Amazon-Web-Services

Exam Questions SAP-C02

AWS Certified Solutions Architect - Professional

About Exambible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1
- (Exam Topic 1)
A solutions architect is designing a publicly accessible web application that is on an Amazon CloudFront distribution with an Amazon S3 website endpoint as the origin. When the solution is deployed, the website returns an Error 403: Access Denied message.
Which steps should the solutions architect take to correct the issue? (Select TWO.)

A. Remove the S3 block public access option from the S3 bucket.
B. Remove the requester pays option trom the S3 bucket.
C. Remove the origin access identity (OAI) from the CloudFront distribution.
D. Change the storage class from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA).
E. Disable S3 object versioning.

Answer: AB

Explanation:
See using S3 to host a static website with Cloudfront: https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/
- Using a REST API endpoint as the origin, with access restricted by an origin access identity (OAI)
- Using a website endpoint as the origin, with anonymous (public) access allowed
- Using a website endpoint as the origin, with access restricted by a Referer header

NEW QUESTION 2
- (Exam Topic 1)
A solutions architect is designing the data storage and retrieval architecture for a new application that a company will be launching soon. The application is designed to ingest millions of small records per minute from devices all around the world. Each record is less than 4 KB in size and needs to be stored in a durable location where it can be retrieved with low latency. The data is ephemeral and the company is required to store the data for 120 days only, after which the data can be deleted.
The solutions architect calculates that, during the course of a year, the storage requirements would be about 10-15 TB.
Which storage strategy is the MOST cost-effective and meets the design requirements?

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

Answer: B

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

NEW QUESTION 3
- (Exam Topic 1)
A solutions architect has an operational workload deployed on Amazon EC2 instances in an Auto Scaling group. The VPC architecture spans two Availability Zones (AZ) with a subnet in each that the Auto Scaling group is targeting. The VPC is connected to an on-premises environment and connectivity cannot be interrupted. The maximum size ol the Auto Scaling group is 20 instances in service. The VPC IPv4 addressing is as follows:
VPC CIDR: 10.0.0.0/23
AZ1 subnet CIDR: 10.0.0.0/24 AZ2 subnet CIDR: 10.0.1.0/24
Since deployment, a third AZ has become available in the Region. The solutions architect wants to adopt the new AZ without adding additional IPv4 address space and without service downtime.
Which solution will meet these requirements?

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

Answer: A

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

NEW QUESTION 4
- (Exam Topic 1)
A company has developed an application that is running Windows Server on VMware vSphere VMs that the company hosts or premises. The application data is stored in a proprietary format that must be read through the application. The company manually provisioned the servers and the application.
As pan of us disaster recovery plan, the company warns the ability to host its application on AWS temporarily me company's on-premises environment becomes unavailable The company wants the application to return to on-premises hosting after a disaster recovery event is complete The RPO 15 5 minutes.
Which solution meets these requirements with the LEAST amount of operational overhead?

A. Configure AWS DataSyn
B. Replicate the data lo Amazon Elastic Block Store (Amazon EBS) volumes When the on-premises environment is unavailable, use AWS CloudFormation templates to provision Amazon EC2 instances and attach the EBS volumes
C. Configure CloudEndure Disaster Recovery Replicate the data to replication Amazon EC2 instances that are attached to Amazon Elastic Block Store (Amazon EBS) volumes When the on-premises environment is unavailable, use CloudEndure to launch EC2 instances that use the replicated volumes.
D. Provision an AWS Storage Gateway We gatewa
E. Recreate the data lo an Amazon S3 bucke
F. When the on-premises environment is unavailable, use AWS Backup to restore the data to Amazon Elastic Block Store (Amazon EBS) volumes and launch Amazon EC2 instances from these EBS volumes
G. Provision an Amazon FS* for Windows File Server file system on AWS Replicate :ne data to the «e system When the on-premoes environment is unavailable, use AWS CloudFormation templates to provision Amazon EC2 instances and use AWS :CloudFofmation::lnit commands to mount the Amazon FSx file shares

Answer: D

NEW QUESTION 5
- (Exam Topic 1)
A company wants to deploy an AWS WAF solution to manage AWS WAF rules across multiple AWS accounts. The accounts are managed under different OUs in AWS Organizations.
Administrators must be able to add or remove accounts or OUs from managed AWS WAF rule sets as needed Administrators also must have the ability to automatically update and remediate noncompliant AWS WAF rules in all accounts
Which solution meets these requirements with the LEAST amount of operational overhead?

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

Answer: B

NEW QUESTION 6
- (Exam Topic 1)
A company hosts a photography website on AWS that has global visitors. The website has experienced steady increases in traffic during the last 12 months, and users have reported a delay in displaying images. The company wants to configure Amazon CloudFront lo deliver photos to visitors with minimal latency.
Which actions will achieve this goal? (Select TWO.)

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

Answer: BD

NEW QUESTION 7
- (Exam Topic 1)
A solution architect is designing an AWS account structure for a company that consists of multiple terms. All the team will work in the same AWS Region. The company needs a VPC that is connected to the on-premises network. The company expects less than 50 Mbps of total to and from the on-premises network.
Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO)

A. Create an AWS CloudFormation template that provisions a VPC and the required subnet
B. Deploy the template to each AWS account
C. Create an AWS CloudFormabon template that provisions a VPC and the required subnet
D. Deploy the template to a shared services accoun
E. Share the subnets by using AWS Resource Access Manager
F. Use AWS Transit Gateway along with an AWS Site-to-Site VPN for connectivity to the on-premises networ
G. Share the transit gateway by using AWS Resource Access Manager

H. Use AWS Site-to-Site VPN for connectivity to the on-premises network
I. Use AWS Direct Connect for connectivity to the on-premises network.

Answer: BD

NEW QUESTION 8
- (Exam Topic 1)
A company has a three-tier application running on AWS with a web server, an application server, and an Amazon RDS MySQL DB instance. A solutions architect is designing a disaster recovery (OR) solution with an RPO of 5 minutes.
Which solution will meet the company's requirements?

