Amazon-Web-Services

Exam Questions SAP-C02

AWS Certified Solutions Architect - Professional

NEW QUESTION 1
- (Exam Topic 1)
A company wants to deploy an AWS WAF solution to manage AWS WAF rules across multiple AWS accounts. The accounts are managed under different OUs in AWS Organizations.
Administrators must be able to add or remove accounts or OUs from managed AWS WAF rule sets as needed. Administrators also must have the ability to automatically update and remediate noncompliant AWS WAF rules in all accounts
Which solution meets these requirements with the LEAST amount of operational overhead?

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

Answer: B

NEW QUESTION 2
- (Exam Topic 1)
A company has a website that enables users to upload videos. Company policy states the uploaded videos must be analyzed for restricted content. An uploaded video is placed in Amazon S3, and a message is pushed to an Amazon SOS queue with the video's location. A backend application pulls this location from Amazon SOS and analyzes the video.
The video analysis is compute-intensive and occurs sporadically during the day The website scales with demand. The video analysis application runs on a fixed number of instances. Peak demand occurs during the holidays, so the company must add instances to the application dunng this time. All instances used are currently on-demand Amazon EC2 T2 instances. The company wants to reduce the cost of the current solution.
Which of the following solutions is MOST cost-effective?

A. Keep the website on T2 instance
B. Determine the minimum number of website instances required during off-peak times and use Spot Instances to cover them while using Reserved Instances to cover peak deman
C. Use Amazon EC2 R4 and Amazon EC2 R5 Reserved Instances in an Auto Scaling group for the video analysis application
D. Keep the website on T2 instance
E. Determine the minimum number of website instances required during off-peak times and use Reserved Instances to cover them while using On-Demand Instances to cover peak deman
F. Use Spot Fleet for the video analysis application comprised of Amazon EC2 C4 and Amazon EC2 C5 Spot Instances.
G. Migrate the website to AWS Elastic Beanstalk and Amazon EC2 C4 instance
H. Determine the minimum number of website instances required during off-peak times and use On-Demand Instances to cover them while using Spot capacity to cover peak demand Use Spot Fleet for the video anarysis application comprised of C4 and Amazon EC2 C5 instances.
I. Migrate the website to AWS Elastic Beanstalk and Amazon EC2 R4 instance
J. Determine the minimum number of website instances required during off-peak times and use Reserved Instances to cover them while using On-Demand Instances to cover peak demand Use Spot Fleet for the video analysis application comprised of R4 and Amazon EC2 R5 instances

Answer: B

NEW QUESTION 3
- (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 ElasDcsearch 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 sourc
E. Send all traffic information through Amazon Kinesis Data Firehose to an Amazon Elastic search 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 4
- (Exam Topic 1)

A company needs to architect a hybrid DNS solution. This solution will use an Amazon Route 53 private hosted zone for the domain cloud.example.com for the resources stored within VPCs.
The company has the following DNS resolution requirements:
• On-premises systems should be able to resolve and connect to cloud.example.com.
• All VPCs should be able to resolve cloud.example.com.
There is already an AWS Direct Connect connection between the on-premises corporate network and AWS Transit Gateway. Which architecture should the company use to meet these requirements with the HIGHEST performance?

A. Associate the private hosted zone to all the VPC
B. Create a Route 53 inbound resolver in the shared services VP
C. Attach all VPCs to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the inbound resolver.
D. Associate the private hosted zone to all the VPC
E. Deploy an Amazon EC2 conditional forwarder in the shared services VP
F. Attach all VPCs to the transit gateway and create forwarding rules in theon-premises DNS server for cloud.example.com that point to the conditional forwarder.
G. Associate the private hosted zone to the shared services VP
H. Create a Route 53 outbound resolver in the shared services VP
I. Attach all VPCs to the transit gateway and create forwarding rules in theon-premises DNS server for cloud.example.com that point to the outbound resolver.
J. Associate the private hosted zone to the shared services VP
K. Create a Route 53 inbound resolver in the shared services VP
L. Attach the shared services VPC to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the inbound resolver.

Answer: D

Explanation:
https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-dns-management-of-hybrid-cloud-w

NEW QUESTION 5
- (Exam Topic 1)
A group of research institutions and hospitals are in a partnership to study 2 PBs of genomic data. The institute that owns the data stores it in an Amazon S3 bucket and updates it regularly. The institute would like to give all of the organizations in the partnership read access to the data. All members of the partnership are extremety cost-conscious, and the institute that owns the account with the S3 bucket is concerned about covering the costs tor requests and data transfers from Amazon S3.
Which solution allows for secure datasharing without causing the institute that owns the bucket to assume all the costs for S3 requests and data transfers'?

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

Answer: B

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

NEW QUESTION 6
- (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 lo 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 owne
B. Add each business unit to an Amazon SNS topic for each aler
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 owne
E. Add each business unit to an Amazon SNS topic for each aler
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 lhat are grouped by application, environment, and owne
H. Add each business unit to an Amazon SNS topic for each aler
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 owne
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 7
- (Exam Topic 1)
A solutions architect must analyze a company's Amazon EC2 Instances and Amazon Elastic Block Store (Amazon EBS) volumes to determine whether the company is using resources efficiently The company is
running several large, high-memory EC2 instances lo host database dusters that are deployed in active/passive configurations The utilization of these EC2 instances varies by the applications that use the databases, and the company has not identified a pattern
The solutions architect must analyze the environment and take action based on the findings. Which solution meets these requirements MOST cost-effectively?

A. Create a dashboard by using AWS Systems Manager OpsConter Configure visualizations tor Amazon CloudWatch metrics that are associated with the EC2 instances and their EBS volumes Review the dashboard periodically and identify usage patterns Rightsize the EC2 instances based on the peaks in the metrics
B. Turn on Amazon CloudWatch detailed monitoring for the EC2 instances and their EBS volumes Create and review a dashboard that is based on the metrics Identify usage patterns Rightsize the FC? instances based on the peaks In the metrics
C. Install the Amazon CloudWatch agent on each of the EC2 Instances Turn on AWS Compute Optimizer, and let it run for at least 12 hours Review the recommendations from Compute Optimizer, and rightsize the EC2 instances as directed
D. Sign up for the AWS Enterprise Support plan Turn on AWS Trusted Advisor Wait 12 hours Review the recommendations from Trusted Advisor, and rightsize the EC2 instances as directed

Answer: C

Explanation:
(https://aws.amazon.com/compute-optimizer/pricing/ , https://aws.amazon.com/systems-manager/pricing/). https://aws.amazon.com/compute-optimizer/

NEW QUESTION 8
- (Exam Topic 1)
A company is deploying a new cluster for big data analytics on AWS. The cluster will run across many Linux Amazon EC2 instances that are spread across multiple Availability Zones.
All of the nodes in the cluster must have read and write access to common underlying file storage. The file storage must be highly available, must be resilient, must be compatible with the Portable Operating System Interface (POSIX), and must accommodate high levels of throughput.
Which storage solution will meet these requirements?

A. Provision an AWS Storage Gateway file gateway NFS file share that is attached to an Amazon S3 bucke
B. Mount the NFS file share on each EC2 instance In the cluster.
C. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses General Purpose performance mod
D. Mount the EFS file system on each EC2 instance in the cluster.
E. Provision a new Amazon Elastic Block Store (Amazon EBS) volume that uses the lo2 volume type.Attach the EBS volume to all of the EC2 instances in the cluster.
F. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses Max I/O performance mod
G. Mount the EFS file system on each EC2 instance in the cluster.

Answer: D

NEW QUESTION 9
- (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 tog 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 tog files.
What should the solutions architect do to meet these requirements?

A. Create a cross-account role in the central accoun
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 principa
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 accoun
F. Use the production account ID as the principal.
G. Create a cross-account role in the production accoun
H. Assume the role from the production account when the logs are being copied.

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
A company has a new application that needs to run on five Amazon EC2 instances in a single AWS Region. The application requires high-throughput, low-latency network connections between all of the EC2 instances where the application will run. There is no requirement for the application to be fault tolerant.
Which solution will meet these requirements?

