every hour using a cross-account role.
- C. Use Tag Editor to tag existing resources Create cost allocation tags to define the cost center and project ID Use SCPs to restrict resource creation that do not have the cost center and project ID on the resource.
- D. Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources Update existing federated roles to restrict privileges to provision resources that do not include the cost center and project ID on the resource

Answer: B

NEW QUESTION 80

- (Exam Topic 2)

A solutions architect needs to provide AWS Cost and Usage Report data from a company's AWS Organizations management account The company already has an Amazon S3 bucket to store the reports The reports must be automatically ingested into a database that can be visualized with other tools.

Which combination of steps should the solutions architect take to meet these requirements? (Select THREE)

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that a new object creation in the S3 bucket will trigger
- B. Create an AWS Cost and Usage Report configuration to deliver the data into the S3 bucket
- C. Configure an AWS Glue crawler that a new object creation in the S3 bucket will trigger.
- D. Create an AWS Lambda function that a new object creation in the S3 bucket will trigger
- E. Create an AWS Glue crawler that the AWS Lambda function will trigger to crawl objects in the S3 bucket
- F. Create an AWS Glue crawler that the Amazon EventBridge (Amazon CloudWatch Events) rule will trigger to crawl objects in the S3 bucket

Answer: BDF

NEW QUESTION 84

- (Exam Topic 2)

A solutions architect is migrating an existing workload to AWS Fargate. The task can only run in a private subnet within the VPC where there is no direct connectivity from outside the system to the application. When the Fargate task is launched, the task fails with the following error:

```
CannotPullContainerError: API error (500): Get https://111122223333.dkr.ecr.us-east-1.amazonaws.com/v2/: net/http: request canceled  
While waiting for connection
```

How should the solutions architect correct this error?

- A. Ensure the task is set to ENABLED for the auto-assign public IP setting when launching the task
- B. Ensure the task is set to DISABLED (or the auto-assign public IP setting when launching the task) Configure a NAT gateway in the public subnet in the VPC to route requests to the internet
- C. Ensure the task is set to DISABLED for the auto-assign public IP setting when launching the task. Configure a NAT gateway in the private subnet in the VPC to route requests to the internet
- D. Ensure the network mode is set to bridge in the Fargate task definition

Answer: B

NEW QUESTION 87

- (Exam Topic 2)

A company's AWS architecture currently uses access keys and secret access keys stored on each instance to access AWS services. Database credentials are hard-coded on each instance. SSH keys for command-line remote access are stored in a secured Amazon S3 bucket. The company has asked its solutions architect to improve the security posture of the architecture without adding operational complexity.

Which combination of steps should the solutions architect take to accomplish this? (Select THREE.)

- A. Use Amazon EC2 instance profiles with an IAM role
- B. Use AWS Secrets Manager to store access keys and secret access keys
- C. Use AWS Systems Manager Parameter Store to store database credentials
- D. Use a secure fleet of Amazon EC2 bastion hosts for remote access
- E. Use AWS KMS to store database credentials
- F. Use AWS Systems Manager Session Manager for remote access

Answer: ACF

NEW QUESTION 91

- (Exam Topic 2)

A company's CI/CO 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.
- E. If there are any issues, push another code update.

Answer: B

NEW QUESTION 94

- (Exam Topic 2)

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

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

- A. Set the S3 access point resource policy to deny the s3:CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.
- B. Create an SCP at the root level in the organization to deny the s3:CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.
- C. Use AWS CloudFormation StackSets to create a new IAM policy in each AWS account that allows the s3:CreateAccessPoint action only if the s3:AccessPointNetworkOrigin condition key evaluates to VPC.
- D. Set the S3 bucket policy to deny the s3:CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.

Answer: A

NEW QUESTION 99

- (Exam Topic 2)

A company's site reliability engineer is performing a review of Amazon FSx for Windows File Server deployments within an account that the company acquired. Company policy states that all Amazon FSx file systems must be configured to be highly available across Availability Zones.

During the review, the site reliability engineer discovers that one of the Amazon FSx file systems used a deployment type of Single-AZ 2. A solutions architect needs to minimize downtime while aligning this Amazon FSx file system with company policy.

What should the solutions architect do to meet these requirements?

- A. Reconfigure the deployment type to Multi-AZ for this Amazon FSx file system

- B. Create a new Amazon FSx file system with a deployment type of Multi-AZ
- C. Use AWS DataSync to transfer data to the new Amazon FSx file system
- D. Point users to the new location
- E. Create a second Amazon FSx file system with a deployment type of Single-AZ 2. Use AWS DataSync to keep the data in sync
- F. Switch users to the second Amazon FSx file system in the event of failure
- G. Use the AWS Management Console to take a backup of the Amazon FSx file system. Create a new Amazon FSx file system with a deployment type of Multi-AZ. Restore the backup to the new Amazon FSx file system
- H. Point users to the new location.

