



Amazon-Web-Services

Exam Questions SAP-C02

AWS Certified Solutions Architect - Professional

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

- (Exam Topic 1)

A company 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 organization
- 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 resource
- E. Deploy AWS WAF rules by using an AWS CloudFormation stack set to target the same OUs where the AWS Config rule is applied.
- F. Create AWS WAF rules in the management account of the organization
- G. Use AWS Lambda environment variables to store account numbers and OUs to manage Update environment variables as needed to add or remove accounts or OUs Create cross-account IAM roles in member account
- H. Assume the roles by using AWS Security Token Service (AWS STS) in the Lambda function to create and update AWS WAF rules in the member accounts
- I. Use AWS Control Tower to manage AWS WAF rules across accounts in the organization
- J. Use AWS Key Management Service (AWS KMS) to store account numbers and OUs to manage Update AWS KMS as needed to add or remove accounts or OUs
- K. Create IAM users in member accounts Allow AWS Control Tower in the management account to use the access key and secret access key to create and update AWS WAF rules in the member accounts

Answer: B

NEW QUESTION 2

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: C

Explanation:

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

NEW QUESTION 3

- (Exam Topic 1)

A company needs to architect a hybrid DNS solution. This solution will use an Amazon Route 53 private hosted zone for the domain cloud.example.com for the resources stored within VPCs.

The company has the following DNS resolution requirements:

- On-premises systems should be able to resolve and connect to cloud.example.com.
- All VPCs should be able to resolve cloud.example.com.

There is already an AWS Direct Connect connection between the on-premises corporate network and AWS Transit Gateway. Which architecture should the company use to meet these requirements with the HIGHEST performance?

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

Answer: D

Explanation:

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

NEW QUESTION 4

- (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 of 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 only
- B. Delete and re-create the AZ1 subnet using half the previous address space
- C. Adjust the Auto Scaling group to also use the new AZ1 subnet
- D. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only
- E. Remove the current AZ2 subnet
- F. Create a new AZ2 subnet using the second half of the address space from the original AZ1 subnet
- 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 subnet
- I. Delete and re-create the AZ1 subnet using half the address space
- J. Update the Auto Scaling group to use this new subnet
- K. Repeat this for the second AZ
- 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 AZ
- 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 only
- P. Update the AZ1 subnet to have half the previous address space
- Q. Adjust the Auto Scaling group to also use the AZ1 subnet again
- R. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only
- S. Update the current AZ2 subnet and assign the second half of the address space from the original AZ1 subnet
- T. 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.

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 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 organization
- 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 roles 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 to deliver photos to visitors with minimal latency.

Which actions will achieve this goal? (Select TWO.)

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

Answer: BD

NEW QUESTION 7

- (Exam Topic 1)

A group of research institutions and hospitals are in a partnership to study 2 PBs of genomic data. The institute that owns the data stores it in an Amazon S3 bucket and updates it regularly. The institute would like to give all of the organizations in the partnership read access to the data. All members of the partnership are extremely cost-conscious, and the institute that owns the account with the S3 bucket is concerned about covering the costs for requests and data transfers from Amazon S3.

Which solution allows for secure datasharing without causing the institute that owns the bucket to assume all the costs for S3 requests and data transfers'?

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

Answer: B

Explanation:

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

NEW QUESTION 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 (DR) 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 minutes
- 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 detection
- D. Configure cross-Region snapshots of the DB instance to the DR Region every 5 minutes
- 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 Region
- 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 AMIs of the web and application servers in the DR Region
- J. Use scheduled AWS Glue jobs to synchronize the DB instance with another DB instance in the DR Region
- 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 company has 50 AWS accounts that are members of an organization in AWS Organizations Each account contains multiple VPCs The company wants to use AWS Transit Gateway to establish connectivity between the VPCs in each member account Each time a new member account is created, the company wants to automate the process of creating a new VPC and a transit gateway attachment.

