

Exam Questions SAP-C01

AWS Certified Solutions Architect- Professional

<https://www.2passeasy.com/dumps/SAP-C01/>



NEW QUESTION 1

An organization has two Amazon EC2 instances:

- The first is running an ordering application and an inventory application.
- The second is running a queuing system.

During certain times of the year, several thousand orders are placed per second. Some orders were lost when the queuing system was down. Also, the organization's inventory application has the incorrect quantity of products because some orders were processed twice. What should be done to ensure that the applications can handle the increasing number of orders?

- A. Put the ordering and inventory applications into their own AWS Lambda function
- B. Have the ordering application write the messages into an Amazon SQS FIFO queue.
- C. Put the ordering and inventory applications into their own Amazon ECS containers and create an Auto Scaling group for each applicatio
- D. Then, deploy the message queuing server in multiple AvailabilityZones.
- E. Put the ordering and inventory applications into their own Amazon EC2 instances, and create an Auto Scaling group for each applicatio
- F. Use Amazon SQS standard queues for the incoming orders, and implement idempotency in the inventory application.
- G. Put the ordering and inventory applications into their own Amazon EC2 instance
- H. Write the incoming orders to an Amazon Kinesis data stream Configure AWS Lambda to poll the stream and update the inventory application.

Answer: C

Explanation:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/standard-queues.html>

NEW QUESTION 2

A company has an Amazon EC2 deployment that has the following architecture:

- An application tier that contains 8 m4.xlarge instances
- A Classic Load Balancer
- Amazon S3 as a persistent data store

After one of the EC2 instances fails, users report very slow processing of their requests. A Solutions Architect must recommend design changes to maximize system reliability. The solution must minimize costs.

What should the Solution Architect recommend?

- A. Migrate the existing EC2 instances to a serverless deployment using AWS Lambda functions
- B. Change the Classic Load Balancer to an Application Load Balancer
- C. Replace the application tier with m4.large instances in an Auto Scaling group
- D. Replace the application tier with 4 m4.2xlarge instances

Answer: B

Explanation:

By default, connection draining is enabled for Application Load Balancers but must be enabled for Classic Load Balancers. When Connection Draining is enabled and configured, the process of deregistering an instance from an Elastic Load Balancer gains an additional step. For the duration of the configured timeout, the load balancer will allow existing, in-flight requests made to an instance to complete, but it will not send any new requests to the instance. During this time, the API will report the status of the instance as InService, along with a message stating that "Instance deregistration currently in progress." Once the timeout is reached, any remaining connections will be forcibly closed. <https://docs.aws.amazon.com/autoscaling/ec2/userguide/attach-load-balancer-asg.html>
<https://aws.amazon.com/blogs/aws/elb-connection-draining-remove-instances-from-service-with-care/>

NEW QUESTION 3

A company wants to follow its website on AWS using serverless architecture design patterns for global customers. The company has outlined its requirements as follow:

- The website should be responsive.
- The website should offer minimal latency.
- The website should be highly available.
- Users should be able to authenticate through social identity providers such as Google, Facebook, and Amazon.
- There should be baseline DDoS protections for spikes in traffic.

How can the design requirements be met?

- A. Use Amazon CloudFront with Amazon ECS for hosting the websit
- B. Use AWS Secrets Manager for provide user management and authentication function
- C. Use ECS Docker containers to build an API.
- D. Use Amazon Route 53 latency routing with an Application Load Balancer and AWS Fargate in different regions for hosting the websit
- E. use Amazon Cognito to provide user management and authentication function
- F. Use Amazon EKS containers.
- G. Use Amazon CloudFront with Amazon S3 for hosting static web resource
- H. Use Amazon Cognito to provide user management authentication function
- I. Use Amazon API Gateway with AWS Lambda to build an API.
- J. Use AWS Direct Connect with Amazon CloudFront and Amazon S3 for hosting static web resource.Use Amazon Cognito to provide user management authentication function
- K. Use AWS Lambda to build an API.

Answer: C

NEW QUESTION 4

A company is designing a new highly available web application on AWS. The application requires consistent and reliable connectivity from the application servers in AWS to a backend REST API hosted in the company's on-premises environment. The backend connection between AWS and on-premises will be routed over an AWS Direct Connect connection through a private virtual interface. Amazon Route 53 will be used to manage private DNS records for the application to resolve the IP address on the backend REST API.

Which design would provide a reliable connection to the backend API?

- A. Implement at least two backend endpoints for the backend REST API, and use Route 53 health checks to monitor the availability of each backend endpoint and perform DNS-level failover.
- B. Install a second Direct Connect connection from a different network carrier and attach it to the same virtual private gateway as the first Direct Connect connection.
- C. Install a second cross connect for the same Direct Connect connection from the same network carrier, and join both connections to the same link aggregation group (LAG) on the same private virtual interface.
- D. Create an IPSec VPN connection routed over the public internet from the on-premises data center to AWS and attach it to the same virtual private gateway as the Direct Connect connection.

Answer: A

NEW QUESTION 5

A company would like to implement a serverless application by using Amazon API Gateway, AWS Lambda and Amazon DynamoDB. They deployed a proof of concept and stated that the average response time is greater than what their upstream services can accept Amazon CloudWatch metrics did not indicate any issues with DynamoDB but showed that some Lambda functions were hitting their timeout.

Which of the following actions should the Solutions Architect consider to improve performance? (Choose two.)

- A. Configure the AWS Lambda function to reuse containers to avoid unnecessary startup time.
- B. Increase the amount of memory and adjust the timeout on the Lambda function.
- C. Complete performance testing to identify the ideal memory and timeout configuration for the Lambda function.
- D. Create an Amazon ElastiCache cluster running Memcached, and configure the Lambda function for VPC integration with access to the Amazon ElastiCache cluster.
- E. Enable API cache on the appropriate stage in Amazon API Gateway, and override the TTL for individual methods that require a lower TTL than the entire stage.
- F. Increase the amount of CPU, and adjust the timeout on the Lambda function.
- G. Complete performance testing to identify the ideal CPU and timeout configuration for the Lambda function.

Answer: BD

Explanation:

<https://lumigo.io/blog/aws-lambda-timeout-best-practices/>

NEW QUESTION 6

A large company has increased its utilization of AWS over time in an unmanaged way. As such, they have a large number of independent AWS accounts across different business units, projects, and environments. The company has created a Cloud Center of Excellence team, which is responsible for managing all aspects of the AWS Cloud, including their AWS accounts.

Which of the following should the Cloud Center of Excellence team do to BEST address their requirements in a centralized way? (Select two.)

