Exam Questions SAP-C02

AWS Certified Solutions Architect - Professional

https://www.2passeasy.com/dumps/SAP-C02/

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 Is serving files to its customers through an SFTP server that Is accessible over the internet The SFTP server Is running on a single Amazon EC2 instance with an Elastic IP address attached Customers connect to the SFTP server through its Elastic IP address and use SSH for authentication The EC2 instance also has an attached security group that allows access from all customer IP addresses.
A solutions architect must implement a solution to improve availability minimize the complexity ot infrastructure management and minimize the disruption to customers who access files. The solution must not change the way customers connect.
Which solution will meet these requirements?

A. Disassociate the Elastic IP address from me EC2 instance Create an Amazon S3 bucket to be used for sftp file hosting Create an AWS Transfer Family server Configure the Transfer Family server with a publicly accessible endpoin
B. Associate the SFTP Elastic IP address with the new endpoin
C. Point the Transfer Family server to the S3 bucket Sync all files from the SFTP server to the S3 bucket.
D. Disassociate the Elastic IP address from the EC2 instanc
E. Create an Amazon S3 bucket to be used for SFTP file hosting Create an AWS Transfer Family serve
F. Configure the Transfer Family server with a VPC-hoste
G. internet-facing endpoin
H. Associate the SFTP Elastic IP address with the new endpoin
I. Attach the security group with customer IP addresses to the new endpoin
J. Point the Transfer Family server to the S3 bucke
K. Sync all files from the SFTP server to The S3 bucket
L. Disassociate the Elastic IP address from the EC2 instanc
M. Create a new Amazon Elastic File System (Amazon EFS) file system to be used for SFTP file hostin
N. Create an AWS Fargate task definition to run an SFTP serve
O. Specify the EFS file system as a mount in the task definition Create a Fargate service by using the task definition, and place a Network Load Balancer (NLB> «i front of the service When configuring the service, attach the security group with customer IP addresses to the tasks that run the SFTP server Associate the Elastic IP address with the Nl B Sync all files from the SFTP server to the S3 bucket
P. Disassociate the Elastic IP address from the EC2 instance Create a multi-attach Amazon Elastic Block Store (Amazon EBS) volume to be used to SFTP file hosting Create a Network Load Balancer (NLB) with the Elastic IP address attached Create an Auto Scaling group with EC2 instances that run an SFTP server Define in the Auto Scaling group that instances that are launched should attach the newmulti-attach EBS volume Configure the Auto Scaling group to automatically add instances behind the NLB Configure the Auto Scaling group to use the security group that allows customer IP addresses for the EC2 instances that the Auto Scaling group launches Sync all files from the SFTP server to the new multi-attach EBS volume

Answer: B

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

NEW QUESTION 3
- (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 4
- (Exam Topic 1)
A company hosts a large on-premises MySQL database at its main office that supports an issue tracking system used by employees around the world. The company already uses AWS for some workloads and has created an Amazon Route 53 entry for the database endpoint that points to the on-premises database. Management is concerned about the database being a single point of failure and wants a solutions architect to migrate the database to AWS without any data loss or downtime.
Which set of actions should the solutions architect implement?

A. Create an Amazon Aurora DB cluste
B. Use AWS Database Migration Service (AWS DMS) to do a full load from the on-premises database lo Auror
C. Update the Route 53 entry for the database to point to the Aurora cluster endpoin
D. and shut down the on-premises database.
E. During nonbusiness hours, shut down the on-premises database and create a backu
F. Restore this backup to an Amazon Aurora DB cluste
G. When the restoration is complete, update the Route 53 entry for the database to point to the Aurora cluster endpoint, and shut down the on-premises database.
H. Create an Amazon Aurora DB cluste
I. Use AWS Database Migration Service (AWS DMS) to do a full load with continuous replication from the on-premises database to Auror
J. When the migration is complete, update the Route 53 entry for the database to point to the Aurora cluster endpoint, and shut down the on-premises database.
K. Create a backup of the database and restore it to an Amazon Aurora multi-master cluste
L. This Aurora cluster will be in a master-master replication configuration with the on-premises databas
M. Update the Route 53 entry for the database to point to the Aurora cluster endpoin
N. and shut down the on-premises database.

Answer: C

Explanation:
“Around the world” eliminates possibility for the maintenance window at night. The other difference is ability to leverage continuous replication in MySQL to Aurora case.

NEW QUESTION 5
- (Exam Topic 1)
A company is running an application on several Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer. The load on the application varies throughout the day, and EC2 instances are scaled in and out on a regular basis. Log files from the EC2 instances are copied to a central Amazon S3 bucket every 15 minutes. The security team discovers that log files are missing from some of the terminated EC2 instances.
Which set of actions will ensure that log files are copied to the central S3 bucket from the terminated EC2 instances?

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

Answer: B

Explanation:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/adding-lifecycle-hooks.html
- Refer to Default Result section - If the instance is terminating, both abandon and continue allow the instance
to terminate. However, abandon stops any remaining actions, such as other lifecycle hooks, and continue allows any other lifecycle hooks to complete.
https://aws.amazon.com/blogs/infrastructure-and-automation/run-code-before-terminating-an-ec2-auto-scaling-i https://github.com/aws-samples/aws-lambda-lifecycle-hooks-function
https://github.com/aws-samples/aws-lambda-lifecycle-hooks-function/blob/master/cloudformation/template.yam

NEW QUESTION 6

- (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 7
- (Exam Topic 1)
A financial services company logs personally identifiable information 10 its application logs stored in Amazon S3. Due to regulatory compliance requirements, the log files must be encrypted at rest. The security team has mandated that the company's on-premises hardware security modules (HSMs) be used to generate the CMK material.
Which steps should the solutions architect take to meet these requirements?

A. Create an AWS CloudHSM cluste
B. Create a new CMK in AWS KMS using AWS_CloudHSM as the source (or the key material and an origin of AWS_CLOUDHS
C. Enable automatic key rotation on the CMK with a duration of 1 yea
D. Configure a bucket policy on the togging bucket thai disallows uploads of unencrypted data and requires that the encryption source be AWS KMS.
E. Provision an AWS Direct Connect connection, ensuring there is no overlap of the RFC 1918 address space between on-premises hardware and the VPC
F. Configure an AWS bucket policy on the logging bucket that requires all objects to be encrypte
G. Configure the logging application to query theon-premises HSMs from the AWS environment for the encryption key material, and create a unique CMK for each logging event.
H. Create a CMK in AWS KMS with no key material and an origin of EXTERNA
I. Import the key material generated from the on-premises HSMs into the CMK using the public key and import token provided by AW
J. Configure a bucket policy on the logging bucket that disallows uploads ofnon-encrypted data and requires that the encryption source be AWS KMS.
K. Create a new CMK in AWS KMS with AWS-provided key material and an origin of AWS_KM
L. Disable this CM
M. and overwrite the key material with the key material from the on-premises HSM using the public key and import token provided by AW
N. Re-enable the CM
O. Enable automatic key rotation on the CMK with a duration of 1 yea
P. Configure a bucket policy on the logging bucket that disallows uploads of non-encrypted data and requires that the encryption source be AWS KMS.