Answer: B

NEW QUESTION 104

- (Exam Topic 2)

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? (Select 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

Answer: ADF

NEW QUESTION 106

- (Exam Topic 2)

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? (Select THREE.)

- A. Deploy two firewall appliances into the shared services VPC
- B. each in a separate Availability Zone
- C. 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.
- D. Create a new Gateway Load Balancer in the shared services VPC. Create a new target group, and attach it to the new Gateway Load Balancer. Add each of the firewall appliance instances to the target group.
- E. Create a VPC interface endpoint. Add a route to the route table in the shared services VPC.
- F. Designate the new endpoint as the next hop for traffic that enters the shared services VPC from other VPCs.
- G. Deploy two firewall appliances into the shared services VPC
- H. each in the same Availability Zone

Answer: AC

NEW QUESTION 111

- (Exam Topic 2)

A company is using multiple AWS accounts. The DNS records are stored in a private hosted zone for Amazon Route 53 in Account A. The company's applications and databases are running in Account B.

A solutions architect will deploy a two-tier application in a new VPC. To simplify the configuration, the db.example.com CNAME record set for the Amazon RDS endpoint was created in a private hosted zone for Amazon Route 53.

During deployment, the application failed to start. Troubleshooting revealed that db.example.com is not resolvable on the Amazon EC2 instance. The solutions architect confirmed that the record set was created correctly in Route 53.

Which combination of steps should the solutions architect take to resolve this issue? (Select TWO.)

- A. Deploy the database on a separate EC2 instance in the new VPC. Create a record set for the instance's private IP in the private hosted zone.
- B. Use SSH to connect to the application tier EC2 instance. Add an RDS endpoint IP address to the /etc/resolv.conf file.
- C. Create an authorization to associate the private hosted zone in Account A with the new VPC in Account B.
- D. Create a private hosted zone for the example.com domain in Account B. Configure Route 53 replication between AWS accounts.
- E. Associate a new VPC in Account B with a hosted zone in Account A.
- F. Delete the association authorization in Account A.

Answer: CE

NEW QUESTION 115

- (Exam Topic 2)

A company's solutions architect is reviewing a web application that runs on AWS. The application references static assets in an Amazon S3 bucket in the us-east-1 Region. The company needs resiliency across multiple AWS Regions. The company already has created an S3 bucket in a second Region.

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

- A. Configure the application to write each object to both S3 buckets
- B. Set up an Amazon Route 53 public hosted zone with a record set by using a weighted routing policy for each S3 bucket
- C. Configure the application to reference the objects by using the Route 53 DNS name.
- D. Create an AWS Lambda function to copy objects from the S3 bucket in us-east-1 to the S3 bucket in the second Region
- E. Invoke the Lambda function each time an object is written to the S3 bucket in us-east-1. Set up an Amazon CloudFront distribution with an origin group that

contains the two S3 buckets as origins.

F. Configure replication on the S3 bucket in us-east-1 to replicate objects to the S3 bucket in the second Region Set up an Amazon CloudFront distribution with an origin group that contains the two S3 buckets as origins.

G. Configure replication on the S3 bucket in us-east-1 to replicate objects to the S3 bucket in the second Region

H. If failover is required, update the application code to load S3 objects from the S3 bucket in the second Region.

Answer: D

NEW QUESTION 119

- (Exam Topic 2)

A company runs its application in the eu-west-1 Region and has one account for each of its environments development, testing, and production All the environments are running 24 hours a day 7 days a week by using stateful Amazon EC2 instances and Amazon RDS for MySQL databases The databases are between 500 GB and 800 GB in size

The development team and testing team work on business days during business hours, but the production environment operates 24 hours a day. 7 days a week.

The company wants to reduce costs AH resources are tagged with an environment tag with either development, testing, or production as the key.

What should a solutions architect do to reduce costs with the LEAST operational effort?

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs once every day Configure the rule to invoke one AWS Lambda function that starts or stops instances based on the tag day and time.

B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs every business day in the evening

C. Configure the rule to invoke an AWS Lambda function that stops instances based on the tag Create a second EventBridge (CloudWatch Events) rule that runs every business day in the morning Configure the second rule to invoke another Lambda function that starts instances based on the tag

D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs every business day in the evening Configure the rule to invoke an AWS Lambda function that terminates instances based on the tag Create a second EventBridge (CloudWatch Events) rule that runs every business day in the morning Configure the second rule to invoke another Lambda function that restores the instances from their last backup based on the tag.