A. Launch five new EC2 instances into a cluster placement grou
B. Ensure that the EC2 instance type supports enhanced networking.
C. Launch five new EC2 instances into an Auto Scaling group in the same Availability Zon
D. Attach an extra elastic network interface to each EC2 instance.
E. Launch five new EC2 instances into a partition placement grou
F. Ensure that the EC2 instance type supports enhanced networking.
G. Launch five new EC2 instances into a spread placement grou

H. Attach an extra elastic network interface to each EC2 instance.

Answer: A

Explanation:
When you launch EC2 instances in a cluster they benefit from performance and low latency. No redundancy though as per the question
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html.

NEW QUESTION 10
- (Exam Topic 1)
An e-commerce company is revamping its IT infrastructure and is planning to use AWS services. The company's CIO has asked a solutions architect to design a simple, highly available, and loosely coupled order processing application. The application is responsible (or receiving and processing orders before storing them in an Amazon DynamoDB table. The application has a sporadic traffic pattern and should be able to scale during markeling campaigns to process the orders with minimal delays.
Which of the following is the MOST reliable approach to meet the requirements?

A. Receive the orders in an Amazon EC2-hosted database and use EC2 instances to process them.
B. Receive the orders in an Amazon SOS queue and trigger an AWS Lambda function lo process them.
C. Receive the orders using the AWS Step Functions program and trigger an Amazon ECS container lo process them.
D. Receive the orders in Amazon Kinesis Data Streams and use Amazon EC2 instances to process them.

Answer: B

Explanation:
Q: How does Amazon Kinesis Data Streams differ from Amazon SQS?
Amazon Kinesis Data Streams enables real-time processing of streaming big data. It provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications. The Amazon Kinesis Client Library (KCL) delivers all records for a given partition key to the same record processor, making it easier to build multiple applications reading from the same Amazon Kinesis data stream (for example, to perform counting, aggregation, and filtering).
https://aws.amazon.com/kinesis/data-streams/faqs/
https://aws.amazon.com/blogs/big-data/unite-real-time-and-batch-analytics-using-the-big-data-lambda-architect

NEW QUESTION 12
- (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 Servertess 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 Servertess 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 Servertess 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 16
- (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 VP
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 VP
F. and ensure that network access control and security group rules allow the relevant inbound and outbound traffic.

Answer: A

NEW QUESTION 18
- (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 Bloc
C. Connect theweb ACL to the ALB.
D. Use AWS Firewall Manager to create a security group and security group policy to allow access only to specific CIOR ranges.
E. Create an AWS WAF web ACL with an IP set match rule, and set the rule action to Bloc
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 22
- (Exam Topic 1)
A media company uses Amazon DynamoDB to store metadata for its catalog of movies that are available to stream. Each media item Contains user-facing content that concludes a description of the media, a list of search tags, and similar data. In addition, media items include a list of Amazon S3 key names that relate to movie files. The company stores these movie files in a single S3 bucket that has versioning enable. The company uses Amazon CloudFront to serve these movie files.
The company has 100.000 media items, and each media item can have many different S3 objects that represent different encodings of the same media S3 objects that belong to the same media item are grouped together under the same key prefix, which is a random unique ID
Because of an expiring contract with a media provider, the company must remove 2.000 media Items. The company must completely delete all DynamoDB keys and movie files on Amazon S3 that are related to these media items within 36 hours The company must ensure that the content cannot be recovered.
Which combination of actions will meet these requirements? (Select TWO.)

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

Answer: CE

NEW QUESTION 26
- (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 lo 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 connectio
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 connectio
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 connectio
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 28
- (Exam Topic 1)
A large company in Europe plans to migrate its applications to the AWS Cloud. The company uses multiple AWS accounts for various business groups. A data privacy law requires the company to restrict developers'
access to AWS European Regions only.
What should the solutions architect do to meet this requirement with the LEAST amount of management overhead^

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

Answer: B

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

NEW QUESTION 30
- (Exam Topic 1)
A large company is running a popular web application. The application runs on several Amazon EC2 Linux Instances in an Auto Scaling group in a private subnet. An Application Load Balancer is targeting the Instances In the Auto Scaling group in the private subnet. AWS Systems Manager Session Manager Is configured, and AWS Systems Manager Agent is running on all the EC2 instances.
The company recently released a new version of the application Some EC2 instances are now being marked as unhealthy and are being terminated As a result, the application is running at reduced capacity A solutions architect tries to determine the root cause by analyzing Amazon CloudWatch logs that are collected from the application, but the logs are inconclusive
How should the solutions architect gain access to an EC2 instance to troubleshoot the issue1?

A. Suspend the Auto Scaling group's HealthCheck scaling proces
B. Use Session Manager to log in to an instance that is marked as unhealthy
C. Enable EC2 instance termination protection Use Session Manager to log In to an instance that is marked as unhealthy.
D. Set the termination policy to Oldestinstance on the Auto Scaling grou
E. Use Session Manager to log in to an instance that is marked as unhealthy
F. Suspend the Auto Scaling group's Terminate proces
G. Use Session Manager to log in to an instance that is marked as unhealthy

Answer: D

Explanation:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-suspend-resume-processes.html
it shows For Amazon EC2 Auto Scaling, there are two primary process types: Launch and Terminate. The Launch process adds a new Amazon EC2 instance to an Auto Scaling group, increasing its capacity. The Terminate process removes an Amazon EC2 instance from the group, decreasing its capacity. HealthCheck process for EC2 autoscaling is not a primary process! It is a process along with the following AddToLoadBalancer AlarmNotification AZRebalance HealthCheck InstanceRefresh ReplaceUnhealthy ScheduledActions From the requirements, Some EC2 instances are now being marked as unhealthy and are being terminated. Application is running at reduced capacity not because instances are marked unhealthy but because they are being terminated.
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-suspend-resume-processes.html#choosing-suspend-r

NEW QUESTION 35
- (Exam Topic 1)
A company is running an application distributed over several Amazon EC2 instances in an Auto Seating 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 log
B. Send all logs through Amazon Kinesis Data Firehose to an Amazon Elasticsearch Service (Amazon ES) cluster that the security team uses for analysis.
C. 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.
D. 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
E. Enable Traffic Mirroring and specify all EC2 instance network interfaces as the sourc
F. 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 https://docs.aws.amazon.com/vpc/latest/mirroring/what-is-traffic-mirroring.html

NEW QUESTION 37
- (Exam Topic 1)
A company maintains a restaurant review website. The website is a single-page application where files are stored in Amazon S3 and delivered using Amazon CloudFront. The company receives several fake postings every day that are manually removed.
The security team has identified that most of the fake posts are from bots with IP addresses that have a bad reputation within the same global region. The team needs to create a solution to help restrict the bots from accessing the website.
Which strategy should a solutions architect use?

A. Use AWS Firewall Manager to control the CloudFront distribution security setting
B. Create a geographical block rule and associate it with Firewall Manager.
C. Associate an AWS WAF web ACL with the CloudFront distributio

D. Select the managed Amazon IP reputation rule group for the web ACL with a deny action.
E. Use AWS Firewall Manager to control the CloudFront distribution security setting
F. Select the managed Amazon IP reputation rule group and associate it with Firewall Manager with a deny action.
G. Associate an AWS WAF web ACL with the CloudFront distributio
H. Create a rule group for the web ACL with a geographical match statement with a deny action.

Answer: B

Explanation:
IP reputation rule groups allow you to block requests based on their source. Choose one or more of these rule groups if you want to reduce your exposure to BOTS!!!! traffic or exploitation attempts
The Amazon IP reputation list rule group contains rules that are based on Amazon internal threat intelligence. This is useful if you would like to block IP addresses typically associated with bots or other threats. Inspects for a list of IP addresses that have been identified as bots by Amazon threat intelligence.