Answer: C

Explanation:
https://aws.amazon.com/blogs/security/how-to-byok-bring-your-own-key-to-aws-kms-for-less-than-15-00-a-yea
https://docs.aws.amazon.com/kms/latest/developerguide/importing-keys-create-cmk.html

NEW QUESTION 8
- (Exam Topic 1)
An enterprise runs 103 line-of-business applications on virtual machines in an on-premises data center. Many of the applications are simple PHP. Java, or Ruby web applications, are no longer actively developed, and serve little traffic.
Which approach should be used to migrate these applications to AWS with the LOWEST infrastructure costs?

A. Deploy the applications lo single-instance AWS Elastic Beanstalk environments without a load balancer.
B. Use AWS SMS to create AMIs for each virtual machine and run them in Amazon EC2.
C. Convert each application to a Docker image and deploy to a small Amazon ECS cluster behind an Application Load Balancer.
D. Use VM Import/Export to create AMIs for each virtual machine and run them in single-instance AWS Elastic Beanstalk environments by configuring a custom image.

Answer: C

NEW QUESTION 9
- (Exam Topic 1)
A company wants to move a web application to AWS. The application stores session information locally on each web server, which will make auto scaling difficult As part of the migration, the application will be rewritten to decouple the session data from the web servers. The company requires low latency, scalability, and availability.
Which service will meet the requirements for storing the session information in the MOST cost-effective way?

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

Answer: D

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

NEW QUESTION 10
- (Exam Topic 1)
A development team has created a new flight tracker application that provides near-real-time data to users. The application has a front end that consists of an Application Load Balancer (ALB) in front of two large Amazon EC2 instances in a single Availability Zone. Data is stored in a single Amazon RDS MySQL DB instance. An Amazon Route 53 DNS record points to the ALB.
Management wants the development team to improve the solution to achieve maximum reliability with the least amount of operational overhead.
Which set of actions should the team take?

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

Answer: D

Explanation:
Multi AZ ASG + ALB + Aurora = Less over head and automatic scaling

NEW QUESTION 10
- (Exam Topic 1)
A solutions architect is designing the data storage and retrieval architecture for a new application that a company will be launching soon. The application is designed to ingest millions of small records per minute from devices all around the world. Each record is less than 4 KB in size and needs to be stored in a durable location where it can be retrieved with low latency. The data is ephemeral and the company is required to store the data for 120 days only, after which the data can be deleted.
The solutions architect calculates that, during the course of a year, the storage requirements would be about 10-15 TB.
Which storage strategy is the MOST cost-effective and meets the design requirements?

A. Design the application to store each incoming record as a single .csv file in an Amazon S3 bucket to allow for indexed retrieva
B. Configure a lifecycle policy to delete data older than 120 days.
C. Design the application to store each incoming record in an Amazon DynamoDB table properly configured for the scal
D. Configure the DynamoOB Time to Live (TTL) feature to delete records older than 120 days.
E. Design the application to store each incoming record in a single table in an Amazon RDS MySQL databas
F. Run a nightly cron job that executes a query to delete any records older than 120 days.
G. Design the application to batch incoming records before writing them to an Amazon S3 bucke
H. Update the metadata for the object to contain the list of records in the batch and use the Amazon S3 metadatasearch feature to retrieve the dat
I. Configure a lifecycle policy to delete the data after 120 days.

Answer: B

Explanation:
DynamoDB with TTL, cheaper for sustained throughput of small items + suited for fast retrievals. S3 cheaper for storage only, much higher costs with writes. RDS not designed for this use case.

NEW QUESTION 11
- (Exam Topic 1)
A fitness tracking company serves users around the world, with its primary markets in North America and Asia. The company needs to design an infrastructure for its read-heavy user authorization application with the following requirements:
• Be resilient to problems with the application in any Region.
• Write to a database in a single Region.
• Read from multiple Regions.
• Support resiliency across application tiers in each Region.
• Support the relational database semantics reflected in the application. Which combination of steps should a solutions architect take? (Select TWO.)

A. Use an Amazon Route 53 geoproximity routing policy combined with a multivalue answer routing policy.
B. Deploy we
C. application, and MySQL database servers to Amazon EC2 instances in each Regio
D. Set up the application so that reads and writes are local to the Regio
E. Create snapshots of the web, application, and database servers and store the snapshots in an Amazon S3 bucket in both Region
F. Set upcross-Region replication for the database layer.
G. Use an Amazon Route 53 geolocation routing policy combined with a failover routing policy.
H. Set up web, application, and Amazon RDS for MySQL instances in each Regio
I. Set up the application so that reads are local and writes are partitioned based on the use

J. Set up a Multi-AZ failover for the web, application, and database server
K. Set up cross-Region replication for the database layer.
L. Set up active-active web and application servers in each Regio
M. Deploy an Amazon Aurora global database with clusters in each Regio
N. Set up the application to use the in-Region Aurora database endpoint
O. Create snapshots of the web and application servers and store them in an Amazon S3 bucket in both Regions.

Answer: CE

Explanation:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html
Geoproximity routing policy is good to control the user traffic to specific regions. However, a multivalue answer routing policy may cause the users to be randomly sent to other healthy regions that may be far away from the user's location. You can use geolocation routing policy to direct the North American users to your servers on the North America region and configure failover routing to the Asia region in case the North America region fails. You can configure the same for the Asian users pointed to the Asia region servers and have the North America region as its backup.

NEW QUESTION 12
- (Exam Topic 1)
A solutions architect has an operational workload deployed on Amazon EC2 instances in an Auto Scaling group. The VPC architecture spans two Availability Zones (AZ) with a subnet in each that the Auto Scaling group is targeting. The VPC is connected to an on-premises environment and connectivity cannot be interrupted. The maximum size ol the Auto Scaling group is 20 instances in service. The VPC IPv4 addressing is as follows:
VPC CIDR: 10.0.0.0/23
AZ1 subnet CIDR: 10.0.0.0/24 AZ2 subnet CIDR: 10.0.1.0/24
Since deployment, a third AZ has become available in the Region. The solutions architect wants to adopt the new AZ without adding additional IPv4 address space and without service downtime.
Which solution will meet these requirements?

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

Answer: A

Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/vpc-ip-address-range/?nc1=h_ls
It's not possible to modify the IP address range of an existing virtual private cloud (VPC) or subnet. You must delete the VPC or subnet, and then create a new VPC or subnet with your preferred CIDR block.

NEW QUESTION 15
- (Exam Topic 1)
A company that is developing a mobile game is making game assets available in two AWS Regions. Game assets ate served from a set of Amazon EC2 instances behind an Application Load Balancer (ALB) in each Region. The company requires game assets to be (etched from the closest Region. If game assets become unavailable in the closest Region, they should be fetched from the other Region.
What should a solutions architect do to meet these requirements?

