



Amazon-Web-Services

Exam Questions SAP-C02

AWS Certified Solutions Architect - Professional

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

- (Exam Topic 1)

A 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 2

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: C

Explanation:

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

NEW QUESTION 3

- (Exam Topic 1)

A company 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.yam>

NEW QUESTION 4

- (Exam Topic 1)

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

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

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

Answer: D

Explanation:

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 6

- (Exam Topic 1)

A company has a complex web application that leverages Amazon CloudFront for global scalability and performance. Over time, users report that the web application is slowing down.

The company's operations team reports that the CloudFront cache hit ratio has been dropping steadily. The cache metrics report indicates that query strings on some URLs are inconsistently ordered and are specified sometimes in mixed-case letters and sometimes in lowercase letters.

Which set of actions should the solutions architect take to increase the cache hit ratio as quickly as possible?

- A. Deploy a Lambda@Edge function to sort parameters by name and force them to be lowercase
- B. Select the CloudFront viewer request trigger to invoke the function.
- C. Update the CloudFront distribution to disable caching based on query string parameters.
- D. Deploy a reverse proxy after the load balancer to post-process the emitted URLs in the application to force the URL strings to be lowercase.
- E. Update the CloudFront distribution to specify casing-insensitive query string processing.

Answer: A

Explanation:

https://docs.amazonaws.cn/en_us/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html#lambda-ex Before CloudFront serves content from the cache it will trigger any Lambda function associated with the Viewer Request, in which we can normalize parameters.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html#lambda-examp>

NEW QUESTION 7

- (Exam Topic 1)

A fitness tracking company serves users around the world, with its primary markets in North America and Asia. The company needs to design an infrastructure for its read-heavy user authorization application with the following requirements:

- Be resilient to problems with the application in any Region.
- Write to a database in a single Region.
- Read from multiple Regions.
- Support resiliency across application tiers in each Region.
- Support the relational database semantics reflected in the application. Which combination of steps should a solutions architect take? (Select TWO.)

- A. Use an Amazon Route 53 geoproximity routing policy combined with a multivalue answer routing policy.
- B. Deploy the application, and MySQL database servers to Amazon EC2 instances in each Region.
- C. Set up the application so that reads and writes are local to the Region.
- D. Create snapshots of the web, application, and database servers and store the snapshots in an Amazon S3 bucket in both Regions.
- E. Set up cross-Region replication for the database layer.
- F. Use an Amazon Route 53 geolocation routing policy combined with a failover routing policy.
- G. Set up web, application, and Amazon RDS for MySQL instances in each Region.
- H. Set up the application so that reads are local and writes are partitioned based on the user.
- I. Set up a Multi-AZ failover for the web, application, and database server.
- J. Set up cross-Region replication for the database layer.
- K. Set up active-active web and application servers in each Region.
- L. Deploy an Amazon Aurora global database with clusters in each Region.
- M. Set up the application to use the in-Region Aurora database endpoint.
- N. Create snapshots of the web and application servers and store them in an Amazon S3 bucket in both Regions.

Answer: CE

Explanation:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

Geoproximity routing policy is good to control the user traffic to specific regions. However, a multivalue answer routing policy may cause the users to be randomly sent to other healthy regions that may be far away from the user's location. You can use geolocation routing policy to direct the North American users to your servers on the North America region and configure failover routing to the Asia region in case the North America region fails. You can configure the same for the Asian users pointed to the Asia region servers and have the North America region as its backup.

NEW QUESTION 8

- (Exam Topic 1)

A company hosts a photography website on AWS that has global visitors. The website has experienced steady increases in traffic during the last 12 months, and users have reported a delay in displaying images. The company wants to configure Amazon CloudFront to deliver photos to visitors with minimal latency. Which actions will achieve this goal? (Select TWO.)

- A. Set the Minimum TTL and Maximum TTL to 0 in the CloudFront distribution.
- B. Set the Minimum TTL and Maximum TTL to a high value in the CloudFront distribution.
- C. Set the CloudFront distribution to forward all headers, all cookies, and all query strings to the origin.
- D. Set up additional origin servers that are geographically closer to the requester.
- E. Configure latency-based routing in Amazon Route 53.
- F. Select Price Class 100 on the CloudFront distribution.

Answer: BD

NEW QUESTION 9

- (Exam Topic 1)

A company wants to change its internal cloud billing strategy for each of its business units. Currently, the cloud governance team shares reports for overall cloud spending with the head of each business unit. The company uses AWS Organizations to manage the separate AWS accounts for each business unit. The existing tagging standard in Organizations includes the application, environment, and owner. The cloud governance team wants a centralized solution so each business unit receives monthly reports on its cloud spending. The solution should also send notifications for any cloud spending that exceeds a set threshold. Which solution is the MOST cost-effective way to meet these requirements?

- A. Configure AWS Budgets in each account and configure budget alerts that are grouped by application, environment, and owner.
- B. Add each business unit to an Amazon SNS topic for each alert.
- C. Use Cost Explorer in each account to create monthly reports for each business unit.
- D. Configure AWS Budgets in the organization's master account and configure budget alerts that are grouped by application, environment, and owner.
- E. Add each business unit to an Amazon SNS topic for each alert.
- F. Use Cost Explorer in the organization's master account to create monthly reports for each business unit.
- G. Configure AWS Budgets in each account and configure budget alerts that are grouped by application, environment, and owner.
- H. Add each business unit to an Amazon SNS topic for each alert.
- I. Use the AWS Billing and Cost Management dashboard in each account to create monthly reports for each business unit.
- J. Enable AWS Cost and Usage Reports in the organization's master account and configure reports grouped by application, environment, and owner.
- K. Create an AWS Lambda function that processes AWS Cost and Usage Reports, sends budget alerts, and sends monthly reports to each business unit's email list.

Answer: B

Explanation:

Configure AWS Budgets in the organization's master account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in the organization's master account to create monthly reports for each business unit.
<https://aws.amazon.com/about-aws/whats-new/2019/07/introducing-aws-budgets-reports/#:~:text=AWS%20Bud>

NEW QUESTION 10

- (Exam Topic 1)

A company is running a web application on Amazon EC2 instances in a production AWS account. The company requires all logs generated from the web application to be copied to a central AWS account (or analysis and archiving). The company's AWS accounts are currently managed independently. Logging agents are configured on the EC2 instances to upload the log files to an Amazon S3 bucket in the central AWS account.

A solutions architect needs to provide access for a solution that will allow the production account to store log files in the central account. The central account also needs to have read access to the log files.

What should the solutions architect do to meet these requirements?

- A. Create a cross-account role in the central account
- B. Assume the role from the production account when the logs are being copied.
- C. Create a policy on the S3 bucket with the production account ID as the principal
- D. Allow S3 access from a delegated user.
- E. Create a policy on the S3 bucket with access from only the CIDR range of the EC2 instances in the production account
- F. Use the production account ID as the principal.
- G. Create a cross-account role in the production account
- H. Assume the role from the production account when the logs are being copied.

Answer: B

NEW QUESTION 10

- (Exam Topic 1)

A company wants to host a new global website that consists of static content. A solutions architect is working on a solution that uses Amazon CloudFront with an origin access identity (OAI) to access website content that is stored in a private Amazon S3 bucket.

During testing, the solutions architect receives 404 errors from the S3 bucket. Error messages appear only for attempts to access paths that end with a forward slash, such as example.com/path/. These requests should return the existing S3 object path/index.html. Any potential solution must not prevent CloudFront from caching the content.

What should the solutions architect do to resolve this problem?