NEW QUESTION 41
- (Exam Topic 1)
A financial company is building a system to generate monthly, immutable bank account statements for its users. Statements are stored in Amazon S3. Users should have immediate access to their monthly statements for up to 2 years. Some users access their statements frequently, whereas others rarely access their statements. The company's security and compliance policy requires that the statements be retained for at least 7 years.
What is the MOST cost-effective solution to meet the company's needs?

A. Create an S3 bucket with Object Lock disable
B. Store statements in S3 Standar
C. Define an S3 Lifecycle policy to transition the data to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 day
D. Define another S3 Lifecycle policy to move the data to S3 Glacier Deep Archive after 2 year
E. Attach an S3 Glacier Vault Lock policy with deny delete permissions for archives less than 7 years old.
F. Create an S3 bucket with versioning enable
G. Store statements in S3 Intelligent-Tierin
H. Usesame-Region replication to replicate objects to a backup S3 bucke
I. Define an S3 Lifecycle policy for the backup S3 bucket to move the data to S3 Glacie
J. Attach an S3 Glacier Vault Lock policy with deny delete permissions for archives less than 7 years old.
K. Create an S3 bucket with Object Lock enable
L. Store statements in S3 Intelligent-Tierin
M. Enable compliance mode with a default retention period of 2 year
N. Define an S3 Lifecycle policy to move the data to S3 Glacier after 2 year
O. Attach an S3 Glacier Vault Lock policy with deny delete permissionsfor archives less than 7 years old.
P. Create an S3 bucket with versioning disable
Q. Store statements in S3 One Zone-Infrequent Access (S3 One Zone-IA). Define an S3 Lifecyde policy to move the data to S3 Glacier Deep Archive after 2 year
R. Attach an S3 Glader Vault Lock policy with deny delete permissions for archives less than 7 years old.

Answer: C

Explanation:
https://aws.amazon.com/about-aws/whats-new/2018/11/s3-object-lock/
Create an S3 bucket with Object Lock enabled. Store statements in S3 Intelligent-Tiering. Enable compliance mode with a default retention period of 2 years. Define an S3 Lifecycle policy to move the data to S3 Glacier after 2 years. Attach an S3 Glacier Vault Lock policy with deny delete permissions for archives less than 7 years old.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html

NEW QUESTION 43
- (Exam Topic 1)
A company wants to migrate an application to Amazon EC2 from VMware Infrastructure that runs in an on-premises data center. A solutions architect must preserve the software and configuration settings during the migration.
What should the solutions architect do to meet these requirements?

A. Configure the AWS DataSync agent to start replicating the data store to Amazon FSx for Windows File Server Use the SMB share to host the VMware data 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 48
- (Exam Topic 1)
An AWS customer has a web application that runs on premises. The web application fetches data from a third-party API that is behind a firewall. The third party

accepts only one public CIDR block in each client's allow list.
The customer wants to migrate their web application to the AWS Cloud. The application will be hosted on a set of Amazon EC2 instances behind an Application Load Balancer (ALB) in a VPC. The ALB is located in public subnets. The EC2 instances are located in private subnets. NAT gateways provide internet access to the private subnets.
How should a solutions architect ensure that the web application can continue to call the third-parly API after the migration?

A. Associate a block of customer-owned public IP addresses to the VP
B. Enable public IP addressing for public subnets in the VPC.
C. Register a block of customer-owned public IP addresses in the AWS accoun
D. Create Elastic IP addresses from the address block and assign them lo the NAT gateways in the VPC.
E. Create Elastic IP addresses from the block of customer-owned IP addresse
F. Assign the static Elastic IP addresses to the ALB.
G. Register a block of customer-owned public IP addresses in the AWS accoun
H. Set up AWS Global Accelerator to use Elastic IP addresses from the address bloc
I. Set the ALB as the accelerator endpoint.

Answer: B

Explanation:
When EC2 instances reach third-party API through internet, their privates IP addresses will be masked by NAT Gateway public IP address.
https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-bring-your-own-ip-byoip-for-amaz

NEW QUESTION 50
- (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 Regio
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 theus-east-1 Regio
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 inthe us-east-1 Regio
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 Regio
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 Regio
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 Regio
N. Create separate Amazon Route 53 records in each Region that point to the ALB in the Regio
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 53
- (Exam Topic 1)
A company has a data lake in Amazon S3 that needs to be accessed by hundreds of applications across many AWS accounts. The company's information security policy states that the S3 bucket must not be accessed over the public internet and that each application should have the minimum permissions necessary to function.
To meet these requirements, a solutions architect plans to use an S3 access point that is restricted to specific VPCs tor each application.
Which combination of steps should the solutions architect take to implement this solution? (Select TWO.)

A. Create an S3 access point for each application in the AWS account that owns the S3 bucke
B. Configure each access point to be accessible only from the application's VP
C. Update the bucket policy to require access from an access point.
D. Create an interface endpoint for Amazon S3 in each application's VP
E. Configure the endpoint policy to allow access to an S3 access poin
F. Create a VPC gateway attachment for the S3 endpoint.
G. Create a gateway endpoint lor Amazon S3 in each application's VP
H. Configure the endpoint policy to allow access to an S3 access poin
I. Specify the route table that is used to access the access point.
J. Create an S3 access point for each application in each AWS account and attach the access points to the S3 bucke
K. Configure each access point to be accessible only from the application's VP
L. Update the bucket policy to require access from an access point.
M. Create a gateway endpoint for Amazon S3 in the data lake's VP
N. Attach an endpoint policy to allow access to the S3 bucke
O. Specify the route table that is used to access the bucket.

Answer: AC

Explanation:
https://joe.blog.freemansoft.com/2020/04/protect-data-in-cloud-with-s3-access.html https://aws.amazon.com/s3/features/access-points/
https://aws.amazon.com/s3/features/access-points/

&
https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/

NEW QUESTION 58
- (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 Mops internet connection
Which migration strategy meets these requirements?

A. Create an AWS Database Migration Service (AWS DMS) replication instanc
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 bucke
E. Copy the data into the Amazon Redshift cluste
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/prof/computing/transfer_time

NEW QUESTION 63
- (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 66
- (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 applicatio
B. Update the Route 53 record to use a weighted routing policy.
C. Create a Lambda@Edge functio
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 CloudFrontorigin group that contains both origins Configure origin weighting for the origin group.
F. Create two Lambda@Edge function
G. Use each function to serve one of the application versions Set up a CloudFront weighted Lambda@Edge invocation policy

Answer: A

NEW QUESTION 68
- (Exam Topic 2)
A company is in the process of implementing AWS Organizations to constrain its developers to use only Amazon EC2. Amazon S3 and Amazon DynamoDB. The developers account resides In a dedicated organizational unit (OU). The solutions architect has implemented the following SCP on the developers account:

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

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

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

Answer: B

NEW QUESTION 70
- (Exam Topic 2)
A company is migrating its marketing website and content management system from an on-premises data center to AWS. The company wants the AWS application to be deployed in a VPC with Amazon EC2 instances used for the web servers and an Amazon RDS instance for the database.
The company has a runbook document that describes the installation process of the on-premises system. The company would like to base the AWS system on the processes referenced in the runbook document. The runbook document describes the installation and configuration of the operating systems, network settings, the website, and content management system software on the servers After the migration is complete, the company wants to be able to make changes quickly to take advantage of other AWS features.
How can the application and environment be deployed and automated m AWS. while allowing for future changes?

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

Answer: D

NEW QUESTION 71
- (Exam Topic 2)
A company that develops consumer electronics with offices in Europe and Asia has 60 TB of software images stored on premises in Europe. The company wants to transfer the images to an Amazon S3 bucket in the ap-northeast-1 Region. New software images are created daily and must be encrypted in transit. The company needs a solution that does not require custom development to automatically transfer all existing and new software images to Amazon S3.
What is the next step in the transfer process?