A. Configure AWS Backup to perform cross-Region backups of all servers every 5 minute
B. Reprovision the three tiers in the DR Region from the backups using AWS CloudFormation in the event of a disaster.
C. Maintain another running copy of the web and application server stack in the DR Region using AWS CloudFormation drill detectio
D. Configure cross-Region snapshots ol the DB instance to the DR Region every 5 minute
E. In the event of a disaster, restore the DB instance using the snapshot in the DR Region.
F. Use Amazon EC2 Image Builder to create and copy AMIs of the web and application server to both the primary and DR Region
G. Create a cross-Region read replica of the DB instance in the DR Regio
H. In the event of a disaster, promote the read replica to become the master and reprovision the servers with AWS CloudFormation using the AMIs.
I. Create AMts of the web and application servers in the DR Regio
J. Use scheduled AWS Glue jobs to synchronize the DB instance with another DB instance in the DR Regio
K. In the event of a disaster, switch to the DB instance in the DR Region and reprovision the servers with AWS CloudFormation using the AMIs.

Answer: C

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

NEW QUESTION 9
- (Exam Topic 1)
A solutions architect must analyze a company's Amazon EC2 Instances and Amazon Elastic Block Store (Amazon EBS) volumes to determine whether the company is using resources efficiently The company is
running several large, high-memory EC2 instances lo host database dusters that are deployed in active/passive configurations The utilization of these EC2 instances varies by the applications that use the databases, and the company has not identified a pattern
The solutions architect must analyze the environment and take action based on the findings. Which solution meets these requirements MOST cost-effectively?

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

Answer: C

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

NEW QUESTION 10
- (Exam Topic 1)
A company has many services running in its on-premises data center. The data center is connected to AWS using AWS Direct Connect (DX) and an IPSec VPN. The service data is sensitive and connectivity cannot traverse the internet. The company wants to expand into a new market segment and begin offering its services to other companies that are using AWS.
Which solution will meet these requirements?

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

Answer: A

NEW QUESTION 10
- (Exam Topic 1)
An education company is running a web application used by college students around the world. The application runs in an Amazon Elastic Container Service {Amazon ECS) cluster in an Auto Scaling group behind an Application Load Balancer (ALB). A system administrator detects a weekly spike in the number of failed login attempts, which overwhelm the application's authentication service. All the failed login attempts originate from about 500 different IP addresses that change each week, A solutions architect must prevent the failed login attempts from overwhelming the authentication service.
Which solution meets these requirements with the MOST operational efficiency?

A. Use AWS Firewall Manager to create a security group and security group policy to deny access from the IP addresses.
B. Create an AWS WAF web ACL with a rate-based rule, and set the rule action to Bloc
C. Connect theweb ACL to the ALB.
D. Use AWS Firewall Manager to create a security group and security group policy to allow access only to specific CIOR ranges.

E. Create an AWS WAF web ACL with an IP set match rule, and set the rule action to Bloc
F. Connect the web ACL to the ALB.

Answer: B

Explanation:
https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-rate-based.html
The IP set match statement inspects the IP address of a web request against a set of IP addresses and address ranges. Use this to allow or block web requests based on the IP addresses that the requests originate from. By default, AWS WAF uses the IP address from the web request origin, but you can configure the rule to use an HTTP header like X-Forwarded-For instead.
https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-ipset-match.html
https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-rate-based.html

NEW QUESTION 11
- (Exam Topic 1)
A company has a photo sharing social networking application. To provide a consistent experience for users, the company performs some image processing on the photos uploaded by users before publishing on the application. The image processing is implemented using a set of Python libraries.
The current architecture is as follows:
• The image processing Python code runs in a single Amazon EC2 instance and stores the processed images in an Amazon S3 bucket named ImageBucket.
• The front-end application, hosted in another bucket, loads the images from ImageBucket to display to users. With plans for global expansion, the company wants to implement changes in its existing architecture to be able to scale for increased demand on the application and reduce management complexity as the application scales.
Which combination of changes should a solutions architect make? (Select TWO.)

A. Place the image processing EC2 instance into an Auto Scaling group.
B. Use AWS Lambda to run the image processing tasks.
C. Use Amazon Rekognition for image processing.
D. Use Amazon CloudFront in front of ImageBucket.
E. Deploy the applications in an Amazon ECS cluster and apply Service Auto Scaling.

Answer: BD

Explanation:
https://prismatic.io/blog/why-we-moved-from-lambda-to-ecs/

NEW QUESTION 13
- (Exam Topic 1)
A company is building a hybrid solution between its existing on-premises systems and a new backend in AWS. The company has a management application to monitor the state of its current IT infrastructure and automate responses to issues. The company wants to incorporate the status of its consumed AWS services into the application. The application uses an HTTPS endpoint to receive updates.
Which approach meets these requirements with the LEAST amount of operational overhead?

A. Configure AWS Systems Manager OpsCenter to ingest operational events from the on-premises systems Retire the on-premises management application and adopt OpsCenter as the hub
B. Configure Amazon EventBridge (Amazon CloudWatch Events) to detect and react to changes for AWS Health events from the AWS Personal Health Dashboard Configure the EventBridge (CloudWatch Events) event to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic and subscribe the topic to the HTTPS endpoint of the management application
C. Modify the on-premises management application to call the AWS Health API to poll for status events of AWS services.
D. Configure Amazon EventBridge (Amazon CloudWatch Events) to detect and react to changes for AWS Health events from the AWS Service Health Dashboard Configure the EventBridge (CloudWatch Events) event to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic and subscribe the topic to an HTTPS endpoint for the management application with a topic filter corresponding to the services being used

Answer: A

Explanation:
ALB & NLB both supports IPs as targets. Questions is based on TCP traffic over VPN to on-premise. TCP is layer 4 and the , load balancer should be NLB. Then next questions does NLB supports loadbalcning traffic over VPN. And answer is YEs based on below URL.
https://aws.amazon.com/about-aws/whats-new/2018/09/network-load-balancer-now-supports-aws-vpn/
Target as IPs for NLB & ALB: https://aws.amazon.com/elasticloadbalancing/faqs/?nc=sn&loc=5 https://aws.amazon.com/elasticloadbalancing/application-load-balancer/

NEW QUESTION 18
- (Exam Topic 1)
A company plans to migrate to AWS. A solutions architect uses AWS Application Discovery Service over the fleet and discovers that there is an Oracle data warehouse and several PostgreSQL databases. Which combination of migration patterns will reduce licensing costs and operational overhead? (Select TWO.)

A. Lift and shift the Oracle data warehouse to Amazon EC2 using AWS DMS.
B. Migrate the Oracle data warehouse to Amazon Redshift using AWS SCT and AWS QMS.
C. Lift and shift the PostgreSQL databases to Amazon EC2 using AWS DMS.
D. Migrate the PostgreSQL databases to Amazon RDS for PostgreSQL using AWS DMS
E. Migrate the Oracle data warehouse to an Amazon EMR managed cluster using AWS DMS.