- A. Control all AWS account root user credential
- B. Assign AWS IAM users in the account of each user who needs to access AWS resource
- C. Follow the policy of least privilege in assigning permissions to each user.
- D. Tag all AWS resources with details about the business unit, project, and environment
- E. Send all AWS Cost and Usage reports to a central Amazon S3 bucket, and use tools such as Amazon Athena and Amazon QuickSight to collect billing details by business unit.
- F. Use the AWS Marketplace to choose and deploy a Cost Management tool
- G. Tag all AWS resources with details about the business unit, project, and environment
- H. Send all AWS Cost and Usage reports for the AWS accounts to this tool for analysis.
- I. Set up AWS Organization
- J. Enable consolidated billing, and link all existing AWS accounts to a master billing account
- K. Tag all AWS resources with details about the business unit, project and environment
- L. Analyze Cost and Usage reports using tools such as Amazon Athena and Amazon QuickSight to collect billing details by business unit.
- M. Using a master AWS account, create IAM users within the master account
- N. Define IAM roles in the other AWS accounts, which cover each of the required functions in the account
- O. Follow the policy of least privilege in assigning permissions to each role, then enable the IAM users to assume the roles that they need to use.

Answer: DE

NEW QUESTION 7

A company uses Amazon S3 to store documents that may only be accessible to an Amazon EC2 instance in a certain virtual private cloud (VPC). The company fears that a malicious insider with access to this instance could also set up an EC2 instance in another VPC to access these documents.

Which of the following solutions will provide the required protection?

- A. Use an S3 VPC endpoint and an S3 bucket policy to limit access to this VPC endpoint.
- B. Use EC2 instance profiles and an S3 bucket policy to limit access to the role attached to the instance profile.
- C. Use S3 client-side encryption and store the key in the instance metadata.
- D. Use S3 server-side encryption and protect the key with an encryption context.

Answer: A

Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html>

Endpoint connections cannot be extended out of a VPC. Resources on the other side of a VPN connection, VPC peering connection, AWS Direct Connect connection, or ClassicLink connection in your VPC cannot use the endpoint to communicate with resources in the endpoint service.

NEW QUESTION 8

A company is running an email application across multiple AWS Regions. The company uses Ohio (us-east-2) as the primary Region and Northern Virginia (us-east-1) as the Disaster Recovery (DR) Region. The data is continuously replicated from the primary Region to the DR Region by a single instance on the public subnet in both Regions. The replication messages between the Regions have a significant backlog during certain times of the day. The backlog clears on its own after a short time, but it affects the application's RPO.

Which of the following solutions should help remediate this performance problem? (Select TWO)

- A. Increase the size of the instances.
- B. Have the instance in the primary Region write the data to an Amazon SQS queue in the primary Region instead, and have the instance in the DR Region poll from this queue.
- C. Use multiple instances on the primary and DR Regions to send and receive the replication data.
- D. Change the DR Region to Oregon (us-west-2) instead of the current DR Region.
- E. Attach an additional elastic network interface to each of the instances in both Regions and set up load balancing between the network interfaces.

Answer: AC

NEW QUESTION 9

A company had a tight deadline to migrate its on-premises environment to AWS. It moved over Microsoft SQL Servers and Microsoft Windows Servers using the virtual machine import/export service and rebuild other applications native to the cloud. The team created both Amazon EC2 databases and used Amazon RDS. Each team in the company was responsible for migrating their applications, and they have created individual accounts for isolation of resources. The company did not have much time to consider costs, but now it would like suggestions on reducing its AWS spend.

Which steps should a Solutions Architect take to reduce costs?

- A. Enable AWS Business Support and review AWS Trusted Advisor's cost check
- B. Create Amazon EC2 Auto Scaling groups for applications that experience fluctuating demand
- C. Save AWS Simple Monthly Calculator reports in Amazon S3 for trend analysis
- D. Create a master account under Organizations and have teams join for consolidating billing.
- E. Enable Cost Explorer and AWS Business Support Reserve Amazon EC2 and Amazon RDS DB instance
- F. Use Amazon CloudWatch and AWS Trusted Advisor for monitoring and to receive cost-savings suggestion
- G. Create a master account under Organizations and have teams join for consolidated billing.
- H. Create an AWS Lambda function that changes the instance size based on Amazon CloudWatch alarms. Reserve instances based on AWS Simple Monthly Calculator suggestion
- I. Have an AWS Well-Architected framework review and apply recommendation
- J. Create a master account under Organizations and have teams join for consolidated billing.
- K. Create a budget and monitor for costs exceeding the budget
- L. Create Amazon EC2 Auto Scaling groups for applications that experience fluctuating demand
- M. Create an AWS Lambda function that changes instance sizes based on Amazon CloudWatch alarm
- N. Have each team upload their bill to an Amazon S3 bucket for analysis of team spending
- O. Use Spot instances on nightly batch processing jobs.

Answer: B

Explanation:

Import/Export supports importing and exporting data into and out of Amazon S3 buckets. For significant data sets, AWS Import/Export is often faster than Internet transfer and more cost effective than upgrading your connectivity.

NEW QUESTION 10

A company has an Amazon VPC that is divided into a public subnet and a private subnet. A web application runs in Amazon VPC, and each subnet has its own NACL. The public subnet has a CIDR of 10.0.0.0/24. An Application Load Balancer is deployed to the public subnet. The private subnet has a CIDR of 10.0.1.0/24. Amazon EC2 instances that run a web server on port 80 are launched into the private subnet.

Only network traffic that is required for the Application Load Balancer to access the web application can be allowed to travel between the public and private subnets.

What collection of rules should be written to ensure that the private subnet's NACL meets the requirement? (Select TWO.)

- A. An inbound rule for port 80 from source 0.0.0.0/0
- B. An inbound rule for port 80 from source 10.0.0.0/24
- C. An outbound rule for port 80 to destination 0.0.0.0/0
- D. An outbound rule for port 80 to destination 10.0.0.0/24
- E. An outbound rule for ports 1024 through 65535 to destination 10.0.0.0/24

Answer: BE

NEW QUESTION 10

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 for 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://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.html>

NEW QUESTION 13

A company is migrating an application to AWS. It wants to use fully managed services as much as possible during the migration. The company needs to store large, important documents within the application with the following requirements:

- The data must be highly durable and available.
- The data must always be encrypted at rest and in transit.
- The encryption key must be managed by the company and rotated periodically. Which of the following solutions should the Solutions Architect recommend?

- A. Deploy the storage gateway to AWS in file gateway mod
- B. Use Amazon EBS volume encryption using an AWS KMS key to encrypt the storage gateway volumes.
- C. Use Amazon S3 with a bucket policy to enforce HTTPS for connections to the bucket and to enforce server-side encryption and AWS KMS for object encryption.
- D. Use Amazon DynamoDB with SSL to connect to DynamoD
- E. Use an AWS KMS key to encrypt DynamoDB objects at rest.
- F. Deploy instances with Amazon EBS volumes attached to store this dat
- G. Use EBS volume encryption using an AWS KMS key to encrypt the data.

Answer: B

Explanation:

<https://aws.amazon.com/blogs/security/how-to-use-bucket-policies-and-apply-defense-in-depth-to-help-secure-y>

NEW QUESTION 18

A company's CISO has asked a Solutions Architect to re-engineer the company's current CI/CD practices to make sure patch deployments to its applications 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
- B. Monitor the newly deployed code, and if there are any issues, push another code update.
- C. Configure CodePipeline with a deploy stage using AWS CodeDeploy configure for blue/green deployment
- D. Monitor the new deployed code and if there are any issues, trigger a manual rollback using CodeDeploy.
- E. Configure CodePipeline with a deploy stage using AWS CloudFormation to create a pipeline for test and production stack
- F. Monitor the newly deployed code and if there are any issues push another code update.
- G. 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.