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

Answer: D

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

NEW QUESTION 19
- (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 account numbers and OUs to manage Update the parameter as needed to add or remove accounts or OUs Use an Amazon EventBridge (Amazon CloudWatch Events) rule to identify any changes to the parameter and to invoke an AWS Lambda function to update the security policy in the Firewall Manager administrative account
C. Deploy an organization-wide AWS Config rule that requires all resources in the selected OUs to associate the AWS WAF rule
D. Deploy automated remediation actions by using AWS Lambda to fix noncompliant resources Deploy AWS WAF rules by using an AWS CloudFormation stack set to target the same OUs where the AWS Config rule is applied.
E. Create AWS WAF rules in the management account of the organization 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 accounts Assume the rotes by using AWS Security Token Service (AWS STS) in the Lambda function to create and update AWS WAF rules in the member accounts.
F. Use AWS Control Tower to manage AWS WAF rules across accounts in the organization 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 OUs 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 20
- (Exam Topic 1)
A company has an Amazon VPC that is divided into a public subnet and a pnvate subnet. A web application runs in Amazon VPC. and each subnet has its own NACL The public subnet has a CIDR of 10.0.0 0/24 An Application Load Balancer is deployed to the public subnet The private subnet has a CIDR of 10.0.1.0/24. Amazon EC2 instances that run a web server on port 80 are launched into the private subnet
Onty network traffic that is required for the Application Load Balancer to access the web application can be allowed to travel between the public and private subnets
What collection of rules should be written to ensure that the private subnet's NACL meets the requirement? (Select TWO.)

A. An inbound rule for port 80 from source 0.0 0.0/0
B. An inbound rule for port 80 from source 10.0 0 0/24
C. An outbound rule for port 80 to destination 0.0.0.0/0
D. An outbound rule for port 80 to destination 10.0.0.0/24
E. An outbound rule for ports 1024 through 65535 to destination 10.0.0.0/24

Answer: BE

Explanation:
Ephemeral ports are not covered in the syllabus so be careful that you don't confuse day to day best practise with what is required for the exam. Link to an explanation on Ephemeral ports here. https://acloud.guru/forums/aws-certified-solutions-architect-associate/discussion/-KUbcwo4lXefMl7janaK/netw

NEW QUESTION 24
- (Exam Topic 1)
A travel company built a web application that uses Amazon Simple Email Service (Amazon SES) to send email notifications to users. The company needs to enable logging to help troubleshoot email delivery issues. The company also needs the ability to do searches that are based on recipient, subject, and time sent.
Which combination of steps should a solutions architect take to meet these requirements? (Select TWO.)

A. Create an Amazon SES configuration set with Amazon Kinesis Data Firehose as the destinatio
B. Choose to send logs to an Amazon S3 bucket.
C. Enable AWS CloudTrail loggin
D. Specify an Amazon S3 bucket as the destination for the logs.
E. Use Amazon Athena to query the fogs in the Amazon S3 bucket for recipient, subject, and time sent.
F. Create an Amazon CloudWatch log grou
G. Configure Amazon SES to send logs to the log group
H. Use Amazon Athena to query the logs in Amazon CloudWatch for recipient, subject, and time sent.

Answer: AC

Explanation:
https://docs.aws.amazon.com/ses/latest/dg/event-publishing-retrieving-firehose.html
To enable you to track your email sending at a granular level, you can set up Amazon SES to publish email sending events to Amazon CloudWatch, Amazon Kinesis Data Firehose, or Amazon Simple Notification Service based on characteristics that you define.
https://docs.aws.amazon.com/ses/latest/dg/monitor-using-event-publishing.html
https://aws.amazon.com/getting-started/hands-on/build-serverless-real-time-data-processing-app-lambda-kinesis

NEW QUESTION 25
- (Exam Topic 1)
A company has a three-tier application running on AWS with a web server, an application server, and an Amazon RDS MySQL DB instance. A solutions architect is designing a disaster recovery (OR) solution with an RPO of 5 minutes.
Which solution will meet the company's requirements?

A. Configure AWS Backup to perform cross-Region backups of all servers every 5 minute
B. Reprovision the three tiers in the DR Region from the backups using AWS CloudFormation in the event of a disaster.
C. Maintain another running copy of the web and application server stack in the DR Region using AWS CloudFormation drill detectio
D. Configure cross-Region snapshots ol the DB instance to the DR Region every 5 minute
E. In the event of a disaster, restore the DB instance using the snapshot in the DR Region.

F. Use Amazon EC2 Image Builder to create and copy AMIs of the web and application server to both the primary and DR Region
G. Create a cross-Region read replica of the DB instance in the DR Regio
H. In the event of a disaster, promote the read replica to become the master and reprovision the servers with AWS CloudFormation using the AMIs.
I. Create AMts of the web and application servers in the DR Regio
J. Use scheduled AWS Glue jobs to synchronize the DB instance with another DB instance in the DR Regio
K. In the event of a disaster, switch to the DB instance in the DR Region and reprovision the servers with AWS CloudFormation using the AMIs.

Answer: C

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

NEW QUESTION 27
- (Exam Topic 1)
A company has 50 AWS accounts that are members of an organization in AWS Organizations Each account contains multiple VPCs The company wants to use AWS Transit Gateway to establish connectivity between the VPCs in each member account Each time a new member account is created, the company wants to automate the process of creating a new VPC and a transit gateway attachment.
Which combination of steps will meet these requirements? (Select TWO)

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

Answer: AC

NEW QUESTION 31
- (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 35
- (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 39
- (Exam Topic 1)
A company wants to host a new global website that consists of static content. A solutions architect is working on a solution that uses Amazon CloudFront with an origin access identity <OAI) to access website content that is stored in a private Amazon S3 bucket.
During testing, the solutions architect receives 404 errors from the S3 bucket. Error messages appear only for attempts to access paths that end with a forward slash. such as example.com/path/. These requests should return the existing S3 object path/index.html. Any potential solution must not prevent CloudFront from caching the content.
What should the solutions architect do to resolve this problem?

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

Answer: C

NEW QUESTION 41
- (Exam Topic 1)
A large company with hundreds of AWS accounts has a newly established centralized internal process for purchasing new or modifying existing Reserved Instances. This process requires all business units that want to purchase or modify Reserved Instances to submit requests to a dedicated team for procurement or execution. Previously, business units would directly purchase or modify Reserved Instances in their own respective AWS accounts autonomously.
Which combination of steps should be taken to proactively enforce the new process in the MOST secure way possible? (Select TWO.)

A. Ensure all AWS accounts are part of an AWS Organizations structure operating in all features mode.
B. Use AWS Contig lo report on the attachment of an IAM policy that denies access to the ec2:PurchaseReservedInstancesOffering and ec2:ModifyReservedInstances actions.
C. In each AWS account, create an IAM policy with a DENY rule to the ec2:PurchaseReservedInstancesOffering and ec2:ModifyReservedInstances actions.
D. Create an SCP that contains a deny rule to the ec2:PurchaseReservedInstancesOffering and ec2: Modify Reserved Instances action
E. Attach the SCP to each organizational unit (OU) of the AWS Organizations structure.
F. Ensure that all AWS accounts are part of an AWS Organizations structure operating in consolidated billing features mode.

Answer: AD

Explanation:
https://docs.aws.amazon.com/organizations/latest/APIReference/API_EnableAllFeatures.html
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp-strategies.html

NEW QUESTION 43
- (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 48
- (Exam Topic 1)
A solutions architect needs to advise a company on how to migrate its on-premises data processing application to the AWS Cloud. Currently, users upload input files through a web portal. The web server then stores the uploaded files on NAS and messages the processing server over a message queue. Each media file can take up to 1 hour to process. The company has determined that the number of media files awaiting processing is significantly higher during business hours, with the number of files rapidly declining after business hours.
What is the MOST cost-effective migration recommendation?

