Amazon

Exam Questions AWS-Certified-Solutions-Architect-Professional

Amazon AWS Certified Solutions Architect Professional

NEW QUESTION 1
- (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 2
- (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 3
- (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 run incrementally 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 AWSSMS 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 4
- (Exam Topic 1)
A developer reports receiving an Error 403: Access Denied message when they try to download an object from an Amazon S3 bucket. The S3 bucket is accessed using an S3 endpoint inside a VPC. and is encrypted with an AWS KMS key. A solutions architect has verified that (he developer is assuming the correct IAM role in the account that allows the object to be downloaded. The S3 bucket policy and the NACL are also valid.

Which additional step should the solutions architect take to troubleshoot this issue?

A. Ensure that blocking all public access has not been enabled in the S3 bucket.
B. Verify that the IAM rote has permission to decrypt the referenced KMS key.
C. Verify that the IAM role has the correct trust relationship configured.
D. Check that local firewall rules are not preventing access to the S3 endpoint.

Answer: B

NEW QUESTION 5
- (Exam Topic 1)
A company has a new application that needs to run on five Amazon EC2 instances in a single AWS Region. The application requires high-throughput, low-latency network connections between all of the EC2 instances where the application will run. There is no requirement for the application to be fault tolerant.
Which solution will meet these requirements?

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

Answer: A

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

NEW QUESTION 6
- (Exam Topic 1)
A company runs a popular web application in an on-premises data center. The application receives four million views weekly. The company expects traffic to increase by 200% because of an advertisement that will be published soon.
The company needs to decrease the load on the origin before the increase of traffic occurs. The company does not have enough time to move the entire application to the AWS Cloud.
Which solution will meet these requirements?

A. Create an Amazon CloudFront content delivery network (CDN). Enable query forwarding to the origin.Create a managed cache policy that includes query string
B. Use an on-premises load balancer as the origi
C. Offload the DNS querying to AWS to handle CloudFront CDN traffic.
D. Create an Amazon CloudFront content delivery network (CDN) that uses a Real Time Messaging Protocol (RTMP) distributio
E. Enable query forwarding to the origi
F. Use an on-premises load balancer as the origi
G. Offload the DNS querying to AWS to handle CloudFront CDN traffic.
H. Create an accelerator in AWS Global Accelerato
I. Add listeners for HTTP and HTTPS TCP ports.Create an endpoint grou
J. Create a Network Load Balancer (NLB), and attach it to the endpoint grou
K. Point the NLB to the on-premises server
L. Offload the DNS querying to AWS to handle AWS Global Accelerator traffic.
M. Create an accelerator in AWS Global Accelerato
N. Add listeners for HTTP and HTTPS TCP ports.Create an endpoint grou
O. Create an Application Load Balancer (ALB), and attach it to the endpoint grou
P. Point the ALB to the on-premises server
Q. Offload the DNS querying to AWS to handle AWS Global Accelerator traffic.

Answer: D

NEW QUESTION 7
- (Exam Topic 1)
A company is running a containerized application in the AWS Cloud. The application is running by using Amazon Elastic Container Service (Amazon ECS) on a set Amazon EC2 instances. The EC2 instances run in an Auto Scaling group.
The company uses Amazon Elastic Container Registry (Amazon ECRJ to store its container images When a new image version is uploaded, the new image version receives a unique tag
The company needs a solution that inspects new image versions for common vulnerabilities and exposures The solution must automatically delete new image tags that have Critical or High severity findings The solution also must notify the development team when such a deletion occurs
Which solution meets these requirements?

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

H. Configure periodic image scan on the repository Configure scan results to be added to an Amazon Simple Queue Service (Amazon SQS) queue Invoke an AWS Step Functions state machine when a new message is added to the SQS queue Use the Step Functions state machine to delete the image tag for images that have Critical or High severity finding
I. Notify the development team by using Amazon Simple Email Service (Amazon SES).

Answer: C

NEW QUESTION 8
- (Exam Topic 1)
A company with global offices has a single 1 Gbps AWS Direct Connect connection to a single AWS Region. The company's on-premises network uses the connection to communicate with the company's resources in the AWS Cloud. The connection has a single private virtual interface that connects to a single VPC.
A solutions architect must implement a solution that adds a redundant Direct Connect connection in the same Region. The solution also must provide connectivity to other Regions through the same pair of Direct Connect connections as the company expands into other Regions.
Which solution meets these requirements?

A. Provision a Direct Connect gatewa
B. Delete the existing private virtual interface from the existing connectio
C. Create the second Direct Connect connectio
D. Create a new private virtual interlace on each connection, and connect both private victual interfaces to the Direct Connect gatewa
E. Connect the Direct Connect gateway to the single VPC.
F. Keep the existing private virtual interfac
G. Create the second Direct Connect connectio
H. Create a new private virtual interface on the new connection, and connect the new private virtual interface to the single VPC.
I. Keep the existing private virtual interfac
J. Create the second Direct Connect connectio
K. Create a new public virtual interface on the new connection, and connect the new public virtual interface to the single VPC.
L. Provision a transit gatewa
M. Delete the existing private virtual interface from the existing connection.Create the second Direct Connect connectio
N. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the transit gatewa
O. Associate the transit gateway with the single VPC.

Answer: A

Explanation:
A Direct Connect gateway is a globally available resource. You can create the Direct Connect gateway in any Region and access it from all other Regions. The following describe scenarios where you can use a Direct Connect gateway.
https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html

NEW QUESTION 9
- (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 the repository 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 10
- (Exam Topic 1)
A company wants to host a new global website that consists of static content. A solutions architect is working on a solution that uses Amazon CloudFront with an origin access identity <OAI) to access website content that is stored in a private Amazon S3 bucket.
During testing, the solutions architect receives 404 errors from the S3 bucket. Error messages appear only for attempts to access paths that end with a forward slash. such as example.com/path/. These requests should return the existing S3 object path/index.html. Any potential solution must not prevent CloudFront from caching the content.
What should the solutions architect do to resolve this problem?

A. Change the CloudFront origin to an Amazon API Gateway proxy 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 10
- (Exam Topic 1)
A media company uses Amazon DynamoDB to store metadata for its catalog of movies that are available to

stream. Each media item Contains user-facing content that concludes a description of the media, a list of search tags, and similar data. In addition, media items include a list of Amazon S3 key names that relate to movie files. The company stores these movie files in a single S3 bucket that has versioning enable. The company uses Amazon CloudFront to serve these movie files.
The company has 100.000 media items, and each media item can have many different S3 objects that represent different encodings of the same media S3 objects that belong to the same media item are grouped together under the same key prefix, which is a random unique ID
Because of an expiring contract with a media provider, the company must remove 2.000 media Items. The company must completely delete all DynamoDB keys and movie files on Amazon S3 that are related to these media items within 36 hours The company must ensure that the content cannot be recovered.
Which combination of actions will meet these requirements? (Select TWO.)

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

Answer: CE

NEW QUESTION 14
- (Exam Topic 1)
A company uses AWS Transit Gateway for a hub-and-spoke model to manage network traffic between many VPCs. The company is developing a new service that must be able to send data at 100 Gbps. The company needs a faster connection to other VPCs in the same AWS Region.
Which solution will meet these requirements?

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

Answer: D

NEW QUESTION 15
- (Exam Topic 1)
A company is storing data in several Amazon DynamoDB tables. A solutions architect must use a serverless architecture to make the data accessible publicly through a simple API over HTTPS. The solution must scale automatically in response to demand.
Which solutions meet these requirements? (Choose two.)

A. Create an Amazon API Gateway REST AP
B. Configure this API with direct integrations to DynamoDB by using API Gateway’s AWS integration type.
C. Create an Amazon API Gateway HTTP AP
D. Configure this API with direct integrations to Dynamo DB by using API Gateway’s AWS integration type.
E. Create an Amazon API Gateway HTTP AP
F. Configure this API with integrations to AWS Lambda functions that return data from the DynamoDB tables.
G. Create an accelerator in AWS Global Accelerato
H. Configure this accelerator with AWS Lambda@Edge function integrations that return data from the DynamoDB tables.
I. Create a Network Load Balance
J. Configure listener rules to forward requests to the appropriate AWS Lambda functions

Answer: CD

Explanation:
https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-dynamo-db.html

NEW QUESTION 17
- (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 18
- (Exam Topic 1)

A company has registered 10 new domain names. The company uses the domains for online marketing. The company needs a solution that will redirect online visitors to a specific URL for each domain. All domains and target URLs are defined in a JSON document. All DNS records are managed by Amazon Route 53.
A solutions architect must implement a redirect service that accepts HTTP and HTTPS requests.
Which combination of steps should the solutions architect take to meet these requirements with the LEAST amount of operational effort? (Choose three.)

A. Create a dynamic webpage that runs on an Amazon EC2 instanc
B. Configure the webpage to use the JSON document in combination with the event message to look up and respond with a redirect URL.
C. Create an Application Load Balancer that includes HTTP and HTTPS listeners.
D. Create an AWS Lambda function that uses the JSON document in combination with the event message to look up and respond with a redirect URL.
E. Use an Amazon API Gateway API with a custom domain to publish an AWS Lambda function.
F. Create an Amazon CloudFront distributio
G. Deploy a Lambda@Edge function.
H. Create an SSL certificate by using AWS Certificate Manager (ACM). Include the domains as Subject Alternative Names.