Answer: B

NEW QUESTION 23

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 permission 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 create
- B. Train users to launch the template from the CloudFormation console.
- C. Create an AWS Service Catalog product from the environment template
- D. Add a launch constraint to the product with the existing role
- E. Give users in the QA department permission to use AWS Service Catalog APIs only
- F. Train users to launch the templates from the AWS Service Catalog console.
- G. 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 permission to the template and the resources it create
- H. Train users to launch the template from the CloudFormation console.
- I. Create an AWS Elastic Beanstalk application from the environment template
- J. Give users in the QA department permission to use Elastic Beanstalk permissions only
- K. 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

Explanation:

<https://aws.amazon.com/blogs/mt/how-to-launch-secure-and-governed-aws-resources-with-aws-cloudformation->

NEW QUESTION 28

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

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

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

- A. Reconfigure Amazon EFS to enable maximum I/O.
- B. Update the 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 distributio
- 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 suite contents, and point the distribution at the ALB.

Answer: C

Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-https-connection-fails/>

NEW QUESTION 30

A company deployed a three-tier web application in two regions: us-east-1 and eu-west-1. The application must be active in both regions at the same time. The database tier of the application uses a single Amazon RDS Aurora database globally, with a master in us-east-1 and a read replica in eu-west-1. Both regions are connected by a VPN.

The company wants to ensure that the application remains available even in the event of a region-level failure of all of the application's components. It is acceptable for the application to be in read-only mode for up to 1 hour. The company plans to configure two Amazon Route 53 record sets, one for each of the regions.

How should the company complete the configuration to meet its requirements while providing the lowest latency for the application end-users? (Choose two.)

- A. Use failover routing and configure the us-east-1 record set as primary and the eu-west-1 record set as secondar
- B. Configure an HTTP health check for the web application in us-east-1, and associate it to the us-east-1 record set.
- C. Use weighted routing and configure each record set with a weight of 50. Configure an HTTP health check for each region, and attach it to the record set for that region.
- D. Use latency-based routing for both record set
- E. Configure a health check for each region and attach it to the record set for that region.
- F. Configure an Amazon CloudWatch alarm for the health checks in us-east-1, and have it invoke an AWS Lambda function that promotes the read replica in eu-west-1.
- G. Configure an Amazon RDS event notifications to react to the failure of the database in us-east-1 by invoking an AWS Lambda function that promotes the read replica in eu-west-1.

Answer: CE

Explanation:

<https://docs.aws.amazon.com/lambda/latest/dg/services-rds.html>

NEW QUESTION 35

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 gatewa
- C. Use the catalog of faces to build a collection in Amazon Rekognitio
- D. 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.
- E. Set up an AWS Storage Gateway, tape gateway appliance on-premise
- F. Use the MAM solution to extract the videos from the current archive and push them into the tape gatewa
- G. Use the catalog of faces to build a collection in Amazon Rekognitio
- H. 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.
- I. Configure a video ingestion stream by using Amazon Kinesis Video Stream
- J. Use the catalog of faces to build a collection in Amazon Rekognitio
- K. Stream the videos from the MAM solution into Kinesis Video Stream
- L. Configure Amazon Rekognition to process the streamed video
- M. Then, use a stream consumer to retrieve the required metadata, and push the metadata into the MAM solutio
- N. Configure the stream to store the videos in Amazon S3.
- O. Set up an Amazon EC2 instance that runs the OpenCV librarie
- P. Copy the videos, images, and face catalog from the on-premises library into an Amazon EBS volume mounted on this EC2 instanc
- Q. 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

Explanation:

<https://docs.aws.amazon.com/rekognition/latest/dg/streaming-video.html>

NEW QUESTION 37

A company has created an account for individual Development teams, resulting in a total of 200 accounts. All accounts have a single virtual private cloud (VPC) in a single region with multiple microservices running in Docker containers that need to communicate with microservices in other accounts. The Security team requirements state that these microservices must not traverse the public internet, and only certain internal services should be allowed to call other individual services. If there is any denied network traffic for a service, the Security team must be notified of any denied requests, including the source IP.

How can connectivity be established between services while meeting the security requirements?

- A. Create a VPC peering connection between the VPC
- B. Use security groups on the instances to allow traffic from the security group IDs that are permitted to call the microservic
- C. Apply network ACLs to and allow traffic from the local VPC and peered VPCs onl
- D. Within the task definition in Amazon ECS for each of the microservices, specify a log configuration by using the awslogs drive

- E. Within Amazon CloudWatch Logs, create a metric filter and alarm off of the number of HTTP 403 response
- F. Create an alarm when the number of messages exceeds a threshold set by the Security team.
- G. Ensure that no CIDR ranges are overlapping, and attach a virtual private gateway (VGW) to each VPC. Provision an IPsec tunnel between each VGW and enable route propagation on the route table
- H. Configure security groups on each service to allow the CIDR ranges of the VPCs on the other account
- I. Enable VPC Flow Logs, and use an Amazon CloudWatch Logs subscription filter for rejected traffic
- J. Create an IAM role and allow the Security team to call the AssumeRole action for each account.
- K. Deploy a transit VPC by using third-party marketplace VPN appliances running on Amazon EC2, dynamically routed VPN connections between the VPN appliance, and the virtual private gateways (VGWs) attached to each VPC within the region
- L. Adjust network ACLs to allow traffic from the local VPC only
- M. Apply security groups to the microservices to allow traffic from the VPN appliances only
- N. Install the awslogs agent on each VPN appliance, and configure logs to forward to Amazon CloudWatch Logs in the security account for the Security team to access.
- O. Create a Network Load Balancer (NLB) for each microservice
- P. Attach the NLB to a PrivateLink endpoint service and whitelist the accounts that will be consuming this service
- Q. Create an interface endpoint in the consumer VPC and associate a security group that allows only the security group IDs of the services authorized to call the producer service
- R. On the producer services, create security groups for each microservice and allow only the CIDR range of the allowed service
- S. Create VPC Flow Logs on each VPC to capture rejected traffic that will be delivered to an Amazon CloudWatch Logs group
- T. Create a CloudWatch Logs subscription that streams the log data to a security account.

Answer: D

Explanation:

AWS PrivateLink provides private connectivity between VPCs, AWS services, and on-premises applications, securely on the Amazon network. AWS PrivateLink makes it easy to connect services across different accounts and VPCs to significantly simplify the network architecture. It seems like the next VPC peering.
<https://aws.amazon.com/privatelink/>

NEW QUESTION 39

A company is creating an account strategy so that they can begin using AWS. The Security team will provide each team with the permissions they need to follow the principle of least privileged access. Teams would like to keep their resources isolated from other groups, and the Finance team would like each team's resource usage separated for billing purposes.

Which account creation process meets these requirements and allows for changes?

