

SAP-C02 Dumps

AWS Certified Solutions Architect - Professional

<https://www.certleader.com/SAP-C02-dumps.html>



NEW QUESTION 1

- (Exam Topic 1)

A solutions architect is designing a publicly accessible web application that is on an Amazon CloudFront distribution with an Amazon S3 website endpoint as the origin. When the solution is deployed, the website returns an Error 403: Access Denied message.

Which steps should the solutions architect take to correct the issue? (Select TWO.)

- A. Remove the S3 block public access option from the S3 bucket.
- B. Remove the requester pays option from the S3 bucket.
- C. Remove the origin access identity (OAI) from the CloudFront distribution.
- D. Change the storage class from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA).
- E. Disable S3 object versioning.

Answer: AB

Explanation:

See using S3 to host a static website with Cloudfront: <https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/>

- Using a REST API endpoint as the origin, with access restricted by an origin access identity (OAI)
- Using a website endpoint as the origin, with anonymous (public) access allowed
- Using a website endpoint as the origin, with access restricted by a Referer header

NEW QUESTION 2

- (Exam Topic 1)

A company wants to deploy an AWS WAF solution to manage AWS WAF rules across multiple AWS accounts. The accounts are managed under different OUs in AWS Organizations.

Administrators must be able to add or remove accounts or OUs from managed AWS WAF rule sets as needed. Administrators also must have the ability to automatically update and remediate noncompliant AWS WAF rules in all accounts

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

- A. Use AWS Firewall Manager to manage AWS WAF rules across accounts in the organization
- B. Use an AWS Systems Manager Parameter Store parameter to store account numbers and OUs to manage Update the parameter as needed to add or remove accounts or OUs Use an Amazon EventBridge (Amazon CloudWatch Events) rule to identify any changes to the parameter and to invoke an AWS Lambda function to update the security policy in the Firewall Manager administrative account
- C. Deploy an organization-wide AWS Config rule that requires all resources in the selected OUs to associate the AWS WAF rule
- D. Deploy automated remediation actions by using AWS Lambda to fix noncompliant resource
- E. Deploy AWS WAF rules by using an AWS CloudFormation stack set to target the same OUs where the AWS Config rule is applied.
- F. Create AWS WAF rules in the management account of the organization
- G. Use AWS Lambda environment variables to store account numbers and OUs to manage Update environment variables as needed to add or remove accounts or OUs Create cross-account IAM roles in member account
- H. Assume the roles by using AWS Security Token Service (AWS STS) in the Lambda function to create and update AWS WAF rules in the member accounts
- I. Use AWS Control Tower to manage AWS WAF rules across accounts in the organization
- J. Use AWS Key Management Service (AWS KMS) to store account numbers and OUs to manage Update AWS KMS as needed to add or remove accounts or OU
- K. Create IAM users in member accounts Allow AWS Control Tower in the management account to use the access key and secret access key to create and update AWS WAF rules in the member accounts

Answer: B

NEW QUESTION 3

- (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 for authentication. The EC2 instance also has an attached security group that allows access from all customer IP addresses.

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

Which solution will meet these requirements?

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

<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 4

- (Exam Topic 1)

A company is running an application on several Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer. The load on the application varies throughout the day, and EC2 instances are scaled in and out on a regular basis. Log files from the EC2 instances are copied to a central Amazon S3 bucket every 15 minutes. The security team discovers that log files are missing from some of the terminated EC2 instances.

Which set of actions will ensure that log files are copied to the central S3 bucket from the terminated EC2 instances?

- A. Create a script to copy log files to Amazon S3, and store the script in a file on the EC2 instance
- B. Create an Auto Scaling lifecycle hook and an Amazon EventBridge (Amazon CloudWatch Events) rule to detect lifecycle events from the Auto Scaling group
- C. Invoke an AWS Lambda function on the `autoscaling:EC2_INSTANCE_TERMINATING` transition to send `ABANDON` to the Auto Scaling group to prevent termination, run the script to copy the log files, and terminate the instance using the AWS SDK.
- D. Create an AWS Systems Manager document with a script to copy log files to Amazon S3. Create an Auto Scaling lifecycle hook and an Amazon EventBridge (Amazon CloudWatch Events) rule to detect lifecycle events from the Auto Scaling group
- E. Invoke an AWS Lambda function on the `autoscaling:EC2_INSTANCE_TERMINATING` transition to call the AWS Systems Manager API `SendCommand` operation to run the document to copy the log files and send `CONTINUE` to the Auto Scaling group to terminate the instance.
- F. Change the log delivery rate to every 5 minutes
- G. Create a script to copy log files to Amazon S3, and add the script to EC2 instance user data
- H. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to detect EC2 instance termination
- I. Invoke an AWS Lambda function from the EventBridge (CloudWatch Events) rule that uses the AWS CLI to run the user-data script to copy the log files and terminate the instance.
- J. Create an AWS Systems Manager document with a script to copy log files to Amazon S3. Create an Auto Scaling lifecycle hook that publishes a message to an Amazon Simple Notification Service (Amazon SNS) topic
- K. From the SNS notification, call the AWS Systems Manager API `SendCommand` operation to run the document to copy the log files and send `ABANDON` to the Auto Scaling group to terminate the instance.

Answer: B

Explanation:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/adding-lifecycle-hooks.html>

- Refer to Default Result section - If the instance is terminating, both `abandon` and `continue` allow the instance

to terminate. However, `abandon` stops any remaining actions, such as other lifecycle hooks, and `continue` allows any other lifecycle hooks to complete.

<https://aws.amazon.com/blogs/infrastructure-and-automation/run-code-before-terminating-an-ec2-auto-scaling-i> <https://github.com/aws-samples/aws-lambda-lifecycle-hooks-function>

<https://github.com/aws-samples/aws-lambda-lifecycle-hooks-function/blob/master/cloudformation/template.yaml>

NEW QUESTION 5

- (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 Regions
- 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 Regions
- 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 6

- (Exam Topic 1)

A company has developed an application that is running Windows Server on VMware vSphere VMs that the company hosts on-premises. The application data is stored in a proprietary format that must be read through the application. The company manually provisioned the servers and the application.

As part of its disaster recovery plan, the company wants the ability to host its application on AWS temporarily if the company's on-premises environment becomes unavailable. The company wants the application to return to on-premises hosting after a disaster recovery event is complete. The RPO is 15 minutes.

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

- A. Configure AWS DataSync
- B. Replicate the data to Amazon Elastic Block Store (Amazon EBS) volumes. When the on-premises environment is unavailable, use AWS CloudFormation templates to provision Amazon EC2 instances and attach the EBS volumes
- C. Configure CloudEndure Disaster Recovery. Replicate the data to replication Amazon EC2 instances that are attached to Amazon Elastic Block Store (Amazon EBS) volumes. When the on-premises environment is unavailable, use CloudEndure to launch EC2 instances that use the replicated volumes.
- D. Provision an AWS Storage Gateway File Gateway

- E. Recreate the data to an Amazon S3 bucket
- F. When the on-premises environment is unavailable, use AWS Backup to restore the data to Amazon Elastic Block Store (Amazon EBS) volumes and launch Amazon EC2 instances from these EBS volumes
- G. Provision an Amazon FSx for Windows File Server file system on AWS Replicate the data to the on-premises system. When the on-premises environment is unavailable, use AWS CloudFormation templates to provision Amazon EC2 instances and use AWS CloudFormation Init commands to mount the Amazon FSx file shares

Answer: D

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

Answer: B

NEW QUESTION 8

- (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 minutes
- 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 detection
- D. Configure cross-Region snapshots of the DB instance to the DR Region every 5 minutes
- 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 Region
- 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 AMIs of the web and application servers in the DR Region
- J. Use scheduled AWS Glue jobs to synchronize the DB instance with another DB instance in the DR Region
- 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 9

- (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 company has multiple AWS accounts as part of an organization created with AWS Organizations. Each account has a VPC in the us-east-2 Region and is used for either production or development workloads. Amazon EC2 instances across production accounts need to communicate with each other, and EC2 instances across development accounts need to communicate with each other, but production and development instances should not be able to communicate with each other.

To facilitate connectivity, the company created a common network account. The company used AWS Transit Gateway to create a transit gateway in the us-east-2 Region in the network account and shared the transit gateway with the entire organization by using AWS Resource Access Manager. Network administrators then attached VPCs in each account to the transit gateway, after which the EC2 instances were able to communicate across accounts. However, production and development accounts were also able to communicate with one another.

Which set of steps should a solutions architect take to ensure production traffic and development traffic are completely isolated?