Answer: CEF

Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-edge-how-it-works-tutorial.ht

NEW QUESTION 19
- (Exam Topic 1)
A company is providing weather data over a REST-based API to several customers. The API is hosted by Amazon API Gateway and is integrated with different AWS Lambda functions for each API operation. The company uses Amazon Route 53 for DNS and has created a resource record of weather.example.com. The company stores data for the API in Amazon DynamoDB tables. The company needs a solution that will give the API the ability to fail over to a different AWS Region.
Which solution will meet these requirements?

A. Deploy a new set of Lambda functions in a new Regio
B. Update the API Gateway API to use an edge-optimized API endpoint with Lambda functions from both Regions as target
C. Convert the DynamoDB tables to global tables.
D. Deploy a new API Gateway API and Lambda functions in another Regio
E. Change the Route 53 DNS record to a multivalue answe
F. Add both API Gateway APIs to the answe
G. Enable target health monitorin
H. Convert the DynamoDB tables to global tables.
I. Deploy a new API Gateway API and Lambda functions in another Regio
J. Change the Route 53 DNS record to a failover recor
K. Enable target health monitorin
L. Convert the DynamoDB tables to global tables.
M. Deploy a new API Gateway API in a new Regio
N. Change the Lambda functions to global functions.Change the Route 53 DNS record to a multivalue answe
O. Add both API Gateway APIs to the answe
P. Enable target health monitorin
Q. Convert the DynamoDB tables to global tables.

Answer: C

Explanation:
https://docs.aws.amazon.com/apigateway/latest/developerguide/dns-failover.html

NEW QUESTION 24
- (Exam Topic 1)
A company wants to retire its Oracle Solaris NFS storage arrays. The company requires rapid data migration over its internet network connection to a combination of destinations for Amazon S3. Amazon Elastic File System (Amazon EFS), and Amazon FSx lor Windows File Server. The company also requires a full initial copy, as well as incremental transfers of changes until the retirement of the storage arrays. All data must be encrypted and checked for integrity.
What should a solutions architect recommend to meet these requirements?

A. Configure CloudEndur
B. Create a project and deploy the CloudEndure agent and token to the storage arra
C. Run the migration plan to start the transfer.
D. Configure AWS DataSyn
E. Configure the DataSync agent and deploy it to the local networ
F. Create a transfer task and start the transfer.
G. Configure the aws S3 sync comman
H. Configure the AWS client on the client side with credential
I. Run the sync command to start the transfer.
J. Configure AWS Transfer (or FT
K. Configure the FTP client with credential
L. Script the client to connect and sync to start the transfer.

Answer: B

NEW QUESTION 27
- (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 Amazon S3 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 28
- (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 32
- (Exam Topic 1)
A company uses a service to collect metadata from applications that the company hosts on premises. Consumer devices such as TVs and internet radios access the applications. Many older devices do not support certain HTTP headers and exhibit errors when these headers are present in responses. The company has configured an on-premises load balancer to remove the unsupported headers from responses sent to older devices, which the company identified by the User-Agent headers.
The company wants to migrate the service to AWS, adopt serverless technologies, and retain the ability to support the older devices. The company has already migrated the applications into a set of AWS Lambda functions.
Which solution will meet these requirements?

A. Create an Amazon CloudFront distribution for the metadata servic
B. Create an Application Load Balancer (ALB). Configure the CloudFront distribution to forward requests to the AL
C. Configure the ALB to invoke the correct Lambda function for each type of reques
D. Create a CloudFront function to remove the problematic headers based on the value of the User-Agent header.
E. Create an Amazon API Gateway REST API for the metadata servic
F. Configure API Gateway to invoke the correct Lambda function for each type of reques
G. Modify the default gateway responses to remove the problematic headers based on the value of the User-Agent header.
H. Create an Amazon API Gateway HTTP API for the metadata servic
I. Configure API Gateway to invoke the correct Lambda function for each type of reques
J. Create a response mapping template to remove the problematic headers based on the value of the User-Agen
K. Associate the response data mapping withthe HTTP API.
L. Create an Amazon CloudFront distribution for the metadata servic
M. Create an Application Load Balancer (ALB). Configure the CloudFront distribution to forward requests to the AL
N. Configure the ALB to invoke the correct Lambda function for each type of reques
O. Create a Lambda@Edge function that will remove the problematic headers in response to viewer requests based on the value of theUser-Agent header.

Answer: D

Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html

NEW QUESTION 37
- (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 40
- (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 theVPC peering connection.
L. Configure a virtual private gateway for the shared VPC and create customer gateways for each of the authorized 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 45
- (Exam Topic 1)
A finance company hosts a data lake in Amazon S3. The company receives financial data records over SFTP each night from several third parties. The company runs its own SFTP server on an Amazon EC2 instance in a public subnet of a VPC. After the files ate uploaded, they are moved to the data lake by a cron job that runs on the same instance. The SFTP server is reachable on DNS sftp.examWe.com through the use of Amazon Route 53.
What should a solutions architect do to improve the reliability and scalability of the SFTP solution?

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

Answer: B

Explanation:
https://aws.amazon.com/aws-transfer-family/faqs/ https://docs.aws.amazon.com/transfer/latest/userguide/what-is-aws-transfer-family.html
https://aws.amazon.com/about-aws/whats-new/2018/11/aws-transfer-for-sftp-fully-managed-sftp-for-s3/?nc1=h_

NEW QUESTION 49
- (Exam Topic 1)
A start up company hosts a fleet of Amazon EC2 instances in private subnets using the latest Amazon Linux 2 AMI. The company's engineers rely heavily on SSH access to the instances for troubleshooting.
The company's existing architecture includes the following:
- A VPC with private and public subnets, and a NAT gateway
- Site-to-Site VPN for connectivity with the on-premises environment
- EC2 security groups with direct SSH access from the on-premises environment

The company needs to increase security controls around SSH access and provide auditing of commands executed by the engineers.
Which strategy should a solutions architect use?

A. Install and configure EC2 Instance Connect on the fleet of EC2 instance
B. Remove all security group rules attached to EC2 instances that allow inbound TCP on port 22. Advise the engineers to remotely access the instances by using the EC2 Instance Connect CLI.
C. Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's device
D. Install the Amazon CloudWatch agent on all EC2 instances and send operating system audit logs to CloudWatch Logs.
E. Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's device
F. Enable AWS Config for EC2 security group resource change
G. Enable AWS Firewall Manager and apply a security group policy that automatically remediates changes to rules.
H. Create an IAM role with the AmazonSSMManagedInstanceCore managed policy attache
I. Attach the IAM role to all the EC2 instance
J. Remove all security group rules attached to the EC2 instances that allow inbound TCP on port 22. Have the engineers install the AWS Systems Manager Session Manager plugin for their devices and remotely access the instances by using the start-session API call from Systems Manager.

Answer: D

Explanation:
Allows client machines to be able to connect to Session Manager using the AWS CLI instead of going through the AWS EC2 or AWS Server Manager console. https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-working-with-install-plugin.ht https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-working-with-install-plugin.ht

NEW QUESTION 52
- (Exam Topic 1)
A company runs a popular public-facing ecommerce website. Its user base is growing quickly from a local market to a national market. The website is hosted in an on-premises data center with web servers and a MySQL database. The company wants to migrate its workload (o AWS. A solutions architect needs to create a solution to:
• Improve security
• Improve reliability Improve availability
• Reduce latency
• Reduce maintenance
Which combination of steps should the solutions architect take to meet these requirements? (Select THREE.)

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

Answer: ABE

NEW QUESTION 54
- (Exam Topic 1)
A company runs an application on AWS. An AWS Lambda function uses credentials to authenticate to an Amazon RDS tor MySQL DB instance. A security risk assessment identified that these credentials are not frequently rotated. Also, encryption at rest is not enabled for the DB instance. The security team requires that both of these issues be resolved.
Which strategy should a solutions architect recommend to remediate these security risks?

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

Answer: A

Explanation:
Parameter store can store DB credentials as secure string but CANNOT rotate secrets, hence, go with A + Cannot enable encryption on existing MySQL RDS instance, must create a new encrypted one from unencrypted snapshot.
https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets- Encrypting a unencrypted instance of DB or creating a encrypted replica of an un encrypted DB instance are not possible Hence A is the only solution possible.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html#Overview.Encryption.

NEW QUESTION 58
- (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 60
- (Exam Topic 1)
A medical company is running a REST API on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group behind an Application Load Balancer (ALB). The ALB runs in three public subnets, and the EC2 instances run in three private subnets. The company has deployed an Amazon CloudFront distribution that has the AL8 as the only origin.
Which solution should a solutions architect recommend to enhance the origin security?