- A. Change the CloudFront origin to an Amazon API Gateway proxy endpoint
- B. Rewrite the S3 request URL by using an AWS Lambda function.
- C. Change the CloudFront origin to an Amazon API Gateway endpoint
- D. Rewrite the S3 request URL in an AWS service integration.
- E. Change the CloudFront configuration to use an AWS Lambda@Edge function that is invoked by a viewer request event to rewrite the S3 request URL.
- F. Change the CloudFront configuration to use an AWS Lambda@Edge function that is invoked by an origin request event to rewrite the S3 request URL.

Answer: C

NEW QUESTION 12

- (Exam Topic 1)

A scientific organization requires the processing of text and picture data stored in an Amazon S3 bucket. The data is gathered from numerous radar stations during a mission's live, time-critical phase. The data is uploaded by the radar stations to the source S3 bucket. The data is preceded with the identification number of the radar station.

In a second account, the business built a destination S3 bucket. To satisfy a compliance target, data must be transferred from the source S3 bucket to the destination S3 bucket. Replication is accomplished by using an S3 replication rule that covers all items in the source S3 bucket.

A single radar station has been recognized as having the most precise data. At this radar station, data replication must be completed within 30 minutes of the radar station uploading the items to the source S3 bucket.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Set up an AWS DataSync agent to replicate the prefixed data from the source S3 bucket to the destination S3 bucket
- B. Select to use available bandwidth on the task, and monitor the task to ensure that it is in the TRANSFERRING status
- C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an alert if this status changes.
- D. In the second account, create another S3 bucket to receive data from the radar station with the most accurate data. Set up a new replication rule for this new S3 bucket to separate the replication from the other radar stations. Monitor the maximum replication time to the destination
- E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an alert when the time exceeds the desired threshold
- F. Enable Amazon S3 Transfer Acceleration on the source S3 bucket, and configure the radar station with the most accurate data to use the new endpoint. Monitor the S3 destination bucket's TotalRequestLatency metric. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an alert if this status changes
- G. Create a new S3 replication rule on the source S3 bucket that filters for the keys that use the prefix of the radar station with the most accurate data. Enable S3 Replication Time Control (S3 RTC). Monitor the maximum replication time to the destination. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an alert when the time exceeds the desired threshold

Answer: D

Explanation:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-time-control.html>

NEW QUESTION 16

- (Exam Topic 1)

The company needs to determine which costs on the monthly AWS bill are attributable to each application or team. The company also must be able to create reports to compare costs from the last 12 months and to help forecast costs for the next 12 months. A solutions architect must recommend an AWS Billing and Cost Management solution that provides these cost reports.

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

- A. Activate the user-defined cost allocation tags that represent the application and the team.
- B. Activate the AWS generated cost allocation tags that represent the application and the team.
- C. Create a cost category for each application in Billing and Cost Management.
- D. Activate IAM access to Billing and Cost Management.
- E. Create a cost budget.
- F. Enable Cost Explorer.

Answer: ACF

Explanation:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/manage-cost-categories.html> <https://aws.amazon.com/premiumsupport/knowledge-center/cost-explorer-analyze-spending-and-usage/> <https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/manage-cost-categories.html>
<https://docs.aws.amazon.com/cost-management/latest/userguide/ce-enable.html>

NEW QUESTION 19

- (Exam Topic 1)

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

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

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

- A. Create CloudFormation templates and re-use parts of the Python scripts as instance user dat
- B. Use the AWS Cloud Development Kit (AWS CDK) to deploy the application using these template
- C. Incorporate the AWS CDK into CodePipeline and deploy the application to AWS using these templates.
- D. Use a third-party resource provisioning engine inside AWS CodeBuild to standardize the deployment processes of the existing and acquired compan
- E. Orchestrate the CodeBuild job using CodePipeline.
- F. Standardize on AWS OpsWork
- G. Integrate OpsWorks with CodePipelin
- H. Have the developers create Chef recipes to deploy their applications on AWS.
- I. Define the AWS resources using Typescript or Pytho
- J. Use the AWS Cloud Development Kit (AWS CDK) to create CloudFormation templates from the developers' code, and use the AWS CDK to create CloudFormation stack
- K. Incorporate the AWS CDK as a CodeBuild job in CodePipeline.

Answer: D

NEW QUESTION 21

- (Exam Topic 1)

A 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 gateways 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 onl
- 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 VP
- 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 onl
- F. Detach the internet gateway and remove the NAT gateways from the VP
- 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 onl
- I. Detach the internet gateway from the VPC, and use an Aurora Serverless databas
- 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 bucke
- M. Use Amazon
- N. CloudWatch and AWS Lambda to stop and start the Aurora DB cluster so it operates during business hours onl
- 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 22

- (Exam Topic 1)

A company is running an Apache Hadoop cluster on Amazon EC2 instances. The Hadoop cluster stores approximately 100 TB of data for weekly operational reports and allows occasional access for data scientists to retrieve data. The company needs to reduce the cost and operational complexity for storing and serving this data.

Which solution meets these requirements in the MOST cost-effective manner?

- A. Move the Hadoop cluster from EC2 instances to Amazon EM
- B. Allow data access patterns to remain the same.
- C. Write a script that resizes the EC2 instances to a smaller instance type during downtime and resizes the instances to a larger instance type before the reports are created.
- D. Move the data to Amazon S3 and use Amazon Athena to query the data for report
- E. Allow the data scientists to access the data directly in Amazon S3.
- F. Migrate the data to Amazon DynamoDB and modify the reports to fetch data from DynamoD
- G. Allow the data scientists to access the data directly in DynamoDB.

Answer: C

Explanation:

"The company needs to reduce the cost and operational complexity for storing and serving this data. Which solution meets these requirements in the MOST cost-effective manner?" EMR storage is ephemeral. The company has 100TB that need to persist, they would have to use EMRFS to backup to S3 anyway.

<https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-storage.html>

100TB

EBS - 8.109\$ S3 - 2.355\$

You have saved 5.752\$

This amount can be used for Athen. BTW. we don't know indexes, amount of data that is scanned. What we know is that it will be: "occasional access for data scientists to retrieve data"

NEW QUESTION 24

- (Exam Topic 1)

A company is running a tone-of-business (LOB) application on AWS to support its users. The application runs in one VPC, with a backup copy in a second VPC in a different AWS Region for disaster recovery. The company has a single AWS Direct Connect connection between its on-premises network and AWS. The connection terminates at a Direct Connect gateway.

All access to the application must originate from the company's on-premises network, and traffic must be encrypted in transit through the use of Psec. The company is routing traffic through a VPN tunnel over the Direct Connect connection to provide the required encryption.

A business continuity audit determines that the Direct Connect connection represents a potential single point of failure for access to the application. The company needs to remediate this issue as quickly as possible.

Which approach will meet these requirements?

- A. Order a second Direct Connect connection to a different Direct Connect location.
- B. Terminate the second Direct Connect connection at the same Direct Connect gateway.
- C. Configure an AWS Site-to-Site VPN connection over the internet. Terminate the VPN connection at a virtual private gateway in the secondary Region.
- D. Create a transit gateway. Attach the VPCs to the transit gateway, and connect the transit gateway to the Direct Connect gateway. Configure an AWS Site-to-Site VPN connection, and terminate it at the transit gateway.
- E. Create a transit gateway.
- F. Attach the VPCs to the transit gateway, and connect the transit gateway to the Direct Connect gateway.
- G. Order a second Direct Connect connection, and terminate it at the transit gateway.

Answer: C

Explanation:

Create a transit gateway. Attach the VPCs to the transit gateway, and connect the transit gateway to the Direct Connect gateway. Configure an AWS Site-to-Site VPN connection, and terminate it at the transit gateway.

<https://aws.amazon.com/premiumsupport/knowledge-center/dx-configure-dx-and-vpn-failover-tgw/>

All access to the application must originate from the company's on-premises network, and traffic must be encrypted in transit through the use of IPsec. = need to use VPN.