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

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

Answer: AC

NEW QUESTION 10

- (Exam Topic 1)

A finance company is running its business-critical application on current-generation Linux EC2 instances The application includes a self-managed MySQL database performing heavy I/O operations. The application is working fine to handle a moderate amount of traffic during the month. However, it slows down during the final three days of each month due to month-end reporting, even though the company is using Elastic Load Balancers and Auto Scaling within its infrastructure to meet the increased demand.

Which of the following actions would allow the database to handle the month-end load with the LEAST impact on performance?

- A. Pre-warming Elastic Load Balancers, using a bigger instance type, changing all Amazon EBS volumes to GP2 volumes.
- B. Performing a one-time migration of the database cluster to Amazon RD
- C. and creating several additional read replicas to handle the load during end of month
- D. Using Amazon CioudWatch with AWS Lambda to change the typ
- E. size, or IOPS of Amazon EBS volumes in the cluster based on a specific CloudWatch metric
- F. Replacing all existing Amazon EBS volumes with new PIOPS volumes that have the maximum available storage size and I/O per second by taking snapshots before the end of the month and reverting back afterwards.

Answer: B

Explanation:

In this scenario, the Amazon EC2 instances are in an Auto Scaling group already which means that the database read operations is the possible bottleneck especially during the month-end wherein the reports are generated. This can be solved by creating RDS read replicas.

NEW QUESTION 10

- (Exam Topic 1)

A company is deploying a new cluster for big data analytics on AWS. The cluster will run across many Linux Amazon EC2 instances that are spread across multiple Availability Zones.

All of the nodes in the cluster must have read and write access to common underlying file storage. The file storage must be highly available, must be resilient, must be compatible with the Portable Operating System Interface (POSIX), and must accommodate high levels of throughput.

Which storage solution will meet these requirements?

- A. Provision an AWS Storage Gateway file gateway NFS file share that is attached to an Amazon S3 bucke
- B. Mount the NFS file share on each EC2 instance In the cluster.
- C. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses General Purpose performance mod
- D. Mount the EFS file system on each EC2 instance in the cluster.
- E. Provision a new Amazon Elastic Block Store (Amazon EBS) volume that uses the io2 volume type. Attach the EBS volume to all of the EC2 instances in the cluster.
- F. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses Max I/O performance mod
- G. Mount the EFS file system on each EC2 instance in the cluster.

Answer: D

NEW QUESTION 11

- (Exam Topic 1)

A company that tracks medical devices in hospitals wants to migrate its existing storage solution to the AWS Cloud. The company equips all of its devices with sensors that collect location and usage information. This sensor data is sent in unpredictable patterns with large spikes. The data is stored in a MySQL database running on premises at each hospital. The company wants the cloud storage solution to scale with usage.

The company's analytics team uses the sensor data to calculate usage by device type and hospital. The team needs to keep analysis tools running locally while fetching data from the cloud. The team also needs to use existing Java application and SQL queries with as few changes as possible.

How should a solutions architect meet these requirements while ensuring the sensor data is secure?

- A. Store the data in an Amazon Aurora Serverless databas
- B. Serve the data through a Network Load Balancer (NLB). Authenticate users using the NLB with credentials stored in AWS Secrets Manager.
- C. Store the data in an Amazon S3 bucke
- D. Serve the data through Amazon QuickSight using an IAM user authorized with AWS Identity and Access Management (IAM) with the S3 bucket as the data source.
- E. Store the data in an Amazon Aurora Serverless databas
- F. Serve the data through the Aurora Data API using an IAM user authorized with AWS Identity and Access Management (IAM) and the AWS Secrets Manager ARN.
- G. Store the data in an Amazon S3 bucke
- H. Serve the data through Amazon Athena using AWS PrivateLink to secure the data in transit.