- A. Modify the security groups assigned to development EC2 instances to block traffic from production EC2 instance
- B. Modify the security groups assigned to production EC2 instances to block traffic from development EC2 instances.
- C. Create a tag on each VPC attachment with a value of either production or development, according to the type of account being attached
- D. Using the Network Manager feature of AWS Transit Gateway, create policies that restrict traffic between VPCs based on the value of this tag.
- E. Create separate route tables for production and development traffic
- F. Delete each account's association and route propagation to the default AWS Transit Gateway route table
- G. Attach development VPCs to the development AWS Transit Gateway route table and production VPCs to the production route table, and enable automatic route propagation on each attachment.
- H. Create a tag on each VPC attachment with a value of either production or development, according to the type of account being attached
- I. Modify the AWS Transit Gateway routing table to route production tagged attachments to one another and development tagged attachments to one another.

Answer: C

Explanation:

<https://docs.aws.amazon.com/vpc/latest/tgw/vpc-tgw.pdf>

NEW QUESTION 10

- (Exam Topic 1)

A finance company is running its business-critical application on current-generation Linux EC2 instances. The application includes a self-managed MySQL database performing heavy I/O operations. The application is working fine to handle a moderate amount of traffic during the month. However, it slows down during the final three days of each month due to month-end reporting, even though the company is using Elastic Load Balancers and Auto Scaling within its infrastructure to meet the increased demand.

Which of the following actions would allow the database to handle the month-end load with the LEAST impact on performance?

- A. Pre-warming Elastic Load Balancers, using a bigger instance type, changing all Amazon EBS volumes to GP2 volumes.
- B. Performing a one-time migration of the database cluster to Amazon RDS
- C. and creating several additional read replicas to handle the load during end of month
- D. Using Amazon CloudWatch with AWS Lambda to change the type
- E. size, or IOPS of Amazon EBS volumes in the cluster based on a specific CloudWatch metric
- F. Replacing all existing Amazon EBS volumes with new PIOPS volumes that have the maximum available storage size and I/O per second by taking snapshots before the end of the month and reverting back afterwards.

Answer: B

Explanation:

In this scenario, the Amazon EC2 instances are in an Auto Scaling group already which means that the database read operations is the possible bottleneck especially during the month-end wherein the reports are generated. This can be solved by creating RDS read replicas.

NEW QUESTION 13

- (Exam Topic 1)

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

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

Which storage solution will meet these requirements?

- A. Provision an AWS Storage Gateway file gateway NFS file share that is attached to an Amazon S3 bucket
- B. Mount the NFS file share on each EC2 instance in the cluster.
- C. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses General Purpose performance mode
- D. Mount the EFS file system on each EC2 instance in the cluster.
- E. Provision a new Amazon Elastic Block Store (Amazon EBS) volume that uses the io2 volume type. Attach the EBS volume to all of the EC2 instances in the cluster.
- F. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses Max I/O performance mode
- G. Mount the EFS file system on each EC2 instance in the cluster.

Answer: D

NEW QUESTION 16

- (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 18

- (Exam Topic 1)

A company runs an e-commerce platform with front-end and e-commerce tiers. Both tiers run on LAMP stacks with the front-end instances running behind a load balancing appliance that has a virtual offering on AWS Current*/, the operations team uses SSH to log in to the instances to maintain patches and address other concerns. The platform has recently been the target of multiple attacks, including.

- A DDoS attack.
- An SQL injection attack
- Several successful dictionary attacks on SSH accounts on the web servers

The company wants to improve the security of the e-commerce platform by migrating to AWS. The company's solutions architects have decided to use the following approach;

- Code review the existing application and fix any SQL injection issues.
- Migrate the web application to AWS and leverage the latest AWS Linux AMI to address initial security patching.
- Install AWS Systems Manager to manage patching and allow the system administrators to run commands on all instances, as needed.

What additional steps will address all of the identified attack types while providing high availability and minimizing risk?

- A. Enable SSH access to the Amazon EC2 instances using a security group that limits access to specific IP
- B. Migrate on-premises MySQL to Amazon RDS Multi-AZ Install the third-party load balancer from the AWS Marketplace and migrate the existing rules to the load balancer's AWS instances Enable AWS Shield Standard for DDoS protection
- C. Disable SSH access to the Amazon EC2 instance
- D. Migrate on-premises MySQL to Amazon RDS Multi-AZ Leverage an Elastic Load Balancer to spread the load and enable AWS Shield Advanced for protection
- E. Add an Amazon CloudFront distribution in front of the website Enable AWS WAF on the distribution to manage the rules.
- F. Enable SSH access to the Amazon EC2 instances through a bastion host secured by limiting access to specific IP addresses
- G. Migrate on-premises MySQL to a self-managed EC2 instance
- H. Leverage an AWS Elastic Load Balancer to spread the load, and enable AWS Shield Standard for DDoS protection Add an Amazon CloudFront distribution in front of the website.
- I. Disable SSH access to the EC2 instance
- J. Migrate on-premises MySQL to Amazon RDS Single-A
- K. Leverage an AWS Elastic Load Balancer to spread the load Add an Amazon CloudFront distribution in front of the website Enable AWS WAF on the distribution to manage the rules.

Answer: B

NEW QUESTION 20

- (Exam Topic 1)

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

What should a solutions architect do to meet these requirements?

- A. Create an AWS Config rule in the specific member accounts to limit Regions and apply a tag policy.
- B. From the AWS Billing and Cost Management console, in the master account, disable Regions for the specific member accounts and apply a tag policy on the root.
- C. Associate the specific member accounts with the root
- D. Apply a tag policy and an SCP using conditions to limit Regions.
- E. Associate the specific member accounts with a new O
- F. Apply a tag policy and an SCP using conditions to limit Regions.

Answer: D

NEW QUESTION 23

- (Exam Topic 1)

A web application is hosted in a dedicated VPC that is connected to a company's on-premises data center over a Site-to-Site VPN connection. The application is accessible from the company network only. This is a temporary non-production application that is used during business hours. The workload is generally low with occasional surges.

The application has an Amazon Aurora MySQL provisioned database cluster on the backend. The VPC has an internet gateway and a NAT gateway attached. The web servers are in private subnets in an Auto Scaling group behind an Elastic Load Balancer. The web servers also upload data to an Amazon S3 bucket through the internet.

A solutions architect needs to reduce operational costs and simplify the architecture. Which strategy should the solutions architect use?

- A. Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only
- B. Use 3-year scheduled Reserved Instances for the web server EC2 instance
- C. Detach the internet gateway and remove the NAT gateways from the VPC
- D. Use an Aurora Serverless database and set up a VPC endpoint for the S3 bucket.
- E. Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only
- F. Detach the internet gateway and remove the NAT gateways from the VPC
- G. Use an Aurora Serverless database and set up a VPC endpoint for the S3 bucket, then update the network routing and security rules and policies related to the changes.
- H. Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only
- I. Detach the internet gateway from the VPC, and use an Aurora Serverless database
- J. Set up a VPC endpoint for the S3 bucket, then update the network routing and security rules and policies related to the changes.
- K. Use 3-year scheduled Reserved Instances for the web server Amazon EC2 instance
- L. Remove the NAT gateways from the VPC, and set up a VPC endpoint for the S3 bucket
- M. Use Amazon
- N. CloudWatch and AWS Lambda to stop and start the Aurora DB cluster so it operates during business hours only
- O. Update the network routing and security rules and policies related to the changes.

Answer: B

Explanation:

The application is accessible from the company network only remove NAT and IGW, application - S3 with VPC endpoint. Non-Production application no need to go for Reserved instances

To build site-to-site vpn, you don't need internet gateway. Instead, customer gateway is needed.

<https://docs.aws.amazon.com/vpn/latest/s2svpn/SetUpVPNConnections.html#vpn-create-cgw>

NEW QUESTION 28

- (Exam Topic 1)

An education company is running a web application used by college students around the world. The application runs in an Amazon Elastic Container Service (Amazon ECS) cluster in an Auto Scaling group behind an Application Load Balancer (ALB). A system administrator detects a weekly spike in the number of failed login attempts, which overwhelm the application's authentication service. All the failed login attempts originate from about 500 different IP addresses that change each week. A solutions architect must prevent the failed login attempts from overwhelming the authentication service.

Which solution meets these requirements with the MOST operational efficiency?

- A. Use AWS Firewall Manager to create a security group and security group policy to deny access from the IP addresses.
- B. Create an AWS WAF web ACL with a rate-based rule, and set the rule action to Block
- C. Connect the web ACL to the ALB.
- D. Use AWS Firewall Manager to create a security group and security group policy to allow access only to specific CIDR ranges.
- E. Create an AWS WAF web ACL with an IP set match rule, and set the rule action to Block
- F. Connect the web ACL to the ALB.

Answer: B

Explanation:

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-rate-based.html>

The IP set match statement inspects the IP address of a web request against a set of IP addresses and address ranges. Use this to allow or block web requests based on the IP addresses that the requests originate from. By default, AWS WAF uses the IP address from the web request origin, but you can configure the rule to use an HTTP header like X-Forwarded-For instead.