Answer: BD

Explanation:
https://aws.amazon.com/getting-started/hands-on/migrate-oracle-to-amazon-redshift/ https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-postgresql-database

NEW QUESTION 21

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

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

Answer: D

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

NEW QUESTION 26
- (Exam Topic 1)
A company provides a centralized Amazon EC2 application hosted in a single shared VPC. The centralized application must be accessible from client applications running in the VPCs of other business units. The centralized application front end is configured with a Network Load Balancer (NLB) for scalability.
Up to 10 business unit VPCs will need to be connected to the shared VPC. Some of the business unit VPC CIDR blocks overlap with the shared VPC. and some overlap with each other. Network connectivity to the centralized application in the shared VPC should be allowed from authorized business unit VPCs only.
Which network configuration should a solutions architect use to provide connectivity from the client applications in the business unit VPCs to the centralized application in the shared VPC?

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

Answer: B

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

NEW QUESTION 28
- (Exam Topic 1)
A company is launching a new web application on Amazon EC2 instances. Development and production workloads exist in separate AWS accounts.
According to the company's security requirements, only automated configuration tools are allowed to access the production account. The company's security team wants to receive immediate notification if any manual access to the production AWS account or EC2 instances occurs
Which combination of actions should a solutions architect take in the production account to meet these
requirements? (Select THREE.)

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

Answer: CDE

NEW QUESTION 33

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

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

Answer: BCF

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

NEW QUESTION 34
- (Exam Topic 1)
A North American company with headquarters on the East Coast is deploying a new web application running on Amazon EC2 in the us-east-1 Region. The application should dynamically scale to meet user demand and maintain resiliency. Additionally, the application must have disaster recovery capabilities in an active-passive configuration with the us-west-1 Region.
Which steps should a solutions architect take after creating a VPC in the us-east-1 Region?

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

Answer: B

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

NEW QUESTION 39
- (Exam Topic 1)
A company has a data lake in Amazon S3 that needs to be accessed by hundreds of applications across many AWS accounts. The company's information security policy states that the S3 bucket must not be accessed over the public internet and that each application should have the minimum permissions necessary to function.
To meet these requirements, a solutions architect plans to use an S3 access point that is restricted to specific VPCs tor each application.
Which combination of steps should the solutions architect take to implement this solution? (Select TWO.)

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

Answer: AC

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

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

NEW QUESTION 42
- (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 43
- (Exam Topic 1)
A company has implemented an ordering system using an event-dnven architecture. Dunng initial testing, the system stopped processing orders Further tog analysis revealed that one order message in an Amazon Simple Queue Service (Amazon SOS) standard queue was causing an error on the backend and blocking all subsequent order messages The visibility timeout of the queue is set to 30 seconds, and the backend processing timeout is set to 10 seconds. A solutions architect needs to analyze faulty order messages and ensure that the system continues to process subsequent messages
Which step should the solutions architect take to meet these requirements?

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

Answer: D

NEW QUESTION 44
- (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 46
- (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 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 Ama2onSSMManagedlnstanceCore managed policy attache
I. Attach the IAM role to all the EC2 instance
J. Remove all security group rules attached to the EC2
K. 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: B

NEW QUESTION 52
- (Exam Topic 1)
A solutions architect at a largo company needs to set up network security for outbound traffic to the internet from all AWS accounts within an organization m AWS Organizations The organization has more than 100 AWS accounts, and the accounts route to each other by using a centralized AWS Transit Gateway. Each account has both an internet gateway and a NAT gateway for outbound traffic to the interne) The company deploys resources only Into a single AWS Region The company needs the ability to add centrally managed rule-based filtering on all outbound traffic to the internet for all AWS accounts in the organization The peak load of outbound traffic will not exceed 25 Gbps in each Availability Zone
Which solution meets these requirements?

A. Creates a new VPC for outbound traffic to the internet Connect the existing transit gateway to the new VPC Configure a new NAT gateway Create an Auto Scaling group of Amazon EC2 Instances that run an open-source internet proxy for rule-based filtering across all Availability Zones in the Region Modify all default routes to point to the proxy's Auto Scaling group
B. Create a new VPC for outbound traffic to the internet Connect the existing transit gateway to the new VPC Configure a new NAT gateway Use an AWS Network Firewall firewall for rule-based filtering Create Network Firewall endpoints In each Availability Zone Modify all default routes to point to the Network Firewall endpoints
C. Create an AWS Network Firewall firewal for rule-based filtering in each AWS account Modify all default routes to point to the Network Firewall firewalls in each account.
D. In each AWS account, create an Auto Scaling group of network-optimized Amazon EC2 instances that run an open-source internet proxy for rule-based filtering Modify all default routes to point to the proxy's Auto Scaling group.

Answer: B

Explanation:
https://aws.amazon.com/blogs/networking-and-content-delivery/deployment-models-for-aws-network-firewall/
https://aws.amazon.com/blogs/networking-and-content-delivery/deploy-centralized-traffic-filtering-using-aws-n

NEW QUESTION 55
- (Exam Topic 2)
A company that develops consumer electronics with offices in Europe and Asia has 60 TB of software images stored on premises in Europe. The company wants to transfer the images to an Amazon S3 bucket in the ap-northeast-1 Region. New software images are created daily and must be encrypted in transit. The company needs a solution that does not require custom development to automatically transfer all existing and new software images to Amazon S3.
What is the next step in the transfer process?

A. Deploy an AWS DataSync agent and configure a task to transfer the images to the S3 bucket.

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

Answer: A

NEW QUESTION 60
- (Exam Topic 2)
A company wants to allow its marketing team to perform SQL queries on customer records to identify market segments. The data is spread across hundreds of files. The records must be encrypted in transit and at rest. The team manager must have the ability to manage users and groups but no team members should have access to services or resources not required for the SQL queries Additionally, administrators need to audit the queries made and receive notifications when a query violates rules defined by the security team.
AWS Organizations has been used to create a new account and an AWS IAM user with administrator permissions for the team manager. Which design meets these requirements'?

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

Answer: B

NEW QUESTION 64
- (Exam Topic 2)
A company's solution architect is designing a diasaster recovery (DR) solution for an application that runs on AWS. The application uses PostgreSQL 11.7 as its database. The company has an PRO of 30 seconds. The solutions architect must design a DR solution with the primary database in the us-east-1 Region and the database in the us-west-2 Region.
What should the solution architect do to meet these requirements with minimum application change?