- A. Create a new AWS Organizations account
- B. Create groups in Active Directory and assign them to roles in AWS to grant federated access
- C. Require each team to tag their resources, and separate bills based on tag
- D. Control access to resources through IAM granting the minimally required privilege.
- E. Create individual accounts for each team
- F. Assign the security account as the master account, and enable consolidated billing for all other accounts
- G. Create a cross-account role for security to manage accounts, and send logs to a bucket in the security account.
- H. Create a new AWS account, and use AWS Service Catalog to provide teams with the required resources. Implement a third-party billing to provide the Finance team with the resource use for each team based on tagging
- I. Isolate resources using IAM to avoid account sprawl
- J. Security will control and monitor logs and permissions.
- K. Create a master account for billing using Organizations, and create each team's account from that master account
- L. Create a security account for logs and cross-account access
- M. Apply service control policies on each account, and grant the Security team cross-account access to all accounts
- N. Security will create IAM policies for each account to maintain least privilege access.

Answer: B

NEW QUESTION 41

A company runs a Windows Server host in a public subnet that is configured to allow a team of administrators to connect over RDP to troubleshoot issues with hosts in a private subnet. The host must be available at all times outside of a scheduled maintenance window, and needs to receive the latest operating system updates within 3 days of release.

What should be done to manage the host with the LEAST amount of administrative effort?

- A. Run the host in a single-instance AWS Elastic Beanstalk environment
- B. Configure the environment with a custom AMI to use a hardened machine image from AWS Marketplace
- C. Apply system updates with AWS Systems Manager Patch Manager.
- D. Run the host on AWS WorkSpace
- E. Use Amazon WorkSpaces Application Manager (WAM) to harden the host
- F. Configure Windows automatic updates to occur every 3 days.
- G. Run the host in an Auto Scaling group with a minimum and maximum instance count of 1. Use a hardened machine image from AWS Marketplace
- H. Apply system updates with AWS Systems Manager Patch Manager.
- I. Run the host in AWS OpsWorks Stack
- J. Use a Chef recipe to harden the AMI during instance launch. Use an AWS Lambda scheduled event to run the Upgrade Operating System stack command to apply system updates.

Answer: B

NEW QUESTION 43

A company has been using a third-party provider for its content delivery network and recently decided to switch to Amazon CloudFront. The Development team wants to maximize performance for the global user base. The company uses a content management system (CMS) that serves both static and dynamic content. The CMS is behind an Application Load Balancer (ALB) which is set as the default origin for the distribution. Static assets are served from an Amazon S3 bucket. The Origin Access Identity (OAI) was created properly and the S3 bucket policy has been updated to allow the GetObject action from the OAI, but static assets are receiving a 404 error.

Which combination of steps should the Solutions Architect take to fix the error? (Select TWO.)

- A. Add another origin to the CloudFront distribution for the static assets
- B. Add a path based rule to the ALB to forward requests for the static assets
- C. Add an RTMP distribution to allow caching of both static and dynamic content
- D. Add a behavior to the CloudFront distribution for the path pattern and the origin of the static assets
- E. Add a host header condition to the ALB listener and forward the header from CloudFront to add traffic to the allow list

Answer: AD

NEW QUESTION 46

A company's application is increasingly popular and experiencing latency because of high volume reads on the database server. The service has the following properties:

- A highly available REST API hosted in one region using Application Load Balancer (ALB) with auto scaling.
- A MySQL database hosted on an Amazon EC2 instance in a single Availability Zone.

The company wants to reduce latency, increase in-region database read performance, and have multi-region disaster recovery capabilities that can perform a live recovery automatically without any data or performance loss (HA/DR).

Which deployment strategy will meet these requirements?

- A. Use AWS CloudFormation StackSets to deploy the API layer in two region
- B. Migrate the database to an Amazon Aurora with MySQL database cluster with multiple read replicas in one region and a read replica in a different region than the source database cluste
- C. Use Amazon Route 53 health checks to trigger a DNS failover to the standby region if the health checks to the primary load balancer fai
- D. In the event of Route 53 failover, promote the cross-region database replica to be the master and build out new read replicas in the standby region.
- E. Use Amazon ElastiCache for Redis Multi-AZ with an automatic failover to cache the database readquerie
- F. Use AWS OpsWorks to deploy the API layer, cache layer, and existing database layer in two region
- G. In the event of failure, use Amazon Route 53 health checks on the database to trigger a DNS failover to the standby region if the health checks in the primary region fai
- H. Back up the MySQL database frequently, and in the event of a failure in an active region, copy the backup to the standby region and restore the standby database.
- I. Use AWS CloudFormation StackSets to deploy the API layer in two region
- J. Add the database to an Auto Scaling grou
- K. Add a read replica to the database in the second regio
- L. Use Amazon Route 53 health checks on the database to trigger a DNS failover to the standby region if the health checks in the primary region fai
- M. Promote the cross-region database replica to be the master and build out new read replicas in the standby region.
- N. Use Amazon ElastiCache for Redis Multi-AZ with an automatic failover to cache the database read querie
- O. Use AWS OpsWorks to deploy the API layer, cache layer, and existing database layer in two region
- P. Use Amazon Route 53 health checks on the ALB to trigger a DNS failover to the standby region if the health checks in the primary region fai
- Q. Back up the MySQL database frequently, and in the event of a failure in an active region, copy the backup to the standby region and restore the standby database.

Answer: A

NEW QUESTION 47

A company is adding a new approved external vendor that only supports IPv6 connectivity. The company's backend systems sit in the private subnet of an Amazon VPC. The company uses a NAT gateway to allow these systems to communicate with external vendors over IPv4. Company policy requires systems that communicate with external vendors use a security group that limits access to only approved external vendors. The virtual private cloud (VPC) uses the default network ACL.

The Systems Operator successfully assigns IPv6 addresses to each of the backend systems. The Systems Operator also updates the outbound security group to include the IPv6 CIDR of the external vendor (destination). The systems within the VPC are able to ping one another successfully over IPv6. However, these systems are unable to communicate with the external vendor.

What changes are required to enable communication with the external vendor?

- A. Create an IPv6 NAT instanc
- B. Add a route for destination 0.0.0.0/0 pointing to the NAT instance.
- C. Enable IPv6 on the NAT gatewa
- D. Add a route for destination ::/0 pointing to the NAT gateway.
- E. Enable IPv6 on the internet gatewa
- F. Add a route for destination 0.0.0.0/0 pointing to the IGW.
- G. Create an egress-only internet gatewa
- H. Add a route for destination ::/0 pointing to the gateway.

Answer: D

Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html>

NEW QUESTION 52

A company is using AWS to run an internet-facing production application written in Node.js. The Development team is responsible for pushing new versions of their software directly to production. The application software is updated multiple times a day. The team needs guidance from a Solutions Architect to help them deploy the software to the production fleet quickly and with the least amount of disruption to the service.

Which option meets these requirements?