NEW QUESTION 25

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: A

NEW QUESTION 30

- (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 34

- (Exam Topic 1)

A solutions architect is designing an application to accept timesheet entries from employees on their mobile devices. Timesheets will be submitted weekly, with most of the submissions occurring on Friday. The data must be stored in a format that allows payroll administrators to run monthly reports. The infrastructure must be highly available and scale to match the rate of incoming data and reporting requests.

Which combination of steps meets these requirements while minimizing operational overhead? (Select TWO.)

- A. Deploy the application to Amazon EC2 On-Demand Instances With load balancing across multiple Availability Zone
- B. Use scheduled Amazon EC2 Auto Scaling to add capacity before the high volume of submissions on Fridays.
- C. Deploy the application in a container using Amazon Elastic Container Service (Amazon ECS) with load balancing across multiple Availability Zone
- D. Use scheduled Service Auto Scaling to add capacity before the high volume of submissions on Fridays.
- E. Deploy the application front end to an Amazon S3 bucket served by Amazon CloudFront
- F. Deploy the application backend using Amazon API Gateway with an AWS Lambda proxy integration.
- G. Store the timesheet submission data in Amazon Redshift
- H. Use Amazon QuickSight to generate the reports using Amazon Redshift as the data source.
- I. Store the timesheet submission data in Amazon S3. Use Amazon Athena and Amazon QuickSight to generate the reports using Amazon S3 as the data source.

Answer: AE

NEW QUESTION 36

- (Exam Topic 1)

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

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

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

Answer: D

Explanation:

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

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-g>

NEW QUESTION 37

- (Exam Topic 1)

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

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

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

Which solution meets these requirements?

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

Answer: C

NEW QUESTION 38

- (Exam Topic 1)

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

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

- A. Create a REST API in Amazon API Gateway and use AWS Lambda functions as the application layer.
- B. Create an Application Load Balancer and migrate the Docker container to AWS Fargate.
- C. Migrate the storage layer to Amazon DynamoD8.
- D. Migrate the storage layer to Amazon DocumentD8 (with MongoDB compatibility).
- E. Create an Application Load Balancer and move the storage layer to an EC2 Auto Scaling group.

Answer: BD

Explanation:

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

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

NEW QUESTION 39

- (Exam Topic 1)

A company is launching a new web application on Amazon EC2 instances. Development and production workloads exist in separate AWS accounts.

According to the company's security requirements, only automated configuration tools are allowed to access the production account. The company's security team wants to receive immediate notification if any manual access to the production AWS account or EC2 instances occurs

Which combination of actions should a solutions architect take in the production account to meet these requirements? (Select THREE.)

- A. Turn on AWS CloudTrail logs in the application's primary AWS Region Use Amazon Athena to queue the logs for AwsConsoleSignIn events.
- B. Configure Amazon Simple Email Service (Amazon SES) to send email to the security team when an alarm is activated.
- C. Deploy EC2 instances in an Auto Scaling group Configure the launch template to deploy instances without key pairs Configure Amazon CloudWatch Logs to capture system access logs Create an Amazon CloudWatch alarm that is based on the logs to detect when a user logs in to an EC2 instance
- D. Configure an Amazon Simple Notification Service (Amazon SNS) topic to send a message to the security team when an alarm is activated
- E. Turn on AWS CloudTrail logs for all AWS Region
- F. Configure Amazon CloudWatch alarms to provide an alert when an AwsConsoleSignin event is detected.
- G. Deploy EC2 instances in an Auto Scaling grou
- H. Configure the launch template to delete the key pair after launc
- I. Configure Amazon CloudWatch Logs for the system access logs Create an Amazon CloudWatch dashboard to show user logins over time.

Answer: CDE

NEW QUESTION 40

- (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 gatewa
- B. Delete the existing private virtual interface from the existing connectio
- C. Create the second Direct Connect connectio
- D. Create a new private virtual interlace on each connection, and connect both private virtual interfaces to the Direct Connect gatewa
- E. Connect the Direct Connect gateway to the single VPC.
- F. Keep the existing private virtual interfac
- G. Create the second Direct Connect connectio
- 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 interfac
- J. Create the second Direct Connect connectio
- 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 gatewa
- M. Delete the existing private virtual interface from the existing connection.Create the second Direct Connect connectio
- N. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the transit gatewa
- 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 44

- (Exam Topic 1)

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:

- * 1. The data must be highly durable and available.
- * 2. The data must always be encrypted at rest and in transit.
- * 3. 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:

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.

NEW QUESTION 46

- (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 49

- (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
- B. Create an Amazon S3 bucket to be used for SFTP file hosting
- C. Create an AWS Transfer Family server. Configure the Transfer Family server with a publicly accessible endpoint. Associate the SFTP Elastic IP address with the new endpoint. Point the Transfer Family server to the S3 bucket.
- D. Sync all files from the SFTP server to the S3 bucket.
- E. Disassociate the Elastic IP address from the EC2 instance
- F. Create an Amazon S3 bucket to be used for SFTP file hosting
- G. Create an AWS Transfer Family server
- H. Configure the Transfer Family server with a VPC-hosted, internet-facing endpoint
- I. Associate the SFTP Elastic IP address with the new endpoint
- J. Attach the security group with customer IP addresses to the new endpoint
- K. Point the Transfer Family server to the S3 bucket. 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
- P. 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
- Q. Associate the Elastic IP address with the NLB
- R. Sync all files from the SFTP server to the S3 bucket.
- T. Disassociate the Elastic IP address from the EC2 instance
- . Create a multi-attach Amazon Elastic Block Store (Amazon EBS) volume to be used for SFTP file hosting
- . Create a Network Load Balancer (NLB) with the Elastic IP address attached
- . Create an Auto Scaling group with EC2 instances that run an SFTP server. Define in the Auto Scaling group that instances that are launched should attach the new multi-attach EBS volume. Configure the Auto Scaling group to automatically add instances behind the NLB. Configure the Auto Scaling group to use the security group that allows customer IP addresses for the EC2 instances that the Auto Scaling group launches
- . Sync all files from the SFTP server to the new multi-attach EBS volume.

Answer: B

Explanation:

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

NEW QUESTION 53

- (Exam Topic 1)

A solutions architect is building a web application that uses an Amazon RDS for PostgreSQL DB instance. The DB instance is expected to receive many more reads than writes. The solutions architect needs to ensure that the large amount of read traffic can be accommodated and that the DB instance is highly available. Which steps should the solutions architect take to meet these requirements? (Select THREE)

- A. Create multiple read replicas and put them into an Auto Scaling group.
- B. Create multiple read replicas in different Availability Zones.
- C. Create an Amazon Route 53 hosted zone and a record set for each read replica with a TTL and a weighted routing policy.
- D. Create an Application Load Balancer (ALB) and put the read replicas behind the ALB.
- E. Configure an Amazon CloudWatch alarm to detect a failed read replica

- F. Set the alarm to directly invoke an AWS Lambda function to delete its Route 53 record set.
- G. Configure an Amazon Route 53 health check for each read replica using its endpoint

Answer: BCF

Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/requests-rds-read-replicas/>

You can use Amazon Route 53 weighted record sets to distribute requests across your read replicas. Within a Route 53 hosted zone, create individual record sets for each DNS endpoint associated with your read replicas and give them the same weight. Then, direct requests to the endpoint of the record set. You can incorporate Route 53 health checks to be sure that Route 53 directs traffic away from unavailable read replicas

NEW QUESTION 57

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 62

- (Exam Topic 1)

A solutions architect is building a web application that uses an Amazon RDS for PostgreSQL DB instance The DB instance is expected to receive many more reads than writes The solutions architect needs to ensure that the large amount of read traffic can be accommodated and that the DB instance is highly available. Which steps should the solutions architect take to meet these requirements? (Select THREE.)