A. Migrate the database to Amazon RDS for PostgreSQL in us-east-1. Set up a read replica up a read replica in us-west-2. Set the managed PRO for the RDS database to 30 seconds.
B. Migrate the database to Amazon for PostgreSQL in us-east-1. Set up a standby replica in an Availability Zone in us-west-2, Set the managed PRO for the RDS database to 30 seconds.
C. Migrate the database to an Amazon Aurora PostgreSQL global database with the primary Region as us-east-1 and the secondary Region as us-west-2. Set the managed PRO for the Aurora database to 30 seconds.
D. Migrate the database to Amazon DynamoDB in us-east-1. Set up global tables with replica tables that are created in us-west-2.

Answer: A

NEW QUESTION 67
- (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 69
- (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 ranges Configure 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 72
- (Exam Topic 2)
A company is migrating its data centre from on premises to the AWS Cloud. The migration will take several months to complete. The company will use Amazon Route 53 for private DNS zones.
During the migration, the company must Keep its AWS services pointed at the VPC's Route 53 Resolver for DNS. The company also must maintain the ability to resolve addresses from its on-premises DNS server A solutions architect must set up DNS so that Amazon EC2 instances can use native Route 53 endpoints to resolve on-premises DNS queries
Which configuration writ meet these requirements?

A. Configure Vie VPC DHCP options set to point to on-premises DNS server IP addresse
B. Ensure that security groups for EC2 instances allow outbound access to port 53 on those DNS server IP addresses.
C. Launch an EC2 instance that has DNS BIND installed and configure
D. Ensure that the security groups that are attached to the EC2 instance can access the on-premises DNS server IP address on port 53. Configure BIND to forward DNS queries to on-premises DNS server IP addresses Configure each migrated EC2 instances DNS settings to point to the BIND server IP address.
E. Create a new outbound endpoint in Route 53. and attach me endpoint to the VP
F. Ensure that the security groups that are attached to the endpoint can access the on-premises DNS server IP address on port 53 Create a new Route 53 Resolver rule that routes on-premises designated traffic to theon-premises DNS server.
G. Create a new private DNS zone in Route 53 with the same domain name as the on-premises domain.Create a single wildcard record with the on-premises DNS server IP address as the record's address.

Answer: A

NEW QUESTION 76
- (Exam Topic 2)
A company owns a chain of travel agencies and is running an application in the AWS Cloud. Company employees use the application to search (or Information about travel destinations. Destination content is updated four times each year.
Two fixed Amazon EC2 instances serve the application. The company uses an Amazon Route 53 public hosted zone with a multivalue record of travel.example.com that returns the Elastic IP addresses for the EC2 instances. The application uses Amazon DynamoDB as its primary data store. The company uses a self-hosted Redis instance as a caching solution.
During content updates, the load on the EC2 instances and the caching solution increases drastically. This increased load has led to downtime on several occasions. A solutions architect must update the application so that the application is highly available and can handle the load that is generated by the content updates.
Which solution will meet these requirements?

A. Set up DynamoDB Accelerator (DAX} as in-memory cach
B. Update the application to use DA
C. Create an Auto Scaling group for the EC2 instance
D. Create an Application Load Balancer (ALB). Set the Auto Scaling group as a target for the AL
E. Update the Route 53 record to use a simple routing policy that targets the ALB's DNS alia
F. Configure scheduled scaling for the EC2 instances before the content updates.
G. Set up Amazon ElastiCache for Redi
H. Update the application to use ElastiCach
I. Create an Auto Scaling group for the EC2 instance
J. Create an AmazonCloudFront distnbutio
K. and set the Auto Scaling group as an origin for the distributio
L. Update the Route 53 record to use a simple routing policy that targets the CloudFront distribution's DNS alias Manually scale up EC2 instances before the content updates
M. Set up Amazon ElastiCache for Memcache
N. Update the application to use ElastiCach
O. Create an Auto Scaling group for the EC2 instances Create an Application Load Balancer (ALB). Set the Auto Scaling group as a target for the AL
P. Update the Route 53 record to use a simple routing policy that targets the ALB's DNS alia
Q. Configure scheduled scaling for the application before the content updates.
R. Set up DynamoDB Accelerator (DAX) as in-memory cach
S. Update the application to use DA
T. Create an Auto Scaling group for the EC2 instance
. Create an Amazon CloudFront distribution, and set the Auto Scaling group as an origin for the distributio
. Update the Route 53 record to use a simple routing policy that targets the CloudFront distribution's DNS alia
. Manually scale up EC2 instances before the content updates.

Answer: B

NEW QUESTION 78
- (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 80
- (Exam Topic 2)
A financial services company loaded millions of historical stock trades into an Amazon DynamoDB table The table uses on-demand capacity mode Once each day at midnight, a few million new records are loaded into the table Application read activity against the table happens in bursts throughout the day, and a limited set of keys are repeatedly looked up. The company needs to reduce costs associated with DynamoDB.
Which strategy should a solutions architect recommend to meet this requirement?

A. Deploy an Amazon ElastiCache cluster in front of the DynamoDB table.
B. Deploy DynamoDB Accelerator (DAX) Configure DynamoDB auto scaling Purchase Savings Plans in Cost Explorer
C. Use provisioned capacity mode Purchase Savings Plans in Cost Explorer
D. Deploy DynamoDB Accelerator (DAX) Use provisioned capacity mode Configure DynamoDB auto scaling

Answer: D

NEW QUESTION 84
- (Exam Topic 2)
A solutions architect is migrating an existing workload to AWS Fargate. The task can only run in a private subnet within the VPC where there is no direct connectivity from outside the system to the application When the Fargate task is launched the task fails with the following error:

```
CannotPullContainerError: API error (500): Get https://111122223333.dkr.ecr.us-east-1.amazonaws.com/v2/: net/http: request canceled
while waiting for connection
```

How should the solutions architect correct this error?

A. Ensure the task is set to ENABLED for the auto-assign public IP setting when launching the task
B. Ensure the task is set to DISABLED (or the auto-assign public IP setting when launching the task Configure a NAT gateway in the public subnet in the VPC to route requests to the internet
C. Ensure the task is set to DISABLED for the auto-assign public IP setting when launching the task Configure a NAT gateway in the private subnet in the VPC to route requests to the internet
D. Ensure the network mode is set to bridge in the Fargate task definition

Answer: B

NEW QUESTION 86
- (Exam Topic 2)
A company is running a critical application that uses an Amazon RDS for MySQL database to store data. The RDS DB instance is deployed in Multi-AZ mode. A recent RDS database failover test caused a 40-second outage to the application A solutions architect needs to design a solution to reduce the outage time to less than 20 seconds.
Which combination of steps should the solutions architect take to meet these requirements? (Select THREE.)