A. Store a random string in AWS Secrets Manage
B. Create an AWS Lambda (unction for automatic secret rotatio
C. Configure CloudFront to inject the random string as a custom HTTP header for the origin reques
D. Create an AWS WAF web ACL rule with a string match rule for the custom heade
E. Associate the web ACL with the ALB.
F. Create an AWS WAF web ACL rule with an IP match condition of the CloudFront service IP address range
G. Associate the web ACL with the AL
H. Move the ALB into the three private subnets.
I. Store a random string in AWS Systems Manager Parameter Stor
J. Configure Parameter Store automatic rotation for the strin
K. Configure CloudFront to inject the random siring as a custom HTTP header for the origin reques
L. Inspect the value of the custom HTTP header, and block access in the ALB.
M. Configure AWS Shield Advance
N. Create a security group policy to allow connections from CloudFront service IP address range
O. Add the policy to AWS Shield Advanced, and attach the policy to the ALB.

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 62
- (Exam Topic 1)
A company runs an application that gives users the ability to search for videos and related information by using keywords that are curated from content providers. The application data is stored in an on-premises Oracle database that is 800 GB in size.
The company wants to migrate the data to an Amazon Aurora MySQL DB instance. A solutions architect plans to use the AWS Schema Conversion Tool and AWS Database Migration Service (AWS DMS) for the migration. During the migration, the existing database must serve ongoing requests. The migration must be completed with minimum downtime
Which solution will meet these requirements?

A. Create primary key indexes, secondary indexes, and referential integrity constraints in the target database before starting the migration process
B. Use AWS DMS to run the conversion report for Oracle to Aurora MySQ
C. Remediate any issues Then use AWS DMS to migrate the data
D. Use the M5 or CS DMS replication instance type for ongoing replication
E. Turn off automatic backups and logging of the target database until the migration and cutover processes are complete

Answer: B

Explanation:
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Backups.html

NEW QUESTION 65
- (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 70
- (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 71
- (Exam Topic 1)
A company is storing data on premises on a Windows file server. The company produces 5 GB of new data
daily.
The company migrated part of its Windows-based workload to AWS and needs the data to be available on a file system in the cloud. The company already has established an AWS Direct Connect connection between the on-premises network and AWS.
Which data migration strategy should the company use?

A. Use the file gateway option in AWS Storage Gateway to replace the existing Windows file server, and point the existing file share to the new file gateway.
B. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon FSx.
C. Use AWS Data Pipeline to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS).
D. Use AWS DataSync to schedule a daily task lo replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS),

Answer: B

Explanation:
https://aws.amazon.com/storagegateway/file/ https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-files-to-fsx-datasync.html
https://docs.aws.amazon.com/systems-manager/latest/userguide/prereqs-operating-systems.html#prereqs-os-win

NEW QUESTION 73
- (Exam Topic 1)
A company wants to use a third-party software-as-a-service (SaaS) application. The third-party SaaS application is consumed through several API calls. The third-party SaaS application also runs on AWS inside a VPC.
The company will consume the third-party SaaS application from inside a VPC. The company has internal security policies that mandate the use of private connectivity that does not traverse the internet. No resources that run in the company VPC are allowed to be accessed from outside the company’s VPC. All permissions must conform to the principles of least privilege.
Which solution meets these requirements?

A. Create an AWS PrivateLink interface VPC endpoin
B. Connect this endpoint to the endpoint service that the third-party SaaS application provide
C. Create a security group to limit the access to the endpoin
D. Associate the security group with the endpoint.

E. Create an AWS Site-to-Site VPN connection between the third-party SaaS application and the company VP
F. Configure network ACLs to limit access across the VPN tunnels.
G. Create a VPC peering connection between the third-party SaaS application and the company VPUpdate route tables by adding the needed routes for the peering connection.
H. Create an AWS PrivateLink endpoint servic
I. Ask the third-party SaaS provider to create an interface VPC endpoint for this endpoint servic
J. Grant permissions for the endpoint service to the specific account of the third-party SaaS provider.

Answer: A

Explanation:
Reference architecture - https://docs.aws.amazon.com/vpc/latest/privatelink/privatelink-access-saas.html Note from documentation that Interface Endpoint is at client side

NEW QUESTION 76
- (Exam Topic 1)
A company wants to change its internal cloud billing strategy for each of its business units. Currently, the cloud governance team shares reports for overall cloud spending with the head of each business unit. The company uses AWS Organizations lo manage the separate AWS accounts for each business unit. The existing tagging standard in Organizations includes the application, environment, and owner. The cloud governance team wants a centralized solution so each business unit receives monthly reports on its cloud spending. The solution should also send notifications for any cloud spending that exceeds a set threshold.
Which solution is the MOST cost-effective way to meet these requirements?

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

Answer: B

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

NEW QUESTION 78
- (Exam Topic 1)
A company is migrating an application to AWS. It wants to use fully managed services as much as possible during the migration. The company needs to store large, important documents within the application with the following requirements:
* 1. The data must be highly durable and available.
* 2. The data must always be encrypted at rest and in transit.
* 3. The encryption key must be managed by the company and rotated periodically.
Which of the following solutions should the solutions architect recommend?

A. Deploy the storage gateway to AWS in file gateway mod
B. Use Amazon EBS volume encryption using an AWS KMS key to encrypt the storage gateway volumes.
C. Use Amazon S3 with a bucket policy to enforce HTTPS for connections to the bucket and to enforce server-side encryption and AWS KMS for object encryption.
D. Use Amazon DynamoDB with SSL to connect to DynamoD
E. Use an AWS KMS key to encrypt DynamoDB objects at rest.
F. Deploy instances with Amazon EBS volumes attached to store this dat
G. Use E8S volume encryption using an AWS KMS key to encrypt the data.

Answer: B

Explanation:
Use Amazon S3 with a bucket policy to enforce HTTPS for connections to the bucket and to enforce server-side encryption and AWS KMS for object encryption.

NEW QUESTION 83
- (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 88
- (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 93
- (Exam Topic 2)
A company is running an application in the AWS Cloud. The application uses AWS Lambda functions and Amazon Elastic Container Service (Amazon ECS) containers that run with AWS Fargate technology as its primary compute. The load on the application is irregular. The application experiences long periods of no usage, followed by sudden and significant increases and decreases in traffic. The application is write-heavy and stores data in an Amazon Aurora MySQL database. The database runs on an Amazon RDS memory optimized D8 instance that is not able to handle the load.
What is the MOST cost-effective way for the company to handle the sudden and significant changes in traffic?

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

Answer: D

NEW QUESTION 97
- (Exam Topic 2)
A company has several applications running in an on-premises data center. The data center runs a mix of Windows and Linux VMs managed by VMware vCenter.
A solutions architect needs to create a plan to migrate the applications to AWS However, the solutions architect discovers that the documentation for the applications is not up to date and that mere are no complete infrastructure diagrams The company's developers lack time to discuss their applications and current usage with the solutions architect
What should the solutions architect do to gather the required information?

A. Deploy the AWS Server Migration Service (AWS SMS) connector using the OVA image on the VMware cluster to collect configuration and utilization data from the VMs
B. Use the AWS Migration Portfolio Assessment (MPA) tool to connect to each of the VMs to collect the configuration and utilization data.
C. Install the AWS Application Discovery Service on each of the VMs to collect the configuration and utilization data
D. Register the on-premises VMs with the AWS Migration Hub to collect configuration and utilization data

Answer: A

NEW QUESTION 101
- (Exam Topic 2)
A company is building a software-as-a-service (SaaS) solution on AWS. The company has deployed an Amazon API Gateway REST API with AWS Lambda integration in multiple AWS Regions and in the same production account.
The company offers tiered pricing that gives customers the ability to pay for the capacity to make a certain number of API calls per second. The premium tier offers up to 3,000 calls per second, and customers are identified by a unique API key. Several premium tier customers in various Regions report that they receive error responses of 429 Too Many Requests from multiple API methods during peak usage hours. Logs indicate that the Lambda function is never invoked.
What could be the cause of the error messages for these customers?

A. The Lambda function reached its concurrency limit.
B. The Lambda function its Region limit for concurrency.
C. The company reached its API Gateway account limit for calls per second.
D. The company reached its API Gateway default per-method limit for calls per second.

Answer: C

Explanation:
https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html#apig-reques

NEW QUESTION 106
- (Exam Topic 2)
A company wants to improve cost awareness for its Amazon EMR platform The company has aWocated budgets for each team's Amazon EMR usage When a budgetary threshold is reached a notification should be sent by email to the budget office's distribution list Teams should be able lo view their EMR cluster expenses to date A solutions architect needs to create a solution that ensures this policy is proactively and centrally enforced in a multi-account environment
Which combination of steps should the solutions architect take to meet these requirements? (Select TWO.)

A. Update the AWS CloudFormation template to include the AWS Budgets Budget resource with the NotificationsWithSubscnbers property
B. Implement Amazon CloudWatch dashboards for Amazon EMR usage
C. Create an EMR bootstrap action that runs at startup that calls the Cost Explorer API to set the budget on the cluster with the GetCostForecast and NotificationsWithSubscnbers actions
D. Create an AWS Service Catalog portfolio for each tea
E. Add each team's Amazon EMR cluster as an AWS CloudFormation template to their Service Catalog portfolio as a Product
F. Create an Amazon CloudWatch metric for billing Create a custom alert when costs exceed the budgetary threshold.