A. Deploy an AWS DataSync agent and configure a task to transfer the images to the S3 bucket.
B. Configure Amazon Kinesis Data Firehose to transfer the images using S3 Transfer Acceleration.
C. Use an AWS Snowball device to transfer the images with the S3 bucket as the target.
D. Transfer the images over a Site-to-Site VPN connection using the S3 API with multipart upload.

Answer: A

NEW QUESTION 76
- (Exam Topic 2)
A company has developed a new billing application that will be released in two weeks. Developers are testing the application running on 10 EC2 instances managed by an Auto Scaling group in subnet 172.31.0.0/24 within VPC A with CIDR block 172.31.0.0/16. The developers noticed connection timeout errors in the application logs while connecting to an Oracle database running on an Amazon EC2 instance in the same region within VPC B with CIDR block 172.50.0.0/16. The IP of the database instance is hard-coded in the application instances.
Which recommendations should a solutions architect present to the developers to solve the problem in a secure way with minimal maintenance and overhead"

A. Disable the SrcDestCheck attribute for all instances running the application and Oracle Database.Change the default route of VPC A to point ENI of the Oracle Database that has an IP address assigned within the range of 172.50.0.0/16
B. Create and attach internet gateways for both VPC
C. Configure default routes to the internet gateways for both VPC
D. Assign an Elastic IP for each Amazon EC2 instance in VPC A
E. Create a VPC peering connection between the two VPCs and add a route to the routing table of VPC A that points to the IP address range of 172.50.0.0/16
F. Create an additional Amazon EC2 instance for each VPC as a customer gateway; create one virtual private gateway (VGW) for each VP
G. configure an end-to-end VPC, and advertise the routes for 172.50.0.0/16

Answer: C

NEW QUESTION 77
- (Exam Topic 2)
A company that runs applications on AWS recently subscribed to a new software-as-a-service (SaaS) data vendor. The vendor provides the data by way of a REST API that the vendor hosts in its AWS environment The vendor offers multiple options for connectivity to the API and Is working with the company to find the best way to connect.
The company's AWS account does not allow outbound internet access from Its AWS environment The vendor's services run on AWS in the same AWS Region as the company's applications
A solutions architect must Implement connectivity to the vendor's API so that the API is highly available In the company's VPC.
Which solution will meet these requirements?

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

Answer: C

NEW QUESTION 81
- (Exam Topic 2)
A company is using an Amazon CloudFront distribution to distribute both static and dynamic content from a web application running behind an Application Load Balancer The web application requires user authorization and session tracking tor dynamic content The CloudFront distribution has a single cache behavior configured to forward the Authorization, Host, and Agent HTTP allow list headers and a session cookie to the origin All other cache behavior settings are set to their default value
A valid ACM certificate is applied to the CloudFront distribution with a matching CNAME in the distribution settings The ACM certificate is also applied to the HTTPS listener for the Application Load Balancer The CloudFront origin protocol policy is set to HTTPS only Analysis of the cache statistics report shows that the miss rate for this distribution is very high
What can the solutions architect do to improve the cache hit rate for this distribution without causing the SSL/TLS handshake between CloudFront and the Application Load Balancer to fail?

A. Create two cache behaviors for static and dynamic content Remove the user-Agent and Host HTTP headers from the allow list headers section on both of the cache behaviors Remove the session cookie from the allow list cookies section and the Authorization HTTP header from the allow list headers section for cache behavior configured for static content
B. Remove the user-Agent and Authorization HTTP headers from the allow list headers section of the cache behaviou
C. Then update the cache behaviour to use resigned cookies for authorization
D. Remove the Host HTTP header from the allow list headers section and remove the session cookie from the allow list cookies section for the default cache behaviour Enable automatic object compression and use Lambda@Edge viewer request events for user authorization
E. Create two cache behaviours for static and dynamic content Remove the User-Agent HTTP header from the allow list headers section on both of the cache behavioursRemove the session cookie from the allow list cookies section and the Authorization HTTP header from the allow list headers section for cache behaviour configured for static content

Answer: D

Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/understanding-the-cache-key.html Removing the host header will result in failed flow between CloudFront and ALB, because they have same certificate.

NEW QUESTION 86
- (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 90
- (Exam Topic 2)
A company is running a three-tier web application in an on-premises data center. The frontend is served by an Apache web server, the middle tier is a monolithic Java application, and the storage tier is a PostgreSOL database.
During a recent marketing promotion, customers could not place orders through the application because the application crashed An analysis showed that all three tiers were overloaded. The application became unresponsive, and the database reached its capacity limit because of read operations. The company already has

several similar promotions scheduled in the near future.
A solutions architect must develop a plan for migration to AWS to resolve these issues. The solution must maximize scalability and must minimize operational effort.
Which combination of steps will meet these requirements? (Select THREE.)

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

Answer: BCF

NEW QUESTION 91
- (Exam Topic 2)
A company has a new security policy. The policy requires the company to log any event that retrieves data from Amazon S3 buckets. The company must save these audit logs in a dedicated S3 bucket. The company created the audit logs S3 bucket in an AWS account that is designated for centralized logging. The S3 bucket has a bucket policy that allows write-only cross-account access A solutions architect must ensure that all S3 object-level access is being logged for current S3 buckets and future S3 buckets. Which solution will meet these requirements?

A. Enable server access logging for all current S3 bucket
B. Use the audit logs S3 bucket as a destination foraudit logs
C. Enable replication between all current S3 buckets and the audit logs S3 bucket Enable S3 Versioning in the audit logs S3 bucket
D. Configure S3 Event Notifications for all current S3 buckets to invoke an AWS Lambda function every time objects are accessed . Store Lambda logs in the audit logs S3 bucket.
E. Enable AWS CloudTrai
F. and use the audit logs S3 bucket to store logs Enable data event logging for S3 event sources, current S3 buckets, and future S3 buckets.

Answer: D

NEW QUESTION 95
- (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 tie system on premises, and the application servers connect to the shared We system through SMB.
A solutions architect must implement a solution that uses an Amazon S3 bucket tor 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 Server fie system Configure AWS DataSync with one location tor 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 applicatio
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 environmen
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 applicatio
G. Deploy a new AWS Storage Gateway Me gateway on anon-premises V
H. Create a new file share that stores data in the S3 bucket and is associated with the tie gatewa
I. Copy the data from the on-premises storage to the new file gateway endpoint.

Answer: A

NEW QUESTION 96
- (Exam Topic 2)
A company is using a lift-and-shift strategy to migrate applications from several on-premises Windows servers to AWS. The Windows servers will be hosted on Amazon EC2 instances in the us-east-1 Region.
The company's security policy allows the installation of migration tools on servers. The migration data must be encrypted in transit and encrypted at rest. The applications are business critical. The company needs to minimize the cutover window and minimize the downtime that results from the migration. The company wants to use Amazon CloudWatch and AWS CloudTrail for monitoring.
Which solution will meet these requirements?

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

L. Use AWS Migration Hub to migrate the Windows servers to AW
M. Create a project in Migration Hub.Track the progress of server migration by using the built-in dashboard.

Answer: A

NEW QUESTION 98
- (Exam Topic 2)
A company is migrating its infrastructure to the AW5 Cloud. The company must comply with a variety of regulatory standards for different projects. The company needs a multi-account environment.
A solutions architect needs to prepare the baseline infrastructure The solution must provide a consistent baseline of management and security but it must allow flexibility for different compliance requirements within various AWS accounts. The solution also needs to integrate with the existing on-premises Active Directory Federation Services (AD FS) server.
Which solution meets these requirements with the LEAST amount of operational overhead?

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

Answer: A

NEW QUESTION 99
- (Exam Topic 2)
A company has multiple business units Each business unit has its own AWS account and runs a single website within that account. The company also has a single logging account. Logs from each business unit website are aggregated into a single Amazon S3 bucket in the logging account. The S3 bucket policy provides each business unit with access to write data into the bucket and requires data to be encrypted.
The company needs to encrypt logs uploaded into the bucket using a Single AWS Key Management Service
{AWS KMS) CMK The CMK that protects the data must be rotated once every 365 days
Which strategy is the MOST operationally efficient for the company to use to meet these requirements?