E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs every hour Configure the rule to invoke one AWS Lambda function that terminates or restores instances from theirbased on the ta

F. day, and time

Answer: C

NEW QUESTION 120

- (Exam Topic 2)

A company is hosting a three-tier web application in an on-premises environment. Due to a recent surge in traffic that resulted in downtime and a significant financial impact, company management has ordered that the application be moved to AWS. The application is written in .NET and has a dependency on a MySQL database A solutions architect must design a scalable and highly available solution to meet the demand of 200000 daily users.

Which steps should the solutions architect take to design an appropriate solution?

A. Use AWS Elastic Beanstalk to create a new application with a web server environment and an Amazon RDS MySQL Multi-AZ DB instance The environment should launch a Network Load Balancer (NLB) in front of an Amazon EC2 Auto Scaling group in multiple Availability Zones Use an Amazon Route 53 alias record to route traffic from the company's domain to the NLB.

B. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon EC2 Auto Scaling group spanning three Availability Zones

C. The stack should launch a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a Retain deletion policy

D. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB

E. Use AWS Elastic Beanstalk to create an automatically scaling web server environment that spans two separate Regions with an Application Load Balancer (ALB) in each Region

F. Create a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a cross-Region read replica Use Amazon Route 53 with a geoproximity routing policy to route traffic between the two Regions.

G. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon ECS cluster of Spot Instances spanning three Availability Zones The stack should launch an Amazon RDS MySQL DB instance with a Snapshot deletion policy Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB

Answer: B

NEW QUESTION 125

- (Exam Topic 2)

A company's solution architect is designing a disaster recovery (DR) solution for an application that runs on AWS. The application uses PostgreSQL 11.7 as its database. The company has an RPO of 30 seconds. The solutions architect must design a DR solution with the primary database in the us-east-1 Region and the database in the us-west-2 Region.

What should the solution architect do to meet these requirements with minimum application change?

A. Migrate the database to Amazon RDS for PostgreSQL in us-east-1. Set up a read replica in us-west-2. Set the managed RPO for the RDS database to 30 seconds.

B. Migrate the database to Amazon for PostgreSQL in us-east-1. Set up a standby replica in an Availability Zone in us-west-2, Set the managed RPO for the RDS database to 30 seconds.

C. Migrate the database to an Amazon Aurora PostgreSQL global database with the primary Region as us-east-1 and the secondary Region as us-west-2. Set the managed RPO for the Aurora database to 30 seconds.

D. Migrate the database to Amazon DynamoDB in us-east-1. Set up global tables with replica tables that are created in us-west-2.

Answer: A

NEW QUESTION 126

- (Exam Topic 2)

A company used Amazon EC2 instances to deploy a web fleet to host a blog site The EC2 instances are behind an Application Load Balancer (ALB) and are configured in an Auto Scaling group The web application stores all blog content on an Amazon EFS volume.

The company recently added a feature for bloggers to add video to their posts, attracting 10 times the previous user traffic At peak times of day, users report buffering and timeout issues while attempting to reach the site or watch videos

Which is the MOST cost-efficient and scalable deployment that will resolve the issues for users?

- A. Reconfigure Amazon EFS to enable maximum I/O.
- B. Update the Nginx site to use instance store volumes for storage.
- C. Copy the site contents to the volumes at launch and to Amazon S3 at shutdown.
- D. Configure an Amazon CloudFront distribution.
- E. Point the distribution to an S3 bucket, and migrate the videos from EFS to Amazon S3.
- F. Set up an Amazon CloudFront distribution for all site contents, and point the distribution at the ALB.

Answer: C

NEW QUESTION 131

- (Exam Topic 2)

A company is using multiple AWS accounts. The company has a shared services account and several other accounts (or different projects). A team has a VPC in a project account. The team wants to connect this VPC to a corporate network through an AWS Direct Connect gateway that exists in the shared services account. The team wants to automatically perform a virtual private gateway association with the Direct Connect gateway by using an already-tested AWS Lambda function while deploying its VPC networking stack. The Lambda function code can assume a role by using AWS Security Token Service (AWS STS). The team is using AWS CloudFormation to deploy its infrastructure.