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

Answer: D

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

NEW QUESTION 53
- (Exam Topic 1)
A company runs an e-commerce platform with front-end and e-commerce tiers. Both tiers run on LAMP stacks with the front-end instances running behind a load balancing appliance that has a virtual offering on AWS Current*/, the operations team uses SSH to log in to the instances to maintain patches and address other concerns. The platform has recently been the target of multiple attacks, including.
• A DDoS attack.
• An SOL injection attack
• Several successful dictionary attacks on SSH accounts on the web servers
The company wants to improve the security of the e-commerce platform by migrating to AWS. The company's solutions architects have decided to use the following approach;
• Code review the existing application and fix any SQL injection issues.
• Migrate the web application to AWS and leverage the latest AWS Linux AMI to address initial security patching.
• Install AWS Systems Manager to manage patching and allow the system administrators to run commands on all instances, as needed.
What additional steps will address all of the identified attack types while providing high availability and minimizing risk?

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

Answer: B

NEW QUESTION 57
- (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 61
- (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 64
- (Exam Topic 1)
An online retail company hosts its stateful web-based application and MySQL database in an on-premises data center on a single server. The company wants to increase its customer base by conducting more marketing campaigns and promotions. In preparation, the company wants to migrate its application and database to AWS to increase the reliability of its architecture.
Which solution should provide the HIGHEST level of reliability?

A. Migrate the database to an Amazon RDS MySQL Multi-AZ DB instanc
B. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balance
C. Store sessions in Amazon Neptune.
D. Migrate the database to Amazon Aurora MySQ
E. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balance
F. Store sessions in an Amazon ElastiCache for Redis replication group.
G. Migrate the database to Amazon DocumentDB (with MongoDB compatibility). Deploy the application in an Auto Scaling group on Amazon EC2 instances behind a Network Load Balance
H. Store sessions in Amazon Kinesis Data Firehose.
I. Migrate the database to an Amazon RDS MariaDB Multi-AZ DB instanc
J. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balance
K. Store sessions in Amazon ElastiCache for Memcached.

Answer: B

NEW QUESTION 66
- (Exam Topic 1)
A company built an ecommerce website on AWS using a three-tier web architecture. The application is
Java-based and composed of an Amazon CloudFront distribution, an Apache web server layer of Amazon EC2 instances in an Auto Scaling group, and a backend Amazon Aurora MySQL database.
Last month, during a promotional sales event, users reported errors and timeouts while adding items to their shopping carts. The operations team recovered the logs created by the web servers and reviewed Aurora DB cluster performance metrics. Some of the web servers were terminated before logs could be collected and the Aurora metrics were not sufficient for query performance analysis.
Which combination of steps must the solutions architect take to improve application performance visibility during peak traffic events? (Select THREE.)

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

Answer: ABD

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

NEW QUESTION 69
- (Exam Topic 1)
A company has an application that generates reports and stores them in an Amazon S3 bucket. When a user accesses their report, the application generates a signed URL to allow the user to download the report. The company's security team has discovered that the files are public and that anyone can download them without authentication. The company has suspended the generation of new reports until the problem is resolved.
Which set of actions will immediately remediate the security issue without impacting the application's normal workflow?

A. Create an AWS Lambda function that applies a deny all policy for users who are not authenticated.Create a scheduled event to invoke the Lambda function.
B. Review the AWS Trusted Advisor bucket permissions check and implement the recommended actions.
C. Run a script that puts a private ACL on all of the objects in the bucket.
D. Use the Block Public Access feature in Amazon S3 to set the IgnorePublicAcls option to TRUE on the bucket.

Answer: D

Explanation:
The S3 bucket is allowing public access and this must be immediately disabled. Setting the IgnorePublicAcls option to TRUE causes Amazon S3 to ignore all public ACLs on a bucket and any objects that it contains. The other settings you can configure with the Block Public Access Feature are:

o BlockPublicAcls – PUT bucket ACL and PUT objects requests are blocked if granting public access. o BlockPublicPolicy – Rejects requests to PUT a bucket policy if granting public access.
o RestrictPublicBuckets – Restricts access to principles in the bucket owners' AWS account. https://aws.amazon.com/s3/features/block-public-access/

NEW QUESTION 73
- (Exam Topic 1)
A solutions architect is responsible (or redesigning a legacy Java application to improve its availability, data durability, and scalability. Currently, the application runs on a single high-memory Amazon EC2 instance. It accepts HTTP requests from upstream clients, adds them to an in-memory queue, and responds with a 200 status. A separate application thread reads items from the queue, processes them, and persists the results to an Amazon RDS MySQL instance. The processing time for each item takes 90 seconds on average, most of which is spent waiting on external service calls, but the application is written to process multiple items in parallel.
Traffic to this service is unpredictable. During periods of high load, items may sit in the internal queue for over an hour while the application processes the backlog. In addition, the current system has issues with availability and data loss if the single application node fails.
Clients that access this service cannot be modified. They expect to receive a response to each HTTP request they send within 10 seconds before they will time out and retry the request.
Which approach would improve the availability and durability of (he system while decreasing the processing latency and minimizing costs?

A. Create an Amazon API Gateway REST API that uses Lambda proxy integration to pass requests to an AWS Lambda functio
B. Migrate the core processing code to a Lambda function and write a wrapper class that provides a handler method that converts the proxy events to the internal application data model and invokes the processing module.
C. Create an Amazon API Gateway REST API that uses a service proxy to put items in an Amazon SOS queu
D. Extract the core processing code from the existing application and update it to pull items from Amazon SOS instead of an in-memory queu
E. Deploy the new processing application to smaller EC2 instances within an Auto Scaling group that scales dynamically based on the approximate number of messages in the Amazon SOS queue.
F. Modify the application to use Amazon DynamoDB instead of Amazon RD
G. Configure Auto Scaling for the DynamoDB tabl
H. Deploy the application within an Auto Scaling group with a scaling policy based on CPU utilizatio
I. Back the in-memory queue with a memory-mapped file to an instance store volume and periodically write that file to Amazon S3.
J. Update the application to use a Redis task queue instead of the in-memory queu
K. 8uild a Docker container image for the applicatio
L. Create an Amazon ECS task definition that includes the application container and a separate container to host Redi
M. Deploy the new task definition as an ECS service using AWS Fargate, and enable Auto Scaling.

Answer: B

Explanation:
The obvious challenges here are long workloads, scalability based on queue load, and reliability. Almost always the defacto answer to queue related workload is SQS. Since the workloads are very long (90 minutes) Lambdas cannot be used (15 mins max timeout). So, autoscaled smaller EC2 nodes that wait on external services to complete the task makes more sense. If the task fails, the message is returned to the queue and retried.