Answer: C

Explanation:

<https://aws.amazon.com/blogs/aws/new-data-api-for-amazon-aurora-serverless/> <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/data-api.html>
<https://aws.amazon.com/blogs/aws/aws-privatelink-for-amazon-s3-now-available/> <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/data-api.html#data-api.access>

The data is currently stored in a MySQL database running on-prem. Storing MySQL data in S3 doesn't sound good so B & D are out. Aurora Data API "enables the SQL HTTP endpoint, a connectionless Web Service API for running SQL queries against this database. When the SQL HTTP endpoint is enabled, you can also query your database from inside the RDS console (these features are free to use)."

NEW QUESTION 16

- (Exam Topic 1)

A company has a new application that needs to run on five Amazon EC2 instances in a single AWS Region. The application requires high-throughput, low-latency network connections between all of the EC2 instances where the application will run. There is no requirement for the application to be fault tolerant.

Which solution will meet these requirements?

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

Answer: A

Explanation:

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

NEW QUESTION 21

- (Exam Topic 1)

A large payroll company recently merged with a small staffing company. The unified company now has multiple business units, each with its own existing AWS account.

A solutions architect must ensure that the company can centrally manage the billing and access policies for all the AWS accounts. The solutions architect configures AWS Organizations by sending an invitation to all member accounts of the company from a centralized management account.

What should the solutions architect do next to meet these requirements?

- A. Create the OrganizationAccountAccess IAM group in each member account
- B. Include the necessary IAM roles for each administrator.
- C. Create the OrganizationAccountAccessPolicy IAM policy in each member account
- D. Connect the member accounts to the management account by using cross-account access.
- E. Create the OrganizationAccountAccessRole IAM role in each member account
- F. Grant permission to the management account to assume the IAM role.
- G. Create the OrganizationAccountAccessRole IAM role in the management account Attach the Administrator Access AWS managed policy to the IAM role
- H. Assign the IAM role to the administrators in each member account.

Answer: C

NEW QUESTION 25

- (Exam Topic 1)

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

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

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

Answer: C

Explanation:

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

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

100TB

EBS - 8.109\$ S3 - 2.355\$

You have saved 5.752\$

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

NEW QUESTION 26

- (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 29

- (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 34

- (Exam Topic 1)

A media company uses Amazon DynamoDB to store metadata for its catalog of movies that are available to stream. Each media item Contains user-facing content that concludes a description of the media, a list of search tags, and similar data. In addition, media items include a list of Amazon S3 key names that relate to movie files. The company stores these movie files in a single S3 bucket that has versioning enable. The company uses Amazon CloudFront to serve these movie files.

The company has 100.000 media items, and each media item can have many different S3 objects that represent different encodings of the same media S3 objects that belong to the same media item are grouped together under the same key prefix, which is a random unique ID

Because of an expiring contract with a media provider, the company must remove 2.000 media Items. The company must completely delete all DynamoDB keys and movie files on Amazon S3 that are related to these media items within 36 hours The company must ensure that the content cannot be recovered.

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

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

Answer: CE

NEW QUESTION 39

- (Exam Topic 1)

A large company in Europe plans to migrate its applications to the AWS Cloud. The company uses multiple AWS accounts for various business groups. A data privacy law requires the company to restrict developers' access to AWS European Regions only.

What should the solutions architect do to meet this requirement with the LEAST amount of management overhead^

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

Answer: B

Explanation:

"This policy uses the Deny effect to deny access to all requests for operations that don't target one of the two approved regions (eu-central-1 and eu-west-1)."

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_general.htm

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition.html

NEW QUESTION 42

- (Exam Topic 1)

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

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

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

Which solution meets these requirements?

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

AWS Step Functions state machine when a new message is added to the SQS queue Use the Step Functions state machine to delete the image tag for images that have Critical or High severity finding

I. Notify the development team by using Amazon Simple Email Service (Amazon SES).

Answer: C

NEW QUESTION 45

- (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 47

- (Exam Topic 1)

A company runs an application that gives users the ability to search for videos and related information by using keywords that are curated from content providers. The application data is stored in an on-premises Oracle database that is 800 GB in size.