- A. Create multiple read replicas and put them into an Auto Scaling group
- B. Create multiple read replicas in different Availability Zones.
- C. Create an Amazon Route 53 hosted zone and a record set for each read replica with a TTL and a weighted routing policy
- D. Create an Application Load Balancer (ALBJ and put the read replicas behind the ALB.
- E. Configure an Amazon CloudWatch alarm to detect a failed read replica Set the alarm to directly invoke an AWS Lambda function to delete its Route 53 record set.
- F. Configure an Amazon Route 53 health check for each read replica using its endpoint

Answer: BCF

Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/requests-rds-read-replicas/>

You can use Amazon Route 53 weighted record sets to distribute requests across your read replicas. Within a Route 53 hosted zone, create individual record sets for each DNS endpoint associated with your read replicas and give them the same weight. Then, direct requests to the endpoint of the record set. You can incorporate Route 53 health checks to be sure that Route 53 directs traffic away from unavailable read replicas

NEW QUESTION 65

- (Exam Topic 1)

A company wants to migrate its corporate data center from on premises to the AWS Cloud. The data center includes physical servers and VMs that use VMware and Hyper-V. An administrator needs to select the correct services to collect data (or the initial migration discovery process. The data format should be supported by AWS Migration Hub. The company also needs the ability to generate reports from the data. Which solution meets these requirements?

- A. Use the AWS Agentless Discovery Connector for data collection on physical servers and all VM
- B. Store the collected data in Amazon S3. Query the data with S3 Selec
- C. Generate reports by using Kibana hosted on Amazon EC2.
- D. Use the AWS Application Discovery Service agent for data collection on physical servers and all VMs.Store the collected data in Amazon Elastic File System (Amazon EFS). Query the data and generate reports with Amazon Athena.
- E. Use the AWS Application Discovery Service agent for data collection on physical servers and Hyper-
- F. Use the AWS Agentless Discovery Connector for data collection on VMwar
- G. Store the collected data in Amazon S3. Query the data with Amazon Athen
- H. Generate reports by using Amazon QuickSight.
- I. Use the AWS Systems Manager agent for data collection on physical server
- J. Use the AWS Agentless Discovery Connector for data collection on all VM
- K. Store, query, and generate reports from the collected data by using Amazon Redshift.

Answer: C

Explanation:

<https://docs.aws.amazon.com/application-discovery/latest/userguide/discovery-agent.html> <https://docs.aws.amazon.com/application-discovery/latest/userguide/discovery-connector.html>

NEW QUESTION 70

- (Exam Topic 1)

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

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

- A. Create a VPC in the us-west-1 Region
- B. Use inter-Region VPC peering to connect both VPC
- C. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region
- D. Deploy EC2 instances across multiple AZs in each Region as part of an Auto Scaling group spanning both VPCs and served by the ALB.
- E. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region
- F. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the AL
- G. Deploy the same solution to the us-west-1 Region Create an Amazon Route 53 record set with a failover routing policy and health checks enabled to provide high availability across both Regions.
- H. Create a VPC in the us-west-1 Region
- I. Use inter-Region VPC peering to connect both VPCs Deploy an Application Load Balancer (ALB) that spans both VPCs Deploy EC2 instances across multiple Availability Zones as part of an Auto Scaling group in each VPC served by the AL
- J. Create an Amazon Route 53 record that points to the ALB.
- K. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region
- L. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the AL
- M. Deploy the same solution to the us-west-1 Region
- N. Create separate Amazon Route 53 records in each Region that point to the ALB in the Region
- O. Use Route 53 health checks to provide high availability across both Regions.

Answer: B

Explanation:

A new web application in a active-passive DR mode. a Route 53 record set with a failover routing policy.

NEW QUESTION 74

- (Exam Topic 1)

A company runs a popular public-facing ecommerce 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 77

- (Exam Topic 1)

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

Which step should the solutions architect take to meet these requirements?

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

Answer: D

NEW QUESTION 78

- (Exam Topic 1)

A multimedia company needs to deliver its video-on-demand (VOD) content to its subscribers in a cost-effective way. The video files range in size from 1-15 GB and are typically viewed frequently for the first 6 months after creation, and then access decreases considerably. The company requires all video files to remain immediately available for subscribers. There are now roughly 30,000 files, and the company anticipates doubling that number over time.

What is the MOST cost-effective solution for delivering the company's VOD content?

- A. Store the video files in an Amazon S3 bucket using S3 Intelligent-Tiering
- B. Use Amazon CloudFront to deliver the content with the S3 bucket as the origin.
- C. Use AWS Elemental MediaConvert and store the adaptive bitrate video files in Amazon S3. Configure an AWS Elemental MediaPackage endpoint to deliver the content from Amazon S3.
- D. Store the video files in Amazon Elastic File System (Amazon EFS) Standard
- E. Enable EFS lifecycle management to move the video files to EFS Infrequent Access after 6 months
- F. Create an Amazon EC2 Auto Scaling group behind an Elastic Load Balancer to deliver the content from Amazon EFS.
- G. Store the video files in Amazon S3 Standard
- H. Create S3 Lifecycle rules to move the video files to S3 Standard-Infrequent Access (S3 Standard-IA) after 6 months and to S3 Glacier Deep Archive after 1 year
- I. Use Amazon CloudFront to deliver the content with the S3 bucket as the origin.

Answer: A

Explanation:

<https://d1.awsstatic.com/whitepapers/amazon-cloudfront-for-media.pdf> <https://aws.amazon.com/solutions/implementations/video-on-demand-on-aws/>

NEW QUESTION 81

- (Exam Topic 1)

A team collects and routes behavioral data for an entire company. The company runs a Multi-AZ VPC environment with public subnets, private subnets, and an internet gateway. Each public subnet also contains a NAT gateway. Most of the company's applications read from and write to Amazon Kinesis Data Streams. Most of the workloads are in private subnets.

A solutions architect must review the infrastructure. The solutions architect needs to reduce costs and maintain the function of the applications. The solutions architect uses Cost Explorer and notices that the cost in the EC2-Other category is consistently high. A further review shows that NatGateway-Bytes charges are increasing the cost in the EC2-Other category.

What should the solutions architect do to meet these requirements?

- A. Enable VPC Flow Log
- B. Use Amazon Athena to analyze the logs for traffic that can be removed
- C. Ensure that security groups are blocking traffic that is responsible for high costs.
- D. Add an interface VPC endpoint for Kinesis Data Streams to the VPC
- E. Ensure that applications have the correct IAM permissions to use the interface VPC endpoint.
- F. Enable VPC Flow Logs and Amazon Detective. Review Detective findings for traffic that is not related to Kinesis Data Streams. Configure security groups to block that traffic.
- G. Add an interface VPC endpoint for Kinesis Data Streams to the VPC
- H. Ensure that the VPC endpoint policy allows traffic from the applications.

Answer: D

Explanation:

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-access.html>

<https://aws.amazon.com/premiumsupport/knowledge-center/vpc-reduce-nat-gateway-transfer-costs/>

VPC endpoint policies enable you to control access by either attaching a policy to a VPC endpoint or by using additional fields in a policy that is attached to an IAM user, group, or role to restrict access to only occur via the specified VPC endpoint.

NEW QUESTION 83

- (Exam Topic 1)

A company wants to migrate a 30 TB Oracle data warehouse from on-premises to Amazon Redshift. The company used the AWS Schema Conversion Tool (AWS SCT) to convert the schema of the existing data warehouse to an Amazon Redshift schema. The company also used a migration assessment report to identify manual tasks to complete.

The company needs to migrate the data to the new Amazon Redshift cluster during an upcoming data freeze period of 2 weeks. The only network connection between the on-premises data warehouse and AWS is a 50 Mbps internet connection.