NEW QUESTION 77
- (Exam Topic 1)
A company has developed a single-page web application in JavaScript. The source code is stored in a single Amazon S3 bucket in the us-east-1 Region. The company serves the web application to a global user base through Amazon CloudFront.
The company wants to experiment with two versions of the website without informing application users. Each version of the website will reside in its own S3 bucket. The company wants to determine which version is most successful in marketing a new product.
The solution must send application users that are based in Europe to the new website design. The solution must send application users that are based in the United States to the current website design. However, some exceptions exist. The company needs to be able to redirect specific users to the new website design, regardless of the users' location.
Which solution meets these requirements?

A. Configure two CloudFront distribution
B. Configure a geolocation routing policy in Amazon Route 53 to route traffic to the appropriate CloudFront endpoint based on the location of clients.
C. Configure a single CloudFront distributio
D. Create a behavior with different paths for each version of the sit
E. Configure Lambda@Edge on the default path to generate redirects and send the client to the correct version of the website.
F. Configure a single CloudFront distributio
G. Configure an alternate domain name on the distribution.Configure two behaviors to route users to the different S3 origins based on the domain name that the client uses in the HTTP request.
H. Configure a single CloudFront distribution with Lambda@Edg
I. Use Lambda@Edge to send user requests to different origins based on request attributes.

Answer: A

NEW QUESTION 81
- (Exam Topic 1)
A team collects and routes behavioral data for an entire company. The company runs a Multi-AZ VPC environment with public subnets, private subnets, and in internet gateway Each public subnet also contains a NAT gateway Most of the company's applications read from and write to Amazon Kinesis Data Streams. Most of the workloads run in private subnets.
A solutions architect must review the infrastructure The solutions architect needs to reduce costs and maintain the function of the applications. The solutions architect uses Cost Explorer and notices that the cost in the EC2-Other category is consistently high A further review shows that NatGateway-Bytes charges are increasing the cost in the EC2-Other category.
What should the solutions architect do to meet these requirements?

A. Enable VPC Flow Log
B. Use Amazon Athena to analyze the logs for traffic that can be remove
C. Ensure that security groups are blocking traffic that is responsible for high costs.
D. Add an interface VPC endpoint for Kinesis Data Streams to the VP
E. Ensure that applications have thecorrect IAM permissions to use the interface VPC endpoint.
F. Enable VPC Flow Logs and Amazon Detectiv

G. Review Detective findings for traffic that is not related to Kinesis Data Streams Configure security groups to block that traffic
H. Add an interface VPC endpoint for Kinesis Data Streams to the VPC Ensure that the VPC endpoint policy allows traffic from the applications

Answer: D

Explanation:
https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-access.html https://aws.amazon.com/premiumsupport/knowledge-center/vpc-reduce-nat-gateway-transfer-costs/
VPC endpoint policies enable you to control access by either attaching a policy to a VPC endpoint or by using additional fields in a policy that is attached to an IAM user, group, or role to restrict access to only occur via the specified VPC endpoint

NEW QUESTION 84
- (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 85
- (Exam Topic 1)
A company provides a centralized Amazon EC2 application hosted in a single shared VPC. The centralized application must be accessible from client applications running in the VPCs of other business units. The centralized application front end is configured with a Network Load Balancer (NLB) for scalability.
Up to 10 business unit VPCs will need to be connected to the shared VPC. Some of the business unit VPC CIDR blocks overlap with the shared VPC. and some overlap with each other. Network connectivity to the centralized application in the shared VPC should be allowed from authorized business unit VPCs only.
Which network configuration should a solutions architect use to provide connectivity from the client applications in the business unit VPCs to the centralized application in the shared VPC?

A. Create an AW5 Transit Gatewa
B. Attach the shared VPC and the authorized business unit VPCs to the transit gatewa
C. Create a single transit gateway route table and associate it with all of the attached VPC
D. Allow automatic propagation of routes from the attachments into the route tabl
E. Configure VPC routing tables to send traffic to the transit gateway.
F. Create a VPC endpoint service using the centralized application NLB and enable (he option to require endpoint acceptanc
G. Create a VPC endpoint in each of the business unit VPCs using the service name of the endpoint servic
H. Accept authorized endpoint requests from the endpoint service console.
I. Create a VPC peering connection from each business unit VPC to Ihe shared VP
J. Accept the VPC peering connections from the shared VPC consol
K. Configure VPC routing tables to send traffic to the VPC peering connection.
L. Configure a virtual private gateway for the shared VPC and create customer gateways for each of theauthorized business unit VPC
M. Establish a Sile-to-Site VPN connection from the business unit VPCs to the shared VP
N. Configure VPC routing tables to send traffic to the VPN connection.

Answer: B

Explanation:
Amazon Transit Gateway doesn’t support routing between Amazon VPCs with overlapping CIDRs. If you attach a new Amazon VPC that has a CIDR which overlaps with an already attached Amazon VPC, Amazon Transit Gateway will not propagate the new Amazon VPC route into the Amazon Transit Gateway route table.
https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html#client-ip-pre

NEW QUESTION 86
- (Exam Topic 1)
A company needs to create and manage multiple AWS accounts for a number of departments from a central location. The security team requires read-only access to all accounts from its own AWs account. The company is using AWS Organizations and created an account tor the security team.
How should a solutions architect meet these requirements?

A. Use the OrganizationAccountAccessRole IAM role to create a new IAM policy wilh read-only access in each member accoun
B. Establish a trust relationship between the IAM policy in each member account and the security accoun

C. Ask the security team lo use the IAM policy to gain access.
D. Use the OrganizationAccountAccessRole IAM role to create a new IAM role with read-only access in each member accoun
E. Establish a trust relationship between the IAM role in each member account and the security accoun
F. Ask the security team lo use the IAM role to gain access.
G. Ask the security team to use AWS Security Token Service (AWS STS) to call the AssumeRole API for the OrganizationAccountAccessRole IAM role in the master account from the security accoun
H. Use the generated temporary credentials to gain access.
I. Ask the security team to use AWS Security Token Service (AWS STS) to call the AssumeRole API for the OrganizationAccountAccessRole IAM role in the member account from the security accoun
J. Use the generated temporary credentials to gain access.

Answer: D

NEW QUESTION 90
- (Exam Topic 1)
A company is launching a new web application on Amazon EC2 instances. Development and production workloads exist in separate AWS accounts.
According to the company's security requirements, only automated configuration tools are allowed to access the production account. The company's security team wants to receive immediate notification if any manual access to the production AWS account or EC2 instances occurs
Which combination of actions should a solutions architect take in the production account to meet these
requirements? (Select THREE.)

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

Answer: CDE

NEW QUESTION 92
- (Exam Topic 1)
A solutions architect is designing a network for a new cloud deployment. Each account will need autonomy to modify route tables and make changes. Centralized and controlled egress internet connectivity is also needed. The cloud footprint is expected to grow to thousands of AWS accounts.
Which architecture will meet these requirements?

A. A centralized transit VPC with a VPN connection to a standalone VPC in each accoun
B. Outbound internet traffic will be controlled by firewall appliances.
C. A centralized shared VPC with a subnet for each accoun
D. Outbound internet traffic will controlled through a fleet of proxy servers.
E. A shared services VPC to host central assets to include a fleet of firewalls with a route to the internet.Each spoke VPC will peer to the central VPC.
F. A shared transit gateway to which each VPC will be attache
G. Outbound internet access will route through a fleet of VPN-attached firewalls.