The company wants to migrate the data to an Amazon Aurora MySQL DB instance. A solutions architect plans to use the AWS Schema Conversion Tool and AWS Database Migration Service (AWS DMS) for the migration. During the migration, the existing database must serve ongoing requests. The migration must be completed with minimum downtime Which solution will meet these requirements?

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

Answer: B

Explanation:

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

NEW QUESTION 50

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 53

- (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 query the logs for AwsConsoleSignIn events.
- B. Configure Amazon Simple Email Service (Amazon SES) to send email to the security team when an alarm is activated.
- C. Deploy EC2 instances in an Auto Scaling group Configure the launch template to deploy instances without key pairs Configure Amazon CloudWatch Logs to capture system access logs Create an Amazon CloudWatch alarm that is based on the logs to detect when a user logs in to an EC2 instance
- D. Configure an Amazon Simple Notification Service (Amazon SNS) topic to send a message to the security team when an alarm is activated
- E. Turn on AWS CloudTrail logs for all AWS Region
- F. Configure Amazon CloudWatch alarms to provide an alert when an AwsConsoleSignIn event is detected.

- G. Deploy EC2 instances in an Auto Scaling group
 - H. Configure the launch template to delete the key pair after launch
 - 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 57

- (Exam Topic 1)

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

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

Answer: D

Explanation:

<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/centralized-transit-vpc/>

<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/centralized-transit-vpc/>

AWS Transit Gateway helps you design and implement networks at scale by acting as a cloud router. As your network grows, the complexity of managing incremental connections can slow you down. AWS Transit Gateway connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships -- each new connection is only made once.

NEW QUESTION 62

- (Exam Topic 1)

A company manages an on-premises JavaScript front-end web application. The application is hosted on two servers secured with a corporate Active Directory. The application calls a set of Java-based microservices on an application server and stores data in a clustered MySQL database. The application is heavily used during the day on weekdays. It is lightly used during the evenings and weekends.

Daytime traffic to the application has increased rapidly, and reliability has diminished as a result. The company wants to migrate the application to AWS with a solution that eliminates the need for server maintenance, with an API to securely connect to the microservices.

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

- A. Host the web application on Amazon S3. Use Amazon Cognito identity pools (federated identities) with SAML for authentication and authorization.
- B. Host the web application on Amazon EC2 with Auto Scaling
- C. Use Amazon Cognito federation and Login with Amazon for authentication and authorization.
- D. Create an API layer with Amazon API Gateway
- E. Rehost the microservices on AWS Fargate containers.
- F. Create an API layer with Amazon API Gateway
- G. Rehost the microservices on Amazon Elastic Container Service (Amazon ECS) containers.
- H. Replatform the database to Amazon RDS for MySQL.
- I. Replatform the database to Amazon Aurora MySQL Serverless.

Answer: ACE

NEW QUESTION 66

- (Exam Topic 1)

A company is creating a REST API to share information with six of its partners based in the United States. The company has created an Amazon API Gateway Regional endpoint. Each of the six partners will access the API once per day to post daily sales figures.

After initial deployment, the company observes 1,000 requests per second originating from 500 different IP addresses around the world. The company believes this traffic is originating from a botnet and wants to secure its API while minimizing cost.

Which approach should the company take to secure its API?

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

Answer: D

Explanation:

"A usage plan specifies who can access one or more deployed API stages and methods—and also how much and how fast they can access them. The plan uses API keys to identify API clients and meters access to the associated API stages for each key. It also lets you configure throttling limits and quota limits that are

enforced on individual client API keys."

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>

NEW QUESTION 71

- (Exam Topic 1)

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

Which solution meets these requirements?

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

Answer: A

Explanation:

A Direct Connect gateway is a globally available resource. You can create the Direct Connect gateway in any Region and access it from all other Regions. The following describe scenarios where you can use a Direct Connect gateway.

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html>

NEW QUESTION 75

- (Exam Topic 1)

A solution architect needs to deploy an application on a fleet of Amazon EC2 instances. The EC2 instances run in private subnets in an Auto Scaling group. The application is expected to generate logs at a rate of 100 MB each second on each of the EC2 instances.