Which migration strategy meets these requirements?

- A. Create an AWS Database Migration Service (AWS DMS) replication instance.
- B. Authorize the public IP address of the replication instance to reach the data warehouse through the corporate firewall. Create a migration task to run at the beginning of the data freeze period.
- C. Install the AWS SCT extraction agents on the on-premises server.
- D. Define the extract, upload, and copy tasks to send the data to an Amazon S3 bucket.
- E. Copy the data into the Amazon Redshift cluster.
- F. Run the tasks at the beginning of the data freeze period.
- G. Install the AWS SCT extraction agents on the on-premises server.
- H. Create a Site-to-Site VPN connection. Create an AWS Database Migration Service (AWS DMS) replication instance that is the appropriate size. Authorize the IP address of the replication instance to be able to access the on-premises data warehouse through the VPN connection.
- I. Create a job in AWS Snowball Edge to import data into Amazon S3. Install AWS SCT extraction agents on the on-premises servers. Define the local and AWS Database Migration Service (AWS DMS) tasks to send the data to the Snowball Edge device. When the Snowball Edge device is returned to AWS and the data is available in Amazon S3, run the AWS DMS subtask to copy the data to Amazon Redshift.

Answer: D

Explanation:

AWS Database Migration Service (AWS DMS) can use Snowball Edge and Amazon S3 to migrate large databases more quickly than by other methods.

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_LargeDBs.html

https://www.calctool.org/CALC/proof/computing/transfer_time

NEW QUESTION 87

- (Exam Topic 1)

A company runs an application on AWS. An AWS Lambda function uses credentials to authenticate to an Amazon RDS MySQL DB instance. A security risk assessment identified that these credentials are not frequently rotated. Also, encryption at rest is not enabled for the DB instance. The security team requires that

both of these issues be resolved.

Which strategy should a solutions architect recommend to remediate these security risks?

- A. Configure the Lambda function to store and retrieve the database credentials in AWS Secrets Manager and enable rotation of the credential
- B. Take a snapshot of the DB instance and encrypt a copy of that snapshot
- C. Replace the DB instance with a new DB instance that is based on the encrypted snapshot.
- D. Enable IAM DB authentication on the DB instance
- E. Grant the Lambda execution role access to the DB instance
- F. Modify the DB instance and enable encryption.
- G. Enable IAM DB authentication on the DB instance
- H. Grant the Lambda execution role access to the DB instance
- I. Create an encrypted read replica of the DB instance
- J. Promote the encrypted read replica to be the new primary node.
- K. Configure the Lambda function to store and retrieve the database credentials as encrypted AWS Systems Manager Parameter Store parameter
- L. Create another Lambda function to automatically rotate the credential
- M. Create an encrypted read replica of the DB instance
- N. Promote the encrypted read replica to be the new primary node.

Answer: A

Explanation:

Parameter store can store DB credentials as secure string but CANNOT rotate secrets, hence, go with A + Cannot enable encryption on existing MySQL RDS instance, must create a new encrypted one from unencrypted snapshot.

[https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-](https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets/) Encrypting a unencrypted instance of DB or creating an encrypted replica of an unencrypted DB instance are not possible. Hence A is the only solution possible.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html#Overview.Encryption>.

NEW QUESTION 92

- (Exam Topic 1)

A company uses AWS Transit Gateway for a hub-and-spoke model to manage network traffic between many VPCs. The company is developing a new service that must be able to send data at 100 Gbps. The company needs a faster connection to other VPCs in the same AWS Region.

Which solution will meet these requirements?

- A. Establish VPC peering between the necessary VPC
- B. Ensure that all route tables are updated as required.
- C. Attach an additional transit gateway to the VPC
- D. Update the route tables accordingly.
- E. Create AWS Site-to-Site VPN connections that use equal-cost multi-path (ECMP) routing between the necessary VPCs.
- F. Create an additional attachment from the necessary VPCs to the existing transit gateway.

Answer: D

NEW QUESTION 96

- (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.examWe.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 99

- (Exam Topic 1)

An ecommerce website running on AWS uses an Amazon RDS for MySQL DB instance with General Purpose SSD storage. The developers chose an appropriate instance type based on demand, and configured 100 GB of storage with a sufficient amount of free space.

The website was running smoothly for a few weeks until a marketing campaign launched. On the second day of the campaign, users reported long wait times and time outs. Amazon CloudWatch metrics indicated that both reads and writes to the DB instance were experiencing long response times. The CloudWatch metrics show 40% to 50% CPU and memory utilization, and sufficient free storage space is still available. The application server logs show no evidence of database connectivity issues.

What could be the root cause of the issue with the marketing campaign?

- A. It exhausted the I/O credit balance due to provisioning low disk storage during the setup phase.
- B. It caused the data in the tables to change frequently, requiring indexes to be rebuilt to optimize queries.
- C. It exhausted the maximum number of allowed connections to the database instance.
- D. It exhausted the network bandwidth available to the RDS for MySQL DB instance.

Answer: A

Explanation:

"When using General Purpose SSD storage, your DB instance receives an initial I/O credit balance of 5.4 million I/O credits. This initial credit balance is enough to sustain a burst performance of 3,000 IOPS for 30 minutes."

<https://aws.amazon.com/blogs/database/how-to-use-cloudwatch-metrics-to-decide-between-general-purpose-or>

NEW QUESTION 103

- (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 in AWS Organizations. 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 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 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 105

- (Exam Topic 1)

A company needs to implement a patching process for its servers. The on-premises servers and Amazon EC2 instances use a variety of tools to perform patching. Management requires a single report showing the patch status of all the servers and instances. Which set of actions should a solutions architect take to meet these requirements?

- A. Use AWS Systems Manager to manage patches on the on-premises servers and EC2 instances.
- B. Use Systems Manager to generate patch compliance reports.
- C. Use AWS OpsWorks to manage patches on the on-premises servers and EC2 instances.
- D. Use Amazon QuickSight integration with OpsWorks to generate patch compliance reports.
- E. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to apply patches by scheduling an AWS Systems Manager patch remediation job.
- F. Use Amazon Inspector to generate patch compliance reports.
- G. Use AWS OpsWorks to manage patches on the on-premises servers and EC2 instances.
- H. Use AWS X-Ray to post the patch status to AWS Systems Manager OpsCenter to generate patch compliance reports.

Answer: A

Explanation:

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

NEW QUESTION 108

- (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 112

- (Exam Topic 2)

A life sciences company is using a combination of open source tools to manage data analysis workflows and Docker containers running on servers in its on-premises data center to process genomics data. Sequencing data is generated and stored on a local storage area network (SAN), and then the data is processed. The research and development teams are running into capacity issues and have decided to re-architect their genomics analysis platform on AWS to scale based on workload demands and reduce the turnaround time from weeks to days. The company has a high-speed AWS Direct Connect connection. Sequencers will generate around 200 GB of data for each genome, and individual jobs can take several hours to process the data with ideal compute capacity. The end result will be stored in Amazon S3. The company is expecting 10-15 job requests each day. Which solution meets these requirements?

- A. Use regularly scheduled AWS Snowball Edge devices to transfer the sequencing data into AWS. When AWS receives the Snowball Edge device and the data is loaded into Amazon S3, use S3 events to trigger an AWS Lambda function to process the data.
- B. Use AWS Data Pipeline to transfer the sequencing data to Amazon S3. Use S3 events to trigger an Amazon EC2 Auto Scaling group to launch custom-AMI EC2 instances running the Docker containers to process the data.