Answer: BE

NEW QUESTION 108
- (Exam Topic 2)
A company is planning to migrate an application from on premises to the AWS Cloud. The company will begin the migration by moving the application's underlying data storage to AWS The application data is stored on a shared tie system on premises, and the application servers connect to the shared We system through SMB.
A solutions architect must implement a solution that uses an Amazon S3 bucket tor shared storage Until the application Is fully migrated and code is rewritten to use native Amazon S3 APIs, the application must continue to have access to the data through SMB The solutions architect must migrate the application data to AWS to its new location while still allowing the on-premises application to access the data.
Which solution will meet these requirements?

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

Answer: A

NEW QUESTION 109
- (Exam Topic 2)
A company has an organization in AWS Organizations that has a large number of AWS accounts. One of the AWS accounts is designated as a transit account and has a transit gateway that is shared with all of the other AWS accounts AWS Site-to-Site VPN connections are configured between ail of the company's global offices and the transit account The company has AWS Config enabled on all of its accounts.
The company's networking team needs to centrally manage a list of internal IP address ranges that belong to the global offices Developers Will reference this list to gain access to applications securely.
Which solution meets these requirements with the LEAST amount of operational overhead?

A. Create a JSON file that is hosted in Amazon S3 and that lists all of the internal IP address rangesConfigure an Amazon Simple Notification Service (Amazon SNS) topic in each of the accounts that can be involved when the JSON file is update
B. Subscribe an AWS Lambda function to the SNS topic to update all relevant security group rules with Vie updated IP address ranges.
C. Create a new AWS Config managed rule that contains all of the internal IP address ranges Use the rule to check the security groups in each of the accounts to ensure compliance with the list of IP address range
D. Configure the rule to automatically remediate any noncompliant security group that is detected.
E. In the transit account, create a VPC prefix list with all of the internal IP address range
F. Use AWS Resource Access Manager to share the prefix list with all of the other account
G. Use the shared prefix list to configure security group rules is the other accounts.
H. In the transit account create a security group with all of the internal IP address range
I. Configure the security groups in me other accounts to reference the transit account's securitygroup by using a nested security group reference of *<transit-account-id>./sg-1a2b3c4d".

Answer: C

NEW QUESTION 111
- (Exam Topic 2)
A company wants to send data from its on-premises systems to Amazon S3 buckets. The company created the S3 buckets in three different accounts. The company must send the data privately without the data traveling across the internet. The company has no existing dedicated connectivity to AWS
Which combination of steps should a solutions architect take to meet these requirements? (Select TWO.)

A. Establish a networking account in the AWS Cloud Create a private VPC in the networking account Set up an AWS Direct Connect connection with a private VIF between the on-premises environment and the private VPC
B. Establish a networking account in the AWS Cloud Create a private VPC in the networking account Set up an AWS Direct Connect connection with a public VIF between the on-premises environment and the private VPC

C. Create an Amazon S3 interface endpoint in the networking account
D. Create an Amazon S3 gateway endpoint in the networking account
E. Establish a networking account in the AWS Clou
F. Create a private VPC in the networking account Peer VPCs from the accounts that host the S3 buckets with the VPC in the network account

Answer: AD

NEW QUESTION 116
- (Exam Topic 2)
A video processing company has an application that downloads images from an Amazon S3 bucket, processes the images, stores a transformed image in a second S3 bucket, and updates metadata about the image in an Amazon DynamoDB table. The application is written in Node.js and runs by using an AWS Lambda function. The Lambda function is invoked when a new image is uploaded to Amazon S3.
The application ran without incident for a while. However, the size of the images has grown significantly. The Lambda function is now failing frequently with timeout errors. The function timeout is set to its maximum value. A solutions architect needs to refactor the application's architecture to prevent invocation failures. The company does not want to manage the underlying infrastructure.
Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

A. Modify the application deployment by building a Docker image that contains the application code.Publish the image to Amazon Elastic Container Registry (Amazon ECR).
B. Create a new Amazon Elastic Container Service (Amazon ECS) task definition with a compatibility type of AWS Fargat
C. Configure the task definition to use the new image in Amazon Elastic Container Registry (Amazon ECR). Adjust the Lambda function to invoke an ECS task by using the ECS task definition when a new file arrives in Amazon S3.
D. Create an AWS Step Functions state machine with a Parallel state to invoke the Lambda function.Increase the provisioned concurrency of the Lambda function.
E. Create a new Amazon Elastic Container Service (Amazon ECS) task definition with a compatibility type of Amazon EC2. Configure the task definition to use the new image in Amazon Elastic Container Registry (Amazon ECR). Adjust the Lambda function to invoke an ECS task by using the ECS task definition when a new file arrives in Amazon S3.
F. Modify the application to store images on Amazon Elastic File System (Amazon EFS) and to store metadata on an Amazon RDS DB instanc
G. Adjust the Lambda function to mount the EFS file share.

Answer: DE

NEW QUESTION 120
- (Exam Topic 2)
A company runs an application on AWS. The company curates data from several different sources. The company uses proprietary algorithms to perform data transformations and aggregations. After the company performs E TL processes, the company stores the results in Amazon Redshift tables. The company sells this data to other companies. The company downloads the data as files from the Amazon Redshift tables and transmits the files to several data customers by using FTP. The number of data customers has grown significantly. Management of the data customers has become difficult.
The company will use AWS Data Exchange to create a data product that the company can use to share data with customers. The company wants to confirm the identities of the customers before the company shares data. The customers also need access to the most recent data when the company publishes the data.
Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS Data Exchange for APIs to share data with customer
B. Configure subscription verification In the AWS account of the company that produces the data, create an Amazon API Gateway Data API service integration with Amazon Redshif
C. Require the data customers to subscribe to the data product In the AWS account of the company that produces the data, create an AWS Data Exchange datashare by connecting AWS Data Exchange to the Redshift
D. cluste
E. Configure subscription verificatio
F. Require the data customers to subscribe to the data product.
G. Download the data from the Amazon Redshift tables to an Amazon S3 bucket periodicall
H. Use AWS Data Exchange for S3 to share data with customers.
I. Configure subscription verificatio
J. Require the data customers to subscribe to the data product Publish the Amazon Redshift data to an Open Data on AWS Data Exchang
K. Require the customers to subscribe to the data product in AWS Data Exchang
L. In the AWS account of the company that produces the data, attach IAM resource-based policies to the Amazon Redshift tables to allow access only to verified AWS accounts.

Answer: D

NEW QUESTION 123
- (Exam Topic 2)
A company is running a workload that consists of thousands of Amazon EC2 instances The workload is running in a VPC that contains several public subnets and private subnets The public subnets have a route for 0 0 0 0/0 to an existing internet gateway. The private subnets have a route for 0 0 0 0/0 to an existing NAT gateway
A solutions architect needs to migrate the entire fleet of EC2 instances to use IPv6 The EC2 instances that are in private subnets must not be accessible from the public internet
What should the solutions architect do to meet these requirements?

A. Update the existing VPC and associate a custom IPv6 CIDR block with the VPC and all subnets Update all the VPC route tables and add a route for /0 to the internet gateway
B. Update the existing VP
C. and associate an Amazon-provided IPv6 CIDR block with the VPC and all subnets Update the VPC route tables for all private subnets, and add a route for /0 to the NAT gateway
D. Update the existing VP
E. and associate an Amazon-provided IPv6 CIDR block with the VPC and ail subnets Create an egress-only internet gateway Update the VPC route tables for all private subnets, and add a route for /0 to the egress-only internet gateway
F. Update the existing VPC and associate a custom IPv6 CIDR block with the VPC and all subnets Create a new NAT gateway, and enable IPv6 support Update the VPC route tables for all private subnets and add a route for 70 to the IPv6-enabled NAT gateway.

Answer: C

NEW QUESTION 127
- (Exam Topic 2)
A company is migrating an on-premises application and a MySQL database to AWS. The application processes highly sensitive data, and new data is constantly updated in the database. The data must not be transferred over the internet. The company also must encrypt the data in transit and at rest.
The database is 5 TB in size. The company already has created the database schema in an Amazon RDS for MySQL DB instance The company has set up a 1 Gbps AWS Direct Connect connection to AWS. The company also has set up a public VIF and a private VIF. A solutions architect needs to design a solution that will migrate the data to AWS with the least possible downtime
Which solution will meet these requirements?