- A. Deploy the Lambda function to the project account.
- B. Update the Lambda function's IAM role with the `directconnect:*` permission.
- C. Create a cross-account IAM role in the shared services account that grants the Lambda function the `directconnect:*` permission.
- D. Add the `sts:AssumeRole` permission to the IAM role that is associated with the Lambda function in the shared services account.
- E. Add a custom resource to the CloudFormation networking stack that references the Lambda function in the project account.
- F. Deploy the Lambda function that is performing the association to the shared services account.
- G. Update the Lambda function's IAM role with the `directconnect:` permission.
- H. Create a cross-account IAM role in the shared services account that grants the `sts: Assume Role` permission to the Lambda function with the `directconnect:` permission acting as a resource.
- I. Add the `sts AssumeRole` permission with this cross-account IAM role as a resource to the IAM role that belongs to the Lambda function in the project account.
- J. Add a custom resource to the CloudFormation networking stack that references the Lambda function in the shared services account.

Answer: BCE

NEW QUESTION 136

- (Exam Topic 2)

A company has developed a new release of a popular video game and wants to make it available for public download. The new release package is approximately 5 GB in size. The company provides downloads for existing releases from a Linux-based, publicly facing FTP site hosted in an on-premises data center. The company expects the new release will be downloaded by users worldwide. The company wants a solution that provides improved download performance and low transfer costs, regardless of a user's location. Which solutions will meet these requirements?

- A. Store the game files on Amazon EBS volumes mounted on Amazon EC2 instances within an Auto Scaling group. Configure an FTP service on the EC2 instances. Use an Application Load Balancer in front of the Auto Scaling group.
- B. Publish the game download URL for users to download the package.
- C. Store the game files on Amazon EFS volumes that are attached to Amazon EC2 instances within an Auto Scaling group. Configure an FTP service on each of the EC2 instances. Use an Application Load Balancer in front of the Auto Scaling group. Publish the game download URL for users to download the package.
- D. Configure Amazon Route 53 and an Amazon S3 bucket for website hosting. Upload the game files to the S3 bucket. Use Amazon CloudFront for the website. Publish the game download URL for users to download the package.
- E. Configure Amazon Route 53 and an Amazon S3 bucket for website hosting. Upload the game files to the S3 bucket. Set Requester Pays for the S3 bucket. Publish the game download URL for users to download the package.

Answer: C

NEW QUESTION 141

- (Exam Topic 2)

A solutions architect is designing a multi-account structure that has 10 existing accounts. The design must meet the following requirements:

- Consolidate all accounts into one organization
- Allow full access to the Amazon EC2 service from the management account and the secondary accounts
- Minimize the effort required to add additional secondary accounts

Which combination of steps should be included in the solution? (Select TWO)

- A. Create an organization from the management account. Send invitations to the secondary accounts from the management account. Accept the invitations and create an OU.
- B. Create an organization from the management account.
- C. Send a join request to the management account from each secondary account. Accept the requests and create an OU.
- D. Create a VPC peering connection between the management account and the secondary accounts. Accept the request for the VPC peering connection.
- E. Create a service control policy (SCP) that enables full EC2 access, and attach the policy to the OU.
- F. Create a full EC2 access policy and map the policy to a role in each account. Trust every other account to assume the role.

Answer: AE

NEW QUESTION 143

- (Exam Topic 2)

A media company has a 30-TB repository of digital news videos. These videos are stored on tape in an on-premises tape library and referenced by a Media Asset Management (MAM) system. The company wants to enrich the metadata for these videos in an automated fashion and put them into a searchable catalog by using a MAM feature. The company must be able to search based on information in the video such as objects, scenery, items, or people's faces. A catalog is available that contains faces of people who have appeared in the videos that include an image of each person. The company would like to migrate these videos to AWS. The company has a high-speed AWS Direct Connect connection with AWS and would like to move the MAM solution video content directly from its current file system. How can these requirements be met by using the LEAST amount of ongoing management overhead and causing MINIMAL disruption to the existing system?

- A. Set up an AWS Storage Gateway file gateway appliance on-premise
- B. Use the MAM solution to extract the videos from the current archive and push them into the file gateway Use the catalog of faces to build a collection in Amazon Rekognition Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Rekognition pull the video from the Amazon S3 files backing the file gateway, retrieve the required metadata and push the metadata into the MAM solution
- C. Set up an AWS Storage Gateway tape gateway appliance on-premises Use the MAM solution to extract the videos from the current archive and push them into the tape gateway Use the catalog of faces to build a collection in Amazon Rekognition Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Amazon Rekognition process the video in the tape gateway retrieve the required metadata, and push the metadata into the MAM solution
- D. Configure a video ingestion stream by using Amazon Kinesis Video Streams Use the catalog of faces to build a collection in Amazon Rekognition Stream the videos from the MAM solution into Kinesis Video Streams Configure Amazon Rekognition to process the streamed videos Then, use a stream consumer to retrieve the required metadata and push the metadata into the MAM solution Configure the stream to store the videos in Amazon S3
- E. Set up an Amazon EC2 instance that runs the OpenCV libraries Copy the videos, images, and facecatalog from the on-premises library into an Amazon EBS volumemounted on this EC2 instance Process the videos to retrieve the required metadata, and push the metadata into the MAM solution, while also copying the video files to an Amazon S3 bucket