- A. Prepackage the software into an AMI and then use Auto Scaling to deploy the production flee
- B. For software changes, update the AMI and allow Auto Scaling to automatically push the new AMI to production.
- C. Use AWS CodeDeploy to push the prepackaged AMI to productio
- D. For software changes, reconfigure CodeDeploy with new AMI identification to push the new AMI to the production fleet.
- E. Use AWS Elastic Beanstalk to host the production applicatio
- F. For software changes, upload the new application version to Elastic Beanstalk to push this to the production fleet using a blue/green deployment method.
- G. Deploy the base AMI through Auto Scaling and bootstrap the software using user dat

H. For software changes, SSH to each of the instances and replace the software with the new version.

Answer: C

NEW QUESTION 56

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, and creating several additional read replicas to handle the load during end of month.
- C. Using Amazon CloudWatch with AWS Lambda to change the type, size, or IOPS of Amazon EBS volumes in the cluster based on a specific CloudWatch metric.
- D. 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

NEW QUESTION 57

A Solutions Architect must create a cost-effective backup solution for a company's 500MB source code repository of proprietary and sensitive applications. The repository runs on Linux and backs up daily to tape. Tape backups are stored for 1 year.

The current solutions are not meeting the company's needs because it is a manual process that is prone to error, expensive to maintain, and does not meet the need for a Recovery Point Objective (RPO) of 1 hour or Recovery Time Objective (RTO) of 2 hours. The new disaster recovery requirement is for backups to be stored offsite and to be able to restore a single file if needed.

Which solution meets the customer's needs for RTO, RPO, and disaster recovery with the LEAST effort and expense?

- A. Replace local tapes with an AWS Storage Gateway virtual tape library to integrate with current backup software
- B. Run backups nightly and store the virtual tapes on Amazon S3 standard storage in US-EAST-1. Use cross-region replication to create a second copy in US-WEST-2. Use Amazon S3 lifecycle policies to perform automatic migration to Amazon Glacier and deletion of expired backups after 1 year?
- C. Configure the local source code repository to synchronize files to an AWS Storage Gateway file Amazon gateway to store backup copies in an Amazon S3 Standard bucket
- D. Enable versioning on the Amazon S3 bucket
- E. Create Amazon S3 lifecycle policies to automatically migrate old versions of objects to Amazon S3 Standard 0 Infrequent Access, then Amazon Glacier, then delete backups after 1 year.
- F. Replace the local source code repository storage with a Storage Gateway stored volume
- G. Change the default snapshot frequency to 1 hour
- H. Use Amazon S3 lifecycle policies to archive snapshots to Amazon Glacier and remove old snapshots after 1 year
- I. Use cross-region replication to create a copy of the snapshots in US-WEST-2.
- J. Replace the local source code repository storage with a Storage Gateway cached volume
- K. Create a snapshot schedule to take hourly snapshots
- L. Use an Amazon CloudWatch Events schedule expression rule to run on hourly AWS Lambda task to copy snapshots from US-EAST -1 to US-WEST-2.

Answer: B

Explanation:

<https://d1.awsstatic.com/whitepapers/aws-storage-gateway-file-gateway-for-hybrid-architectures.pdf>

NEW QUESTION 60

A company manages more than 200 separate internet-facing web applications. All of the applications are deployed to AWS in a single AWS Region. The fully qualified domain names (FQDNs) of all of the applications are made available through HTTPS using Application Load Balancers (ALBs). The ALBs are configured to use public SSL/TLS certificates.

A Solutions Architect needs to migrate the web applications to a multi-region architecture. All HTTPS services should continue to work without interruption.

Which approach meets these requirements?

- A. Request a certificate for each FQDN using AWS KMS
- B. Associate the certificates with the ALBs in the primary AWS Region
- C. Enable cross-region availability in AWS KMS for the certificates and associate the certificates with the ALBs in the secondary AWS Region.
- D. Generate the key pairs and certificate requests for each FQDN using AWS KMS
- E. Associate the certificates with the ALBs in both the primary and secondary AWS Regions.
- F. Request a certificate for each FQDN using AWS Certificate Manager
- G. Associate the certificates with the ALBs in both the primary and secondary AWS Regions.
- H. Request certificates for each FQDN in both the primary and secondary AWS Regions using AWS Certificate Manager
- I. Associate the certificates with the corresponding ALBs in each AWS Region.

Answer: D

Explanation:

<https://docs.aws.amazon.com/acm/latest/userguide/acm-regions.html>

Certificates in ACM are regional resources. To use a certificate with Elastic Load Balancing for the same fully qualified domain name (FQDN) or set of FQDNs in more than one AWS region, you must request or import a certificate for each region. For certificates provided by ACM, this means you must revalidate each domain name in the certificate for each region. You cannot copy a certificate between regions.

NEW QUESTION 65

A company has more than 100 AWS accounts, with one VPC per account, that need outbound HTTPS connectivity to the internet. The current design contains one NAT gateway per Availability Zone (AZ) in each VPC. To reduce costs and obtain information about outbound traffic, management has asked for a new architecture for internet access.

Which solution will meet the current needs, and continue to grow as new accounts are provisioned, while reducing costs?

- A. Create a transit VPC across two AZs using a third-party routing appliance
- B. Create a VPN connection to each VP
- C. Default route internet traffic to the transit VPC.
- D. Create multiple hosted-private AWS Direct Connect VIFs, one per account, each with a Direct Connect gateway
- E. Default route internet traffic back to an on-premises router to route to the internet.
- F. Create a central VPC for outbound internet traffic
- G. Use VPC peering to default route to a set of redundant NAT gateway in the central VPC.
- H. Create a proxy fleet in a central VPC account
- I. Create an AWS PrivateLink endpoint service in the central VP
- J. Use PrivateLink interface for internet connectivity through the proxy fleet.

Answer: D

Explanation:

user proxy fleet over PrivateLink. As explained in this AWS website:

<https://aws.amazon.com/blogs/networking-and-content-delivery/how-to-use-aws-privatelink-to-secure-and-scale>

NEW QUESTION 66

A company operating a website on AWS requires high levels of scalability, availability and performance. The company is running a Ruby on Rails application on Amazon EC2. It has a data tier on MySQL 5.6 on Amazon EC2 using 16 TB of Amazon EBS storage. Amazon CloudFront is used to cache application content. The Operations team is reporting continuous and unexpected growth of EBS volumes assigned to the MySQL database. The Solutions Architect has been asked to design a highly scalable, highly available, and high-performing solution. Which solution is the MOST cost-effective at scale?

- A. Implement Multi-AZ and Auto Scaling for all EC2 instances in the current configuration
- B. Ensure that all EC2 instances are purchased as reserved instance
- C. Implement new elastic Amazon EBS volumes for the data tier.
- D. Design and implement the Docker-based containerized solution for the application using Amazon EC
- E. Migrate to an Amazon Aurora MySQL Multi-AZ cluster
- F. Implement storage checks for Aurora MySQL storage utilization and an AWS Lambda function to grow the Aurora MySQL storage, as necessary
- G. Ensure that Multi-AZ architectures are implemented.
- H. Ensure that EC2 instances are right-sized and behind an Elastic Load Balancing load balancer. Implement Auto Scaling with EC2 instances
- I. Ensure that the reserved instances are purchased for fixed capacity and that Auto Scaling instances run on demand
- J. Migrate to an Amazon Aurora MySQL Multi-AZ cluster
- K. Ensure that Multi-AZ architectures are implemented.
- L. Ensure that EC2 instances are right-sized and behind an Elastic Load Balance
- M. Implement Auto Scaling with EC2 instances
- N. Ensure that Reserved instances are purchased for fixed capacity and that Auto Scaling instances run on demand
- O. Migrate to an Amazon Aurora MySQL Multi-AZ cluster
- P. Implement storage checks for Aurora MySQL storage utilization and an AWS Lambda function to grow Aurora MySQL storage, as necessary
- Q. Ensure Multi-AZ architectures are implemented.