Answer: D

Explanation:
https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/centr
https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/centr
AWS Transit Gateway helps you design and implement networks at scale by acting as a cloud router. As your network grows, the complexity of managing incremental connections can slow you down. AWS Transit Gateway connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships -- each new connection is only made once.

NEW QUESTION 93
- (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 94
- (Exam Topic 1)
A company is creating a REST API to share information with six of its partners based in the United States. The company has created an Amazon API Gateway Regional endpoint. Each of the six partners will access the API once per day to post daily sales figures.
After initial deployment, the company observes 1.000 requests per second originating from 500 different IP addresses around the world. The company believes this traffic is originating from a botnet and wants to secure its API while minimizing cost.
Which approach should the company take to secure its API?

A. Create an Amazon CloudFront distribution with the API as the origi
B. Create an AWS WAF web ACL with a rule to block clients "hat submit more than five requests per da
C. Associate the web ACL with the CloudFront distributio
D. Configure CloudFront with an origin access identity (OAI) and associate it with the distributio
E. Configure API Gateway to ensure only the OAI can execute the POST method.
F. Create an Amazon CloudFront distribution with the API as the origi
G. Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per da
H. Associate the web ACL with the CloudFront distributio
I. Add a custom header to the CloudFront distribution populated with an API ke
J. Configure the API to require an API key on the POST method.
K. Create an AWS WAF web ACL with a rule to allow access to the IP addresses used by the six partners.Associate the web ACL with the AP
L. Create a resource policy with a request limit and associate it with the AP
M. Configure the API to require an API key on the POST method.
N. Associate the web ACL with the AP
O. Create a usage plan with a request limit and associate it with the AP
P. Create an API key and add it to the usage plan.

Answer: D

Explanation:
"A usage plan specifies who can access one or more deployed API stages and methods—and also how much and how fast they can access them. The plan uses API keys to identify API clients and meters access to the associated API stages for each key. It also lets you configure throttling limits and quota limits that are enforced on individual client API keys."
https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html

NEW QUESTION 99
- (Exam Topic 1)
A company has a project that is launching Amazon EC2 instances that are larger than required. The project's account cannot be part of the company's organization in AWS Organizations due to policy restrictions to keep this activity outside of corporate IT. The company wants to allow only the launch of t3.small EC2 instances by developers in the project's account. These EC2 instances must be restricted to the us-east-2 Region.
What should a solutions architect do to meet these requirements?

A. Create a new developer accoun
B. Move all EC2 instances, users, and assets into us-east-2. Add the account to the company's organization in AWS Organization
C. Enforce a tagging policy that denotes Region affinity.
D. Create an SCP that denies the launch of all EC2 instances except I3.small EC2 instances in us-east-2.Attach the SCP to the project's account.
E. Create and purchase a t3.small EC2 Reserved Instance for each developer in us-east-2. Assign each developer a specific EC2 instance with their name as the tag.
F. Create an IAM policy than allows the launch of only t3.small EC2 instances in us-east-2. Attach the policy to the roles and groups that the developers use in the project's account.

Answer: D

NEW QUESTION 104
- (Exam Topic 1)
A company is serving files to Its customers through an SFTP server that is accessible over the internet The SFTP server is running on a single Amazon EC2 instance with an Elastic IP address attached Customers connect to the SFTP server through its Elastic IP address and use SSH (or authentication. The EC2 instance also has an attached security group that allows access from all customer IP addresses.
A solutions architect must implement a solution to improve availability, minimize the complexity of infrastructure management, and minimize the disruption to customers who access files The solution must not change the way customers connect.
Which solution will meet these requirements?

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

T. Disassociate the Elastic IP address from the EC2 instanc
. Create a multi-attach Amazon Elastic Block Store (Amazon EBS) volume to be used for SFTP file hostin
. Create a Network Load Balancer (NLB) with the Elastic IP address attache
. Create an Auto Scaling group with EC2 instances that run an SFTP server Define in the Auto Scaling group that instances that are launched should attach the newmulti-attach EBS volume Configure the Auto Scaling group to automatically add instances behind the NLB Configure the Auto Scaling group to use the security group that allows customer IP addresses for the EC2 instances that the Auto Scaling group launche
. Sync all files from the SFTP server to the new multi-attach EBS volume.

Answer: B

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

NEW QUESTION 106
- (Exam Topic 1)
A solutions architect is building a web application that uses an Amazon RDS for PostgreSQL DB instance The DB instance is expected to receive many more reads than writes The solutions architect needs to ensure that the large amount of read traffic can be accommodated and that the DB instance is highly available. Which steps should the solutions architect take to meet these requirements? (Select THREE.)

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

Answer: BCF

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

NEW QUESTION 111
- (Exam Topic 1)
A company is moving a business-critical multi-tier application to AWS. The architecture consists of a desktop client application and server infrastructure. The server infrastructure resides in an on-premises data center that frequently fails to maintain the application uptime SLA of 99.95%. A solutions architect must re-architect the application to ensure that it can meet or exceed the SLA.
The application contains a PostgreSQL database running on a single virtual machine. The business logic and presentation layers are load balanced between multiple virtual machines. Remote users complain about slow load times while using this latency-sensitive application.
Which of the following will meet the availability requirements with little change to the application while improving user experience and minimizing costs?

A. Migrate the database to a PostgreSQL database in Amazon EC2. Host the application and presentation layers in automatically scaled Amazon ECS containers behind an Application Load Balance
B. Allocate an Amazon Workspaces Workspace for each end user to improve the user experience.
C. Migrate the database to an Amazon RDS Aurora PostgreSQL configuratio
D. Host the application and presentation layers in an Auto Scaling configuration on Amazon EC2 instances behind an Application Load Balance
E. Use Amazon AppStream 2.0 to improve the user experience.
F. Migrate the database to an Amazon RDS PostgreSQL Mulli-AZ configuratio
G. Host the application and presentation layers in automatically scaled AWS Fargate containers behind a Network Load Balance
H. Use Amazon ElastiCache to improve the user experience.
I. Migrate the database to an Amazon Redshift cluster with at least two node
J. Combine and host the application and presentation layers in automatically scaled Amazon ECS containers behind an Application Load Balance
K. Use Amazon CloudFront to improve the user experience.

Answer: B

Explanation:
Aurora would improve availability that can replicate to multiple AZ (6 copies). Auto scaling would improve the performance together with a ALB. AppStream is like Citrix that deliver hosted Apps to users.

NEW QUESTION 115
- (Exam Topic 1)
A company wants to migrate its corporate data center from on premises to the AWS Cloud. The data center includes physical servers and VMs that use VMware and Hyper-V. An administrator needs to select the correct services to collect data (or the initial migration discovery process. The data format should be supported by AWS Migration Hub. The company also needs the ability to generate reports from the data.
Which solution meets these requirements?

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

I. Use the AWS Systems Manager agent for data collection on physical server
J. Use the AWS Agentless Discovery Connector for data collection on all VM
K. Store, query, and generate reports from the collected data by using Amazon Redshift.

Answer: C

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

NEW QUESTION 118
- (Exam Topic 1)
A company needs to run a software package that has a license that must be run on the same physical host for the duration of Its use. The software package is only going to be used for 90 days The company requires patching and restarting of all instances every 30 days
How can these requirements be met using AWS?