Answer: C

NEW QUESTION 145

- (Exam Topic 2)

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 T.he 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 proxyConfigure 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 s 3: Putobject permissions in the bucket policy Have the browser interface upload objects using the CloudFront distribution

Answer: D

NEW QUESTION 150

- (Exam Topic 2)

A company has several applications running in an on-premises data center. The data center runs a mix of Windows and Linux VMs managed by VMware vCenter. A solutions architect needs to create a plan to migrate the applications to AWS However, the solutions architect discovers that the documentation for the applications is not up to date and that there are no complete infrastructure diagrams The company's developers lack time to discuss their applications and current usage with the solutions architect

What should the solutions architect do to gather the required information?

- A. Deploy the AWS Server Migration Service (AWS SMS) connector using the OVA image on the VMware cluster to collect configuration and utilization data from the VMs
- B. Use the AWS Migration Portfolio Assessment (MPA) tool to connect to each of the VMs to collect the configuration and utilization data.
- C. Install the AWS Application Discovery Service on each of the VMs to collect the configuration and utilization data
- D. Register the on-premises VMs with the AWS Migration Hub to collect configuration and utilization data

Answer: A

NEW QUESTION 153

- (Exam Topic 2)

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

The solutions architect must review the architecture and suggest a solution to minimize the compute costs Which solution should the solutions architect recommend to meet these requirements?

- A. Launch all task, master, and core nodes on Spot Instances in an instance flee
- B. Terminate the cluster, including all instances, when the processing is completed.
- C. Launch the master and core nodes on On-Demand Instance
- D. Launch the task nodes on Spot Instances In an instance flee
- E. Terminate the cluster, including all instances, when the processing is complete
- F. Purchase Compute Savings Plans to cover the On-Demand Instance usage.
- G. Continue to launch all nodes on On-Demand Instance
- H. Terminate the cluste
- I. Including all instances, when the processing is complete
- J. Purchase Compute Savings Plans to cover the On-Demand Instance usage.
- K. Launch the master and core nodes on On-Demand Instance
- L. Launch the task nodes on Spot Instances In an instance flee
- M. Terminate only the task node Instances when the processing is completed Purchase Compute Savings Plans to cover the On-Demand Instance usage.

Answer: B

NEW QUESTION 157

- (Exam Topic 2)

A company has an application that runs on Amazon EC2 instances in an Amazon EC2 Auto Scaling group. The company uses AWS CodePipeline to deploy the application. The instances that run in the Auto Scaling group are constantly changing because of scaling events. When the company deploys new application code versions the company installs the AWS CodeDeploy agent on any new target EC2 instances and associates the instances with the CodeDeploy deployment group. The application is set to go live within the next 24 hours. What should a solutions architect recommend to automate the application deployment process with the LEAST amount of operational overhead?

- A. Configure Amazon EventBridge (Amazon CloudWatch Events) to invoke an AWS Lambda function when a new EC2 instance is launched into the Auto Scaling group.
- B. Code the Lambda function to associate the EC2 instances with the CodeDeploy deployment group.
- C. Write a script to suspend Amazon EC2 Auto Scaling operations before the deployment of new code. When the deployment is complete, create a new AMI and configure the Auto Scaling group's launch template to use the new AMI for new launches.
- D. Resume Amazon EC2 Auto Scaling operations.
- E. Create a new AWS CodeBuild project that creates a new AMI that contains the new code. Configure CodeBuild to update the Auto Scaling group's launch template to the new AMI. Run an Amazon EC2 Auto Scaling instance refresh operation.
- F. Create a new AMI that has the CodeDeploy agent installed. Configure the Auto Scaling group's launch template to use the new AMI. Associate the CodeDeploy deployment group with the Auto Scaling group instead of the EC2 instances.

Answer: C

NEW QUESTION 160

- (Exam Topic 2)

A company wants to improve cost awareness for its Amazon EMR platform. The company has allocated budgets for each team's Amazon EMR usage. When a budgetary threshold is reached, a notification should be sent by email to the budget office's distribution list. Teams should be able to view their EMR cluster expenses to date. A solutions architect needs to create a solution that ensures this policy is proactively and centrally enforced in a multi-account environment. Which combination of steps should the solutions architect take to meet these requirements? (Select TWO.)