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-ipset-match.html>

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-rate-based.html>

NEW QUESTION 29

- (Exam Topic 1)

A company has a photo sharing social networking application. To provide a consistent experience for users, the company performs some image processing on the photos uploaded by users before publishing on the application. The image processing is implemented using a set of Python libraries.

The current architecture is as follows:

- The image processing Python code runs in a single Amazon EC2 instance and stores the processed images in an Amazon S3 bucket named ImageBucket.
- The front-end application, hosted in another bucket, loads the images from ImageBucket to display to users. With plans for global expansion, the company wants to implement changes in its existing architecture to be able to scale for increased demand on the application and reduce management complexity as the application scales.

Which combination of changes should a solutions architect make? (Select TWO.)

- A. Place the image processing EC2 instance into an Auto Scaling group.
- B. Use AWS Lambda to run the image processing tasks.
- C. Use Amazon Rekognition for image processing.
- D. Use Amazon CloudFront in front of ImageBucket.
- E. Deploy the applications in an Amazon ECS cluster and apply Service Auto Scaling.

Answer: BD

Explanation:

<https://prismatic.io/blog/why-we-moved-from-lambda-to-ecs/>

NEW QUESTION 34

- (Exam Topic 1)

A company is developing and hosting several projects in the AWS Cloud. The projects are developed across multiple AWS accounts under the same organization in AWS Organizations. The company requires the cost for cloud infrastructure to be allocated to the owning project. The team responsible for all of the AWS accounts has discovered that several Amazon EC2 instances are lacking the Project tag used for cost allocation.

Which actions should a solutions architect take to resolve the problem and prevent it from happening in the future? (Select THREE.)

- A. Create an AWS Config rule in each account to find resources with missing tags.
- B. Create an SCP in the organization with a deny action for ec2:RunInstances if the Project tag is missing.
- C. Use Amazon Inspector in the organization to find resources with missing tags.
- D. Create an IAM policy in each account with a deny action for ec2:RunInstances if the Project tag is missing.
- E. Create an AWS Config aggregator for the organization to collect a list of EC2 instances with the missing Project tag.
- F. Use AWS Security Hub to aggregate a list of EC2 instances with the missing Project tag.

Answer: BDE

NEW QUESTION 39

- (Exam Topic 1)

A media company uses Amazon DynamoDB to store metadata for its catalog of movies that are available to stream. Each media item contains user-facing content that includes a description of the media, a list of search tags, and similar data. In addition, media items include a list of Amazon S3 key names that relate to movie files. The company stores these movie files in a single S3 bucket that has versioning enabled. The company uses Amazon CloudFront to serve these movie files.

The company has 100,000 media items, and each media item can have many different S3 objects that represent different encodings of the same media S3 objects that belong to the same media item are grouped together under the same key prefix, which is a random unique ID

Because of an expiring contract with a media provider, the company must remove 2,000 media items. The company must completely delete all DynamoDB keys and movie files on Amazon S3 that are related to these media items within 36 hours. The company must ensure that the content cannot be recovered.

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

- A. Configure the dynamoDB table with a TTL field
- B. Create and invoke an AWS Lambda function to perform a conditional update Set the TTL field to the time of the contract's expiration on every affected media item.
- C. Configure an S3 Lifecycle object expiration rule that is based on the contract's expiration date
- D. Write a script to perform a conditional delete on all the affected DynamoDB records
- E. Temporarily suspend versioning on the S3 bucket
- F. Create and invoke an AWS Lambda function that deletes affected objects Reactivate versioning when the operation is complete
- G. Write a script to delete objects from Amazon S3 Specify in each request a NoncurrentVersionExpiration property with a NoncurrentDays attribute set to 0.

Answer: CE

NEW QUESTION 43

- (Exam Topic 1)

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

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

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

- A. Configure the Aurora MySQL DB cluster to publish slow query and error logs to Amazon CloudWatch Logs.
- B. Implement the AWS X-Ray SDK to trace incoming HTTP requests on the EC2 instances and implement tracing of SQL queries with the X-Ray SDK for Java.
- C. Configure the Aurora MySQL DB cluster to stream slow query and error logs to Amazon Kinesis.
- D. Install and configure an Amazon CloudWatch Logs agent on the EC2 instances to send the Apache logs to CloudWatch Logs.
- E. Enable and configure AWS CloudTrail to collect and analyze application activity from Amazon EC2 and Aurora.
- F. Enable Aurora MySQL DB cluster performance benchmarking and publish the stream to AWS X-Ray.

Answer: ABD

Explanation:

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_LogAccess.Concepts.MySQL.html <https://aws.amazon.com/blogs/mt/simplifying-apache-server-logs-with-amazon-cloudwatch-logs-insights/> <https://docs.aws.amazon.com/xray/latest/devguide/xray-sdk-dotnet-messagehandler.html> <https://docs.aws.amazon.com/xray/latest/devguide/xray-sdk-java-sqlclients.html>

NEW QUESTION 48

- (Exam Topic 1)

A large company in Europe plans to migrate its applications to the AWS Cloud. The company uses multiple AWS accounts for various business groups. A data privacy law requires the company to restrict developers' access to AWS European Regions only.

What should the solutions architect do to meet this requirement with the LEAST amount of management overhead?

- A. Create IAM users and IAM groups in each account
- B. Create IAM policies to limit access to non-European Regions Attach the IAM policies to the IAM groups
- C. Enable AWS Organizations, attach the AWS accounts, and create OUs for European Regions and non-European Region
- D. Create SCPs to limit access to non-European Regions and attach the policies to the OUs.
- E. Set up AWS Single Sign-On and attach AWS account
- F. Create permission sets with policies to restrict access to non-European Regions Create IAM users and IAM groups in each account.
- G. Enable AWS Organizations, attach the AWS accounts, and create OUs for European Regions and non-European Region
- H. Create permission sets with policies to restrict access to non-European Region
- I. Create IAM users and IAM groups in the primary account.

Answer: B

Explanation:

"This policy uses the Deny effect to deny access to all requests for operations that don't target one of the two approved regions (eu-central-1 and eu-west-1)."
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_general.htm
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition.html

NEW QUESTION 53

- (Exam Topic 1)

A company stores sales transaction data in Amazon DynamoDB tables. To detect anomalous behaviors and respond quickly, all changes to the items stored in the DynamoDB tables must be logged within 30 minutes.

Which solution meets the requirements?

- A. Copy the DynamoDB tables into Apache Hive tables on Amazon EMR every hour and analyze them (or anomalous behavior)
- B. Send Amazon SNS notifications when anomalous behaviors are detected.
- C. Use AWS CloudTrail to capture all the APIs that change the DynamoDB table
- D. Send SNS notifications when anomalous behaviors are detected using CloudTrail event filtering.
- E. Use Amazon DynamoDB Streams to capture and send updates to AWS Lambda
- F. Create a Lambda function to output records to Amazon Kinesis Data Stream
- G. Analyze any anomalies with Amazon Kinesis Data Analytics
- H. Send SNS notifications when anomalous behaviors are detected.
- I. Use event patterns in Amazon CloudWatch Events to capture DynamoDB API call events with an AWS Lambda function as a target to analyze behavior
- J. Send SNS notifications when anomalous behaviors are detected.

Answer: C

Explanation:

[https://aws.amazon.com/blogs/database/dynamodb-streams-use-cases-and-design-patterns/#:~:text=DynamoDB DynamoDb Stream to capture DynamoDB update. And Kinesis Data Analytics for anomaly detection \(it uses AWS proprietary Random Cut Forest Algorithm\)](https://aws.amazon.com/blogs/database/dynamodb-streams-use-cases-and-design-patterns/#:~:text=DynamoDB DynamoDb Stream to capture DynamoDB update. And Kinesis Data Analytics for anomaly detection (it uses AWS proprietary Random Cut Forest Algorithm))

NEW QUESTION 58

- (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 62

- (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 67

- (Exam Topic 1)

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

- A. Create a new developer account
- B. Move all EC2 instances, users, and assets into us-east-2. Add the account to the company's organization in AWS Organization
- C. Enforce a tagging policy that denotes Region affinity.
- D. Create an SCP that denies the launch of all EC2 instances except t3.small EC2 instances in us-east-2. Attach the SCP to the project's account.
- E. Create and purchase a t3.small EC2 Reserved Instance for each developer in us-east-2. Assign each developer a specific EC2 instance with their name as the tag.
- F. Create an IAM policy that allows the launch of only t3.small EC2 instances in us-east-2. Attach the policy to the roles and groups that the developers use in the project's account.

Answer: D

NEW QUESTION 71

- (Exam Topic 1)

A solution architect needs to deploy an application on a fleet of Amazon EC2 instances. The EC2 instances run in private subnets in an Auto Scaling group. The application is expected to generate logs at a rate of 100 MB each second on each of the EC2 instances.