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

Answer: B

Explanation:
Host Affinity is configured at the instance level. It establishes a launch relationship between an instance and a Dedicated Host. (This set which host the instance can run on) Auto-placement allows you to manage whether instances that you launch are launched onto a specific host, or onto any available host that has matching configurations. Auto-placement must be configured at the host level. (This sets which instance the host can run.) When affinity is set to Host, an instance launched onto a specific host always restarts on the same host if stopped. This applies to both targeted and untargeted launches.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/how-dedicated-hosts-work.html
When affinity is set to Off, and you stop and restart the instance, it can be restarted on any available host. However, it tries to launch back onto the last Dedicated Host on which it ran (on a best-effort basis).

NEW QUESTION 123
- (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 127
- (Exam Topic 1)
A company requires that all internal application connectivity use private IP addresses. To facilitate this policy, a solutions architect has created interface endpoints to connect to AWS public services. Upon testing, the solutions architect notices that the service names are resolving to public IP addresses, and that internal services cannot connect to the interface endpoints.
Which step should the solutions architect take to resolve this issue?

A. Update the subnet route table with a route to the interface endpoint.
B. Enable the private DNS option on the VPC attributes.
C. Configure the security group on the interface endpoint to allow connectivity to the AWS services.
D. Configure an Amazon Route 53 private hosted zone with a conditional forwarder for the internal application.

Answer: C

Explanation:
https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-interface.html

NEW QUESTION 130
- (Exam Topic 1)
A company has implemented an ordering system using an event-dnven architecture. Dunng initial testing, the system stopped processing orders Further tog analysis revealed that one order message in an Amazon Simple Queue Service (Amazon SOS) standard queue was causing an error on the backend and blocking all subsequent order messages The visibility timeout of the queue is set to 30 seconds, and the backend processing timeout is set to 10 seconds. A solutions architect needs to analyze faulty order messages and ensure that the system continues to process subsequent messages
Which step should the solutions architect take to meet these requirements?

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

Answer: D

NEW QUESTION 132
- (Exam Topic 1)
A company wants to control its cost of Amazon Athena usage The company has allocated a specific monthly budget for Athena usage A solutions architect must design a solution that will prevent the company from exceeding the budgeted amount
Which solution will moot these requirements?

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

Answer: D

NEW QUESTION 134
- (Exam Topic 1)
A multimedia company needs to deliver its video-on-demand (VOD) content to its subscribers in a
cost-effective way. The video files range in size from 1-15 GB and are typically viewed frequently for the first 6 months alter creation, and then access decreases considerably. The company requires all video files to remain immediately available for subscribers. There are now roughly 30.000 files, and the company anticipates doubling that number over time.
What is the MOST cost-effective solution for delivering the company's VOD content?

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

Answer: A

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

NEW QUESTION 138
- (Exam Topic 1)
A company is planning on hosting its ecommerce platform on AWS using a multi-tier web application designed for a NoSQL database. The company plans to use the us-west-2 Region as its primary Region. The company want to ensure that copies of the application and data are available in a second Region, us-west-1, for disaster recovery. The company wants to keep the time to fail over as low as possible. Failing back to the primary Region should be possible without administrative interaction after the primary service is restored.
Which design should the solutions architect use?

A. Use AWS Cloud Formation StackSets lo create the stacks in both Regions with Auto Scaling groups for the web and application tier
B. Asynchronously replicate static content between Regions using Amazon S3 cross-Region replicatio
C. Use an Amazon Route 53 DNS failover routing policy to direct users to the secondary site in us-west-1 in the event of an outag
D. Use Amazon DynamoDB global tables for the database tier.
E. Use AWS Cloud Formation StackSets to create the stacks in both Regions with Auto Scaling groups for the web and application tier
F. Asynchronously replicate static content between Regions using AmazonS3 cross-Region replicatio
G. Use an Amazon Route 53 DNS failover routing policy to direct users to the secondary site in us-west-1 in the event of an outag
H. Deploy an Amazon Aurora global database for the database tier.
I. Use AWS Service Catalog to deploy the web and application servers in both Region
J. Asynchronously replicate static content between the two Regions using Amazon S3 cross-Region replicatio
K. Use Amazon Route 53 health checks to identify a primary Region failure and update the public DNS entry listing to the secondary Region in the event of an outag
L. Use Amazon RDS for MySQL withcross-Region replication for the database tier.

M. Use AWS CloudFormation StackSets to create the stacks in both Regions using Auto Scaling groups for the web and application tier
N. Asynchronously replicate static content between Regions using Amazon S3 cross-Region replicatio
O. Use Amazon CloudFront with static files in Amazon S3, and multi-Region origins for the front-end web tie
P. Use Amazon DynamoD8 tables in each Region with scheduled backups to Amazon S3.

Answer: A

NEW QUESTION 141
- (Exam Topic 1)
A company has an internal application running on AWS that is used to track and process shipments in the company's warehouse. Currently, after the system receives an order, it emails the staff the information needed to ship a package. Once the package is shipped, the staff replies to the email and the order is marked as shipped.
The company wants to stop using email in the application and move to a serverless application model. Which architecture solution meets these requirements?

A. Use AWS Batch to configure the different tasks required lo ship a packag
B. Have AWS Batch trigger an AWS Lambda function that creates and prints a shipping labe
C. Once that label is scanne
D. as it leaves the warehouse, have another Lambda function move the process to the next step in the AWS Batch job.B.
E. When a new order is created, store the order information in Amazon SQ
F. Have AWS Lambda check the queue every 5 minutes and process any needed wor
G. When an order needs to be shipped, have Lambda print the label in the warehous
H. Once the label has been scanned, as it leaves the warehouse, have an Amazon EC2 instance update Amazon SOS.
I. Update the application to store new order information in Amazon DynamoD
J. When a new order is created, trigger an AWS Step Functions workflow, mark the orders as "in progress," and print a package label to the warehous
K. Once the label has been scanned and fulfilled, the application will trigger an AWS Lambda function that will mark the order as shipped and complete the workflow.
L. Store new order information in Amazon EF
M. Have instances pull the new information from the NFS and send that information to printers in the warehous
N. Once the label has been scanned, as it leaves the warehouse, have Amazon API Gateway call the instances to remove the order information from Amazon EFS.

Answer: C

NEW QUESTION 146
- (Exam Topic 1)
A company is migrating its three-tier web application from on-premises to the AWS Cloud. The company has the following requirements for the migration process:
• Ingest machine images from the on-premises environment.
• Synchronize changes from the on-premises environment to the AWS environment until the production cutover.
• Minimize downtime when executing the production cutover.
• Migrate the virtual machines' root volumes and data volumes.
Which solution will satisfy these requirements with minimal operational overhead?