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

Answer: A

NEW QUESTION 100
- (Exam Topic 2)
A company is processing videos in the AWS Cloud by using Amazon EC2 instances in an Auto Scaling group. It takes 30 minutes to process a video. Several EC2 instances scale in and out depending on the number of videos in an Amazon Simple Queue Service (Amazon SQS) queue.
The company has configured the SQS queue with a redrive policy that specifies a target dead-letter queue and a maxReceiveCount of 1. The company has set the visibility timeout for the SQS queue to 1 hour. The company has set up an Amazon CloudWatch alarm to notify the development team when there are messages in the dead-letter queue.
Several times during the day, the development team receives notification that messages are in the dead-letter queue and that videos have not been processed properly. An investigation finds no errors in the application logs.
How can the company solve this problem?

A. Turn on termination protection for the EC2 instances.
B. Update the visibility timeout for the SOS queue to 3 hours.
C. Configure scale-in protection for the instances during processing.
D. Update the redrive policy and set maxReceiveCount to 0.

Answer: A

NEW QUESTION 102
- (Exam Topic 2)
A large company recently experienced an unexpected increase in Amazon RDS and Amazon DynamoDB costs The company needs to increase visibility into details of AWS Billing and Cost Management There are various accounts associated with AWS Organizations, including many development and production accounts. There is no consistent tagging strategy across the organization, but there are guidelines in place that require all infrastructure to be deployed using AWS Cloud Formation with consistent tagging Management requires cost center numbers and project ID numbers for all existing and future DynamoDB tables and RDS instances
Which strategy should the solutions architect provide to meet these requirements?

A. Use Tag Editor to tag existing resources Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing

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

Answer: B

NEW QUESTION 104
- (Exam Topic 2)
A company operates quick-service restaurants. The restaurants follow a predictable model with high sales traffic for -4 hours daily Sates traffic is lower outside of those peak hours.
The point of sale and management platform is deployed in the AWS Cloud and has a backend that is based or Amazon DynamoDB The database table uses provisioned throughput mode with 100.000 RCUs and 80.000 WCUs to match Known peak resource consumption.
The company wants to reduce its DynamoDB cost and minimize the operational overhead for the IT staff. Which solution meets these requirements MOST cost-effectively?

A. Reduce the provisioned RCUs and WCUs
B. Change the DynamoDB table to use on-demand capacity
C. Enable Dynamo DB auto seating for the table.
D. Purchase 1-year reserved capacity that is sufficient to cover the peak load for 4 hours each day.

Answer: C

NEW QUESTION 107
- (Exam Topic 2)
A company is planning to migrate an Amazon RDS for Oracle database to an RDS for PostgreSQL DB instance in another AWS account A solutions architect needs to design a migration strategy that will require no downtime and that will minimize the amount of time necessary to complete the migration The migration strategy must replicate all existing data and any new data that is created during the migration The target database must be identical to the source database at completion of the migration process
All applications currently use an Amazon Route 53 CNAME record as their endpoint for communication with the RDS for Oracle DB instance The RDS for Oracle DB instance is in a private subnet
Which combination of steps should the solutions architect take to meet these requirements? (Select THREE)

A. Create a new RDS for PostgreSQL DB instance in the target account Use the AWS Schema Conversion Tool (AWS SCT) to migrate the database schema from the source database to the target database.
B. Use the AWS Schema Conversion Tool (AWS SCT) to create a new RDS for PostgreSQL DB instance in the target account with the schema and initial data from the source database
C. Configure VPC peering between the VPCs in the two AWS accounts to provide connectivity to both DB instances from the target accoun
D. Configure the security groups that are attached to each DB instance to allow traffic on the database port from the VPC in the target account
E. Temporarily allow the source DB instance to be publicly accessible to provide connectivity from the VPC in the target account Configure the security groups that are attached to each DB instance to allow traffic on the database port from the VPC in the target account.
F. Use AWS Database Migration Service (AWS DMS) in the target account to perform a full load plus change data capture (CDC) migration from the source database to the target database When the migration is complete, change the CNAME record to point to the target DB instance endpoint
G. Use AWS Database Migration Service (AWS DMS) in the target account to perform a change data capture (CDC) migration from the source database to the target database When the migration is complete change the CNAME record to point to the target DB instance endpoint

Answer: BCE

NEW QUESTION 109
- (Exam Topic 2)
A digital marketing company has multiple AWS accounts that belong to various teams. The creative team uses an Amazon S3 bucket in its AWS account to securely store images and media files that are used as content for the company's marketing campaigns. The creative team wants to share the S3 bucket with the strategy team so that the strategy team can view the objects.
A solutions architect has created an IAM role that is named strategy_reviewer in the Strategy account. The solutions architect also has set up a custom AWS Key Management Service (AWS KMS) key in the Creative account and has associated the key with the S3 bucket. However, when users from the Strategy account assume the IAM role and try to access objects in the S3 bucket, they receive an Account.
The solutions architect must ensure that users in the Strategy account can access the S3 bucket. The solution must provide these users with only the minimum permissions that they need.
Which combination of steps should the solutions architect take to meet these requirements? (Select THREE.)

A. Create a bucket policy that includes read permissions for the S3 bucke
B. Set the principal of the bucket policy to the account ID of the Strategy account
C. Update the strategy_reviewer IAM role to grant full permissions for the S3 bucket and to grant decrypt permissions for the custom KMS key.
D. Update the custom KMS key policy in the Creative account to grant decrypt permissions to the strategy_reviewer IAM role.
E. Create a bucket policy that includes read permissions for the S3 bucke
F. Set the principal of the bucket policy to an anonymous user.
G. Update the custom KMS key policy in the Creative account to grant encrypt permissions to the strategy_reviewer IAM role.
H. Update the strategy_reviewer IAM role to grant read permissions for the S3 bucket and to grant decrypt permissions for the custom KMS key

Answer: ACE

NEW QUESTION 112
- (Exam Topic 2)
A company is running a critical application that uses an Amazon RDS for MySQL database to store data. The RDS DB instance is deployed in Multi-AZ mode.
A recent RDS database failover test caused a 40-second outage to the application A solutions architect needs to design a solution to reduce the outage time to less than 20 seconds.

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

A. Use Amazon ElastiCache for Memcached in front of the database
B. Use Amazon ElastiCache for Redis in front of the database.
C. Use RDS Proxy in front of the database
D. Migrate the database to Amazon Aurora MySQL
E. Create an Amazon Aurora Replica
F. Create an RDS for MySQL read replica

Answer: ABF

NEW QUESTION 115
- (Exam Topic 2)
A company recently deployed a new application that runs on a group of Amazon EC2 Linux instances in a VPC In a peered VPC the company launched an EC2 Linux instance that serves as a bastion host The security group of the application instances allows access only on TCP port 22 from the private IP of the bastion host The security group of the bastion host allows access to TCP port 22 from 0 0 0.0/0 so that system administrators can use SSH to remotely log in to the application instances from several branch offices
While looking through operating system logs on the bastion host, a cloud engineer notices thousands of failed SSH logins to the bastion host from locations around the world The cloud engineer wants to change how remote access is granted to the application instances and wants to meet the following requirements:
• Eliminate brute-force SSH login attempts
• Retain a log of commands run during an SSH session
• Retain the ability to forward ports
Which solution meets these requirements for remote access to the application instances?

A. Configure the application instances to communicate with AWS Systems Manager Grant access to the system administrators to use Session Manager to establish a session with the application instances Terminate the bastion host
B. Update the security group of the bastion host to allow traffic from only the public IP addresses of the branch offices
C. Configure an AWS Client VPN endpoint and provision each system administrator with a certificate to establish a VPN connection to the application VPC Update the security group of the application instances to allow traffic from only the Client VPN IPv4 CID
D. Terminate the bastion host.
E. Configure the application instances to communicate with AWS Systems Manage
F. Grant access to the system administrators to issue commands to the application instances by using Systems Manager Run Comman
G. Terminate the bastion host.