- C. Use AWS DataSync to transfer the sequencing data to Amazon S3 Use S3 events to trigger an AWS Lambda function that starts an AWS Step Functions workflow Store the Docker images in Amazon Elastic Container Registry (Amazon ECR) and trigger AWS Batch to run the container and process the sequencing data
- D. Use an AWS Storage Gateway file gateway to transfer the sequencing data to Amazon S3 Use S3 events to trigger an AWS Batch job that runs on Amazon EC2 instances running the Docker containers to process the data

Answer: C

NEW QUESTION 114

- (Exam Topic 2)

A company hosts a blog post application on AWS using Amazon API Gateway. Amazon DynamoDB, and AWS Lambda The application currently does not use API keys to authorize requests The API model is as follows:

GET /posts/{postId} to get post details

GET /users/{userId}. to get user details

GET /comments/{commentId}: to get comments details

The company has noticed users are actively discussing topics in the comments section, and the company wants to increase user engagement by making the comments appear in real time

Which design should be used to reduce comment latency and improve user experience?

- A. Use edge-optimized API with Amazon CloudFront to cache API responses.
- B. Modify the blog application code to request GET/commentsV{commentId} every 10 seconds
- C. Use AWS AppSync and leverage WebSockets to deliver comments
- D. Change the concurrency limit of the Lambda functions to lower the API response time.

Answer: C

NEW QUESTION 118

- (Exam Topic 2)

A company is running a two-tier web-based application in an on-premises data center. The application layer consists of a single server running a stateful application. The application connects to a PostgreSQL database running on a separate server The application's user base is expected to grow significantly, so the company is migrating the application and database to AWS The solution will use Amazon Aurora PostgreSQL. Amazon EC2 Auto Scaling, and Elastic Load Balancing.

Which solution will provide a consistent user experience that will allow the application and database tiers to scale?

- A. Enable Aurora Auto Scaling for Aurora Replica
- B. Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled
- C. Enable Aurora Auto Scaling for Aurora writer
- D. Use an Application Load Balancer with the round robin routing algorithm and sticky sessions enabled
- E. Aurora Auto Scaling for Aurora Replica
- F. Use an Application Load Balancer with the round robin routing algorithm and sticky sessions enabled.
- G. Aurora Auto Scaling for Aurora writer
- H. Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled.

Answer: C

NEW QUESTION 119

- (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 122

- (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 action
- E. Move the organization's root SCP to the Production O
- F. Move the new account to the Production OU when adjustments to AWS Config are complete.

Answer: D

NEW QUESTION 124

- (Exam Topic 2)

A company is planning to migrate an application from on premises to the AWS Cloud. The company will begin the migration by moving the application's underlying data storage to AWS. The application data is stored on a shared file system on premises, and the application servers connect to the shared file system through SMB.

A solutions architect must implement a solution that uses an Amazon S3 bucket for shared storage. Until the application is fully migrated and code is rewritten to use native Amazon S3 APIs, the application must continue to have access to the data through SMB. The solutions architect must migrate the application data to AWS to its new location while still allowing the on-premises application to access the data.

Which solution will meet these requirements?

- A. Create a new Amazon FSx for Windows File System file system. Configure AWS DataSync with one location for the on-premises file share and one location for the new Amazon FSx file system. Create a new DataSync task to copy the data from the on-premises file share location to the Amazon FSx file system.
- B. Create an S3 bucket for the application.
- C. Copy the data from the on-premises storage to the S3 bucket.
- D. Deploy an AWS Server Migration Service (AWS SMS) VM to the on-premises environment.
- E. Use AWS SMS to migrate the file storage server from on premises to an Amazon EC2 instance.
- F. Create an S3 bucket for the application.
- G. Deploy a new AWS Storage Gateway File gateway on on-premises.
- H. Create a new file share that stores data in the S3 bucket and is associated with the file gateway.
- I. Copy the data from the on-premises storage to the new file gateway endpoint.

Answer: A

NEW QUESTION 126

- (Exam Topic 2)

A company has a web application that allows users to upload short videos. The videos are stored on Amazon EBS volumes and analyzed by custom recognition software for categorization.

The website contains static content that has variable traffic with peaks in certain months. The architecture consists of Amazon EC2 instances running in an Auto Scaling group for the web application and EC2 instances running in an Auto Scaling group to process an Amazon SQS queue. The company wants to re-architect the application to reduce operational overhead using AWS managed services where possible and remove dependencies on third-party software.

Which solution meets these requirements?

- A. Use Amazon ECS containers for the web application and Spot Instances for the Auto Scaling group that processes the SQS queue.
- B. Replace the custom software with Amazon Rekognition to categorize the videos.
- C. Store the uploaded videos on Amazon EFS and mount the file system to the EC2 instances for the web application.
- D. Process the SQS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos.
- E. Host the web application in Amazon S3. Store the uploaded videos in Amazon S3. Use S3 event notifications to publish events to the SQS queue. Process the SQS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos.
- F. Use AWS Elastic Beanstalk to launch EC2 instances in an Auto Scaling group for the web application and launch a worker environment to process the SQS queue. Replace the custom software with Amazon Rekognition to categorize the videos.

Answer: D

NEW QUESTION 130

- (Exam Topic 2)

A company has deployed an application to multiple environments in AWS, including production and testing. The company has separate accounts for production and testing, and users are allowed to create additional

application users for team members or services, as needed. The security team has asked the operations team for better isolation between production and testing with centralized controls on security credentials and improved management of permissions between environments.

Which of the following options would MOST securely accomplish this goal?

- A. Create a new AWS account to hold user and service accounts, such as an identity account. Create users and groups in the identity account.
- B. Create roles with appropriate permissions in the production and testing accounts. Add the identity account to the trust policies for the roles.
- C. Modify permissions in the production and testing accounts to limit creating new IAM users to members of the operations team. Set a strong IAM password policy on each account. Create new IAM users and groups in each account to limit developer access to just the services required to complete their job function.
- D. Create a script that runs on each account that checks user accounts for adherence to a security policy. Disable any user or service accounts that do not comply.
- E. Create all user accounts in the production account. Create roles for access in the production account and testing account.
- F. Grant cross-account access from the production account to the testing account.

Answer: A

NEW QUESTION 133

- (Exam Topic 2)

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

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

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

- A. Create an organization in AWS Organizations. Create a single SCP for least privilege access across all accounts. Create a single OU for all accounts. Configure an IAM identity provider for federation with the on-premises AD FS server. Configure a central logging account with a defined process for log generating services to send log events to the central account.
- 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 organization.
- 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 135

- (Exam Topic 2)

a company needs to create a centralized logging architecture for all of its AWS accounts. The architecture should provide near-real-time data analysis for all AWS CloudTrail logs and VPC Flow logs across an AWS accounts. The company plans to use Amazon Elasticsearch Service (Amazon ES) to perform log analyses in me logging account.

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

- A. Configure CloudTrail and VPC Flow Logs m each AWS account to send data to a centralized Amazon S3 Ducket in the fogging accoun
- B. Create an AWS Lambda function to load data from the S3 bucket to Amazon ES m the togging account
- C. Configure CloudTrail and VPC Flow Logs to send data to a fog group m Amazon CloudWatch Logs n each AWS account Configure a CloudWatch subscription filter m each AWS account to send data to Amazon Kinesis Data Firehose In the fogging account Load data from Kinesis Data Firehose Into Amazon ES in the logging account
- D. Configure CloudTrail and VPC Flow Logs to send data to a separate Amazon S3 bucket In each AWS accoun
- E. Create an AWS Lambda function triggered by S3 evens to copy the data to a centralized logging bucke
- F. Create another Lambda function lo load data from the S3 bucket to Amazon ES in the logging account.
- G. Configure CloudTrail and VPC Flow Logs to send data to a fog group in Amazon CloudWatch Logs n each AWS account Create AWS Lambda functions in each AWS account to subscribe to the tog groups and stream the data to an Amazon S3 bucket in the togging accoun
- H. Create another Lambda function to toad data from the S3 bucket to Amazon ES in the logging account.