The logs must be stored in an Amazon S3 bucket so that an Amazon EMR cluster can consume them for further processing. The logs must be quickly accessible for the first 90 days and should be retrievable within 48 hours thereafter.

What is the MOST cost-effective solution that meets these requirements?

- A. Set up an S3 copy job to write logs from each EC2 instance to the S3 bucket with S3 Standard storage. Use a NAT instance within the private subnets to connect to Amazon S3. Create S3 Lifecycle policies to move logs that are older than 90 days to S3 Glacier.
- B. Set up an S3 sync job to copy logs from each EC2 instance to the S3 bucket with S3 Standard storage. Use a gateway VPC endpoint for Amazon S3 to connect to Amazon S3. Create S3 Lifecycle policies to move logs that are older than 90 days to S3 Glacier Deep Archive.

- C. Set up an S3 batch operation to copy logs from each EC2 instance to the S3 bucket with S3 Standard storage. Use a NAT gateway with the private subnets to connect to Amazon S3. Create S3 Lifecycle policies to move logs that are older than 90 days to S3 Glacier Deep Archive.
- D. Set up an S3 sync job to copy logs from each EC2 instance to the S3 bucket with S3 Standard storage. Use a gateway VPC endpoint for Amazon S3 to connect to Amazon S3. Create S3 Lifecycle policies to move logs that are older than 90 days to S3 Glacier.

Answer: C

NEW QUESTION 73

- (Exam Topic 1)

A company needs to run a software package that has a license that must be run on the same physical host for the duration of its use. The software package is only going to be used for 90 days. The company requires patching and restarting of all instances every 30 days. How can these requirements be met using AWS?

- A. Run a dedicated instance with auto-placement disabled.
- B. Run the instance on a dedicated host with Host Affinity set to Host.
- C. Run an On-Demand Instance with a Reserved Instance to ensure consistent placement.
- D. Run the instance on a licensed host with termination set for 90 days.

Answer: B

Explanation:

Host Affinity is configured at the instance level. It establishes a launch relationship between an instance and a Dedicated Host. (This set which host the instance can run on) Auto-placement allows you to manage whether instances that you launch are launched onto a specific host, or onto any available host that has matching configurations. Auto-placement must be configured at the host level. (This sets which instance the host can run.) When affinity is set to Host, an instance launched onto a specific host always restarts on the same host if stopped. This applies to both targeted and untargeted launches.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/how-dedicated-hosts-work.html>

When affinity is set to Off, and you stop and restart the instance, it can be restarted on any available host. However, it tries to launch back onto the last Dedicated Host on which it ran (on a best-effort basis).

NEW QUESTION 76

- (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 79

- (Exam Topic 1)

A company runs a popular public-facing e-commerce website. Its user base is growing quickly from a local market to a national market. The website is hosted in an on-premises data center with web servers and a MySQL database. The company wants to migrate its workload to AWS. A solutions architect needs to create a solution to:

- Improve security
- Improve reliability
- Improve availability
- Reduce latency
- Reduce maintenance

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

- A. Use Amazon EC2 instances in two Availability Zones for the web servers in an Auto Scaling group behind an Application Load Balancer.
- B. Migrate the database to a Multi-AZ Amazon Aurora MySQL DB cluster.
- C. Use Amazon EC2 instances in two Availability Zones to host a highly available MySQL database cluster.
- D. Host static website content in Amazon S3. Use S3 Transfer Acceleration to reduce latency while serving webpage.
- E. Use AWS WAF to improve website security.
- F. Host static website content in Amazon S3. Use Amazon CloudFront to reduce latency while serving webpage.
- G. Use AWS WAF to improve website security.
- H. Migrate the database to a single-AZ Amazon RDS for MySQL DB instance.

Answer: ABE

NEW QUESTION 82

- (Exam Topic 1)

A company wants to control its cost of Amazon Athena usage. The company has allocated a specific monthly budget for Athena usage. A solutions architect must design a solution that will prevent the company from exceeding the budgeted amount. Which solution will meet these requirements?

- A. Use AWS Budget
- B. Create an alarm (or when the cost of Athena usage reaches the budgeted amount for the month)
- C. Configure AWS Budgets actions to deactivate Athena until the end of the month.

- D. Use Cost Explorer to create an alert for when the cost of Athena usage reaches the budgeted amount for the month
- E. Configure Cost Explorer to publish notifications to an Amazon Simple Notification Service (Amazon SNS) topic.
- F. Use AWS Trusted Advisor to track the cost of Athena usage
- G. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule to deactivate Athena until the end of the month whenever the cost reaches the budgeted amount for the month
- H. Use Athena workgroups to set a limit on the amount of data that can be scanned
- I. Set a limit that is appropriate for the monthly budget and the current pricing for Athena.

Answer: D

NEW QUESTION 85

- (Exam Topic 1)

A company is migrating applications from on-premises to the AWS Cloud. These applications power the company's internal web forms. These web forms collect data for specific events several times each quarter. The web forms use simple SQL statements to save the data to a local relational database. Data collection occurs for each event, and the on-premises servers are idle most of the time. The company needs to minimize the amount of idle infrastructure that supports the web forms.

Which solution will meet these requirements?

- A. Use Amazon EC2 Image Builder to create AMIs for the legacy server
- B. Use the AMIs to provision EC2 instances to recreate the applications in the AWS Cloud
- C. Place an Application Load Balancer (ALB) in front of the EC2 instance
- D. Use Amazon Route 53 to point the DNS names of the web forms to the ALB.
- E. Create one Amazon DynamoDB table to store data for all the data input. Use the application form name as the table key to distinguish data items
- F. Create an Amazon Kinesis data stream to receive the data input and store the input in DynamoDB
- G. Use Amazon Route 53 to point the DNS names of the web forms to the Kinesis data stream's endpoint.
- H. Create Docker images for each server of the legacy web form application
- I. Create an Amazon Elastic Container Service (Amazon ECS) cluster on AWS Fargate
- J. Place an Application Load Balancer in front of the ECS cluster
- K. Use Fargate task storage to store the web form data.
- L. Provision an Amazon Aurora Serverless cluster
- M. Build multiple schemas for each web form's data storage
- N. Use Amazon API Gateway and an AWS Lambda function to recreate the data input form
- O. Use Amazon Route 53 to point the DNS names of the web forms to their corresponding API Gateway endpoint.

Answer: D

Explanation:

Provision an Amazon Aurora Serverless cluster. Build multiple schemas for each web form's data storage. Use Amazon API Gateway and an AWS Lambda function to recreate the data input forms. Use Amazon Route 53 to point the DNS names of the web forms to their corresponding API Gateway endpoint.

NEW QUESTION 90

- (Exam Topic 1)

A finance company hosts a data lake in Amazon S3. The company receives financial data records over SFTP each night from several third parties. The company runs its own SFTP server on an Amazon EC2 instance in a public subnet of a VPC. After the files are uploaded, they are moved to the data lake by a cron job that runs on the same instance. The SFTP server is reachable on DNS `sftp.example.com` through the use of Amazon Route 53.

What should a solutions architect do to improve the reliability and scalability of the SFTP solution?

- A. Move the EC2 instance into an Auto Scaling group
- B. Place the EC2 instance behind an Application Load Balancer (ALB). Update the DNS record `sftp.example.com` in Route 53 to point to the ALB.
- C. Migrate the SFTP server to AWS Transfer for SFTP
- D. Update the DNS record `sftp.example.com` in Route 53 to point to the server endpoint hostname.
- E. Migrate the SFTP server to a file gateway in AWS Storage Gateway
- F. Update the DNS record `sftp.example.com` in Route 53 to point to the file gateway endpoint.
- G. Place the EC2 instance behind a Network Load Balancer (NLB). Update the DNS record `sftp.example.com` in Route 53 to point to the NLB.

Answer: B

NEW QUESTION 94

- (Exam Topic 1)

A solutions architect at a large company needs to set up network security for outbound traffic to the internet from all AWS accounts within an organization. The organization has more than 100 AWS accounts, and the accounts route to each other by using a centralized AWS Transit Gateway. Each account has both an internet gateway and a NAT gateway for outbound traffic to the internet. The company deploys resources only into a single AWS Region. The company needs the ability to add centrally managed rule-based filtering on all outbound traffic to the internet for all AWS accounts in the organization. The peak load of outbound traffic will not exceed 25 Gbps in each Availability Zone.

Which solution meets these requirements?