- A. Update the AWS CloudFormation template to include the AWS Budgets Budget resource with the NotificationsWithSubscribers property.
- B. Implement Amazon CloudWatch dashboards for Amazon EMR usage.
- C. Create an EMR bootstrap action that runs at startup that calls the Cost Explorer API to set the budget on the cluster with the GetCostForecast and NotificationsWithSubscribers actions.
- D. Create an AWS Service Catalog portfolio for each team.
- E. Add each team's Amazon EMR cluster as an AWS CloudFormation template to their Service Catalog portfolio as a Product.
- F. Create an Amazon CloudWatch metric for billing. Create a custom alert when costs exceed the budgetary threshold.

Answer: BE

NEW QUESTION 161

- (Exam Topic 2)

A company is using an Amazon EMR cluster to run its big data jobs. The cluster's jobs are invoked by AWS Step Functions Express Workflows that consume various Amazon Simple Queue Service (Amazon SQS) queues. The workload of this solution is variable and unpredictable. Amazon CloudWatch metrics show that the cluster's peak utilization is only 25% at times and that the cluster sits idle the rest of the time. A solutions architect must optimize the costs of the cluster without negatively impacting the time it takes to run the various jobs. What is the MOST cost-effective solution that meets these requirements?

- A. Modify the EMR cluster by turning on automatic scaling of the core nodes and task nodes with a custom policy that is based on cluster utilization. Purchase Reserved Instance capacity to cover the master node.
- B. Modify the EMR cluster to use an instance fleet of Dedicated On-Demand Instances for the master node and core nodes, and to use Spot Instances for the task nodes.
- C. Define target capacity for each node type to cover the load.
- D. Purchase Reserved Instances for the master node and core nodes. Terminate all existing task nodes in the EMR cluster.
- E. Modify the EMR cluster to use capacity-optimized Spot Instances and a diversified task fleet.
- F. Define target capacity for each node type with a mix of On-Demand Instances and Spot Instances.

Answer: B

NEW QUESTION 163

- (Exam Topic 2)

A company is using AWS CloudFormation to deploy its infrastructure. The company is concerned that if a production CloudFormation stack is deleted, important data stored in Amazon RDS databases or Amazon EBS volumes might also be deleted. How can the company prevent users from accidentally deleting data in this way?

- A. Modify the CloudFormation templates to add a DeletionPolicy attribute to RDS and EBS resources.
- B. Configure a stack policy that disallows the deletion of RDS and EBS resources.
- C. Modify IAM policies to deny deleting RDS and EBS resources that are tagged with an "aws:cloudformation:stack-name" tag.
- D. Use AWS Config rules to prevent deleting RDS and EBS resources.

Answer: A

NEW QUESTION 168

- (Exam Topic 2)

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 duster by using an elastic resize operation when the duster's CPU metrics in Amazon CloudWatch leach 80%.

D. Turn on the Concurrency Scaling feature for the Amazon Redshift duster

Answer: D

NEW QUESTION 172

- (Exam Topic 2)

A retail company needs to provide a series of data files to another company, which is its business partner. These files are saved in an Amazon S3 bucket under Account A, which belongs to the retail company. The business partner company wants one of its IAM users User_DataProcessor to access the files from its own AWS account (Account B)

Which combination of steps must the companies take so that User_DataProcessor can access the S3 bucket successfully? (Select TWO.)

A. Turn on the cross-origin resource sharing (CORS) feature for the S3 bucket in Account A.

B. In Account

C. set the S3 bucket policy to the following.

```
{
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource": "arn:aws:s3:::AccountABucketName/*"
}
```

D. In Account A, set the S3 bucket policy to the following: Text, letter Description automatically generated

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::AccountB:user/User_DataProcessor"
  },
  "Action": [
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource": [
    "arn:aws:s3:::AccountABucketName/*"
  ]
}
```

E. InAccount B, set the permissions of User_DataProcessor to the following:Text Description automatically generated

```
{
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource": "arn:aws:s3:::AccountABucketName/*"
}
```

F. InAccount B, set the permissions of User_DataProcessor to the following:Text, letter Description automatically generated

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::AccountB:user/User_DataProcessor"
  },
  "Action": [
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource": [
    "arn:aws:s3:::AccountABucketName/*"
  ]
}
```

Answer: AD

NEW QUESTION 175

- (Exam Topic 2)

A company has implemented a global multiplayer gaming platform The platform requires gaming clients to have reliable, low-latency access to the server infrastructure that is hosted on a fleet of Amazon EC2 instances in a single AWS Region

The gaming clients use a custom TCP protocol to connect to the server infrastructure The application architecture requires client IP addresses to be available to the server software

Which solution meets these requirements?