Answer: C

NEW QUESTION 69

A company has decided to move some workloads onto AWS to create a grid environment to run market analytics. The grid will consist of many similar instances, spun-up by a job-scheduling function. Each time a large analytics workload is completed, a new VPC is deployed along with job scheduler and grid nodes. Multiple grids could be running in parallel.

Key requirements are:

- Grid instances must communicate with Amazon S3 to retrieve data to be processed.
- Grid instances must communicate with Amazon DynamoDB to track intermediate data,
- The job scheduler needs only to communicate with the Amazon EC2 API to start new grid nodes.

A key requirement is that the environment has no access to the internet, either directly or via the on-premises proxy. However, the application needs to be able to seamlessly communicate to Amazon S3, Amazon DynamoDB, and Amazon EC2 API, without the need for reconfiguration for each new deployment.

Which of the following should the Solutions Architect do to achieve this target architecture? (Choose three.)

- A. Enable VPC endpoints for Amazon S3 and DynamoDB.
- B. Disable Private DNS Name Support.
- C. Configure the application on the grid instances to use the private DNS name of the Amazon S3 endpoint.
- D. Populate the on-premises DNS server with the private IP addresses of the EC2 endpoint.
- E. Enable an interface VPC endpoint for EC2.
- F. Configure Amazon S3 endpoint policy to permit access only from the grid nodes.

Answer: ACE

Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/connect-s3-vpc-endpoint/> <https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html>

NEW QUESTION 72

A retail company is running an application that stores invoice files in Amazon S3 bucket and metadata about the files in an Amazon. The S3 bucket and DynamoDB table are in us-east-1. The company wants to protect itself from data corruption and loss of connectivity to either Region.

Which option meets these requirements?

- A. Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable continuous backup on the DynamoDB table in us-east-1. Enable versioning on the S3 bucket.
- B. Create an AWS Lambda function triggered by Amazon CloudWatch Events to make regular backups of the DynamoDB table
- C. Set up S3 cross-region replication from us-east-1 to eu-west-1. Set up MFA delete on the S3 bucket in us-east-1.
- D. Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable versioning on the S3 bucket

- E. Implement strict ACLs on the S3 bucket.
F. Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable continuous backup on the DynamoDB table in us-east-1. Set up S3 cross-region replication from us-east-1 to eu-west-1.

Answer: A

Explanation:

<https://aws.amazon.com/blogs/aws/new-cross-region-replication-for-amazon-s3/>

NEW QUESTION 77

A financial services company logs personality identifiable information to its application logs stored in Amazon S3. Due to regulatory compliance requirements, the log files must be encrypted at rest. The Security team has mandated that the company's on-premises hardware security modules (HSMs) be used to generate the CMK material.

Which steps should the Solution Architect take to meet these requirements?

- A. Create an AWS CloudHSM cluster
- B. Create a new CMK in AWS KMS using AWS_CloudHSM as the source for the key material and an origin of AWS-CLOUDHSM
- C. Enable automatic key rotation on the CMK with a duration of 1 year
- D. Configure a bucket policy on the logging bucket to disallow uploads of unencrypted data and requires that the encryption source be AWS KMS.
- E. Provision an AWS Direct Connect connection, ensuring there is no overlap of the RFC 1918 address space between on-premises hardware and the VPC
- F. Configure an AWS bucket policy on the logging bucket requires all objects to be key material, and create a unique CMK for each logging event.
- G. Create a CMK in AWS KMS with no key material and an origin of EXTERNAL
- H. Import the key material generated from the on-premises HSMs into the CMK using the public key and import token provided by AWS
- I. Configure a bucket policy on the logging bucket that disallows uploads of non-encrypted data and requires that the encryption source be AWS KMS.
- J. Create a new CMK in AWS KMS with AWS-provided key material and an origin of AWS-KM
- K. Disable this CMK, and overwrite the key material with the material from the on-premises HSM using the public key and import token provided by AWS. Re-enable the CMK
- L. Enable automatic key rotation on the CMK with a duration of 1 year
- M. Configure a bucket policy on the logging bucket that disallows uploads of non-encrypted data and requires that the encryption source be AWS KMS.

Answer: A

NEW QUESTION 79

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

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

Which combination of steps should be included in the solution? (Choose two.)

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

Answer: AD

Explanation:

There is a concept of Permission Boundary vs Actual IAM Policies. That is, we have a concept of "Allow" vs "Grant". In terms of boundaries, we have the following three boundaries: 1. SCP 2. User/Role boundaries 3. Session boundaries (ex. AssumeRole ...) In terms of actual permission granting, we have the following: 1. Identity Policies 2. Resource Policies

NEW QUESTION 81

A financial services company is moving to AWS and wants to enable Developers to experiment and innovate while preventing access to production applications. The company has the following requirements:

- Production workloads cannot be directly connected to the internet
- All workloads must be restricted to the us-west-2 and eu-central-1 Regions
- Notification should be sent when Developer sandboxes exceed \$500 in AWS spending monthly

Which combination of actions needs to be taken to create a multi-account structure that meets the company's requirements? (Select THREE)

- A. Create accounts for each production workload within an organization in AWS Organizations. Place the production accounts within an organizational unit (OU). For each account, delete the default VPC. Create an SCP with a Deny rule for the attach an internet gateway and create a default VPC actions. Attach the SCP to the OU for the production accounts.
- B. Create accounts for each production workload within an organization in AWS Organizations. Place the production accounts within an organizational unit (OU). Create an SCP with a Deny rule on the attach an internet gateway action. Create an SCP with a Deny rule to prevent use of the default VPC. Attach the SCPs to the OU for the production accounts.
- C. Create a SCP containing a Deny Effect for cloudfront". iam:*, route53* and support* with a StringNotEquals condition on an aws:RequestedRegion condition key with us-west-2 and eu-central-1 values. Attach the SCP to the organization's root.
- D. Create an IAM permission boundary containing a Deny Effect for cloudfront". iam:*, route53* and support* with a StringNotEquals condition on an aws:RequestedRegion condition key with us-west-2 and eu-central-1 values. Attach the permission boundary to an IAM group containing the development and production users.
- E. Create accounts for each development workload within an organization in AWS Organizations. Place the development accounts within an organizational unit.