Answer: A

NEW QUESTION 140

- (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 cach
- B. Update the application to use DA
- 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 AL
- E. Update the Route 53 record to use a simple routing policy that targets the ALB's DNS alia
- F. Configure scheduled scaling for the EC2 instances before the content updates.
- G. Set up Amazon ElastiCache for Redi
- H. Update the application to use ElastiCach
- I. Create an Auto Scaling group for the EC2 instance
- J. Create an AmazonCloudFront distnbutio
- K. and set the Auto Scaling group as an origin for the distributio
- 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 Memcache
- N. Update the application to use ElastiCach
- 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 AL
- P. Update the Route 53 record to use a simple routing policy that targets the ALB's DNS alia
- Q. Configure scheduled scaling for the application before the content updates.
- R. Set up DynamoDB Accelerator (DAX) as in-memory cach
- S. Update the application to use DA
- 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 distributio
- . Update the Route 53 record to use a simple routing policy that targets the CloudFront distribution's DNS alia
- . Manually scale up EC2 instances before the content updates.

Answer: B

NEW QUESTION 144

- (Exam Topic 2)

A company is running an application in the AWS Cloud. The company's security team must approve the creation of all new IAM users. When a new 1AM user is created, all access for the user must be removed automatically. The security team must then receive a notification to approve the user. The company has a multi-Region AWS CloudTrail trail In the AWS account.

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

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rul
- B. Define a pattern with the detail-type value set to AWS API Call via CloudTrail and an eventName of CreateUser.
- C. Configure CloudTrail to send a notification for the CreateUser event to an Amazon Simple Notification Service (Amazon SNS) topic.
- D. Invoke a container that runs in Amazon Elastic Container Service (Amazon ECS) with AWS Fargatetechnology to remove access

- E. Invoke an AWS Step Functions state machine to remove access.
- F. Use Amazon Simple Notification Service (Amazon SNS) to notify the security team.
- G. Use Amazon Pinpoint to notify the security team.

Answer: ABE

NEW QUESTION 149

- (Exam Topic 2)

A company wants to send data from its on-premises systems to Amazon S3 buckets. The company created the S3 buckets in three different accounts. The company must send the data privately without the data traveling across the internet. The company has no existing dedicated connectivity to AWS. Which combination of steps should a solutions architect take to meet these requirements? (Select TWO.)

- A. Establish a networking account in the AWS Cloud Create a private VPC in the networking account Set up an AWS Direct Connect connection with a private VIF between the on-premises environment and the private VPC
- B. Establish a networking account in the AWS Cloud Create a private VPC in the networking account Set up an AWS Direct Connect connection with a public VIF between the on-premises environment and the private VPC
- C. Create an Amazon S3 interface endpoint in the networking account
- D. Create an Amazon S3 gateway endpoint in the networking account
- E. Establish a networking account in the AWS Clou
- F. Create a private VPC in the networking account Peer VPCs from the accounts that host the S3 buckets with the VPC in the network account

Answer: AD

NEW QUESTION 151

- (Exam Topic 2)

A gaming company created a game leaderboard by using a Multi-AZ deployment of an Amazon RDS database. The number of users is growing, and the queries to get individual player rankings are getting slower over time. The company expects a surge in users for an upcoming version and wants to optimize the design for scalability and performance.

Which solution will meet these requirements?

- A. Migrate the database to Amazon DynamoD
- B. Store the leader different table
- C. Use Apache HiveQL JOIN statements to build the leaderboard
- D. Keep the leaderboard data in the RDS DB instanc
- E. Provision a Multi-AZ deployment of an Amazon ElastiCache for Redis cluster.
- F. Stream the leaderboard data by using Amazon Kinesis Data Firehose with an Amazon S3 bucket as the destinatio
- G. Query the S3 bucket by using Amazon Athena for the leaderboard.
- H. Add a read-only replica to the RDS DB instanc
- I. Add an RDS Proxy database proxy.

Answer: C

NEW QUESTION 156

- (Exam Topic 2)

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

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

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

Answer: ACF

NEW QUESTION 159

- (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 164

- (Exam Topic 2)

A car rental company has built a serverless REST API to provide data to its mobile app. The app consists of an Amazon API Gateway API with a Regional endpoint, AWS Lambda functions and an Amazon Aurora MySQL Serverless DB cluster The company recently opened the API to mobile apps of partners A

significant increase in the number of requests resulted causing sporadic database memory errors Analysis of the API traffic indicates that clients are making multiple HTTP GET requests for the same queries in a short period of time Traffic is concentrated during business hours, with spikes around holidays and other events

The company needs to improve its ability to support the additional usage while minimizing the increase in costs associated with the solution. Which strategy meets these requirements?

- A. Convert the API Gateway Regional endpoint to an edge-optimized endpoint Enable caching in the production stage.
- B. Implement an Amazon ElastiCache for Redis cache to store the results of the database calls Modify the Lambda functions to use the cache
- C. Modify the Aurora Serverless DB cluster configuration to increase the maximum amount of available memory
- D. Enable throttling in the API Gateway production stage Set the rate and burst values to limit the incoming calls

Answer: A

NEW QUESTION 169

- (Exam Topic 2)

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

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

What CI/CD configuration meets all of the requirements?

- A. Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for in-place deployment Monitor the newly deployed code, and, if there are any issues, push another code update
- B. Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for blue/green deployments Monitor the newly deployed code and if there are any issues, trigger a manual rollback using CodeDeploy
- C. Configure CodePipeline with a deploy stage using AWS CloudFormation to create a pipeline for test and production stacks Monitor the newly deployed code, and, if there are any issues, push another code update
- D. Configure the CodePipeline with a deploy stage using AWS OpsWorks and m-place deployments Monitor the newly deployed code and
- E. if there are any issues, push another code update

Answer: B

NEW QUESTION 173

- (Exam Topic 2)

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

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

What should the solutions architect do to meet these requirements?

- A. Reconfigure the deployment type to Multi-AZ for this Amazon FSx tile system
- B. Create a new Amazon FSx fie system with a deployment type o(Multi-A
- C. Use AWS DataSync to transfer data to the new Amazon FSx file syste
- D. Point users to the new location
- E. Create a second Amazon FSx file system with a deployment type of Single-AZ 2. Use AWS DataSync to keep the data n syn
- F. Switch users to the second Amazon FSx fie system in the event of failure
- G. Use the AWS Management Console to take a backup of the Amazon FSx He system Create a new Amazon FSx file system with a deployment type of Multi-AZ Restore the backupto the new Amazon FSx file syste
- H. Point users to the new location.

Answer: B

NEW QUESTION 177

- (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 179

- (Exam Topic 2)

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

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

- A. AWS Application Discovery Service
- B. AWS SMS
- C. AWS X-Ray

- D. AWS Cloud Adoption Readiness Tool (CART)
- E. Amazon Inspector
- F. AWS Migration Hub

Answer: ADF

NEW QUESTION 182

- (Exam Topic 2)

A company hosts its primary API on AWS by using an Amazon API Gateway API and AWS Lambda functions that contain the logic for the API methods. The company's internal applications use the API for core functionality and business logic. The company's customers use the API to access data from their accounts. Several customers also have access to a legacy API that is running on a single standalone Amazon EC2 instance. The company wants to increase the security for these APIs to better prevent denial of service (DoS) attacks, check for vulnerabilities, and guard against common exploits. What should a solutions architect do to meet these requirements?