A. Create a Network Load Balancer (NLB), and add the EC2 instances to a target group Create an Amazon CloudFront Real Time Messaging Protocol (RTMP) distribution and configure the origin to point to the DNS endpoint of the NLB Use proxy protocol version 2 headers to preserve client IP addresses

B. Use an AWS Direct Connect gateway to connect multiple Direct Connect locations in different Regions globally Configure Amazon Route 53 with geolocation routing to send traffic to the nearest Direct Connect location Associate the VPC that contains the EC2 instances with the Direct Connect gateway

C. Create an accelerator in AWS Global Accelerator and configure the listener to point to a single endpoint group Add each of the EC2 instances as endpoints to the endpoint group Configure the endpoint group weighting equally across all of the EC2 endpoints

D. Create an Application Load Balancer (ALB) and add the EC2 instances to a target group Create a set of Amazon Route 53 latency-based alias records that point to the DNS endpoint of the ALB UseX-Forwarded-For headers to preserve client IP addresses

Answer: B

NEW QUESTION 177

- (Exam Topic 2)

A company has an application Once a month, the application creates a compressed file that contains every object within an Amazon S3 bucket The total size of the objects before compression is 1 TB.

The application runs by using a scheduled cron job on an Amazon EC2 instance that has a 5 TB Amazon Elastic Block Store (Amazon EBS) volume attached The application downloads all the files from the source S3 bucket to the EBS volume, compresses the file, and uploads the file to a target S3 bucket Every invocation of the application takes 2 hours from start to finish

Which combination of actions should a solutions architect take to OPTIMIZE costs for this application? (Select TWO.)

A. Migrate the application to run an AWS Lambda function Use Amazon EventBridge (Amazon CloudWatch Events) to schedule the Lambda function to run once each month

B. Configure the application to download the source files by using streams Direct the streams into a compression library Direct the output of the compression library into a target object in Amazon S3

C. Configure the application to download the source files from Amazon S3 and save the files to local storage Compress the files and upload them to Amazon S3

- D. Configure the application to run as a container in AWS Fargate Use Amazon EventBridge (Amazon CloudWatch Events) to schedule the task to run once each month
- E. Provision an Amazon Elastic File System (Amazon EFS) file system Attach the file system to the AWS Lambda function

Answer: CD

NEW QUESTION 179

- (Exam Topic 2)

A new application is running on Amazon Elastic Container Service (Amazon ECS) with AWS Fargate The application uses an Amazon Aurora MySQL database The application and the database run in the same subnets of a VPC with distinct security groups that are configured.

The password (or the database is stored in AWS Secrets Manager and is passed to the application through the D8_PASSWORD environment variable The hostname of the database is passed to the application through the DB_HOST environment variable The application is failing to access the database.

Which combination of actions should a solutions architect take to resolve this error? (Select THREE)

- A. Ensure that the container has the environment variable with name "DB_PASSWORD" specified with a "ValueFrom" and the ARN of the secret
- B. Ensure that the container has the environment variable with name "D8_PASSWORD" specified with a "ValueFrom" and the secret name of the secret.
- C. Ensure that the Fargate service security group allows inbound network traffic from the Aurora MySQL database on the MySQL TCP port 3306.
- D. Ensure that the Aurora MySQL database security group allows inbound network traffic from the Fargate service on the MySQL TCP port 3306.
- E. Ensure that the container has the environment variable with name "D8_HOST" specified with the hostname of a DB instance endpoint.
- F. Ensure that the container has the environment variable with name "DB_HOST" specified with the hostname of the OB duster endpoint.

Answer: ADE

NEW QUESTION 184

- (Exam Topic 2)

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

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

- A. Evaluate and adjust the RCUs for the DynamoDB tables.
- B. Evaluate and adjust the WCUs for the DynamoDB tables.
- C. Add an Amazon ElastiCache layer to increase the performance of Lambda functions.
- D. Add an Amazon Simple Queue Service (Amazon SQS) queue and reprocessing logic between Amazon S3 and the Lambda functions.
- E. Use S3 Transfer Acceleration to provide lower latency to users.

Answer: BD

NEW QUESTION 189

- (Exam Topic 2)

A company is developing a gene reporting device that will collect genomic information to assist researchers with collecting large samples of data from a diverse population. The device will push 8 KB of genomic data every second to a data platform that will need to process and analyze the data and provide information back to researchers The data platform must meet the following requirements:

- Provide near-real-time analytics of the inbound genomic data
- Ensure the data is flexible, parallel, and durable
- Deliver results of processing to a data warehouse

Which strategy should a solutions architect use to meet these requirements?