- A. Create a new VPC for outbound traffic to the internet. Connect the existing transit gateway to the new VPC. Configure a new NAT gateway. Create an Auto Scaling group of Amazon EC2 instances that run an open-source internet proxy for rule-based filtering across all Availability Zones in the Region. Modify all default routes to point to the proxy's Auto Scaling group.
- B. Create a new VPC for outbound traffic to the internet. Connect the existing transit gateway to the new VPC. Configure a new NAT gateway. Use an AWS Network Firewall for rule-based filtering. Create Network Firewall endpoints in each Availability Zone. Modify all default routes to point to the Network Firewall endpoints.
- C. Create an AWS Network Firewall for rule-based filtering in each AWS account. Modify all default routes to point to the Network Firewall firewalls in each account.
- D. In each AWS account, create an Auto Scaling group of network-optimized Amazon EC2 instances that run an open-source internet proxy for rule-based filtering. Modify all default routes to point to the proxy's Auto Scaling group.

Answer: B

Explanation:

<https://aws.amazon.com/blogs/networking-and-content-delivery/deployment-models-for-aws-network-firewall/>
<https://aws.amazon.com/blogs/networking-and-content-delivery/deploy-centralized-traffic-filtering-using-aws-n>

NEW QUESTION 99

- (Exam Topic 1)

A company is hosting a single-page web application in the AWS Cloud. The company is using Amazon CloudFront to reach its goal audience. The CloudFront distribution has an Amazon S3 bucket that is configured as its origin. The static files for the web application are stored in this S3 bucket. The company has used a simple routing policy to configure an Amazon Route 53 A record. The record points to the CloudFront distribution. The company wants to use a canary deployment release strategy for new versions of the application. What should a solutions architect recommend to meet these requirements?

- A. Create a second CloudFront distribution for the new version of the application.
- B. Update the Route 53 record to use a weighted routing policy.
- C. Create a Lambda@Edge function.
- D. Configure the function to implement a weighting algorithm and rewrite the URL to direct users to a new version of the application.
- E. Create a second S3 bucket and a second CloudFront origin for the new S3 bucket. Create a CloudFront origin group that contains both origins. Configure origin weighting for the origin group.
- F. Create two Lambda@Edge functions.
- G. Use each function to serve one of the application versions. Set up a CloudFront weighted Lambda@Edge invocation policy.

Answer: A

NEW QUESTION 101

- (Exam Topic 2)

A finance company is storing financial records in an Amazon S3 bucket. The company persists a record for every financial transaction. According to regulatory requirements, the records cannot be modified for at least 1 year after they are written. The records are read on a regular basis and must be immediately accessible. Which solution will meet these requirements?

- A. Create a new S3 bucket.
- B. Turn on S3 Object Lock, set a default retention period of 1 year, and set the retention mode to compliance mode.
- C. Store all records in the new S3 bucket.
- D. Create an S3 Lifecycle rule to immediately transfer new objects to the S3 Glacier storage tier. Create an S3 Glacier Vault Lock policy that has a retention period of 1 year.
- E. Create an S3 Lifecycle rule to immediately transfer new objects to the S3 Intelligent-Tiering storage tier. Set a retention period of 1 year.
- F. Create an S3 bucket policy with a Deny action for PutObject operations with a condition where the s3:x-amz-object-retention header is not equal to 1 year.

Answer: A

NEW QUESTION 103

- (Exam Topic 2)

A company that runs applications on AWS recently subscribed to a new software-as-a-service (SaaS) data vendor. The vendor provides the data by way of a REST API that the vendor hosts in its AWS environment. The vendor offers multiple options for connectivity to the API and is working with the company to find the best way to connect. The company's AWS account does not allow outbound internet access from its AWS environment. The vendor's services run on AWS in the same AWS Region as the company's applications. A solutions architect must implement connectivity to the vendor's API so that the API is highly available in the company's VPC. Which solution will meet these requirements?

- A. Connect to the vendor's public API address for the data service.
- B. Connect to the vendor by way of a VPC peering connection between the vendor's VPC and the company's VPC.
- C. Connect to the vendor by way of a VPC endpoint service that uses AWS PrivateLink.
- D. Connect to a public bastion host that the vendor provides. Tunnel the API traffic.

Answer: C

NEW QUESTION 105

- (Exam Topic 2)

A company runs a proprietary stateless ETL application on an Amazon EC2 Linux instance. The application is a Linux binary, and the source code cannot be modified. The application is single-threaded, uses 2 GB of RAM, and is highly CPU intensive. The application is scheduled to run every 4 hours and runs for up to 20 minutes. A solutions architect wants to revise the architecture for the solution. Which strategy should the solutions architect use?

- A. Use AWS Lambda to run the application.
- B. Use Amazon CloudWatch Logs to invoke the Lambda function every 4 hours.
- C. Use AWS Batch to run the application. Use an AWS Step Functions state machine to invoke the AWS Batch job every 4 hours.
- D. Use AWS Fargate to run the application. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke the Fargate task every 4 hours.
- E. Use Amazon EC2 Spot Instances to run the application. Use AWS CodeDeploy to deploy and run the application every 4 hours.

Answer: C

NEW QUESTION 109

- (Exam Topic 2)

A company wants to migrate its website from an on-premises data center onto AWS. At the same time it wants to migrate the website to a containerized microservice-based architecture to improve the availability and cost efficiency. The company's security policy states that privileges and network permissions must be configured according to best practice, using least privilege. A solutions architect must create a containerized architecture that meets the security requirements and has deployed the application to an Amazon ECS cluster. What steps are required after the deployment to meet the requirements? (Select TWO.)

- A. Create tasks using the bridge network mode
- B. Create tasks using the awsvpc network mode
- C. Apply security groups to Amazon EC2 instances and use IAM roles for EC2 instances to access other resources
- D. Apply security groups to the tasks, and pass IAM credentials into the container at launch time to access other resources
- E. Apply security groups to the tasks; and use IAM roles for tasks to access other resources

Answer: BE

NEW QUESTION 113

- (Exam Topic 2)

A company has more than 10,000 sensors that send data to an on-premises Apache Kafka server by using the Message Queuing Telemetry Transport (MQTT) protocol. The on-premises Kafka server transforms the data and then stores the results as objects in an Amazon S3 bucket. Recently, the Kafka server crashed. The company lost sensor data while the server was being restored. A solutions architect must create a new design on AWS that is highly available and scalable to prevent a similar occurrence. Which solution will meet these requirements?

- A. Launch two Amazon EC2 instances to host the Kafka server in an active/standby configuration across two Availability Zones
- B. Create a domain name in Amazon Route 53. Create a Route 53 failover policy. Route the sensors to send the data to the domain name.
- C. Migrate the on-premises Kafka server to Amazon Managed Streaming for Apache Kafka (Amazon MSK). Create a Network Load Balancer (NLB) that points to the Amazon MSK broker.
- D. Enable NLB health checks. Route the sensors to send the data to the NLB.
- E. Deploy AWS IoT Core, and connect it to an Amazon Kinesis Data Firehose delivery stream. Use an AWS Lambda function to handle data transformation. Route the sensors to send the data to AWS IoT Core.
- F. Deploy AWS IoT Core, and launch an Amazon EC2 instance to host the Kafka server. Configure AWS IoT Core to send the data to the EC2 instance. Route the sensors to send the data to AWS IoT Core.

Answer: A

NEW QUESTION 116

- (Exam Topic 2)

A development team is deploying new APIs as serverless applications within a company. The team is currently using the AWS Management Console to provision Amazon API Gateway, AWS Lambda, and Amazon DynamoDB resources. A solutions architect has been tasked with automating the future deployments of these serverless APIs. How can this be accomplished?

- A. Use AWS CloudFormation with a Lambda-backed custom resource to provision API Gateway. Use the `MyDynamoDB::Table` and `AWS::Lambda::Function` resources to create the Amazon DynamoDB table and Lambda functions. Write a script to automate the deployment of the CloudFormation template.
- B. Use the AWS Serverless Application Model to define the resources. Upload a YAML template and application files to the code repository. Use AWS CodePipeline to connect to the code repository and to create an action to build using AWS CodeBuild.
- C. Use the AWS CloudFormation deployment provider in CodePipeline to deploy the solution.
- D. Use AWS CloudFormation to define the serverless application.
- E. Implement versioning on the Lambda functions and create aliases to point to the version.
- F. When deploying, configure weights to implement shifting traffic to the newest version, and gradually update the weights as traffic moves over.
- G. Commit the application code to the AWS CodeCommit code repository.
- H. Use AWS CodePipeline and connect to the CodeCommit code repository. Use AWS CodeBuild to build and deploy the Lambda functions using AWS CodeDeploy. Specify the deployment preference type in CodeDeploy to gradually shift traffic over to the new version.

Answer: B

NEW QUESTION 118

- (Exam Topic 2)

A company uses AWS Organizations with a single OU named Production to manage multiple accounts. All accounts are members of the Production OU. Administrators use deny list SCPs in the root of the organization to manage access to restricted services. The company recently acquired a new business unit and invited the new unit's existing AWS account to the organization. Once onboarded, the administrators of the new business unit discovered that they are not able to update existing AWS Config rules to meet the company's policies. Which option will allow administrators to make changes and continue to enforce the current policies without introducing additional long-term maintenance?