Answer: A

Explanation:
"Session Manager removes the need to open inbound ports, manage SSH keys, or use bastion hosts" Ref: https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html

NEW QUESTION 116
- (Exam Topic 2)
A company runs a software-as-a-service (SaaS) application on AWS. The application comets of AWS Lambda function and an Amazon RDS for MySQL Multi-AZ database During market events the application has a much higher workload than normal Users notice slow response times during the peak periods because of many database connections. The company needs to improve the scalable performance and availability of the database.
Which solution meets these requirements?

A. Create an Amazon CloudWatch alarm action that triggers a Lambda function to add an Amazon RDS for MySQL read replica when resource utilization hits a threshold.
B. Migrate the database to Amazon Aurora and add a read replica Add a database connection pool outside of the Lambda hardier function.
C. Migrate the database to Amazon Aurora and add a read replic
D. Use Amazon Route 53 weighted records
E. Migrate the database to Amazon Aurora and add an Aurora Replic
F. Configure Amazon RDS Proxy to manage database connection pools.

Answer: D

NEW QUESTION 118
- (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 121
- (Exam Topic 2)
A company has an organization that has many AWS accounts in AWS Organizations A solutions architect must improve how the company manages common security group rules for the AWS accounts in the organization.
The company has a common set of IP CIDR ranges in an allow list in each AWS account lo allow access to and from the company's on-premises network Developers within each account are responsible for adding new IP CIDR ranges to their security groups. The security team has its own AWS account. Currently,

the security team notifies the owners of the other AWS accounts when changes are made to the allow list.
The solutions architect must design a solution that distributes the common set of CIDR ranges across all accounts Which solution meets these requirements with the LEAST amount of operational overhead.

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

Answer: A

NEW QUESTION 126
- (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 128
- (Exam Topic 2)
A company is configuring connectivity to a multi-account AWS environment to support application workloads fiat serve users in a single geographic region. The workloads depend on a highly available, on-premises legacy system deployed across two locations It is critical for the AWS workloads to manias connectivity to the legacy system, and a minimum of 5 Gbps of bandwidth is required All application workloads within AWS must have connectivity with one another.
Which solution will meet these requirements?

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

Answer: B

NEW QUESTION 129
- (Exam Topic 2)
A company runs applications on Amazon EC2 instances. The company plans to begin using an Auto Scaling group for the instances. As part of this transition, a solutions architect must ensure that Amazon CloudWatch Logs automatically collects logs from all new instances The new Auto Scaling group will use a launch template that includes the Amazon Linux 2 AMI and no key pair
Which solution meets these requirements?

A. Create an Amazon CloudWatch agent configuration for the workload Store the CloudWatch agent configuration in an Amazon S3 bucket Write an EC2 user data script to fetch the configuration He from Amazon S3. Configure the cloudWatch agent on the instance during Initial boot.
B. Create an Amazon CloudWatch agent configuration for the workload In AWS Systems Manager Parameter Store Create a Systems Manager document that Installs and configures the CloudWatch agent by using the configuration Create an Amazon EventBridge (Amazon CloudWatch Events) rule on the default event bus with a Systems Manager Run Command target that runs the document whenever an instance enters the running state.
C. Create an Amazon CloudWatch agent configuration for the workload Create an AWS Lambda function to Install and configure CloudWatch agent by using AWS Systems Manager Session Manage
D. Include the agent configuration inside the Lambda package Create an AWS Config custom rule to identify changes to the EC2 instances and invoke the Lambda function
E. Create an Amazon CloudWatch agent configuration for the workloa
F. Save the CloudWatch agent configuration as pan of an AWS Lambda deployment packag
G. Use AWS CloudTrail to capture EC2 tagging events and initiate agent installatio
H. Use AWS CodeBuild to configure the CloudWatch agent on the instances that run the workload.

Answer: B

NEW QUESTION 134
- (Exam Topic 2)
A large education company recently introduced Amazon Workspaces to provide access to internal applications across multiple universities. The company is storing user proxies on an Amazon FSx for Windows File Server tile system. The Me system is configured with a DNS alias and is connected to a self-managed Active Directory As more users begin to use the Workspaces login time increases to unacceptable levels
An investigation reveals a degradation in performance of the file system. The company created the file system on HDD storage with a throughput of 16 MBps A solutions architect must improve the performance of the file system during a defined maintenance window
What should the solutions architect do to meet these requirements with the LEAST administrative effort?

A. Use AWS Backup to create a point-in-time backup of the file system Restore the backup to a new FSx for Windows File Server file system Select SSD as the storage type Select 32 MBps as the throughput capacity When the backup and restore process is completed adjust the DNS alias accordingly Delete the original file system
B. Disconnect users from the file system In the Amazon FSx console, update the throughput capacity to 32 MBps Update the storage type to SSD Reconnect users to the file system
C. Deploy an AWS DataSync agent onto a new Amazon EC2 instanc
D. Create a task Configure the existing file system as the source location Configure a new FSx forWindows File Server file system with SSD storage and 32 MBps of throughput as the target location Schedule the task When the task is completed adjust the DNS alias accordingly Delete the original file system.
E. Enable shadow copies on the existing file system by using a Windows PowerShell command Schedule the shadow copy job to create a point-in-time backup of the file system Choose to restore previousversions Create a new FSx for Windows File Server file system with SSD storage and 32 MBps of throughput When the copy job is completed, adjust the DNS alias Delete the original file system

Answer: D

NEW QUESTION 136
- (Exam Topic 2)
A news company wants to implement an AWS Lambda function that calls an external API to receive new press releases every 10 minutes. The API provider Is planning to use an IP address allow list to protect the API. so the news company needs to provide any public IP addresses that access the API. The company's current architecture includes a VPC with an internet gateway and a NAT gateway. A solutions architect must implement a static IP address for the Lambda function.
Which combination of steps should the solutions architect take to meet these requirements? (Select TWO.)

A. Use the Elastic IP address that is associated with the NAT gateway for the IP address allow list.
B. Assign an Elastic IP address to the Lambda functio
C. Use the Lambda function's Elastic IP address for the IP address allow list.
D. Configure the Lambda function to launch in the private subnet of the VPC.
E. Configure the Lambda function to launch in the public subnet of the VPC.
F. Create a transit gatewa
G. Attach the VPC and the Lambda function to the transit gateway.

Answer: AC

NEW QUESTION 137
- (Exam Topic 2)
A company's solutions architect is reviewing a web application that runs on AWS. The application references static assets in an Amazon S3 bucket in the us-east-1 Region. The company needs resiliency across multiple AWS Regions. The company already has created an S3 bucket in a second Region.
Which solution will meet these requirements with the LEAST operational overhead?

A. Configure the application to write each object to both S3 bucket
B. Set up an Amazon Route 53 public hosted zone with a record set by using a weighted routing policy for each S3 bucke
C. Configure the application to reference the objects by using the Route 53 DNS name.
D. Create an AWS Lambda function to copy objects from the S3 bucket in us-east-1 to the S3 bucket in the second Regio
E. Invoke the Lambda function each time an object is written to the S3 bucket in us-east-1. Set up an Amazon CloudFront distribution with an origin group that contains the two S3 buckets as origins.
F. Configure replication on the S3 bucket in us-east-1 to replicate objects to the S3 bucket in the second Region Set up an Amazon CloudFront distribution with an origin group that contains the two S3 bucketsas origins.
G. Configure replication on the S3 bucket in us-east-1 to replicate objects to the S3 bucket in the second Regio
H. If failover is required, update the application code to load S3 objects from the S3 bucket in the second Region.