A. Perform a database backu
B. Copy the backup files to an AWS Snowball Edge Storage Optimized device.Import the backup to Amazon S3. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) for encryption at rest Use TLS for encryption in transit Import the data from Amazon S3 to the DB instance.
C. Use AWS Database Migration Service (AWS DMS) to migrate the data to AW
D. Create a DMS replication instance in a private subne
E. Create VPC endpoints for AWS DM
F. Configure a DMS task to copy data from the on-premises database to the DB instance by using full load plus change data capture (CDC). Use the AWS Key Management Service (AWS KMS) default key for encryption at res
G. Use TLS for encryption in transit.
H. Perform a database backu
I. Use AWS DataSync to transfer the backup files to Amazon S3 Useserver-side encryption with Amazon S3 managed encryption keys (SSE-S3) for encryption at res
J. Use TLS for encryption in transit Import the data from Amazon S3 to the DB instance.
K. Use Amazon S3 File Gateway Set up a private connection to Amazon S3 by using AWS PrivateLink.Perform a database backu
L. Copy the backup files to Amazon S3. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) for encryption at res
M. Use TLS for encryption in transi
N. Import the data from Amazon S3 to the DB instance.

Answer: D

NEW QUESTION 128
- (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 132
- (Exam Topic 2)
A company has a latency-sensitive trading platform that uses Amazon DynamoDB as a storage backend. The company configured the DynamoDB table to use on-demand capacity mode. A solutions architect needs to design a solution to improve the performance of the trading platform. The new solution must ensure high availability for the trading platform.
Which solution will meet these requirements with the LEAST latency?

A. Create a two-node DynamoDB Accelerator (DAX) cluster Configure an application to read and write data by using DAX.
B. Create a three-node DynamoDB Accelerator (DAX) cluste
C. Configure an application to read data by using DAX and to write data directly to the DynamoDB table.
D. Create a three-node DynamoDB Accelerator (DAX) cluste
E. Configure an application to read data directly from the DynamoDB table and to write data by using DAX.
F. Create a single-node DynamoD8 Accelerator (DAX) cluste
G. Configure an application to read data by using DAX and to write data directly to the DynamoD8 table.

Answer: A

NEW QUESTION 136
- (Exam Topic 2)
A solutions architect is working with a company that is extremely sensitive to its IT costs and wishes to implement controls that will result in a predictable AWS spend each month Which combination ot steps can help the company control and monitor its monthly AWS usage to achieve a cost that is as close as possible to the target amount? (Select THREE.)

A. Implement an IAM policy that requires users to specify a 'workload' tag for cost allocation when launching Amazon EC2 instances
B. Contact AWS Support and ask that they apply limits to the account so that users are not able to launch more than a certain number of instance types
C. Purchase all upfront Reserved Instances that cover 100% of the account's expected Amazon EC2 usage
D. Place conditions in the users' IAM policies that limit the number of instances they are able to launch
E. Define 'workload' as a cost allocation tag in the AWS Billing and Cost Management console
F. Set up AWS Budgets to alert and notify when a given workload is expected to exceed a defined cost

Answer: AEF

NEW QUESTION 137
- (Exam Topic 2)
A solutions architect uses AWS Organizations to manage several AWS accounts for a company. The full Organizations feature set is activated for the organization. All production AWS accounts exist under an OU that is named "production ‘’ Systems operators have full administrative privileges within these accounts by using IAM roles.
The company wants to ensure that security groups in all production accounts do not allow inbound traffic for TCP port 22. All noncompliant security groups must be remediated immediately, and no new rules that allow port 22 can be created.
Winch solution will meet these requirements?

A. Write an SCP that denies the CreateSecurityGroup action with a condition o(ec2:tngress rule with value 22. Apply the SCP to the 'production' OU.
B. Configure an AWS CloudTrail trail for all accounts Send CloudTrail logs to an Amazon S3 bucket In the Organizations management accoun
C. Configure an AWS Lambda function on the management account with permissions to assume a role in all production accounts to describe and modify security group
D. Configure Amazon S3 to invoke the Lambda function on every PutObject event on the S3 bucket Configure the Lambda function to analyze each CloudTrail event for noncompliant security group actions and to automatically remediate any issues.
E. Create an Amazon EvertBridge (Amazon CloudWatch Events) event bus in the Organizations management accoun
F. Create an AWS Cloud Formation template to deploy configurations that send CreateSecurityGroup events to the even! bus from an production accounts Configure an AWS Lambda function in the management account with permissions to assume a role «i all production accounts to describe and modify security group
G. Configure the event bus to invoke the Lambda function Configure the Lambda function to analyse each event for noncompliant security group actions and to automatically remediate any issues.
H. Create an AWS CloudFormation template to turn on AWS Config Activate the INCOMING_SSH_DISABLED AWS Config managed rule Deploy an AWS Lambda function that will run based on AWS Config findings and will remediate noncompliant resources Deploy the CloudFormation template by using a StackSet that is assigned to the "production" O
I. Apply an SCP to the OU to deny modification of the resources that the CloudFormation template provisions.

Answer: D

NEW QUESTION 139
- (Exam Topic 2)
A company is using AWS CloudFormation to deploy its infrastructure. The company is concerned that if a production CloudFormation stack is deleted, important data stored in Amazon RD5 databases or Amazon EBS volumes might also be deleted.
now can the company prevent users from accidentally deleting data m this way?

A. Modify the CloudFormation templates to add a DeletionPolicy attribute to RDS and EBS resources.
B. Configure a stack policy that disallows the deletion of RDS and EBS resources.
C. Modify IAM policies to deny deleting RDS and EBS resources that ate lagged with an "aws:cloudformation:stack-name" tag.
D. Use AWS Config rules to prevent deleting RDS and EBS resources.

Answer: A

NEW QUESTION 141
- (Exam Topic 2)
A financial company is planning to migrate its web application from on premises to AWS. The company uses a third-party security tool to monitor the inbound traffic to the application. The company has used the security tool for the last 15 years, and the tool has no cloud solutions available from its vendor. The company's security team is concerned about how to integrate the security tool with AWS technology.
The company plans to deploy the application migration to AWS on Amazon EC2 instances. The EC2 instances will run in an Auto Scaling group in a dedicated VPC. The company needs to use the security tool to inspect all packets that come in and out of the VPC. This inspection must occur in real time and must not affect the application's performance. A solutions architect must design a target architecture on AWS that is highly available within an AWS Region.
Which combination of steps should the solutions architect take to meet these requirements? (Select TWO.)

A. Deploy the security tool on EC2 instances in a new Auto Scaling group in the existing VPC.
B. Deploy the web application behind a Network Load Balancer.
C. Deploy an Application Load Balancer in front of the security tool instances.
D. Provision a Gateway Load Balancer for each Availability Zone to redirect the traffic to the security tool.
E. Provision a transit gateway to facilitate communication between VPCs.

Answer: AD

NEW QUESTION 143
- (Exam Topic 2)
A company manages hundreds of AWS accounts centrally in an organization In AWS Organizations. The company recently started to allow product teams to create and manage their own S3 access points in their accounts. The S3 access points can be accessed only within VPCs. not on the internet.
What is the MOST operationally efficient way to enforce this requirement?

A. Set the S3 access point resource policy to deny the s3CreateAccessPoint action unless the s3 AccessPointNetworkOrigin condition key evaluates to VPC.
B. Create an SCP at the root level in the organization to deny the s3: Create Access Point action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.
C. Use AWS Cloud Formation StackSets to create a new IAM policy In each AWS account that allows the s3:CreateAccessPoint action only if the s3:AccessPointNetwofkOngm condition key evaluates to VPC.
D. Set the S3 bucket policy to deny the s3:CreateAccessPoint action unless the s3: AccessPointNetworkOngin condition key evaluates to VPC.

Answer: A

NEW QUESTION 145
- (Exam Topic 2)
An external audit of a company's serverless application reveals IAM policies that grant too many permissions. These policies are attached to the company's AWS Lambda execution roles. Hundreds of the company's Lambda functions have broad access permissions, such as full access to Amazon S3 buckets and Amazon DynamoDB tables. The company wants each function to have only the minimum permissions that the function needs to complete its task.

A solutions architect must determine which permissions each Lambda function needs.
What should the solutions architect do to meet this requirement with the LEAST amount of effort?

A. Set up Amazon CodeGuru to profile the Lambda functions and search for AWS API call
B. Create an inventory of the required API calls and resources for each Lambda functio
C. Create new IAM access policies for each Lambda functio
D. Review the new policies to ensure that they meet the company's business requirements.
E. Turn on AWS CloudTrail logging for the AWS accoun
F. Use AWS Identity and Access Management Access Analyzer to generate IAM access policies based on the activity recorded in the CloudTrail log.Review the generated policies to ensure that they meet the company's business requirements.
G. Turn on AWS CloudTrail logging for the AWS accoun
H. Create a script to parse the CloudTrail log, search for AWS API calls by Lambda execution role, and create a summary repor
I. Review the repor
J. Create IAM access policies that provide more restrictive permissions for each Lambda function.
K. Turn on AWS CloudTrail logging for the AWS accoun
L. Export the CloudTrail logs to Amazon S3. Use Amazon EMR to process the CloudTrail logs in Amazon S3 and produce a report of API calls and resources used by each execution rol
M. Create a new IAM access policy for each rol
N. Export the generated roles to an S3 bucke
O. Review the generated policies to ensure that they meet the company's business requirements.