The logs must be stored in an Amazon S3 bucket so that an Amazon EMR cluster can consume them for further processing. The logs must be quickly accessible for the first 90 days and should be retrievable within 48 hours thereafter.

What is the MOST cost-effective solution that meets these requirements?

- A. Set up an S3 copy job to write logs from each EC2 instance to the S3 bucket with S3 Standard storage. Use a NAT instance within the private subnets to connect to Amazon S3. Create S3 Lifecycle policies to move logs that are older than 90 days to S3 Glacier.
- B. Set up an S3 sync job to copy logs from each EC2 instance to the S3 bucket with S3 Standard storage. Use a gateway VPC endpoint for Amazon S3 to connect to Amazon S3. Create S3 Lifecycle policies to move logs that are older than 90 days to S3 Glacier Deep Archive.
- C. Set up an S3 batch operation to copy logs from each EC2 instance to the S3 bucket with S3 Standard storage. Use a NAT gateway with the private subnets to connect to Amazon S3. Create S3 Lifecycle policies to move logs that are older than 90 days to S3 Glacier Deep Archive.
- D. Set up an S3 sync job to copy logs from each EC2 instance to the S3 bucket with S3 Standard storage. Use a gateway VPC endpoint for Amazon S3 to connect to Amazon S3. Create S3 Lifecycle policies to move logs that are older than 90 days to S3 Glacier.

Answer: C

NEW QUESTION 79

- (Exam Topic 1)

A company hosts a web application that runs on a group of Amazon EC2 instances that are behind an Application Load Balancer (ALB) in a VPC. The company wants to analyze the network payloads to reverse-engineer a sophisticated attack of the application.

Which approach should the company take to achieve this goal?

- A. Enable VPC Flow Log
- B. Store the flow logs in an Amazon S3 bucket for analysis.
- C. Enable Traffic Mirroring on the network interface of the EC2 instance
- D. Send the mirrored traffic to a target for storage and analysis.
- E. Create an AWS WAF web ACL
- F. and associate it with the ALB
- G. Configure AWS WAF logging.
- H. Enable logging for the ALB
- I. Store the logs in an Amazon S3 bucket for analysis.

Answer: A

NEW QUESTION 84

- (Exam Topic 1)

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

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

- A. Create a VPC in the us-west-1 Region

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

Answer: B

Explanation:

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

NEW QUESTION 88

- (Exam Topic 1)

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

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

Answer: B

Explanation:

Host Affinity is configured at the instance level. It establishes a launch relationship between an instance and a Dedicated Host. (This sets which host the instance can run on) Auto-placement allows you to manage whether instances that you launch are launched onto a specific host, or onto any available host that has matching configurations. Auto-placement must be configured at the host level. (This sets which instance the host can run.) When affinity is set to Host, an instance launched onto a specific host always restarts on the same host if stopped. This applies to both targeted and untargeted launches.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/how-dedicated-hosts-work.html>

When affinity is set to Off, and you stop and restart the instance, it can be restarted on any available host. However, it tries to launch back onto the last Dedicated Host on which it ran (on a best-effort basis).

NEW QUESTION 90

- (Exam Topic 1)

A company wants to control its cost of Amazon Athena usage The company has allocated a specific monthly budget for Athena usage A solutions architect must design a solution that will prevent the company from exceeding the budgeted amount Which solution will meet these requirements?

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

Answer: D

NEW QUESTION 91

- (Exam Topic 1)

A public retail web application uses an Application Load Balancer (ALB) in front of Amazon EC2 instances running across multiple Availability Zones (AZs) in a Region backed by an Amazon RDS MySQL Multi-AZ deployment. Target group health checks are configured to use HTTP and pointed at the product catalogue page. Auto Scaling is configured to maintain the web fleet size based on the ALB health check.