Answer: D

NEW QUESTION 142
- (Exam Topic 2)
A greeting card company recently advertised that customers could send cards to their favourite celebrities through the company's platform Since the advertisement was published, the platform has received constant traffic from 10.000 unique users each second.
The platform runs on m5.xlarge Amazon EC2 instances behind an Application Load Balancer (ALB) The instances run in an Auto Scaling group and use a custom AMI that is based on Amazon Linux. The platform uses a highly available Amazon Aurora MySQL DB cluster that uses primary and reader endpoints The platform also uses an Amazon ElastiCache for Redis cluster that uses its cluster endpoint
The platform generates a new process for each customer and holds open database connections to MySQL for the duration of each customer's session However, resource usage for the platform is low.
Many customers are reporting errors when they connect to the platform Logs show that connections to the Aurora database are failing Amazon CloudWatch metrics show that the CPU load is tow across the platform and that connections to the platform are successful through the ALB.
Which solution will remediate the errors MOST cost-effectively?

A. Set up an Amazon CloudFront distribution Set the ALB as the origin Move all customer traffic to the CloudFront distribution endpoint
B. Use Amazon RDS Proxy Reconfigure the database connections to use the proxy
C. Increase the number of reader nodes in the Aurora MySQL cluster
D. Increase the number of nodes in the ElastiCache for Redis cluster

Answer: C

NEW QUESTION 143
- (Exam Topic 2)
A company runs its application in the eu-west-1 Region and has one account for each of its environments development, testing, and production All the environments are running 24 hours a day 7 days a week by using stateful Amazon EC2 instances and Amazon RDS for MySQL databases The databases are between 500 GB and 800 GB in size
The development team and testing team work on business days during business hours, but the production environment operates 24 hours a day. 7 days a week.
The company wants to reduce costs AH resources are tagged with an environment tag with either development, testing, or production as the key.
What should a solutions architect do to reduce costs with the LEAST operational effort?

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs once every day Configure the rule to invoke one AWS Lambda function that starts or stops instances based on the tag day and time.
B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs every business day in the evenin
C. Configure the rule to invoke an AWS Lambda function that stops instances based on thetag-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 their ....based on the ta
F. day, and time

Answer: C

NEW QUESTION 148
- (Exam Topic 2)
A company is hosting a three-tier web application in an on-premises environment. Due to a recent surge in traffic that resulted in downtime and a significant financial impact, company management has ordered that the application be moved to AWS. The application is written in .NET and has a dependency on a MySQL database A solutions architect must design a scalable and highly available solution to meet the demand of 200000 daily users.
Which steps should the solutions architect take to design an appropriate solution?

A. Use AWS Elastic Beanstalk to create a new application with a web server environment and an Amazon RDS MySQL Multi-AZ DB instance The environment should launch a Network Load Balancer (NLB) in front of an Amazon EC2 Auto Scaling group in multiple Availability Zones Use an Amazon Route 53 alias record to route traffic from the company's domain to the NLB.
B. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon EC2 Auto Scaling group spanning three Availability Zone
C. The stack should launch a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a Retain deletion polic
D. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB
E. Use AWS Elastic Beanstalk to create an automatically scaling web server environment that spans two separate Regions with an Application Load Balancer (ALB) in each Regio
F. Create a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a cross-Region read replica Use Amazon Route 53 with a geoproximity routing policy to route traffic between the two Regions.
G. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon ECS cluster of Spot Instances spanning three Availability Zones The stack should launch an Amazon RDS MySQL DB instance with a Snapshot deletion policy Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB

Answer: B

NEW QUESTION 150
- (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 152
- (Exam Topic 2)
A company has its cloud infrastructure on AWS A solutions architect needs to define the infrastructure as code. The infrastructure is currently deployed in one AWS Region. The company's business expansion plan includes deployments in multiple Regions across multiple AWS accounts
What should the solutions architect do to meet these requirements?

A. Use AWS CloudFormation templates Add IAM policies to control the various accounts Deploy the templates across the multiple Regions
B. Use AWS Organizations Deploy AWS CloudFormation templates from the management account Use AWS Control Tower to manage deployments across accounts
C. Use AWS Organizations and AWS CloudFormation StackSets Deploy a CloudFormation template from an account that has the necessary IAM permissions
D. Use nested stacks with AWS CloudFormation templates Change the Region by using nested stacks

Answer: B

NEW QUESTION 153
- (Exam Topic 2)
A company runs an application in the cloud that consists of a database and a website Users can post data to the website, have the data processed, and have the data sent back to them in an email. Data is stored in a MySQL database running on an Amazon EC2 instance The database is running in a VPC with two private

subnets The website is running on Apache Tomcat in a single EC2 instance in a different VPC with one public subnet There is a single VPC peering connection between the database and website VPC.
The website has suffered several outages during the last month due to high traffic
Which actions should a solutions architect take to increase the reliability of the application? (Select THREE)

A. Place the Tomcat server in an Auto Scaling group with multiple EC2 instances behind an Application Load Balancer
B. Provision an additional VPC peering connection
C. Migrate the MySQL database to Amazon Aurora with one Aurora Replica
D. Provision two NAT gateways in the database VPC
E. Move the Tomcat server to the database VPC
F. Create an additional public subnet in a different Availability Zone in the website VPC

Answer: ACF

NEW QUESTION 156
- (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 dock 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 VP
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 Marketplac
E. Configure the time server to synchronize with the on-premises atomic clock network applianc
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 connectio
H. Configure the VPC route tables to direct NTP traffic over the tunnel.

Answer: B

NEW QUESTION 159
- (Exam Topic 2)
A solutions architect is designing a multi-account structure that has 10 existing accounts. The design must meet the following requirements
• Consolidate all accounts into one organization
• Allow full access to the Amazon EC2 service from the management account and the secondary accounts
• Minimize the effort required to add additional secondary accounts
Which combination of steps should be included in the solution? (Select TWO)

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

Answer: AE

NEW QUESTION 161
- (Exam Topic 2)
A company that designs multiplayer online games wants to expand its user base outside of Europe. The company transfers a significant amount of UDP traffic to Keep all the live and interactive sessions of the games The company has plans for rapid expansion and wants to build its architecture to provide an optimized online experience to its users
Which architecture will meet these requirements with the LOWEST latency for users''

A. Set up a Multi-AZ environment in a single AWS Region Use Amazon CloudFront to cache user sessions
B. Set up environments in multiple AWS Regions Create an accelerator in AWS Global Accelerator, and add endpoints from different Regions to it
C. Set up environments in multiple AWS Regions Use Amazon Route 53. and select latency-based routing
D. Set up a Multi-AZ environment in a single AWS Regio
E. Use AWS Lambda@Edge to update sessions closer to the users

Answer: B

NEW QUESTION 165
- (Exam Topic 2)
A company has a web application that securely uploads pictures and videos to an Amazon S3 bucket The company requires that only authenticated users are allowed to post content T.he application generates a presigned URL that is used to upload objects through a browser interface. Most users are reporting slow upload times for objects larger than 100 MB
What can a solutions architect do to improve the performance of these uploads while ensuring only authenticated users are allowed to post content?

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

B. Set up an Amazon API Gateway with a regional API endpoint that has a resource as an S3 service proxyConfigure the PUT method for this resource to expose the S3 Putobject operation Secure the API Gateway using an AWS Lambda authonzer Have the browser interface use API Gateway instead of the presigned URL to upload objects
C. Enable an S3 Transfer Acceleration endpoint on the S3 bucket Use the endpoint when generating the presigned URL Have the browser interface upload the objects to this URL using the S3 multipart upload API
D. Configure an Amazon CloudFront distribution for the destination S3 bucket Enable PUT and POST methods for the CloudFront cache behavior Update the CloudFront origin to use an origin access identity (OAI) Give the OAl user s 3: Putobject permissions in the bucket policy Have the browser interface upload objects using the CloudFront distribution

Answer: D

NEW QUESTION 170
- (Exam Topic 2)
A software company is using three AWS accounts for each of its 1 0 development teams The company has developed an AWS CloudFormation standard VPC template that includes three NAT gateways The template is added to each account for each team The company is concerned that network costs will increase each time a new development team is added A solutions architect must maintain the reliability of the company's solutions and minimize operational complexity
What should the solutions architect do to reduce the network costs while meeting these requirements?