- A. Remove the organization's root SCPs that limit access to AWS Config. Create AWS Service Catalog products for the company's standard AWS Config rules and deploy them throughout the organization, including the new account.
- B. Create a temporary OU named Onboarding for the new account. Apply an SCP to the Onboarding OU to allow AWS Config actions. Move the new account to the Production OU when adjustments to AWS Config are complete.
- C. Convert the organization's root SCPs from deny list SCPs to allow list SCPs to allow the required services only. Temporarily apply an SCP to the organization's root that allows AWS Config actions for principals only in the new account.
- D. Create a temporary OU named Onboarding for the new account. Apply an SCP to the Onboarding OU to allow AWS Config actions.
- E. Move the organization's root SCP to the Production OU.
- F. Move the new account to the Production OU when adjustments to AWS Config are complete.

Answer: D

NEW QUESTION 122

- (Exam Topic 2)

A company is using a lift-and-shift strategy to migrate applications from several on-premises Windows servers to AWS. The Windows servers will be hosted on Amazon EC2 instances in the us-east-1 Region. The company's security policy allows the installation of migration tools on servers. The migration data must be encrypted in transit and encrypted at rest. The applications are business critical. The company needs to minimize the cutover window and minimize the downtime that results from the migration. The company wants to use Amazon CloudWatch and AWS CloudTrail for monitoring. Which solution will meet these requirements?

- A. Use AWS Application Migration Service (CloudEnsure Migration) to migrate the Windows servers to AW
- B. Create a Replication Settings templat
- C. Install the AWS Replication Agent on the source servers
- D. Use AWS DataSync to migrate the Windows servers to AW
- E. Install the DataSync agent on the source server
- F. Configure a blueprint for the target server
- G. Begin the replication process.
- H. Use AWS Server Migration Service (AWS SMS) to migrate the Windows servers to AW
- I. Install the SMS Connector on the source server
- J. Replicate the source servers to AW
- K. Convert the replicated volumes to AMIs to launch EC2 instances.
- L. Use AWS Migration Hub to migrate the Windows servers to AW
- M. Create a project in Migration Hub.Track the progress of server migration by using the built-in dashboard.

Answer: A

NEW QUESTION 123

- (Exam Topic 2)

A company is migrating its infrastructure to the AW5 Cloud. The company must comply with a variety of regulatory standards for different projects. The company needs a multi-account environment.

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

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

- A. Create an organization In AWS Organizations Create a single SCP for least privilege access across all accounts Create a single OU for all accounts Configure an IAM identity provider tor federation with the on-premises AD FS server Configure a central togging account with a defined process for log generating services to send log events to the central accoun
- B. Enable AWS Config in the central account with conformance packs for all accounts.
- C. Create an organization In AWS Organizations Enable AWS Control Tower on the organizatio
- D. Review included guardrails for SCP
- E. Check AWS Config for areas that require additions Add OUs as necessary Connect AWS Single Sign-On to the on-premises AD FS server
- F. Create an organization in AWS Organizations Create SCPs for least privilege access Create an OU structure, and use it to group AWS accounts Connect AWS Single Sign-On to the on-premises AD FS serve
- G. Configure a central logging account with a defined process for tog generating services to send log events to the central account Enable AWS Config in the central account with aggregators and conformance packs.
- H. Create an organization in AWS Organizations Enable AWS Control Tower on the organization Review included guardrails for SCP
- I. Check AWS Config for areas that require additions Configure an IAM identity provider for federation with the on-premises AD FS server.

Answer: A

NEW QUESTION 124

- (Exam Topic 2)

A company has multiple business units Each business unit has its own AWS account and runs a single website within that account. The company also has a single logging account. Logs from each business unit website are aggregated into a single Amazon S3 bucket in the logging account. The S3 bucket policy provides each business unit with access to write data into the bucket and requires data to be encrypted.

The company needs to encrypt logs uploaded into the bucket using a Single AWS Key Management Service

{AWS KMS) CMK The CMK that protects the data must be rotated once every 365 days

Which strategy is the MOST operationally efficient for the company to use to meet these requirements?

- A. Create a customer managed CMK ri the logging account Update the CMK key policy to provide access to the logging account only Manually rotate the CMK every 365 days.
- B. Create a customer managed CMK in the logging accoun
- C. Update the CMK key policy to provide access to the logging account and business unit account
- D. Enable automatic rotation of the CMK
- E. Use an AWS managed CMK m the togging account
- F. Update the CMK key policy to provide access to the logging account and business unit accounts Manually rotate the CMK every 365 days.
- G. Use an AWS managed CMK in the togging account Update the CMK key policy to provide access to the togging account onl
- H. Enable automatic rotation of the CMK.

Answer: A

NEW QUESTION 128

- (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 rote.
- 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 130

- (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 133

- (Exam Topic 2)

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

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

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

Which solution will meet these requirements?

- A. Set up DynamoDB Accelerator (DAX) as in-memory cache
- B. Update the application to use DAX
- C. Create an Auto Scaling group for the EC2 instance
- D. Create an Application Load Balancer (ALB). Set the Auto Scaling group as a target for the ALB
- E. Update the Route 53 record to use a simple routing policy that targets the ALB's DNS alias
- F. Configure scheduled scaling for the EC2 instances before the content updates.
- G. Set up Amazon ElastiCache for Redis
- H. Update the application to use ElastiCache
- I. Create an Auto Scaling group for the EC2 instance
- J. Create an Amazon CloudFront distribution
- K. and set the Auto Scaling group as an origin for the distribution
- L. Update the Route 53 record to use a simple routing policy that targets the CloudFront distribution's DNS alias. Manually scale up EC2 instances before the content updates
- M. Set up Amazon ElastiCache for Memcached
- N. Update the application to use ElastiCache
- O. Create an Auto Scaling group for the EC2 instances. Create an Application Load Balancer (ALB). Set the Auto Scaling group as a target for the ALB
- P. Update the Route 53 record to use a simple routing policy that targets the ALB's DNS alias
- Q. Configure scheduled scaling for the application before the content updates.
- R. Set up DynamoDB Accelerator (DAX) as in-memory cache
- S. Update the application to use DAX
- T. Create an Auto Scaling group for the EC2 instance
- . Create an Amazon CloudFront distribution, and set the Auto Scaling group as an origin for the distribution
- . Update the Route 53 record to use a simple routing policy that targets the CloudFront distribution's DNS alias
- . Manually scale up EC2 instances before the content updates.

Answer: B

NEW QUESTION 138

- (Exam Topic 2)

A large company runs workloads in VPCs that are deployed across hundreds of AWS accounts. Each VPC consists of public subnets and private subnets that span across multiple Availability Zones. NAT gateways are deployed in the public subnets and allow outbound connectivity to the internet from the private subnets.

A solutions architect is working on a hub-and-spoke design. All private subnets in the spoke VPCs must route traffic to the internet through an egress VPC. The solutions architect already has deployed a NAT gateway in an egress VPC in a central AWS account.

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

- A. Create peering connections between the egress VPC and the spoke VPCs. Configure the required routing to allow access to the internet
- B. Create a transit gateway and share it with the existing AWS accounts. Attach existing VPCs to the transit gateway. Configure the required routing to allow access to the internet
- C. Create a transit gateway in every account. Attach the NAT gateway to the transit gateways. Configure the required routing to allow access to the internet
- D. Create an AWS PrivateLink connection between the egress VPC and the spoke VPCs. Configure the required routing to allow access to the internet

Answer: B

NEW QUESTION 139

- (Exam Topic 2)

A company has an organization that has many AWS accounts in AWS Organizations. A solutions architect must improve how the company manages common security group rules for the AWS accounts in the organization.

The company has a common set of IP CIDR ranges in an allow list in each AWS account to allow access to and from the company's on-premises network. Developers within each account are responsible for adding new IP CIDR ranges to their security groups. The security team has its own AWS account. Currently, the security team notifies the owners of the other AWS accounts when changes are made to the allow list.

The solutions architect must design a solution that distributes the common set of CIDR ranges across all accounts. Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Set up an Amazon Simple Notification Service (Amazon SNS) topic in the security team's AWS account. Deploy an AWS Lambda function in each AWS account. Configure the Lambda function to run every time an SNS topic receives a message. Configure the Lambda function to take an IP address as input and add it to a list of security groups in the account. Instruct the security team to distribute changes by publishing messages to its SNS topic.
- B. Create new customer-managed prefix lists in each AWS account within the organization. Populate the prefix lists in each account with all internal CIDR ranges. Notify the owner of each AWS account to allow the new customer-managed prefix list IDs in their accounts in their security groups. Instruct the security team to share updates with each AWS account owner.
- C. Create a new customer-managed prefix list in the security team's AWS account. Populate the customer-managed prefix list with all internal CIDR range.
- D. Share the customer-managed prefix list... organization by using AWS Resource Access Manager. Notify the owner of each AWS account to allow the new customer-managed prefix list ID in their security groups.