(OU) Create a custom AWS Config rule to deactivate all (AM users when an account's monthly bill exceeds \$500.
F. Create accounts for each development workload within an organization in AWS Organizations Place the development accounts within an organizational unit
(OU) Create a budget within AWS Budgets for each development account to monitor and report on monthly spending exceeding \$500.

Answer: ABD

NEW QUESTION 85

A company is running a large application on-premises. Its technology stack consists of Microsoft .NET for the web server platform and Apache Cassandra for the database. The company wants to migrate the application to AWS to improve service reliability. The IT team also wants to reduce the time it spends on capacity management and maintenance of this infrastructure. The Development team is willing and available to make code changes to support the migration. Which design is the LEAST complex to manage after the migration?

- A. Migrate the web servers to Amazon EC2 instances in an Auto Scaling group that is running .NET
- B. Migrate the existing Cassandra database to Amazon Aurora with multiple read replicas, and run both in a Multi-AZ mode.
- C. Migrate the web servers to an AWS Elastic Beanstalk environment that is running the .NET platform in a Multi-AZ Auto Scaling configuration
- D. Migrate the Cassandra database to Amazon EC2 instances that are running in a Multi-AZ configuration.
- E. Migrate the web servers to an AWS Elastic Beanstalk environment that is running the .NET platform in a Multi-AZ Auto Scaling configuration
- F. Migrate the existing Cassandra database to Amazon DynamoDB.
- G. Migrate the web servers to Amazon EC2 instances in an Auto Scaling group that is running .NET
- H. Migrate the existing Cassandra database to Amazon DynamoDB.

Answer: B

NEW QUESTION 87

A company currently runs a secure application on Amazon EC2 that takes files from on-premises locations through AWS Direct Connect, processes them, and uploads them to a single Amazon S3 bucket. The application uses HTTPS for encryption in transit to Amazon S3, and S3 server-side encryption to encrypt at rest. Which of the following changes should the Solutions Architect recommend to make this solution more secure without impeding application's performance?

- A. Add a NAT gateway
- B. Update the security groups on the EC2 instance to allow access to and from the S3 IP range only
- C. Configure an S3 bucket policy that allows communication from the NAT gateway's Elastic IP address only.
- D. Add a VPC endpoint
- E. Configure endpoint policies on the VPC endpoint to allow access to the required Amazon S3 buckets only
- F. Implement an S3 bucket policy that allows communication from the VPC's source IP range only.
- G. Add a NAT gateway
- H. Update the security groups on the EC2 instance to allow access to and from the S3 IP range only
- I. Configure an S3 bucket policy that allows communication from the source public IP address of the on-premises network only.
- J. Add a VPC endpoint
- K. Configure endpoint policies on the VPC endpoint to allow access to the required S3 buckets only
- L. Implement an S3 bucket policy that allows communication from the VPC endpoint only.

Answer: D

Explanation:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html>

NEW QUESTION 90

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

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

- A. Set up an Amazon API Gateway with an edge-optimized API endpoint that has a resource as an S3 service proxy Configure the PUT method for this resource to expose the S3 Putobject operation Secure the API Gateway using a COGNITO_USER_POOLS authorize
- B. Have the browser interface use API Gateway instead of the presigned URL to upload objects
- C. Set up an Amazon API Gateway with a regional API endpoint that has a resource as an S3 service proxy Configure the PUT method for this resource to expose the S3 Putobject operation Secure the API Gateway using an AWS Lambda authorizer Have the browser interface use API Gateway instead of the presigned URL to upload objects
- D. Enable an S3 Transfer Acceleration endpoint on the S3 bucket Use the endpoint when generating the presigned URL Have the browser interface upload the objects to the URL using the S3 multipart upload API.
- E. Configure an Amazon CloudFront distribution for the destination S3 bucket Enable PUT and POST methods for the CloudFront cache behavior Update the CloudFront origin to use an origin access identity (OAI). Give the OAI user s3:PutObject permissions in the bucket policy Have the browser interface upload objects using the CloudFront distribution.

Answer: A

NEW QUESTION 92

The Security team needs to provide a team of interns with an AWS environment so they can build the serverless video transcoding application. The project will use Amazon S3, AWS Lambda, Amazon API Gateway, Amazon Cognito, Amazon DynamoDB, and Amazon Elastic Transcoder.

The interns should be able to create and configure the necessary resources, but they may not have access to create or modify AWS IAM roles. The Solutions Architect creates a policy and attaches it to the interns' group.

How should the Security team configure the environment to ensure that the interns are self-sufficient?

- A. Create a policy that allows creation of project-related resources only
- B. Create roles with required service permissions, which are assumable by the services.
- C. Create a policy that allows creation of all project-related resources, including roles that allow access only to specified resources.
- D. Create roles with the required service permissions, which are assumable by the service
- E. Have the interns create and use a bastion host to create the project resources in the project subnet only.
- F. Create a policy that allows creation of project-related resources only

- G. Require the interns to raise a request for roles to be created with the Security tea
- H. The interns will provide the requirements for the permissions to be set in the role.

Answer: A

NEW QUESTION 95

A company is building an AWS landing zone and has asked a Solutions Architect to design a multi-account access strategy that will allow hundreds of users to use corporate credentials to access the AWS Console. The company is running a Microsoft Active Directory and users will use an AWS Direct Connect connection to connect to AWS. The company also wants to be able to federate to third-party services and providers, including custom applications. Which solution meets the requirements by using the LEAST amount of management overhead?

- A. Connect the Active Directory to AWS by using single sign-on and an Active Directory Federation Services (AD FS) with SAML 2.0, and then configure the identity Provider (IdP) system to use form-based authenticatio
- B. Build the AD FS portal page with corporate branding, and integrate third-party applications that support SAML 2.0 as required.
- C. Create a two-way Forest trust relationship between the on-premises Active Directory and the AWS Directory Servic
- D. Set up AWS Single Sign-On with AWS Organization
- E. Use single sign-on integrations for connections with third-party applications.
- F. Configure single sign-on by connecting the on-premises Active Directory using the AWS Directory Service AD Connecto
- G. Enable federation to the AWS services and accounts by using the IAM applications and services linking functio
- H. Leverage third-party single sign-on as needed.
- I. Connect the company's Active Directory to AWS by using AD FS and SAML 2.0. Configure the AD FS claim rule to leverage Regex and a common Active Directory naming convention for the security group to allow federation of all AWS account
- J. Leverage third-party single sign-on as needed, and add it to the AD FS server.

Answer: D

Explanation:

<https://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directory-federation-services-a>

NEW QUESTION 99

A company has an application that runs a web service on Amazon EC2 instances and stores .jpg images in Amazon S3. The web traffic has a predictable baseline, but often demand spikes unpredictably for short periods of time. The application is loosely coupled and stateless. The .jpg images stored in Amazon S3 are accessed frequently for the first 15 to 20 days, they are seldom accessed thereafter but always need to be immediately available. The CIO has asked to find ways to reduce costs.

Which of the following options will reduce costs? (Choose two.)