- A. Use Amazon Kinesis Data Firehose to collect the inbound sensor data analyze the data with Kinesis client
- B. and save the results to an Amazon RDS instance
- C. Use Amazon Kinesis Data Streams to collect the inbound sensor data analyze the data with Kinesis clients and save the results to an Amazon Redshift duster using Amazon EMR
- D. Use Amazon S3 to collect the inbound device data analyze the data from Amazon SOS with Kinesis and save the results to an Amazon Redshift duster
- E. Use an Amazon API Gateway to put requests into an Amazon SQS queue analyze the data with an AWS Lambda function and save the results » an Amazon Redshift duster using Amazon EMR

Answer: A

NEW QUESTION 190

- (Exam Topic 2)

A company is finalizing the architecture for its backup solution for applications running on AWS. All of the applications run on AWS and use at least two Availability Zones in each tier.

Company policy requires IT to durably store nightly backups of all its data in at least two locations: production and disaster recovery. The locations must be in different geographic regions. The company also needs the backup to be available to restore immediately at the production data center, and within 24 hours at the disaster recovery location backup processes must be fully automated.

What is the MOST cost-effective backup solution that will meet all requirements?

- A. Back up all the data to a large Amazon EBS volume attached to the backup media server in the production region
- B. Run automated scripts to snapshot these volumes nightly
- C. and copy these snapshots to the disaster recovery region.
- D. Back up all the data to Amazon S3 in the disaster recovery region Use a Lifecycle policy to move this data to Amazon Glacier in the production region immediately Only the data is replicated: remove the data from the S3 bucket in the disaster recovery region.
- E. Back up all the data to Amazon Glacier in the production region
- F. Set up cross-region replication of this data to Amazon Glacier in the disaster recovery region
- G. Set up a lifecycle policy to delete any data older than 60 days.
- H. Back up all the data to Amazon S3 in the production region
- I. Set up cross-region replication of this S3 bucket to another region and set up a lifecycle policy in the second region to immediately move this data to Amazon Glacier

Answer: D

NEW QUESTION 193

- (Exam Topic 2)

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

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

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

- A. Create an Amazon Simple Notification Service (Amazon SNS) topic with a subscription of type "Email" that targets the team's mailing list.
- B. Create a task named "Email" that forwards the input arguments to the SNS topic
- C. Add a Catch field to all Task
- D. Map
- E. and Parallel states that have a statement of "ErrorEquals": ["states.all"] and "Next": "Email".
- F. Add a new email address to Amazon Simple Email Service (Amazon SES). Verify the email address.
- G. Create a task named "Email" that forwards the input arguments to the SES email address
- H. Add a Catch field to all Task, Map, and Parallel states that have a statement of "ErrorEquals": ["states.Bun time"] and "Next": "Email".

Answer: BCD

NEW QUESTION 197

- (Exam Topic 2)

A company is currently using AWS CodeCommit for its source control and AWS CodePipeline for continuous integration. The pipeline has a build stage for building the artifacts, which is then staged in an Amazon S3 bucket.

The company has identified various improvement opportunities in the existing process and a solutions architect has been given the following requirements:

- Create a new pipeline to support feature development
 - Support feature development without impacting production applications
 - Incorporate continuous testing with unit tests
 - Isolate development and production artifacts
 - Support the capability to merge tested code into production code
- How should the solutions architect achieve these requirements?

- A. Trigger a separate pipeline from CodeCommit feature branches. Use AWS CodeBuild for running unit tests. Use CodeBuild to stage the artifacts within an S3 bucket in a separate testing account.
- B. Trigger a separate pipeline from CodeCommit feature branches. Use AWS Lambda for running unit tests. Use AWS CodeDeploy to stage the artifacts within an S3 bucket in a separate testing account.
- C. Trigger a separate pipeline from CodeCommit tags. Use Jenkins for running unit tests. Create a stage in the pipeline with S3 as the target for staging the artifacts within an S3 bucket in a separate testing account.
- D. Create a separate CodeCommit repository for feature development and use it to trigger the pipeline. Use AWS Lambda for running unit tests. Use AWS CodeBuild to stage the artifacts within different S3 buckets in the same production account.

Answer: A

NEW QUESTION 200

- (Exam Topic 2)

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.
- 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.
- E. Use Amazon CloudWatch to trace and analyze user requests to API Gateway.

Answer: A

NEW QUESTION 204

.....

Relate Links

100% Pass Your SAP-C02 Exam with ExamBible Prep Materials

<https://www.exambible.com/SAP-C02-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>