Answer: A

NEW QUESTION 144

- (Exam Topic 2)

A company is configuring connectivity to a multi-account AWS environment to support application workloads that serve users in a single geographic region. The workloads depend on a highly available, on-premises legacy system deployed across two locations. It is critical for the AWS workloads to maintain connectivity to the legacy system, and a minimum of 5 Gbps of bandwidth is required. All application workloads within AWS must have connectivity with one another. Which solution will meet these requirements?

- A. Configure multiple AWS Direct Connect (DX) 10 Gbps dedicated connections from a DX partner for each on-premises location. Create private virtual interfaces on each connection for each AWS account VPC. Associate each private virtual interface with a virtual private gateway attached to each VPC.
- B. Configure multiple AWS Direct Connect (DX) 10 Gbps dedicated connections from two DX partners for each on-premises location. Create and attach a virtual private gateway for each AWS account VPC.
- C. Create a DX gateway in a central network account and associate it with the virtual private gateways. Create a public virtual interface on each DX connection and associate the interface with the DX gateway.
- D. Configure multiple AWS Direct Connect (DX) 10 Gbps dedicated connections from two DX partners for each on-premises location. Create a transit gateway and a DX gateway in a central network account.
- E. Create a transit virtual interface for each DX interface and associate them with the DX gateway.
- F. Create a gateway association between the DX gateway and the transit gateway.
- G. Configure multiple AWS Direct Connect (DX) 10 Gbps dedicated connections from a DX partner for each on-premises location. Create and attach a virtual private gateway for each AWS account VPC.
- H. Create a transit gateway in a central network account and associate it with the virtual private gateways. Create a transit virtual interface on each DX connection and attach the interface to the transit gateway.

Answer: B

NEW QUESTION 146

- (Exam Topic 2)

A company's CI/CD 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 151

- (Exam Topic 2)

A new startup is running a serverless application using AWS Lambda as the primary source of compute. New versions of the application must be made available to a subset of users before deploying changes to all users. Developers should also have the ability to stop the deployment and have access to an easy rollback mechanism. A solutions architect decides to use AWS CodeDeploy to deploy changes when a new version is available.

Which CodeDeploy configuration should the solutions architect use?

- A. A blue/green deployment
- B. A linear deployment
- C. A canary deployment
- D. An all-at-once deployment

Answer: C

NEW QUESTION 156

- (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 bucket
- 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 161

- (Exam Topic 2)

A retail company runs a business-critical web service on an Amazon Elastic Container Service (Amazon ECS) cluster that runs on Amazon EC2 instances The web service receives POST requests from end users and writes data to a MySQL database that runs on a separate EC2 instance The company needs to ensure that data loss does not occur.

The current code deployment process includes manual updates of the ECS service During a recent deployment, end users encountered intermittent 502 Bad Gateway errors in response to valid web requests

The company wants to implement a reliable solution to prevent this issue from recurring. The company also wants to automate code deployments. The solution must be highly available and must optimize cost-effectiveness

- A. Run the web service on an ECS cluster that has a Fargate launch type Use AWS CodePipeline and AWS CodeDeploy to perform a blue/green deployment with validation testing to update the ECS service.
- B. Migrate the MySQL database to run on an Amazon RDS for MySQL Multi-AZ DB instance that uses Provisioned IOPS SSD (io2) storage
- C. Configure an Amazon Simple Queue Service (Amazon SQS) queue as an event source to receive the POST requests from the web service Configure an AWS Lambda function to poll the queue Write the data to the database.
- D. Run the web service on an ECS cluster that has a Fargate launch type Use AWS CodePipeline and AWS CodeDeploy to perform a canary deployment to update the ECS service.

Answer: CD

NEW QUESTION 162

- (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 PRO 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 PRO 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 PRO 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 166

- (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 'or Mloggers 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 blog 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 168

- (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 1AM role that is associated with the Lambda function in the shared services account.
- E. Add a custom resource to the Cloud Formation 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 1AM role with the directconnect:' permission.
- H. Create a cross-account 1AM role in the shared services account that grants the sts: Assume Role permission to the Lambda function with the directconnect:"permission acting as a resourc
- I. Add the sts AssumeRole permission with this cross-account 1AM role as a resource to the 1AM role that belongs to the Lambda function in the project account.
- J. Add a custom resource to the Cloud Formation networking stack that references the Lambda function in the shared services account.

Answer: BCE

NEW QUESTION 169

- (Exam Topic 2)

A company is launching a web-based application in multiple regions around the world The application consists of both static content stored in a private Amazon S3 bucket and dyna ECS containers behind an Application Load Balancer (ALB) The company requires that the static and dynamic application content be accessible through Amazon CloudFront only

Which combination of steps should a solutions architect recommend to restrict direct content access to CloudFront? (Select THREE)

- A. Create a web ACL in AWS WAF with a rule to validate the presence of a custom header and associate the web ACL with the ALB
- B. Create a web ACL in AWS WAF with a rule to validate the presence of a custom header and associate the web ACL with the CloudFront distribution
- C. Configure CloudFront to add a custom header to origin requests
- D. Configure the ALB to add a custom header to HTTP requests
- E. Update the S3 bucket ACL to allow access from the CloudFront distribution only
- F. Create a CloudFront Origin Access Identity (OAI) and add it to the CloudFront distribution Update the S3 bucket policy to allow access to the OAI only

Answer: ACF

NEW QUESTION 170

- (Exam Topic 2)

A company has IoT sensors that monitor traffic patterns throughout a large city. The company wants to read and collect data from the sensors and perform aggregations on the data.

A solutions architect designs a solution in which the IoT devices are streaming to Amazon Kinesis Data Streams. Several applications are reading from the stream. However, several consumers are experiencing throttling and are periodically encountering a ReadProvisionedThroughputExceeded error.

Which actions should the solutions architect take to resolve this issue? (Select THREE.)

- A. Reshard the stream to increase the number of shards in the stream.
- B. Use the Kinesis Producer Library (KPL). Adjust the polling frequency.
- C. Use consumers with the enhanced fan-out feature.
- D. Reshard the stream to reduce the number of shards in the stream.
- E. Use an error retry and exponential backoff mechanism in the consumer logic.
- F. Configure the stream to use dynamic partitioning.

Answer: ACD

NEW QUESTION 175

- (Exam Topic 2)

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

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

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

Which combination of steps should a solutions architect recommend to avoid a recurrence of this issue? (Select TWO)

- A. Modify the Auto Scaling group by setting the Update policy to target the oldest launch configuration for replacement.
- B. Create a new Auto Scaling group before the next patch maintenance During the maintenance window patch both groups and reboot the instances.
- C. Create an Elastic Load Balancer in front of the Auto Scaling group Configure monitoring to ensure that target group health checks return healthy after the Auto Scaling group replaces the terminated instances
- D. Create automation scripts to patch an AM
- E. update the launch configuration, and invoke an Auto Scaling instance refresh.
- F. Create an Elastic Load Balancer in front of the Auto Scaling group Configure termination protection on the instances.

Answer: AC

NEW QUESTION 178

- (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 libranes 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 179

- (Exam Topic 2)

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

- A. Upload the AWS CloudFormation template to Amazon S3. Give users in the QA department permission to assume the manager's role and add a policy that restricts the permissions to the template and the resources it creates Train users to launch the template from the CloudFormation console
- B. Create an AWS Service Catalog product from the environment template Add a launch constraint to the product with the existing role Give users in the QA department permission to use AWS Service Catalog APIs only_ Train users to launch the template from the AWS Service Catalog console.
- C. Upload the AWS CloudFormation template to Amazon S3 Give users in the QA department permission to use CloudFormation and S3 APIs, with conditions that restrict the permissions to the template and the resources it creates Train users to launch the template from the CloudFormation console.
- D. Create an AWS Elastic Beanstalk application from the environment template Give users in the QA department permission to use Elastic Beanstalk permissions only Train users to launch Elastic Beanstalk environments with the Elastic Beanstalk CLI, passing the existing role to the environment as a service role

Answer: B

NEW QUESTION 180

- (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 182

- (Exam Topic 2)

A company wants to deploy an API to AWS. The company plans to run the API on AWS Fargate behind a load balancer. The API requires the use of header-based routing and must be accessible from on-premises networks through an AWS Direct Connect connection and a private VIF.

The company needs to add the client IP addresses that connect to the API to an allow list in AWS. The company also needs to add the IP addresses of the API to the allow list. The company's security team will allow /27 CIDR ranges to be added to the allow list. The solution must minimize complexity and operational overhead.

Which solution will meet these requirements?