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

Answer: ABF

NEW QUESTION 88
- (Exam Topic 2)
A company is running its solution on AWS in a manually created VPC. The company is using AWS Cloud Formation to provision other parts of the infrastructure. According to a new requirement, the company must manage all infrastructure in an automatic way.
What should the company do to meet this new requirement with the LEAST effort?

A. Create a new AWS Cloud Development Kit (AWS CDK) stack that stnctly provisions the existing VPC resources and configuratio
B. Use AWS CDK to import the VPC into the stack and to manage the VPC.
C. Create a CloudFormation stack set that creates the VP
D. Use the stack set to import the VPC into the stack.
E. Create a new CloudFormation template that strictly provisions the existing VPC resources and configuratio
F. From the CloudFormation console, create a new stack by importing the existing resources.
G. Create a new CloudFormation template that creates the VP

H. Use the AWS Serverless Application Model {AWS SAM) CLI to import the VPC.

Answer: D

NEW QUESTION 91
- (Exam Topic 2)
A company runs a software-as-a-service (SaaS) application on AWS. The application comets of AWS Lambda function and an Amazon RDS for MySQL Multi-AZ database During market events the application has a much higher workload than normal Users notice slow response times during the peak periods because of many database connections. The company needs to improve the scalable performance and availability of the database.
Which solution meets these requirements?

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

Answer: D

NEW QUESTION 94
- (Exam Topic 2)
A company has an organization that has many AWS accounts in AWS Organizations A solutions architect must improve how the company manages common security group rules for the AWS accounts in the organization.
The company has a common set of IP CIDR ranges in an allow list in each AWS account lo allow access to and from the company's on-premises network Developers within each account are responsible for adding new IP CIDR ranges to their security groups. The security team has its own AWS account. Currently, the security team notifies the owners of the other AWS accounts when changes are made to the allow list.
The solutions architect must design a solution that distributes the common set of CIDR ranges across all accounts Which solution meets these requirements with the LEAST amount of operational overhead.

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

Answer: A

NEW QUESTION 95
- (Exam Topic 2)
A company's site reliability engineer is performing a review of Amazon FSx for Windows File Server deployments within an account that the company acquired Company policy states that all Amazon FSx file systems must be configured to be highly available across Availability Zones.
During the review, the site reliability engineer discovers that one of the Amazon FSx file systems used a deployment type of Single-AZ 2 A solutions architect needs to minimize downtime while aligning this Amazon FSx file system with company policy.
What should the solutions architect do to meet these requirements?

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

Answer: B

NEW QUESTION 97
- (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 98
- (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 99
- (Exam Topic 2)
A company is using multiple AWS accounts The DNS records are stored in a private hosted zone for Amazon Route 53 in Account A The company's applications and databases are running in Account B.
A solutions architect win deploy a two-net application In a new VPC To simplify the configuration, the db.example com CNAME record set tor the Amazon RDS endpoint was created in a private hosted zone for Amazon Route 53.
During deployment, the application failed to start. Troubleshooting revealed that db.example com is not resolvable on the Amazon EC2 instance The solutions architect confirmed that the record set was created correctly in Route 53.
Which combination of steps should the solutions architect take to resolve this issue? (Select TWO J

A. Deploy the database on a separate EC2 instance in the new VPC Create a record set for the instance's private IP in the private hosted zone
B. Use SSH to connect to the application tier EC2 instance Add an RDS endpoint IP address to the/eto/resolv.conf file
C. Create an authorization lo associate the private hosted zone in Account A with the new VPC In Account B
D. Create a private hosted zone for the example.com domain m Account B Configure Route 53 replicationbetween AWS accounts
E. Associate a new VPC in Account B with a hosted zone in Account
F. Delete the association authorization In Account A.

Answer: CE

NEW QUESTION 103
- (Exam Topic 2)
A company runs an loT platform on AWS loT sensors in various locations send data to the company's Node js API servers on Amazon EC2 instances running behind an Application Load Balancer The data is stored in an Amazon RDS MySQL DB instance that uses a 4 TB General Purpose SSD volume
The number of sensors the company has deployed in the field has increased over time and is expected to grow significantly The API servers are consistently overloaded and RDS metrics show high write latency
Which of the following steps together will resolve the issues permanently and enable growth as new sensors are provisioned, while keeping this platform cost-efficient? {Select TWO.)

A. Resize the MySQL General Purpose SSD storage to 6 TB to improve the volume's IOPS
B. Re-architect the database tier to use Amazon Aurora instead of an RDS MySQL DB instance and add read replicas
C. Leverage Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data
D. Use AWS X-Ray to analyze and debug application issues and add more API servers to match the load
E. Re-architect the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance

Answer: CE

NEW QUESTION 106
- (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 109
- (Exam Topic 2)

A company deploys a new web application As part of the setup, the company configures AWS WAF to log to Amazon S3 through Amazon Kinesis Data Firehose. The company develops an Amazon Athena query that runs once daily to return AWS WAF log data from the previous 24 hours. The volume of daily logs is constant However over time, the same query is taking more time to run
A solutions architect needs to design a solution to prevent the query time from continuing to increase. The solution must minimize operational overhead
Which solution will meet these requirements?

A. Create an AWS Lambda function that consolidates each day's AWS WAF logs into one log file
B. Reduce the amount of data scanned by configuring AWS WAF to send logs to a different S3 bucket each day
C. Update the Kinesis Data Firehose configuration to partition the data in Amazon S3 by date and time Create external tables for Amazon Redshift Configure Amazon Redshift Spectrum to query the data source
D. Modify the Kinesis Data Firehose configuration and Athena table definition to partition the data by date and tim
E. Change the Athena query to view the relevant partitions

Answer: D

NEW QUESTION 114
- (Exam Topic 2)
A company processes environmental data. The company has set up sensors to provide a continuous stream of data from different areas in a city. The data is available in JSON format.
The company wants to use an AWS solution to send the data to a database that does not require fixed schemas for storage. The data must be sent in real time.
Which solution will meet these requirements?