Answer: B

Explanation:
IAM Access Analyzer helps you identify the resources in your organization and accounts, such as Amazon S3 buckets or IAM roles, shared with an external entity. This lets you identify unintended access to your resources and data, which is a security risk. IAM Access Analyzer identifies resources shared with external principals by using logic-based reasoning to analyze the resource-based policies in your AWS environment.
https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html

NEW QUESTION 146
- (Exam Topic 2)
A company has VPC flow logs enabled for its NAT gateway. The company is seeing Action = ACCEPT for inbound traffic that comes from public IP address 198.51.100.2 destined for a private Amazon EC2 instance.
A solutions architect must determine whether the traffic represents unsolicited inbound connections from the internet. The first two octets of the VPC CIDR block are 203.0.
Which set of steps should the solutions architect take to meet these requirements?

A. Open the AWS CloudTrail consol
B. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interfac
C. Run a query to filter with the destination address set as "like 203.0" and the source address set as "like 198.51.100.2". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.
D. Open the Amazon CloudWatch consol
E. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interfac
F. Run a query to filter with the destination address set as "like 203.0" and the source address set as "like 198.51.100.2". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.
G. Open the AWS CloudTrail consol
H. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interfac
I. Run a query to filter with the destination address set as "like 198.51.100.2" and the source address set as "like 203.0". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.
J. Open the Amazon CloudWatch consol
K. Select the log group that contains the NAT gateway's elasticnetwork interface and the private instance's elastic network interfac
L. Run a query to filter with the destination address set as "like 198.51.100.2" and the source address set as "like 203.0". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.

Answer: D

Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/vpc-analyze-inbound-traffic-nat-gateway/ by Cloudxie says "select appropriate log"

NEW QUESTION 147
- (Exam Topic 2)
A company is running applications on AWS in a multi-account environment. The company's sales team and marketing team use separate AWS accounts in AWS Organizations.
The sales team stores petabytes of data in an Amazon S3 bucket. The marketing team uses Amazon QuickSight for data visualizations. The marketing team needs access to data that the sates team stores in the S3 bucket. The company has encrypted the S3 bucket with an AWS Key Management Service (AWS KMS) key. The marketing team has already created the IAM service role for QuickSight to provide QuickSight access in the marketing AWS account. The company needs a solution that will provide secure access to the data in the S3 bucket across AWS accounts.
Which solution will meet these requirements with the LEAST operational overhead?

A. Create a new S3 bucket in the marketing accoun
B. Create an S3 replication rule in the sales account to copy the objects to the new S3 bucket in the marketing accoun
C. Update the QuickSight permissions in the marketing account to grant access to the new S3 bucket.
D. Create an SCP to grant access to the S3 bucket to the marketing accoun
E. Use AWS Resource Access Manager (AWS RAM) to share the KMS key from the sates account with the marketing accoun
F. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.
G. Update the S3 bucket policy in the marketing account to grant access to the QuickSight rol
H. Create a KMS grant for the encryption key that is used in the S3 bucke
I. Grant decrypt access to the QuickSight rol
J. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.
K. Create an 1AM role in the sales account and grant access to the S3 bucke
L. From the marketing account,assume the 1AM role in the sales account to access the S3 bucke

M. Update the QuickSight rote, to create a trust relationship with the new 1AM role in the sales account.

Answer: D

NEW QUESTION 150
- (Exam Topic 2)
A company is developing a gene reporting device that will collect genomic information to assist researchers with collecting large samples of data from a diverse population. The device will push 8 KB of genomic data every second to a data platform that will need to process and analyze the data and provide information back to researchers The data platform must meet the following requirements:
• Provide near-real-time analytics of the inbound genomic data
• Ensure the data is flexible, parallel, and durable
• Deliver results of processing to a data warehouse
Which strategy should a solutions architect use to meet these requirements?

A. Use Amazon Kinesis Data Firehose to collect the inbound sensor data analyze the data with Kinesis client
B. and save the results to an Amazon RDS instance
C. Use Amazon Kinesis Data Streams to collect the inbound sensor data analyze the data with Kinesis clients and save the results to an Amazon Redshift duster using Amazon EMR
D. Use Amazon S3 to collect the inbound device data analyze the data from Amazon SOS with Kinesis and save the results to an Amazon Redshift duster
E. Use an Amazon API Gateway to put requests into an Amazon SQS queue analyze the data with an AWS Lambda function and save the results » an Amazon Redshift duster using Amazon EMR

Answer: A

NEW QUESTION 151
- (Exam Topic 2)
A company is using a lift-and-shift strategy to migrate applications from several on-premises Windows servers to AWS. The Windows servers will be hosted on Amazon EC2 instances in the us-east-1 Region.
The company's security policy allows the installation of migration tools on servers. The migration data must be encrypted in transit and encrypted at rest. The applications are business critical. The company needs to minimize the cutover window and minimize the downtime that results from the migration. The company wants to use Amazon CloudWatch and AWS CloudTrail for monitoring.
Which solution will meet these requirements?

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

Answer: A

NEW QUESTION 153
- (Exam Topic 2)
A digital marketing company has multiple AWS accounts that belong to various teams. The creative team uses an Amazon S3 bucket in its AWS account to securely store images and media files that are used as content for the company's marketing campaigns. The creative team wants to share the S3 bucket with the strategy team so that the strategy team can view the objects.
A solutions architect has created an IAM role that is named strategy_reviewer in the Strategy account. The solutions architect also has set up a custom AWS Key Management Service (AWS KMS) key in the Creative account and has associated the key with the S3 bucket. However, when users from the Strategy account assume the IAM role and try to access objects in the S3 bucket, they receive an Account.
The solutions architect must ensure that users in the Strategy account can access the S3 bucket. The solution must provide these users with only the minimum permissions that they need.
Which combination of steps should the solutions architect take to meet these requirements? (Select THREE.)

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

Answer: ACF

Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/cross-account-access-denied-error-s3/

NEW QUESTION 154
- (Exam Topic 2)
A company is running an application in the AWS Cloud. The application collects and stores a large amount of unstructured data in an Amazon S3 bucket. The S3 bucket contains several terabytes of data and uses the S3 Standard storage class. The data increases in size by several gigabytes every day.

The company needs to query and analyze the data. The company does not access data that is more than 1 year old. However, the company must retain all the data indefinitely for compliance reasons.
Which solution will meet these requirements MOST cost-effectively?

A. Use S3 Select to query the dat
B. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.
C. Use Amazon Redshift Spectrum to query the dat
D. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.
E. Use an AWS Glue Data Catalog and Amazon Athena to query the dat
F. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.
G. Use Amazon Redshift Spectrum to query the dat
H. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Intelligent-Tiering.

Answer: A

NEW QUESTION 156
- (Exam Topic 2)
A publishing company's design team updates the icons and other static assets that an ecommerce web application uses. The company serves the icons and assets from an Amazon S3 bucket that is hosted in the company's production account. The company also uses a development account that members of the design team can access.
After the design team tests the static assets in the development account, the design team needs to load the assets into the S3 bucket in the production account. A solutions architect must provide the design team with access to the production account without exposing other parts of the web application to the risk of unwanted changes.
Which combination of steps will meet these requirements? (Select THREE.)

A. In the production account, create a new IAM policy that allows read and write access to the S3 bucket.
B. In the development account, create a new IAM policy that allows read and write access to the S3 bucket.
C. In the production account, create a rol
D. Attach the new policy to the rol
E. Define the development account as a trusted entity.
F. In the development account, create a rol
G. Attach the new policy to the rol
H. Define the production account as a trusted entity.
I. In the development account, create a group that contains all the IAM users of the design tea
J. Attach a different IAM policy to the group to allow the sts:AssumeRole action on the role in the production account.
K. In the development account, create a group that contains all tfje IAM users of the design tea
L. Attach a different IAM policy to the group to allow the sts;AssumeRole action on the role in the development account.

Answer: ADE

NEW QUESTION 157
- (Exam Topic 2)
A software development company has multiple engineers who are working remotely. The company is running Active Directory Domain Services (AD DS) on an Amazon EC2 instance. The company's security policy states that all internal, nonpublic services that are deployed in a VPC must be accessible through a VPN Multi-factor authentication (MFA) must be used for access to a VPN.
Whet should a solution architect do to meet these requirements?

A. Create an AWS Site-to-Site VPN connection Configure integration between a VPN and AD D
B. Use an Amazon Workspaces client with MFA support enabled to establish a VPN connection.
C. Create an AWS Client VPN endpoint Create an AD Connector directory for integration with AD DS Enable MFA for AD Connector Use AWS Client VPN to establish a VPN connection.
D. Create multiple AWS Site-to-Site VPN connections by using AWS VPN CloudHub Configure integration between AWS VPN CloudHub and AD DS Use AWS Cop4ot to establish a VPN connection.
E. Create an Amazon WorkLink endpoint Configure integration between Amazon WorkLink and AD D
F. Enable MFA in Amazon WorkLink Use AWS Client VPN to establish a VPN connection.