A. Create a single VPC with three NAT gateways in a shared services account Configure each account VPC with a default route through a transit gateway to the NAT gateway in the shared services account VPC Remove all NAT gateways from the standard VPC template
B. Create a single VPC with three NAT gateways in a shared services account Configure each account VPC with a default route through a VPC peering connection to the NAT gateway in the shared services account VPC Remove all NAT gateways from the standard VPC template
C. Remove two NAT gateways from the standard VPC template Rely on the NAT gateway SLA to cover reliability for the remaining NAT gateway.
D. Create a single VPC with three NAT gateways in a shared services account Configure a Site-to-Site VPN connection from each account to the shared services account Remove all NAT gateways from the standard VPC template

Answer: A

NEW QUESTION 172
- (Exam Topic 2)
A company has a media metadata extraction pipeline running on AWS. Notifications containing a reference to a file Amazon S3 are sent to an Amazon Simple Notification Service (Amazon SNS) topic The pipeline consists of a number of AWS Lambda functions that are subscribed to the SNS topic The Lambda functions extract the S3 file and write metadata to an Amazon RDS PostgreSQL DB instance.
Users report that updates to the metadata are sometimes stow to appear or are lost. During these times, the CPU utilization on the database is high and the number of failed Lambda invocations increases.
Which combination of actions should a solutions architect take to r-e'p resolve this issue? (Select TWO.)

A. Enable massage delivery status on the SNS topic Configure the SNS topic delivery policy to enable retries with exponential backoff
B. Create an Amazon Simple Queue Service (Amazon SOS) FIFO queue and subscribe the queue to the SNS topic Configure the Lambda functions to consume messages from the SQS queue.
C. Create an RDS proxy for the RDS instance Update the Lambda functions to connect to the RDS instance using the proxy.
D. Enable the RDS Data API for the RDS instanc
E. Update the Lambda functions to connect to the RDS instance using the Data API
F. Create an Amazon Simple Queue Service (Amazon SQS) standard queue for each Lambda function and subscribe the queues to the SNS topi
G. Configure the Lambda functions to consume messages from their respective SQS queue.

Answer: CE

NEW QUESTION 173
- (Exam Topic 2)
A company has an application that uses Amazon EC2 instances in an Auto Scaling group. The quality assurance (QA) department needs to launch a large number of short-lived environments to test the application. The application environments are currently launched by the manager of the department using an AWS CloudFormation template To launch the stack, the manager uses a role with permission to use CloudFormation EC2. and Auto Scaling APIs. The manager wants to allow testers to launch their own environments, but does not want to grant broad permissions to each user
Which set up would achieve these goals?

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

Answer: B

NEW QUESTION 177
- (Exam Topic 2)
A company is planning a large event where a promotional offer will be introduced The company's website is hosted on AWS and backed by an Amazon RDS for PostgreSQL DB instance The website explains the promotion and includes a sign-up page that collects user information and preferences Management expects large and unpredictable volumes of traffic periodically which will create many database writes A solutions architect needs to build a solution that does not change the underlying data model and ensures that submissions are not dropped before they are committed to the database
Which solutions meets these requirements'?

A. Immediately before the event, scale up the existing DB instance to meet the anticipated deman
B. Then scale down after the event
C. Use Amazon SQS to decouple the application and database layers Configure an AWS Lambda function to write items from the queue into the database
D. Migrate to Amazon DynamoDB and manage throughput capacity with automatic scaling

E. Use Amazon ElastiCache for Memcached to increase write capacity to the DB instance

Answer: B

NEW QUESTION 179
- (Exam Topic 2)
A solutions architect needs to review the design of an Amazon EMR cluster that is using the EMR File System (EMRFS). The cluster performs tasks that are critical to business needs. The cluster is running Amazon EC2 On-Demand Instances at all times for all task, master, and core nodes The EMR tasks run each morning, starting at 1:00 AM, and take 6 hours to finish running. The amount of time to complete the processing is not a priority because the data is not referenced until late in the day.
The solutions architect must review the architecture and suggest a solution to minimize the compute costs Which solution should the solutions architect recommend to meet these requirements?

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

Answer: B

NEW QUESTION 184
- (Exam Topic 2)
A company has an application that runs on Amazon EC2 instances in an Amazon EC2 Auto Scaling group. The company uses AWS CodePipeline to deploy the application. The instances that run in the Auto Scaling group are constantly changing because of scaling events
When the company deploys new application code versions the company Installs the AWS CodeDeploy agent on any new target EC2 instances and associates the instances with the CodeDeploy deployment group The application is set to go live within the next 24 hours
What should a solutions architect recommend to automate the application deployment process with the LEAST amount of operational overhead?

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

Answer: C

NEW QUESTION 188
- (Exam Topic 2)
An online magazine will launch Its latest edition this month. This edition will be the first to be distributed globally. The magazine's dynamic website currently uses an Application Load Balancer in front of the web tier a fleet of Amazon EC2 instances for web and application servers, and Amazon Aurora MySQL. Portions of the website include static content and almost all traffic is read-only
The magazine is expecting a significant spike m internet traffic when the new edition is launched Optimal performance is a top priority for the week following the launch
Which combination of steps should a solutions architect take to reduce system response antes for a global audience? (Select TWO)

A. Use logical cross-Region replication to replicate the Aurora MySQL database to a secondary Region Replace the web servers with Amazon S3 Deploy S3 buckets in cross-Region replication mode
B. Ensure the web and application tiers are each m Auto Scaling group
C. Introduce an AWS Direct Connect connection Deploy the web and application tiers in Regions across the world
D. Migrate the database from Amazon Aurora to Amazon RDS for MySQ
E. Ensure all three of the application tiers—we
F. application, and database—are in private subnets.
G. Use an Aurora global database for physical cross-Region replicatio
H. Use Amazon S3 with cross-Region replication for static content and resource
I. Deploy the web and application tiers in Regions across the world
J. Introduce Amazon Route 53 with latency-based routing and Amazon CloudFront distribution
K. Ensure me web and application tiers are each in Auto Scaling groups

Answer: DE

NEW QUESTION 190
- (Exam Topic 2)
A solutions architect has implemented a SAML 2.0 federated identity solution with their company's
on-premises identity provider (IdP) to authenticate users' access to the AWS environment. When the solutions architect tests authentication through the federated identity web portal access to the AWS environment is granted However, when test users attempt to authenticate through the federated identity web portal, they are

not able to access the AWS environment.
Which items should the solutions architect check to ensure identity federation is property configured? (Select THREE)

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

Answer: BCF

NEW QUESTION 195
- (Exam Topic 2)
A company manages multiple AWS accounts by using AWS Organizations. Under the root OU. the company has two OUs: Research and DataOps.
Because of regulatory requirements, all resources that the company deploys in the organization must reside in the ap-northeast-1 Region. Additionally. EC2 instances that the company deploys in the DataOps OU must use a predefined list of instance types
A solutions architect must implement a solution that applies these restrictions. The solution must maximize operational efficiency and must minimize ongoing maintenance
Which combination of steps will meet these requirements? (Select TWO)

A. Create an IAM role in one account under the DataOps OU Use the ec2 Instance Type condition key in an inline policy on the role to restrict access to specific instance types.
B. Create an IAM user in all accounts under the root OU Use the aws RequestedRegion condition key in an inline policy on each user to restrict access to all AWS Regions except ap-northeast-1.
C. Create an SCP Use the aws:RequestedRegion condition key to restrict access to all AWS Regions except ap-northeast-1 Apply the SCP to the root OU.
D. Create an SCP Use the ec2Reo»on condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root O
E. the DataOps O
F. and the Research OU.
G. Create an SCP Use the ec2:lnstanceType condition key to restrict access to specific instance types Apply the SCP to the DataOps OU.

Answer: CE

NEW QUESTION 199
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SAP-C02 Practice Exam Features:

* SAP-C02 Questions and Answers Updated Frequently

* SAP-C02 Practice Questions Verified by Expert Senior Certified Staff

* SAP-C02 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SAP-C02 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year