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

Answer: B

NEW QUESTION 115
- (Exam Topic 2)
An ecommerce company runs its infrastructure on AWS. The company exposes its APIs to its web and mobile clients through an Application Load Balancer (ALB) in front of an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The EKS cluster runs thousands of pods that provide the APIs.
After extending delivery to a new continent, the company adds an Amazon CloudFront distribution and sets the ALB as the origin. The company also adds AWS WAF to its architecture.
After implementation of the new architecture, API calls are significantly. However, there is a sudden increase in HTTP status code 504 (Gateway Timeout) errors and HTTP status code 502 (Bad Gateway) errors. This increase in errors seems to be for a specific domain. Which factors could be a cause of these errors? (Select TWO.)

A. AWS WAF is blocking suspicious requests.
B. The origin is not properly configured in CloudFront.
C. There is an SSL/TLS handshake issue between CloudFront and the origin.
D. EKS Kubernetes pods are being cycled.
E. Some pods are taking more than 30 seconds to answer API calls.

Answer: AE

NEW QUESTION 120
- (Exam Topic 2)
A company has introduced a new policy that allows employees to work remotely from their homes if they connect by using a VPN The company Is hosting Internal applications with VPCs in multiple AWS accounts Currently the applications are accessible from the company's on-premises office network through an AWS Site-to-Site VPN connection The VPC in the company's main AWS account has peering connections established with VPCs in other AWS accounts.
A solutions architect must design a scalable AWS Client VPN solution for employees to use while they work from home
What is the MOST cost-effective solution that meets these requirements?

A. Create a Client VPN endpoint in each AWS account Configure required routing that allows access to internal applications
B. Create a Client VPN endpoint in the mam AWS account Configure required routing that allows access to internal applications
C. Create a Client VPN endpoint in the main AWS account Provision a transit gateway that is connected to each AWS account Configure required routing that allows access to internal applications
D. Create a Client VPN endpoint in the mam AWS account Establish connectivity between the Client VPN endpoint and the AWS Site-to-Site VPN

Answer: C

NEW QUESTION 122
- (Exam Topic 2)
A company has a web application that securely uploads pictures and videos to an Amazon S3 bucket The company requires that only authenticated users are allowed to post content T.he application generates a presigned URL that is used to upload objects through a browser interface. Most users are reporting slow upload times for objects larger than 100 MB
What can a solutions architect do to improve the performance of these uploads while ensuring only authenticated users are allowed to post content?

A. Set up an Amazon API Gateway with an edge-optimized API endpoint that has a resource as an S3 service proxy Configure the PUT method for this resource to expose the S3 Putobject operation Secure the API Gateway using a cognito_user_pools authonzer Have the browser interface use API Gateway instead of the presigned URL to upload objects
B. Set up an Amazon API Gateway with a regional API endpoint that has a resource as an S3 service proxyConfigure the PUT method for this resource to expose the S3 Putobject operation Secure the API Gateway using an AWS Lambda authonzer Have the browser interface use API Gateway instead of the presigned URL to upload objects
C. Enable an S3 Transfer Acceleration endpoint on the S3 bucket Use the endpoint when generating the presigned URL Have the browser interface upload the objects to this URL using the S3 multipart upload API
D. Configure an Amazon CloudFront distribution for the destination S3 bucket Enable PUT and POST methods for the CloudFront cache behavior Update the

CloudFront origin to use an origin access identity (OAI) Give the OAl user s 3: Putobject permissions in the bucket policy Have the browser interface upload objects using the CloudFront distribution

Answer: D

NEW QUESTION 125
- (Exam Topic 2)
A software company is using three AWS accounts for each of its 1 0 development teams The company has developed an AWS CloudFormation standard VPC template that includes three NAT gateways The template is added to each account for each team The company is concerned that network costs will increase each time a new development team is added A solutions architect must maintain the reliability of the company's solutions and minimize operational complexity
What should the solutions architect do to reduce the network costs while meeting these requirements?

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

Answer: A

NEW QUESTION 126
- (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 131
- (Exam Topic 2)
An enterprise company wants to allow its developers to purchase third-party software through AWS Marketplace. The company uses an AWS Organizations account structure with full features enabled, and has a shared services account in each organizational unit (OU) that will be used by procurement managers. The procurement team's policy indicates that developers should be able to obtain third-party software from an approved list only and use Private Marketplace in AWS Marketplace to achieve this requirement . The procurement team wants administration of Private Marketplace to be restricted to a role named procurement-manager-role, which could be assumed by procurement managers Other IAM users groups, roles, and account administrators in the company should be denied Private Marketplace administrative access
What is the MOST efficient way to design an architecture to meet these requirements?

A. Create an IAM role named procurement-manager-role in all AWS accounts in the organization Add the PowerUserAccess managed policy to the role Apply an inline policy to all IAM users and roles in every AWS account to deny permissions on the AWSPrivateMarketplaceAdminFullAccess managed policy.
B. Create an IAM role named procurement-manager-role in all AWS accounts in the organization Add the AdministratorAccess managed policy to the role Define a permissions boundary with the AWSPrivateMarketplaceAdminFullAccess managed policy and attach it to all the developer roles.
C. Create an IAM role named procurement-manager-role in all the shared services accounts in the organization Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role Create an organization root-level SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role Create another organization root-level SCP to deny permissions to create an IAM role named procurement-manager-role to everyone in the organization.
D. Create an IAM role named procurement-manager-role in the AWS accounts that will be used by developers Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the rol
E. Create....Organizations to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role Apply the SCP to all the shared services accounts in the.....

Answer: C

NEW QUESTION 134
- (Exam Topic 2)
A company that uses AWS Organizations is creating several new AWS accounts. The company is setting up controls to properly allocate AWS costs to business units. The company must Implement a solution to ensure that all resources include a tag that has a key of costcenter and a value from a predefined list of business units. The solution must send a notification each time a resource tag does not meet these criteria. The solution must not prevent the creation of resources.
Which solution will meet these requirements with the LEAST operational overhead?

A. Create an 1AM policy for all actions that create AWS resource
B. Add a condition to the policy that aws:RequestTag/costcenter must exist and must contain a valid business unit valu
C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that monitors 1AM service events and Amazon EC2 service events for noncompliant tag policie
D. Configure the rule to send notifications through Amazon Simple Notification Service (Amazon SNS).
E. Create an 1AM policy for all actions that create AWS resource
F. Add a condition to the policy that awsResourceTag/costcenter must exist and must contain avalid business unit value Create an Amazon EventBridge (Amazon

CloudWatch Events) rule that monitors 1AM service events and Amazon EC2 service events for noncompliant tag policie
G. Configure the rule to send notifications through Amazon Simple Notification Service (Amazon SNS).
H. Create an organization tag policy that ensures that all resources have the costcenter tag with a valid business unit valu
I. Do not select the option to prevent operations when tags are noncomplian
J. Create an Amazon Event8ridge (Amazon CloudWatch Events) rule that monitors all events for noncompliant tag policie
K. Configure the rule to send notifications through Amazon Simple Notification Service (Amazon SNS).
L. Create an organization tag policy that ensures that all resources have the costcenter tag with a valid business unit valu
M. Select the option to prevent operations when tags are noncompliant Create an Amazon EventBridge (Amazon CloudWatch Events) rule that monitors all events for noncompliant tag policie
N. Configure the rule to send notifications through Amazon Simple Notification Service (Amazon SNS).