- A. Create a new Network Load Balancer (NLB) in the same subnets as the Fargate task deployments.Create a security group that includes only the client IP addresses that need access to the AP
- B. Attach the new security group to the Fargate task
- C. Provide the security team with the NLB's IP addresses for the allow list.
- D. Create two new /27 subnet
- E. Create a new Application Load Balancer (ALB) that extends across the new subnet
- F. Create a security group that includes only the client IP addresses that need access to the AP
- G. Attach the security group to the AL
- H. Provide the security team with the new subnet IP ranges for the allow list.
- I. Create two new '27 subnet
- J. Create a new Network Load Balancer (NLB) that extends across the new subnet
- K. Create a new Application Load Balancer (ALB) within the new subnet
- L. Create a security group that includes only the client IP addresses that need access to the AP
- M. Attach the security group to the AL
- N. Add the ALB's IP addresses as targets behind the NL
- O. Provide the security team with the NLB's IP addresses for the allow list.
- P. Create a new Application Load Balancer (ALB) in the same subnets as the Fargate task deployments.Create a security group that includes only the client IP

addresses that need access to the AP

Q. Attach the security group to the AL

R. Provide the security team with the ALB's IP addresses for the allow list.

Answer: A

NEW QUESTION 184

- (Exam Topic 2)

A solutions architect has implemented a SAML 2.0 federated identity solution with their company's on-premises identity provider (IdP) to authenticate users' access to the AWS environment. When the solutions architect tests authentication through the federated identity web portal access to the AWS environment is granted. However, when test users attempt to authenticate through the federated identity web portal, they are not able to access the AWS environment.

Which items should the solutions architect check to ensure identity federation is properly configured? (Select THREE)

- A. The IAM user's permissions policy has allowed the use of SAML federation for that user
- B. The IAM roles created for the federated users' or federated groups' trust policy have set the SAML provider as the principle.
- C. Test users are not in the AWSFederatedUsers group in the company's IdP
- D. The web portal calls the AWS STS AssumeRoleWithSAML API with the ARN of the SAML provider the ARN of the IAM role, and the SAML assertion from IdP
- E. The on-premises IdP's DNS hostname is reachable from the AWS environment VPCs.
- F. The company's IdP defines SAML assertions that properly map users or groups in the company to IAM roles with appropriate permissions

Answer: BCF

NEW QUESTION 187

- (Exam Topic 2)

A company is creating a sequel for a popular online game. A large number of users from all over the world will play the game within the first week after launch.

Currently, the game consists of the following components deployed in a single AWS Region:

- Amazon S3 bucket that stores game assets
- Amazon DynamoDB table that stores player scores

A solutions architect needs to design a multi-Region solution that will reduce latency improve reliability, and require the least effort to implement

What should the solutions architect do to meet these requirements?

- A. Create an Amazon CloudFront distribution to serve assets from the S3 bucket. Configure S3 Cross-Region Replication. Create a new DynamoDB table in a new Region. Use the new table as a replica target for DynamoDB global tables.
- B. Create an Amazon CloudFront distribution to serve assets from the S3 bucket.
- C. Configure S3 Same-Region Replication.
- D. Create a new DynamoDB table in a new Region.
- E. Configure asynchronous replication between the DynamoDB tables by using AWS Database Migration Service (AWS DMS) with change data capture (CDC).
- F. Create another S3 bucket in a new Region and configure S3 Cross-Region Replication between the buckets. Create an Amazon CloudFront distribution and configure origin failover with two origins accessing the S3 buckets in each Region.
- G. Configure DynamoDB global tables by enabling Amazon DynamoDB Streams, and add a replica table in a new Region.
- H. Create another S3 bucket in the same Region, and configure S3 Same-Region Replication between the buckets. Create an Amazon CloudFront distribution and configure origin failover with two origins accessing the S3 buckets. Create a new DynamoDB table in a new Region. Use the new table as a replica target for DynamoDB global tables.

Answer: C

NEW QUESTION 192

- (Exam Topic 2)

An auction website enables users to bid on collectible items. The auction rules require that each bid is processed only once and in the order it was received. The current implementation is based on a fleet of Amazon EC2 web servers that write bid records into Amazon Kinesis Data Streams. A single large instance has a cron job that runs the bid processor, which reads incoming bids from Kinesis Data Streams and processes each bid. The auction site is growing in popularity, but users are complaining that some bids are not registering.

Troubleshooting indicates that the bid processor is too slow during peak demand hours, sometimes crashes while processing, and occasionally loses track of which record is being processed.

What changes should be made to make the bid processing more reliable?

- A. Refactor the web application to use the Amazon Kinesis Producer Library (KPL) when posting bids to Kinesis Data Streams. Refactor the bid processor to flag each record in Kinesis Data Streams as being unread, processed, and processed. At the start of each bid processing run; scan Kinesis Data Streams for unprocessed records.
- B. Refactor the web application to post each incoming bid to an Amazon SNS topic in place of Kinesis Data Streams. Configure the SNS topic to trigger an AWS Lambda function that
- C. processes each bid as soon as a user submits it.
- D. Refactor the web application to post each incoming bid to an Amazon SQS FIFO queue in place of Kinesis Data Streams. Refactor the bid processor to continuously consume the SQS queue. Place the bid processing EC2 instance in an Auto Scaling group with a minimum and a maximum size of 1.
- E. Switch the EC2 instance type from t2 large to a larger general compute instance type. Put the bid processor EC2 instances in an Auto Scaling group that scales out the number of EC2 instances running the bid processor based on the incomingRecords metric in Kinesis Data Streams.

Answer: C

Explanation:

<https://aws.amazon.com/sqs/faqs/#:~:text=A%20single%20Amazon%20SQS%20message,20%2C000%20for%2>

NEW QUESTION 194

- (Exam Topic 2)

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

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

- A. Call the MoveAccount operation in the Organizations API from the old organization's management account to migrate the developer accounts to the new developer organization
- B. From the management account remove each developer account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API
- C. From each developer account, remove the account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API
- D. Sign in to the new developer organization's management account and create a placeholder member account that acts as a target for the developer account migration
- E. Call the InviteAccountToOrganization operation in the Organizations API from the new developer organization's management account to send invitations to the developer accounts.
- F. Have each developer sign in to their account and confirm to join the new developer organization.

Answer: BDE

NEW QUESTION 198

- (Exam Topic 2)

A mobile gaming company is expanding into the global market. The company's game servers run in the us-east-1 Region. The game's client application uses UDP to communicate with the game servers and needs to be able to connect to a set of static IP addresses. The company wants its game to be accessible on multiple continents. The company also wants the game to maintain its network performance and global availability.

Which solution meets these requirements?

- A. Provision an Application Load Balancer (ALB) in front of the game servers Create an Amazon CloudFront distribution that has no geographical restrictions Set the ALB as the origin Perform DNS lookups for the cloudfront net domain name Use the resulting IP addresses in the game's client application.
- B. Provision game servers in each AWS Region
- C. Provision an Application Load Balancer in front of the game server
- D. Create an Amazon Route 53 latency-based routing policy for the game's client application to use with DNS lookups
- E. Provision game servers in each AWS Region Provision a Network Load Balancer (NLB) in front of the game servers Create an accelerator in AWS Global Accelerator, and configure endpoint groups in each Region Associate the NLBs with the corresponding Regional endpoint groups Point the game client's application to the Global Accelerator endpoints
- F. Provision game servers in each AWS Region Provision a Network Load Balancer (NLB) in front of the game servers Create an Amazon CloudFront distribution that has no geographical restrictions Set the NLB as the origin Perform DNS lookups for the cloudfront net domain name
- G. Use the resulting IP addresses in the game's client application

Answer: A

NEW QUESTION 202

- (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 Tasks
- 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 207

- (Exam Topic 2)

A company is refactoring its on-premises order-processing platform in the AWS Cloud. The platform includes a web front end that is hosted on a fleet of VMs RabbitMQ to connect the front end to the backend, and a Kubernetes cluster to run a containerized backend system to process the orders. The company does not want to make any major changes to the application

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

- A. Create an AMI of the web server VM Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer Set up Amazon MQ to replace the on-premises messaging queue Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend
- B. Create a custom AWS Lambda runtime to mimic the web server environment Create an Amazon API Gateway API to replace the front-end web servers Set up Amazon MQ to replace the on-premises messaging queue Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend
- C. Create an AMI of the web server VM Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer Set up Amazon MQ to replace the on-premises messaging queue Install Kubernetes on a fleet of different EC2 instances to host the order-processing backend
- D. Create an AMI of the web server VM Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer Set up an Amazon Simple Queue Service (Amazon SQS) queue to replace the on-premises messaging queue Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend

Answer: A

NEW QUESTION 210

- (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 AWSJAM 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 APIGateway
- B. For the API Gateway resource set CORS to enabled and only return the company's domain inAccess-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 212

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SAP-C02 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SAP-C02-dumps.html>