Answer: B

NEW QUESTION 158
- (Exam Topic 2)
A company is deploying a third-party firewall appliance solution from AWS Marketplace to monitor and protect traffic that leaves the company's AWS environments. The company wants to deploy this appliance into a shared services VPC and route all outbound internet-bound traffic through the appliances.
A solutions architect needs to recommend a deployment method that prioritizes reliability and minimizes failover time between firewall appliances within a single AWS Region. The company has set up routing from the shared services VPC to other VPCs.
Which steps should the solutions architect recommend to meet these requirements? (Select THREE)

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

Answer: AC

NEW QUESTION 159
- (Exam Topic 2)
A retail company has an on-premises data center in Europe. The company also has a multi-Region AWS presence that includes the eu-west-1 and us-east-1 Regions. The company wants to be able to route network traffic from its on-premises infrastructure into VPCs in either of those Regions. The company also needs to support traffic that is routed directly between VPCs in those Regions. No single points of failure can exist on the network.
The company already has created two 1 Gbps AWS Direct Connect connections from its on-premises data center. Each connection goes into a separate Direct Connect location in Europe for high availability. These two locations are named DX-A and DX-B, respectively. Each Region has a single AWS Transit Gateway that is configured to route all inter-VPC traffic within that Region.
Which solution will meet these requirements?

A. Create a private VIF from the DX-A connection into a Direct Connect gatewa
B. Create a private VIF from the DX-B connection into the same Direct Connect gateway for high availabilit
C. Associate both the eu-west-1 and us-east-1 transit gateways with the Direct Connect gatewa
D. Peer the transit gateways with each other to support cross-Region routing.
E. Create a transit VIF from the DX-A connection into a Direct Connect gatewa
F. Associate the eu-west-1 transit gateway with this Direct Connect gatewa
G. Create a transit VIF from the DX-B connection into a separate Direct Connect gatewa
H. Associate the us-east-1 transit gateway with this separate Direct Connect gatewa
I. Peer the Direct Connect gateways with each other to support high availability and cross-Region routing.
J. Create a transit VIF from the DX-A connection into a Direct Connect gatewa
K. Create a transit VIF from the DX-B connection into the same Direct Connect gateway for high availabilit
L. Associate both the eu-west-1 and us-east-1 transit gateways with this Direct Connect gatewa
M. Configure the Direct Connect gateway to route traffic between the transit gateways.
N. Create a transit VIF from the DX-A connection into a Direct Connect gatewa
O. Create a transit VIF from the DX-B connection into the same Direct Connect gateway for high availabilit
P. Associate both the eu-west-1 and us-east-1 transit gateways with this Direct Connect gatewa
Q. Peer the transit gateways with each other to support cross-Region routing.

Answer: D

NEW QUESTION 162
- (Exam Topic 2)
A company has used infrastructure as code (laC) to provision a set of two Amazon EC2 instances. The instances have remained the same tor several years.
The company's business has grown rapidly in the past few months. In response, the company's operations team has implemented an Auto Scaling group to manage the sudden increases in traffic Company policy requires a monthly installation of security updates on all operating systems that are running.
The most recent security update required a reboot. As a result the Auto Scaling group terminated the instances and replaced them with new, unpatched instances.
Which combination of steps should a sol-tons architect recommend to avoid a recurrence of this issue? (Select TWO)

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

Answer: AC

NEW QUESTION 167
- (Exam Topic 2)
A greeting card company recently advertised that customers could send cards to their favourite celebrities through the company's platform Since the advertisement was published, the platform has received constant traffic from 10.000 unique users each second.
The platform runs on m5.xlarge Amazon EC2 instances behind an Application Load Balancer (ALB) The instances run in an Auto Scaling group and use a custom AMI that is based on Amazon Linux. The platform uses a highly available Amazon Aurora MySQL DB cluster that uses primary and reader endpoints The platform also uses an Amazon ElastiCache for Redis cluster that uses its cluster endpoint
The platform generates a new process for each customer and holds open database connections to MySQL for the duration of each customer's session However, resource usage for the platform is low.
Many customers are reporting errors when they connect to the platform Logs show that connections to the Aurora database are failing Amazon CloudWatch metrics show that the CPU load is tow across the platform and that connections to the platform are successful through the ALB.
Which solution will remediate the errors MOST cost-effectively?

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

Answer: C

NEW QUESTION 170
- (Exam Topic 2)
A company is planning to migrate its business-critical applications from an on-premises data center to AWS. The company has an on-premises installation of a Microsoft SQL Server Always On cluster. The company wants to migrate to an AWS managed database service. A solutions architect must design a heterogeneous database migration on AWS.
Which solution will meet these requirements?

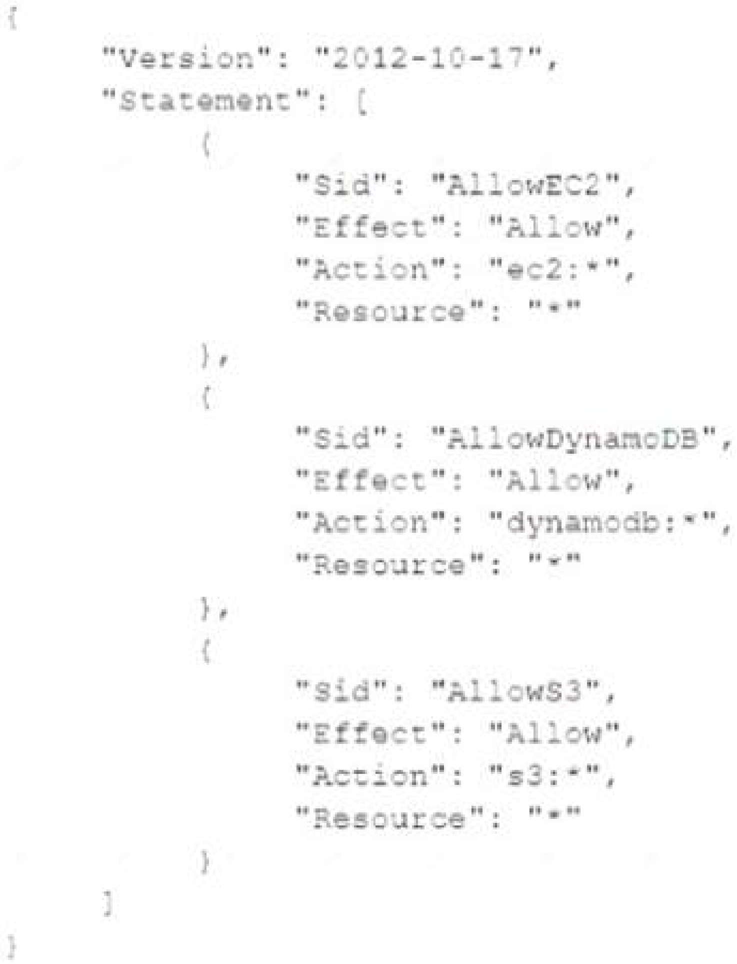
A. Migrate the SQL Server databases to Amazon RDS for MySQL by using backup and restore utilities.
B. Use an AWS Snowball Edge Storage Optimized device to transfer data to Amazon S3. Set up Amazon RDS for MySQ
C. Use S3 integration with SQL Server features, such as BULK INSERT.
D. Use the AWS Schema Conversion Tool to translate the database schema to Amazon RDS for MeSQ
E. Then use AWS Database Migration Service (AWS DMS) to migrate the data from on-premises databases to Amazon RDS.

F. Use AWS DataSync to migrate data over the network between on-premises storage and Amazon S3. Set up Amazon RDS for MySQ
G. Use S3 integration with SQL Server features, such as BULK INSERT.

Answer: C

Explanation:
https://aws.amazon.com/dms/schema-conversion-tool/

NEW QUESTION 174
- (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 176
- (Exam Topic 2)
A company is migrating a legacy application from an on-premises data center to AWS. The application uses MangeDB as a key-value database According to the company's technical guidelines, all Amazon EC2 instances must be hosted in a private subnet without an internet connection In addition, all connectivity between applications and databases must be encrypted. The database must be able to scale based on demand
Which solution will meet these requirements?

A. Create new Amazon DocumentDB (with MangeDB compatibility) tables for the application with Provisioned IOPS volumes Use the instance endpoint to connect to Amazon DocumentDB
B. Create new Amazon DynamoDB tables for the application with on-demand capacity Use a gateway VPC endpoint for DynamoDB to connect lo the DynamoDB tables
C. Create new Amazon DynamoDB tables for the application with on-demand capacity Use an interface VPC endpoint for DynamoDB to connect to the DynamoDB tables
D. Create new Amazon DocumentDB (with MangeDB compatibility) tables for the application with Provisioned IOPS volumes Use the cluster endpoint to connect to Amazon DocumentDB

Answer: C

NEW QUESTION 177
- (Exam Topic 2)
A company runs a highly available data collection application on Amazon EC2 in the eu-north-1 Region. The application collects data from end-user devices and writes records to an Amazon Kinesis data stream and a set of AWS Lambda functions that process the records The company persists the output of the record processing to an Amazon S3 bucket in eu-north-1. The company uses the data in the S3 bucket as a data source for Amazon Athena

A. In each of the Iwo new Regions set up the Lambda functions to run in a VPC Set up an S3 gateway endpoint in that VPC
B. Turn on S3 Transfer Acceleration on the S3 bucket in eu-north-1 Change the application to use the new S3 accelerated endpoint when the application uploads data to the S3 bucket
C. Create an S3 bucket in each of the two new Regions Set the application in each new Region to upload to its respective S3 bucket Set up S3 Cross-Region Replication to replicate data to the S3 bucket ineu-north-1
D. Increase the memory requirements of the Lambda functions to ensure that they have multiple cores available Use the multipart upload feature when the

application uploads data to Amazon S3 Lambda

Answer: A

NEW QUESTION 181
- (Exam Topic 2)
A company uses AWS Organizations with a single OU named Production to manage multiple accounts All accounts are members of the Production OU Administrators use deny list SCPs in the root of the organization to manage access to restricted services.
The company recently acquired a new business unit and invited the new unit's existing AWS account to the organization Once onboarded the administrators of the new business unit discovered that they are not able to update existing AWS Config rules to meet the company's policies.
Which option will allow administrators to make changes and continue to enforce the current policies without introducing additional long-term maintenance?