Answer: B

NEW QUESTION 138
- (Exam Topic 2)
A company uses AWS Cloud Formation to deploy applications within multiple VPCs that are all attached to a transit gateway. Each VPC that sends traffic to the public internet must send the traffic through a shared services VPC. Each subnet within a VPC uses the default VPC route table, and the traffic is routed to the transit gateway. The transit gateway uses its default route table for any VPC attachment.
A security audit reveals that an Amazon EC2 instance that is deployed within a VPC can communicate with an EC2 instance that is deployed in any of the company's other VPCs. A solutions architect needs to limit the traffic between the VPCs. Each VPC must be able to communicate only with a predefined, limited set of authorized VPCs.
What should the solutions architect do to meet these requirements?

A. Update the network ACL of each subnet within a VPC to allow outbound traffic only to the authorized VPC
B. Remove all deny rules except the default deny rule.
C. Update all the security groups that are used within a VPC to deny outbound traffic to security groups that are used within the unauthorized VPCs
D. Create a dedicated transit gateway route table for each VPC attachmen
E. Route traffic only to the authorized VPCs.
F. Update the main route table of each VPC to route traffic only to the authorized VPCs through the transit gateway.

Answer: A

NEW QUESTION 142
- (Exam Topic 2)
A company is hosting a critical application on a single Amazon EC2 instance. The application uses an Amazon ElastiCache for Redis single-node cluster for an in-memory data store. The application uses an Amazon RDS for MariaDB DB instance for a relational database. For the application to function, each piece of the infrastructure must be healthy and must be in an active state.
A solutions architect needs to improve the application's architecture so that the infrastructure can automatically recover from failure with the least possible downtime.
Which combination of steps will meet these requirements? (Select THREE.)

A. Use an Elastic Load Balancer to distribute traffic across multiple EC2 instance
B. Ensure that the EC2 instances are part of an Auto Scaling group that has a minimum capacity of two instances.
C. Use an Elastic Load Balancer to distribute traffic across multiple EC2 instances Ensure that the EC2 instances are configured in unlimited mode.
D. Modify the DB instance to create a read replica in the same Availability Zon
E. Promote the read replica to be the primary DB instance in failure scenarios.
F. Modify the DB instance to create a Multi-AZ deployment that extends across two Availability Zones.
G. Create a replication group for the ElastiCache for Redis cluste
H. Configure the cluster to use an Auto Scaling group that has a minimum capacity of two instances.
I. Create a replication group for the ElastiCache for Redis cluste
J. Enable Multi-AZ on the cluster.

Answer: CDE

NEW QUESTION 147
- (Exam Topic 2)
A company wants to migrate its data analytics environment from on premises to AWS The environment consists of two simple Node js applications One of the applications collects sensor data and loads it into a MySQL database The other application aggregates the data into reports When the aggregation jobs run. some of the load jobs fail to run correctly
The company must resolve the data loading issue The company also needs the migration to occur without interruptions or changes for the company's customers
What should a solutions architect do to meet these requirements'?

A. Set up an Amazon Aurora MySQL database as a replication target for the on-premises database Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica Set up collection endpomts as AWS Lambda functions behind a Network Load Balancer (NLB). and use Amazon RDS Proxy to wnte to the Aurora MySQL database When the databases are synced disable the replication job and restart the Aurora Replica as the primary instanc
B. Point the collector DNS record to the NLB.
C. Set up an Amazon Aurora MySQL database Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora Move the aggregation jobs to run against the Aurora MySQL database Set up collection endpomts behind an Application Load Balancer (ALB) as Amazon EC2 instances in an Auto Scaling group When the databases are synced, point the collector DNS record to the ALB Disable the AWS DMS sync task after the cutover from on premises to AWS
D. Set up an Amazon Aurora MySQL database Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora Create an Aurora Replica for the Aurora MySQL database and move the aggregation jobs to run against the Aurora Replica Set up collection endpoints as AWS Lambda functions behind an Application Load Balancer (ALB) and use Amazon RDS Proxy to write to the Aurora MySQL database When the databases are synced, point the collector DNS record to the ALB Disable the AWS DMS sync task after the cutover from on premises to AWS
E. Set up an Amazon Aurora MySQL database Create an Aurora Replica for the Aurora MySQL database and move the aggregation jobs to run against the Aurora Replica Set up collection endpoints as an Amazon Kinesis data stream Use Amazon Kinesis Data Firehose to replicate the data to the Aurora MySQL database When the databases are synced disable the replication job and restart the Aurora Replica as the primary instance Point the collector DNS record to the Kinesis data stream.

Answer: C

NEW QUESTION 149
- (Exam Topic 2)
A company is using an existing orchestration tool to manage thousands of Amazon EC2 instances. A recent penetration test found a vulnerability in the company's software stack. This vulnerability has prompted the company to perform a full evaluated of its current production environment The analysts determined that the following vulnerabilities exist within the environment:
• Operating systems with outdated libraries and known vulnerabilities are being used in production
• Relational databases hosted and managed by the company are running unsupported versions with known vulnerabilities
• Data stored in databases Is not encrypted.
The solutions architect intends to use AWS Config to continuously audit and assess the compliance of the company's AWS resource configurations with the company's polices and guidelines What additional steps will enable the company to secure its environments and track resources while adhering to best practices?