A. Use AWS Server Migration Service (SMS) to create and launch a replication job for each tier of the applicatio
B. Launch instances from the AMIs created by AWS SM
C. After initial testing, perform a final replication and create new instances from the updated AMIs.
D. Create an AWS CLIVM Import/Export script to migrate each virtual machin
E. Schedule the script to runincrementally to maintain changes in the applicatio
F. Launch instances from the AMIs created by VM Import/Expor
G. Once testing is done, rerun the script to do a final import and launch the instances from the AMIs.
H. Use AWS Server Migration Service (SMS) to upload the operating system volume
I. Use the AWS CLI import-snaps hot command 'or the data volume
J. Launch instances from the AMIs created by AWS SMS and attach the data volumes to the instance
K. After initial testing, perform a final replication, launch new instances from the replicated AMI
L. and attach the data volumes to the instances.
M. Use AWS Application Discovery Service and AWS Migration Hub to group the virtual machines as an applicatio
N. Use the AWS CLI VM Import/Export script to import the virtual machines as AMI
O. Schedule the script to run incrementally to maintain changes in the applicatio
P. Launch instances from the AMI
Q. After initial testing, perform a final virtual machine import and launch new instances from the AMIs.

Answer: A

Explanation:
SMS can handle migrating the data volumes:
https://aws.amazon.com/about-aws/whats-new/2018/09/aws-server-migration-service-adds-support-for-migratin

NEW QUESTION 148
- (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 153
- (Exam Topic 1)
A company is running an application on Amazon EC2 instances in three environments; development, testing, and production. The company uses AMIs to deploy the EC2 instances. The company builds the AMIs by using custom deployment scripts and infrastructure orchestration tools for each release in each environment. The company is receiving errors in its deployment process. Errors appear during operating system package downloads and during application code installation from a third-party Git hosting service. The company needs deployments to become more reliable across all environments.
Which combination of steps will meet these requirements? (Select THREE).

A. Mirror the application code to an AWS CodeCommit Git repositor
B. Use the repository to build EC2 AMIs.
C. Produce multiple EC2 AMI
D. one for each environment, for each release.
E. Produce one EC2 AMI for each release for use across all environments.
F. Mirror the application code to a third-party Git repository that uses Amazon S3 storag
G. Use therepository for deployment.
H. Replace the custom scripts and tools with AWS CodeBuil
I. Update the infrastructure deployment process to use EC2 Image Builder.

Answer: ACE

NEW QUESTION 157
- (Exam Topic 1)
A company is migrating applications from on premises to the AWS Cloud. These applications power the company's internal web forms. These web forms collect data for specific events several times each quarter. The web forms use simple SQL statements to save the data to a local relational database.
Data collection occurs for each event, and the on-premises servers are idle most of the time. The company needs to minimize the amount of idle infrastructure that supports the web forms.
Which solution will meet these requirements?

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

Answer: D

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

NEW QUESTION 161
- (Exam Topic 1)
A company needs to implement a patching process for its servers. The on-premises servers and Amazon EC2 instances use a variety of tools to perform patching. Management requires a single report showing the patch status of all the servers and instances.
Which set of actions should a solutions architect take to meet these requirements?

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

Answer: A

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

NEW QUESTION 162
- (Exam Topic 2)
A finance company is storing financial records in an Amazon S3 bucket. The company persists a record for every financial transaction. According to regulatory requirements, the records cannot be modified for at least 1 year after they are written. The records are read on a regular basis and must be immediately accessible.
Which solution will meet these requirements?

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

Answer: A

NEW QUESTION 165
- (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 168
- (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 171
- (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 173
- (Exam Topic 2)
A company wants to allow its marketing team to perform SQL queries on customer records to identify market segments. The data is spread across hundreds of files. The records must be encrypted in transit and at rest. The team manager must have the ability to manage users and groups but no team members should have access to services or resources not required for the SQL queries Additionally, administrators need to audit the queries made and receive notifications when a query violates rules defined by the security team.
AWS Organizations has been used to create a new account and an AWS IAM user with administrator permissions for the team manager. Which design meets these requirements'?

A. Apply a service control policy (SCP) that allows access to IAM Amazon RD
B. and AWS CloudTrail Load customer records in Amazon RDS MySQL and train users to run queries using the AWS CL
C. Stream the query logs to Amazon CloudWatch Logs from the RDS database instance Use a subscription filter with AWS Lambda functions to audit and alarm on queries against personal data
D. Apply a service control policy (SCP) that denies access to all services except IAM Amazon Athena Amazon S3 and AWS CloudTrail Store customer record files in Amazon S3 and tram users to run queries using the CLI via Athena Analyze CloudTrail events to audit and alarm on queries against personal data
E. Apply a service control policy (SCP) that denies access to all services except IAM Amazon DynamoD
F. and AWS CloudTrail Store customer records in DynamoDB and train users to run queries using the AWS CLI Enable DynamoDB streams to track the queries that are issued and use an AWS Lambda function for real-time monitoring and alerting
G. Apply a service control policy (SCP) that allows access to IAM Amazon Athena; Amazon S3, and AWS CloudTrail Store customer records as files in Amazon S3 and train users to leverage the Amazon S3 Select feature and run queries using the AWS CLI Enable S3 object-level logging and analyze CloudTrail events to audit and alarm on queries against personal data

Answer: B

NEW QUESTION 177
- (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 178
- (Exam Topic 2)
A company is running a two-tier web-based application in an on-premises data center. The application layer consists of a single server running a stateful application. The application connects to a PostgreSQL database running on a separate server The application's user base is expected to grow significantly, so the company is migrating the application and database to AWS The solution will use Amazon Aurora PostgreSQL. Amazon EC2 Auto Scaling, and Elastic Load Balancing.
Which solution will provide a consistent user experience that will allow the application and database tiers to scale?

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

H. Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled.

Answer: C

NEW QUESTION 182
- (Exam Topic 2)
A company runs a proprietary stateless ETL application on an Amazon EC2 Linux instance. The application is a Linux binary, and the source code cannot be modified. The application is single-threaded, uses 2 GB of RAM. and is highly CPU intensive The application is scheduled to run every 4 hours and runs for up to 20 minutes A solutions architect wants to revise the architecture for the solution.
Which strategy should the solutions architect use?

A. Use AWS Lambda to run the applicatio
B. Use Amazon CloudWatch Logs to invoke the Lambda function every 4 hours
C. Use AWS Batch to run the application Use an AWS Step Functions state machine to invoke the AWS Batch job every 4 hours
D. Use AWS Fargate to run the application Use Amazon EventBridge (Amazon CloudWatch Events) to invoke the Fargate task every 4 hours
E. Use Amazon 6C2 Spot Instances to run the application Use AWS CodeDeptoy to deploy and run the application every 4 hours.

Answer: C

NEW QUESTION 186
- (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 188
- (Exam Topic 2)
A fleet of Amazon ECS instances is used to poll an Amazon SQS queue and update items in an Amazon DynamoDB database Items in the table are not being updated, and the SQS queue Is filling up Amazon CloudWatch Logs are showing consistent 400 errors when attempting to update the table The provisioned write capacity units are appropriately configured, and no throttling is occurring
What is the LIKELY cause of the failure*?

A. The ECS service was deleted
B. The ECS configuration does not contain an Auto Scaling group
C. The ECS instance task execution IAM role was modified
D. The ECS task role was modified

Answer: D

NEW QUESTION 190
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SAP-C02 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SAP-C02 Product From:

https://www.2passeasy.com/dumps/SAP-C02/

Money Back Guarantee

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