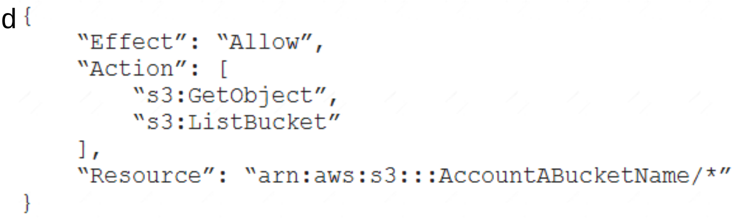
A. Remove the organization's root SCPs that limit access to AWS Config Create AWS Service Catalog products for the company's standard AWS Config rules and deploy them throughout the organization, including the new account.
B. Create a temporary OU named Onboarding for the new account Apply an SCP to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

Answer: D

Explanation:
An SCP at a lower level can't add a permission after it is blocked by an SCP at a higher level. SCPs can only filter; they never add permissions. SO you need to create a new OU for the new account assign an SCP, and move the root SCP to Production OU. Then move the new account to production OU when AWS config is done.

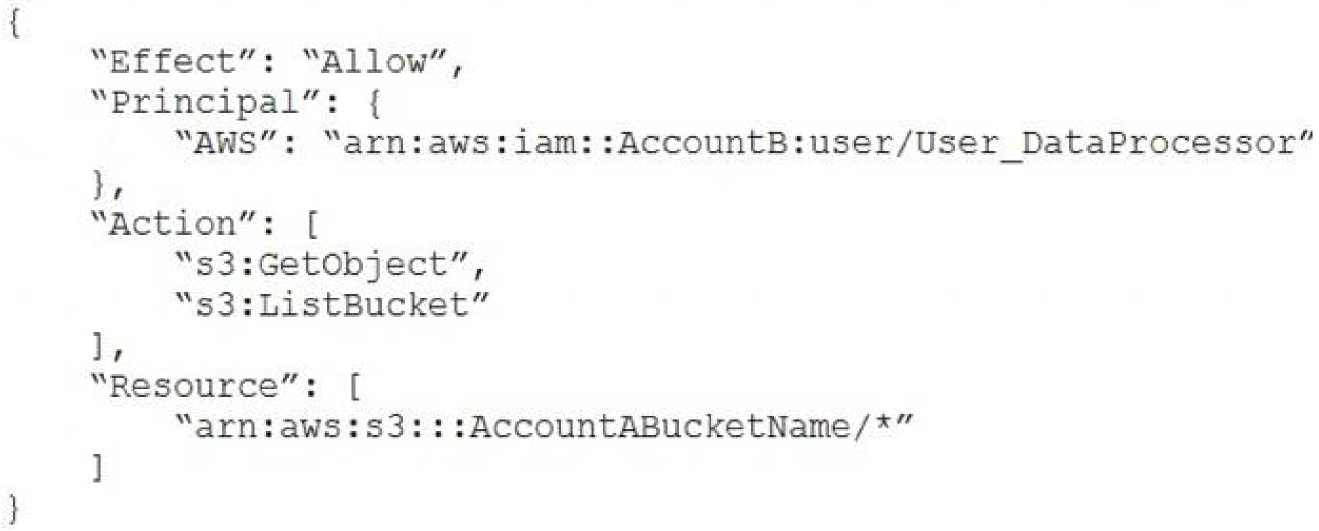
NEW QUESTION 184
- (Exam Topic 2)
A retail company needs to provide a series of data files to another company. which is its business partner. These files are saved in an Amazon S3 bucket under Account A. which belongs to the retail company. The business partner company wants one of its IAM users User_DataProcessor to access the files from its own AWS account (Account B)
Which combination of steps must the companies take so that User_DataProcessor can access the S3 bucket successfully? (Select TWO.)

A. Turn on the cross-origin resource sharing (CORS) feature for the S3 bucket in Account A.
B. In Account A, set the S3 bucket policy to the following: Text, letter Description automatically generated



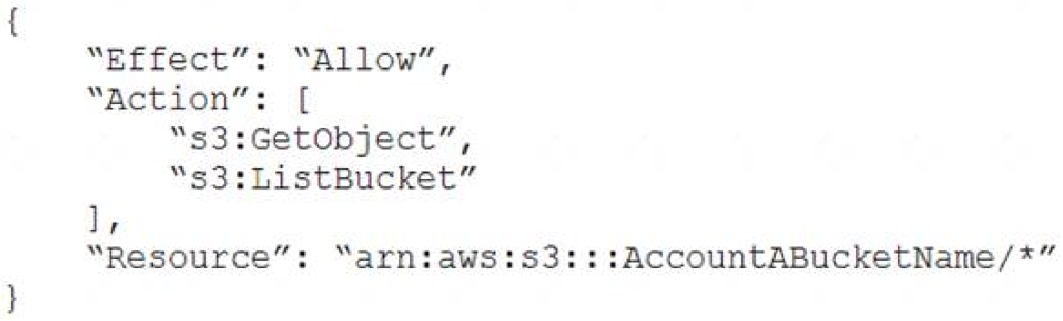
```
{
    “Effect”: “Allow”,
    “Action”: [
        “s3:GetObject”,
        “s3:ListBucket”
    ],
    “Resource”: “arn:aws:s3:::AccountABucketName/*”
}
```

C. In Account A, set the S3 bucket policy to the following:



```
{
    “Effect”: “Allow”,
    “Principal”: {
        “AWS”: “arn:aws:iam::AccountB:user/User_DataProcessor”
    },
    “Action”: [
        “s3:GetObject”,
        “s3:ListBucket”
    ],
    “Resource”: [
        “arn:aws:s3:::AccountABucketName/*”
    ]
}
```

D. In Account B, set the permissions of User_DataProcessor to the following:



```
{
    “Effect”: “Allow”,
    “Action”: [
        “s3:GetObject”,
        “s3:ListBucket”
    ],
    “Resource”: “arn:aws:s3:::AccountABucketName/*”
}
```

E. In Account B, set the permissions of User_DataProcessor to the following: Graphical user interface, text, application, email Description automatically generated

Answer: CD

Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/cross-account-access-s3/

NEW QUESTION 186
- (Exam Topic 2)
A company recently deployed a new application that runs on a group of Amazon EC2 Linux instances in a VPC In a peered VPC the company launched an EC2 Linux instance that serves as a bastion host The security group of the application instances allows access only on TCP port 22 from the private IP of the bastion host The security group of the bastion host allows access to TCP port 22 from 0 0 0.0/0 so that system administrators can use SSH to remotely log in to the application instances from several branch offices
While looking through operating system logs on the bastion host, a cloud engineer notices thousands of failed SSH logins to the bastion host from locations around the world The cloud engineer wants to change how remote access is granted to the application instances and wants to meet the following requirements:
• Eliminate brute-force SSH login attempts
• Retain a log of commands run during an SSH session
• Retain the ability to forward ports
Which solution meets these requirements for remote access to the application instances?

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

Answer: A

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

NEW QUESTION 189
- (Exam Topic 2)
A company is building a serverless application that runs on an AWS Lambda function that is attached to a VPC. The company needs to integrate the application with a new service from an external provider. The external provider supports only requests that come from public IPv4 addresses that are in an allow list.
The company must provide a single public IP address to the external provider before the application can start using the new service.
Which solution will give the application the ability to access the new service?

A. Deploy a NAT gatewa
B. Associate an Elastic IP address with the NAT gatewa
C. Configure the VPC to use the NAT gateway.
D. Deploy an egress-only internet gatewa
E. Associate an Elastic IP address with the egress-only internet gatewa
F. Configure the elastic network interface on the Lambda function to use the egress-only internet gateway.
G. Deploy an internet gatewa
H. Associate an Elastic IP address with the internet gatewa
I. Configure the Lambda function to use the internet gateway.
J. Deploy an internet gatewa
K. Associate an Elastic IP address with the internet gatewa
L. Configure the default route in the public VPC route table to use the internet gateway.

Answer: C

NEW QUESTION 191
......