A. Use AWS Application Discovery Service to evaluate at running EC2 instances Use the AWS CLI lo modify each instance, and use EC2 user data to install the AWS SystemsManager Agent during boot Schedule patching to run as a Systems Manager Maintenance Windowstas
B. Migrate all relational databases lo Amazon RDS and enable AWS KMS encryption
C. Create an AWS CloudFormation template for the EC2 instances Use EC2 user data in the CloudFormation template to install the AWS Systems Manager Agent, and enable AWS KMS encryption on all Amazon EBS volume
D. Have CloudFormation replace al running instance
E. Use Systems Manager Patch Manager to establish a patch baseline and deploy a Systems Manager Maintenance Windows task to run AWS-RunPatchBaseline using the patch baseline
F. Install the AWS Systems Manager Agent on all existing instances using the company's current orchestration tool Use the Systems Manager Run Command to run a list of commands to upgrade software on each instance using operating system-specific tool
G. Enable AWS KMS encryption on all Amazon EBS volumes.
H. install the AWS Systems Manager Agent on all existing instances using the company's current orchestration too
I. Migrate al relational databases to Amazon RDS and enable AWS KMS encryption Use Systems Manager Patch Manager to establish a patch baseline and deploy a Systems Manager Maintenance Windows task to run AWS-RunPatchBaseline using the patch baseline.

Answer: D

NEW QUESTION 154
- (Exam Topic 2)
A company is using a single AWS Region (or its ecommerce website. The website includes a web application that runs on several Amazon EC2 instances behind an Application Load Balancer (ALB). The website also includes an Amazon DynamoDB table. A custom domain name in Amazon Route 53 is linked to the ALB. The company created an SSL/TLS certificate in AWS Certificate Manager (ACM) and attached the certificate to the ALB. The company is not using a content delivery network as part of its design.
The company wants to replicate its entire application stack in a second Region to provide disaster recovery, plan for future growth, and provide improved access time to users. A solutions architect needs to implement a solution that achieves these goals and minimizes administrative overhead.
Which combination of steps should the solutions architect take to meet these requirements? (Select THREE.)

A. Create an AWS Cloud Formation template for the current infrastructure desig
B. Use parameters for important system values, including Regio
C. Use the CloudFormation template to create the new infrastructure in the second Region.
D. Use the AWS Management Console to document the existing infrastructure design in the first Region and to create the new infrastructure in the second Region.
E. Update the Route 53 hosted zone record for the application to use weighted routin
F. Send 50% of the traffic to the ALB in each Region.
G. Update the Route 53 hosted zone record for the application to use latency-based routin
H. Send traffic to the ALB in each Region.
I. Update the configuration of the existing DynamoDB table by enabling DynamoDB Streams Add the second Region to create a global table.
J. Create a new DynamoDB tabl
K. Enable DynamoDB Streams for the new tabl
L. Add the second Region to create a global tabl
M. Copy the data from the existing DynamoDB table to the new table as a one-time operation.

Answer: ADF

NEW QUESTION 156
- (Exam Topic 2)
A retail company has a small ecommerce web application that uses an Amazon RDS for PostgreSQL DB instance The DB instance is deployed with the Multi-AZ option turned on.
Application usage recently increased exponentially and users experienced frequent HTTP 503 errors Users reported the errors, and the company's reputation suffered The company could not identify a definitive root cause.
The company wants to improve its operational readiness and receive alerts before users notice an incident The company also wants to collect enough information to determine the root cause of any future incident.
Which solution will meet these requirements with the LEAST operational overhead?

A. Turn on Enhanced Monitoring for the DB instance Modify the corresponding parameter group to turn on query logging for all the slow queries Create Amazon CloudWatch alarms Set the alarms to appropriate thresholds that are based on performance metrics in CloudWatch
B. Turn on Enhanced Monitoring and Performance Insights for the DB instance Create Amazon CloudWatch alarms Set the alarms to appropriate thresholds that are based on performance metrics in CloudWatch
C. Turn on log exports to Amazon CloudWatch for the PostgreSQL logs on the DB instance Analyze the logs by using Amazon Elasticsearch Service (Amazon ES) and Kibana Create a dashboard in Kibana Configure alerts that are based on the metrics that are collected
D. Turn on Performance Insights for the DB instance Modify the corresponding parameter group to turn on query logging for all the slow queries Create Amazon CloudWatch alarms Set the alarms to appropriate thresholds that are based on performance metrics in CloudWatch

Answer: A

NEW QUESTION 157
- (Exam Topic 2)

A company has created an OU in AWS Organizations for each of its engineering teams Each OU owns multiple AWS accounts. The organization has hundreds of AWS accounts A solutions architect must design a solution so that each OU can view a breakdown of usage costs across its AWS accounts. Which solution meets these requirements?

A. Create an AWS Cost and Usage Report (CUR) for each OU by using AWS Resource Access Manager Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
B. Create an AWS Cost and Usage Report (CUR) from the AWS Organizations management account- Allow each team to visualize the CUR through an Amazon QuickSight dashboard
C. Create an AWS Cost and Usage Report (CUR) in each AWS Organizations member account Allow eachteam to visualize the CUR through an Amazon QuickSight dashboard.
D. Create an AWS Cost and Usage Report (CUR) by using AWS Systems Manager Allow each team to visualize the CUR through Systems Manager OpsCenter dashboards

Answer: B

NEW QUESTION 162
- (Exam Topic 2)
A medical company is running an application in the AWS Cloud. The application simulates the effect of medical drugs in development.
The application consists of two parts configuration and simulation The configuration part runs in AWS Fargate containers in an Amazon Elastic Container Service (Amazon ECS) cluster. The simulation part runs on large, compute optimized Amazon EC2 instances Simulations can restart if they are interrupted
The configuration part runs 24 hours a day with a steady load. The simulation part runs only for a few hours each night with a variable load. The company stores simulation results in Amazon S3, and researchers use the results for 30 days. The company must store simulations for 10 years and must be able to retrieve the simulations within 5 hours
Which solution meets these requirements MOST cost-effectively?

A. Purchase an EC2 Instance Savings Plan to cover the usage for the configuration part Run the simulation part by using EC2 Spot Instances Create an S3 Lifecycle policy to transition objects that are older than 30 days to S3 Intelligent-Tiering
B. Purchase an EC2 Instance Savings Plan to cover the usage for the configuration part and the simulation part Create an S3 Lifecycle policy to transition objects that are older than 30 days to S3 Glacier
C. Purchase Compute Savings Plans to cover the usage for the configuration part Run the simulation part by using EC2 Spot instances Create an S3 Lifecycle policy to transition objects that are older than 30 days to S3 Glacier
D. Purchase Compute Savings Plans to cover the usage for the configuration part Purchase EC2 Reserved Instances for the simulation part Create an S3 Lifecycle policy to transition objects that are older than 30 days to S3 Glacier Deep Archive

Answer: C

NEW QUESTION 166
.....

Relate Links

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

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

Contact us

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

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