- A. Purchase Reserved instances for baseline capacity requirements and use On-Demand instances for the demand spikes.
- B. Configure a lifecycle policy to move the .jpg images on Amazon S3 to S3 IA after 30 days.
- C. Use On-Demand instances for baseline capacity requirements and use Spot Fleet instances for the demand spikes.
- D. Configure a lifecycle policy to move the .jpg images on Amazon S3 to Amazon Glacier after 30 days.
- E. Create a script that checks the load on all web servers and terminates unnecessary On-Demand instances.

Answer: AB

NEW QUESTION 101

A company with multiple accounts is currently using a configuration that does not meet the following security governance policies

- Prevent ingress from port 22 to any Amazon EC2 instance
- Require billing and application tags for resources
- Encrypt all Amazon EBS volumes

A Solutions Architect wants to provide preventive and detective controls including notifications about a specific resource, if there are policy deviations.

Which solution should the Solutions Architect implement?

- A. Create an AWS CodeCommit repository containing policy-compliant AWS Cloud Formation templates.Create an AWS Service Catalog portfolio Import the Cloud Formation templates by attaching the CodeCommit repository to the portfolio Restrict users across all accounts to items from the AWSService Catalog portfolio Use AWS Config managed rules to detect deviations from the policie
- B. Configure an Amazon CloudWatch Events rule for deviations, and associate a CloudWatch alarm to send notifications when the TriggeredRules metric is greater than zero.
- C. Use AWS Service Catalog to build a portfolio with products that are in compliance with the governance policies in a central account Restrict users across all accounts lo AWS Service Catalog products Share a compliant portfolio to other accounts Use AWS Config managed rules to detect deviations from the policies Configure an Amazon CloudWatch Events rule to send a notification when a deviation occurs
- D. Implement policy-compliant AWS Cloud Formation templates for each account and ensure that all provisioning is completed by Cloud Formation Configure Amazon Inspector to perform regular checks against resources Perform policy validation and write the assessment output to Amazon CloudWatch Log
- E. Create a CloudWatch Logs metric filter to increment a metric when a deviation occurs Configure a CloudWatch alarm to send notifications when the configured metric is greater than zero
- F. Restrict users and enforce least privilege access using AWS I A
- G. Consolidate all AWS CloudTrail logs into a single account Send the CloudTrail logs to Amazon Elasticsearch Service (Amazon ES). Implement monitoring alerting, and reporting using the Kibana dashboard in Amazon ES and with Amazon SNS.

Answer: C

NEW QUESTION 102

A Solutions Architect is working with a company that is extremely sensitive to its IT costs and wishes to implement controls that will result in a predictable AWS spend each month.

Which combination of steps can help the company control and monitor its monthly AWS usage to achieve a cost that is as close as possible to the target amount? (Choose three.)

- A. Implement an IAM policy that requires users to specify a 'workload' tag for cost allocation when launching Amazon EC2 instances.
- B. Contact AWS Support and ask that they apply limits to the account so that users are not able to launch more than a certain number of instance types.
- C. Purchase all upfront Reserved Instances that cover 100% of the account's expected Amazon EC2 usage.

- D. Place conditions in the users' IAM policies that limit the number of instances they are able to launch.
- E. Define 'workload' as a cost allocation tag in the AWS Billing and Cost Management console.
- F. Set up AWS Budgets to alert and notify when a given workload is expected to exceed a defined cost.

Answer: AEF

NEW QUESTION 103

A Solutions Architect is designing a highly available and reliable solution for a cluster of Amazon EC2 instances. The Solutions Architect must ensure that any EC2 instance within the cluster recovers automatically after a system failure. The solution must ensure that the recovered instance maintains the same IP address. How can these requirements be met?

- A. Create an AWS Lambda script to restart any EC2 instances that shut down unexpectedly.
- B. Create an Auto Scaling group for each EC2 instance that has a minimum and maximum size of 1.
- C. Create a new t2.micro instance to monitor the cluster instance
- D. Configure the t2.micro instance to issue an `aws ec2 reboot-instances` command upon failure.
- E. Create an Amazon CloudWatch alarm for the `StatusCheckFailed_System` metric, and then configure an EC2 action to recover the instance.

Answer: B

Explanation:

References: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html>

NEW QUESTION 104

A company collects a steady stream of 10 million data records from 100,000 sources each day. These records are written to an Amazon RDS MySQL DB. A query must produce the daily average of a data source over the past 30 days. There are twice as many reads as writes. Queries to the collected data are for one source ID at a time. How can the Solutions Architect improve the reliability and cost effectiveness of this solution?

- A. Use Amazon Aurora with MySQL in a Multi-AZ mod
- B. Use four additional read replicas.
- C. Use Amazon DynamoDB with the source ID as the partition key and the timestamp as the sort ke
- D. Use a Time to Live (TTL) to delete data after 30 days.
- E. Use Amazon DynamoDB with the source ID as the partition ke
- F. Use a different table each day.
- G. Ingest data into Amazon Kinesis using a retention period of 30 day
- H. Use AWS Lambda to write data records to Amazon ElastiCache for read access.

Answer: B

Explanation:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html>

NEW QUESTION 105

A financial company is using a high-performance compute cluster running on Amazon EC2 instances to perform market simulations A DNS record must be created in an Amazon Route 53 private hosted zone when instances start The DNS record must be removed after instances are terminated. Currently the company uses a combination of Amazon CloudWatch Events and AWS Lambda to create the DNS record. The solution worked well in testing with small clusters, but in production with clusters containing thousands of instances the company sees the following error in the Lambda logs: HTTP 400 error (Bad request). The response header also includes a status code element with a value of "Throttling" and a status message element with a value of "Rate exceeded " Which combination of steps should the Solutions Architect take to resolve these issues? (Select THREE)

- A. Configure an Amazon SQS FIFO queue and configure a CloudWatch Events rule to use this queue as a target
- B. Remove the Lambda target from the CloudWatch Events rule
- C. Configure an Amazon Kinesis data stream and configure a CloudWatch Events rule to use this queue as a target Remove the Lambda target from the CloudWatch Events rule
- D. Update the CloudWatch Events rule to trigger on Amazon EC2 "Instance Launch Successful" and "Instance Terminate Successful" events for the Auto Scaling group used by the cluster
- E. Configure a Lambda function to retrieve messages from an Amazon SQS queue Modify the Lambda function to retrieve a maximum of 10 messages then batch the messages by Amazon Route 53 API call type and submit Delete the messages from the SQS queue after successful API calls.
- F. Configure an Amazon SQS standard queue and configure the existing CloudWatch Events rule to use this queue as a target Remove the Lambda target from the CloudWatch Events rule.
- G. Configure a Lambda function to read data from the Amazon Kinesis data stream and configure the batch window to 5 minutes Modify the function to make a single API call to Amazon Route 53 with all records read from the kinesis data stream

Answer: BEF

NEW QUESTION 110

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SAP-C01 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SAP-C01 Product From:

<https://www.2passeasy.com/dumps/SAP-C01/>

Money Back Guarantee

SAP-C01 Practice Exam Features:

- * SAP-C01 Questions and Answers Updated Frequently
- * SAP-C01 Practice Questions Verified by Expert Senior Certified Staff
- * SAP-C01 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SAP-C01 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year