- A. Use AWS WAF to protect both APIs. Configure Amazon Inspector to analyze the legacy API. Configure Amazon GuardDuty to monitor for malicious attempts to access the APIs.
- B. Use AWS WAF to protect the API Gateway API. Configure Amazon Inspector to analyze both APIs. Configure Amazon GuardDuty to block malicious attempts to access the APIs.
- C. Use AWS WAF to protect the API Gateway API. Configure Amazon Inspector to analyze the legacy API. Configure Amazon GuardDuty to monitor for malicious attempts to access the APIs.
- D. Use AWS WAF to protect the API Gateway API. Configure Amazon Inspector to protect the legacy API. Configure Amazon GuardDuty to block malicious attempts to access the APIs.

Answer: C

NEW QUESTION 184

- (Exam Topic 2)

A company is deploying a third-party firewall appliance solution from AWS Marketplace to monitor and protect traffic that leaves the company's AWS environments. The company wants to deploy this appliance into a shared services VPC and route all outbound internet-bound traffic through the appliances. A solutions architect needs to recommend a deployment method that prioritizes reliability and minimizes failover time between firewall appliances within a single AWS Region. The company has set up routing from the shared services VPC to other VPCs. Which steps should the solutions architect recommend to meet these requirements? (Select THREE)

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

Answer: AC

NEW QUESTION 187

- (Exam Topic 2)

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? (Select 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 192

- (Exam Topic 2)

A company runs its application in the eu-west-1 Region and has one account for each of its environments: development, testing, and production. All the environments are running 24 hours a day, 7 days a week, by using stateful Amazon EC2 instances and Amazon RDS for MySQL databases. The databases are between 500 GB and 800 GB in size. The development team and testing team work on business days during business hours, but the production environment operates 24 hours a day, 7 days a week. The company wants to reduce costs. All resources are tagged with an environment tag with either development, testing, or production as the key. What should a solutions architect do to reduce costs with the LEAST operational effort?

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs once every day. Configure the rule to invoke one AWS Lambda function that starts or stops instances based on the tag, day, and time.
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs every business day in the evening.
- C. Configure the rule to invoke an AWS Lambda function that stops instances based on the tag. Create a second EventBridge (CloudWatch Events) rule that runs every business day in the morning. Configure the second rule to invoke another Lambda function that starts instances based on the tag.
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs every business day in the evening. Configure the rule to invoke an AWS Lambda function that terminates instances based on the tag. Create a second EventBridge (CloudWatch Events) rule that runs every business day in the morning. Configure the second rule to invoke another Lambda function that restores the instances from their last backup based on the tag.

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

Answer: C

NEW QUESTION 197

- (Exam Topic 2)

A company is running an application in the AWS Cloud. The application uses AWS Lambda functions and Amazon Elastic Container Service (Amazon ECS) containers that run with AWS Fargate technology as its primary compute. The load on the application is irregular. The application experiences long periods of no usage, followed by sudden and significant increases and decreases in traffic. The application is write-heavy and stores data in an Amazon Aurora MySQL database. The database runs on an Amazon RDS memory optimized D8 instance that is not able to handle the load.

What is the MOST cost-effective way for the company to handle the sudden and significant changes in traffic?

- A. Add additional read replicas to the databases.
- B. Purchase Instance Savings Plans and RDS Reserved Instances.
- C. Migrate the database to an Aurora multi-master DB cluster.
- D. Purchase Instance Savings Plans.
- E. Migrate the database to an Aurora global database. Purchase Compute Savings Plans and RDS Reserved Instances.
- F. Migrate the database to Aurora Serverless v1. Purchase Compute Savings Plans.

Answer: D

NEW QUESTION 201

- (Exam Topic 2)

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

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

- A. Use Amazon Kinesis Data Firehose to send the data to Amazon Redshift.
- B. Use Amazon Kinesis Data Streams to send the data to Amazon DynamoDB.
- C. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to send the data to Amazon Aurora.
- D. Use Amazon Kinesis Data Firehose to send the data to Amazon Keyspaces (for Apache Cassandra).

Answer: B

NEW QUESTION 206

- (Exam Topic 2)

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

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

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

- A. Reconfigure Amazon EFS to enable maximum I/O.
- B. Update the 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 209

- (Exam Topic 2)

A company is using multiple AWS accounts. The company has a shared services account and several other accounts (for different projects).

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

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

Answer: BCE

NEW QUESTION 210

- (Exam Topic 2)

A company plans to deploy a new private Intranet service on Amazon EC2 instances inside a VPC. An AWS Site-to-Site VPN connects the VPC to the company's on-premises network. The new service must communicate with existing on-premises services. The on-premises services are accessible through the use of hostnames that reside in the company example DNS zone. This DNS zone is wholly hosted on premises and is available only on the company's private network. A solutions architect must ensure that the new service can resolve hostnames on the company.example domain to integrate with existing services. Which solution meets these requirements?

- A. Create an empty private zone in Amazon Route 53 for company.example
- B. Add an additional NS record to the company's on-premises company.example zone that points to the authoritative name servers for the new private zone in Route 53
- C. Turn on DNS hostnames for the VPC
- D. Configure a new outbound endpoint with Amazon Route 53 Resolver
- E. Create a Resolver rule to forward requests for company.example to the on-premises name servers.
- F. Turn on DNS hostnames for the VP
- G. Configure a new inbound resolver endpoint with Amazon Route 53 Resolver
- H. Configure the on-premises DNS server to forward requests for company.example to the new resolver.
- I. Use AWS Systems Manager to configure a run document that will install a hosts file that contains any required hostname
- J. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to run the document when an instance is entering the running state.

Answer: C

NEW QUESTION 212

- (Exam Topic 2)

A company is planning to migrate its on-premises data analysis application to AWS. The application is hosted across a fleet of servers and requires consistent system time.

The company has established an AWS Direct Connect connection from its on-premises data center to AWS. The company has a high-precision stratum-0 atomic clock network appliance that acts as an NTP source for all on-premises servers.

After the migration to AWS is complete, the clock on all Amazon EC2 instances that host the application must be synchronized with the on-premises atomic clock network appliance.

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

- A. Configure a DHCP options set with the on-premises NTP server address. Assign the options set to the VPC.
- B. Ensure that NTP traffic is allowed between AWS and the on-premises networks.
- C. Create a custom AMI to use the Amazon Time Sync Service at 169.254.169.123. Use this AMI for the application. Use AWS Config to audit the NTP configuration.
- D. Deploy a third-party time server from the AWS Marketplace.
- E. Configure the time server to synchronize with the on-premises atomic clock network appliance.
- F. Ensure that NTP traffic is allowed inbound in the network ACLs for the VPC that contains the third-party server.
- G. Create an IPsec VPN tunnel from the on-premises atomic clock network appliance to the VPC to encrypt the traffic over the Direct Connect connection.
- H. Configure the VPC route tables to direct NTP traffic over the tunnel.

Answer: B

NEW QUESTION 213

- (Exam Topic 2)

What should the solutions architect do to meet this requirement?

- A. / Use Amazon CloudWatch to monitor the Sample Count statistic for each service in the ECS cluster. Set an alarm for when the math expression `sampleNotification SERVICE_QUOTA(service)"100` is greater than 80. Notify the development team by using Amazon Simple Notification Service (Amazon SNS).
- B. Use Amazon CloudWatch to monitor service quotas that are published under the AWS-Usage metric namespace. Set an alarm for when the math expression `metric SERVICE_QUOTA(metric)"100` is greater than 80. Notify the development team by using Amazon Simple Notification Service (Amazon SNS).
- C. Create an AWS Lambda function to poll detailed metrics from the ECS cluster.
- D. When the number running Fargate tasks is greater than 80, invoke Amazon Simple Email Service (Amazon SES) to notify the development team.
- E. Create an AWS Config rule to evaluate whether the Fargate SERVICE_QUOTA is greater than 80. Use Amazon Simple Email Service (Amazon SES) to notify the development team when the AWS Config rule is not compliant.

Answer: B

NEW QUESTION 214

.....

Relate Links

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

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

Contact us

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

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