Recently, the application experienced an outage. Auto Scaling continuously replaced the instances during the outage. A subsequent investigation determined that the web server metrics were within the normal range, but the database tier was experiencing high load, resulting in severely elevated query response times. Which of the following changes together would remediate these issues while improving monitoring capabilities for the availability and functionality of the entire application stack for future growth? (Select TWO.)

- A. Configure read replicas for Amazon RDS MySQL and use the single reader endpoint in the web application to reduce the load on the backend database tier.
- B. Configure the target group health check to point at a simple HTML page instead of a product catalog page and the Amazon Route 53 health check against the product page to evaluate full application functionality
- C. Configure Amazon CloudWatch alarms to notify administrators when the site fails.
- D. Configure the target group health check to use a TCP check of the Amazon EC2 web server and the Amazon Route 53 health check against the product page to evaluate full application functionality
- E. Configure Amazon CloudWatch alarms to notify administrators when the site fails.

- F. Configure an Amazon CloudWatch alarm for Amazon RDS with an action to recover a high-load, impaired RDS instance in the database tier.
G. Configure an Amazon ElastiCache cluster and place it between the web application and RDS MySQL instances to reduce the load on the backend database tier.

Answer: BE

Explanation:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/health-checks-types.html>

NEW QUESTION 94

- (Exam Topic 1)

A company has an internal application running on AWS that is used to track and process shipments in the company's warehouse. Currently, after the system receives an order, it emails the staff the information needed to ship a package. Once the package is shipped, the staff replies to the email and the order is marked as shipped.

The company wants to stop using email in the application and move to a serverless application model. Which architecture solution meets these requirements?

- A. Use AWS Batch to configure the different tasks required to ship a package
- B. Have AWS Batch trigger an AWS Lambda function that creates and prints a shipping label
- C. Once that label is scanned
- D. as it leaves the warehouse, have another Lambda function move the process to the next step in the AWS Batch job.
- E. When a new order is created, store the order information in Amazon SQS
- F. Have AWS Lambda check the queue every 5 minutes and process any needed work
- G. When an order needs to be shipped, have Lambda print the label in the warehouse
- H. Once the label has been scanned, as it leaves the warehouse, have an Amazon EC2 instance update Amazon S3
- I. Update the application to store new order information in Amazon DynamoDB
- J. When a new order is created, trigger an AWS Step Functions workflow, mark the orders as "in progress," and print a package label to the warehouse
- K. Once the label has been scanned and fulfilled, the application will trigger an AWS Lambda function that will mark the order as shipped and complete the workflow.
- L. Store new order information in Amazon EFS
- M. Have instances pull the new information from the NFS and send that information to printers in the warehouse
- N. Once the label has been scanned, as it leaves the warehouse, have Amazon API Gateway call the instances to remove the order information from Amazon EFS.

Answer: C

NEW QUESTION 95

- (Exam Topic 1)

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

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

Which migration strategy meets these requirements?

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

Answer: D

Explanation:

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

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

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

NEW QUESTION 99

- (Exam Topic 1)

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

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

- A. Configure the Lambda function to store and retrieve the database credentials in AWS Secrets Manager and enable rotation of the credential
- B. Take a snapshot of the DB instance and encrypt a copy of that snapshot
- C. Replace the DB instance with a new DB instance that is based on the encrypted snapshot.
- D. Enable IAM DB authentication on the DB instance
- E. Grant the Lambda execution role access to the DB instance
- F. Modify the DB instance and enable encryption.
- G. Enable IAM DB authentication on the DB instance
- H. Grant the Lambda execution role access to the DB instance

- I. Create an encrypted read replica of the DB instance
- J. Promote the encrypted read replica to be the new primary node.
- K. Configure the Lambda function to store and retrieve the database credentials as encrypted AWS Systems Manager Parameter Store parameter
- L. Create another Lambda function to automatically rotate the credential
- M. Create an encrypted read replica of the DB instance
- N. Promote the encrypted read replica to be the new primary node.

Answer: A

Explanation:

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

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

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

NEW QUESTION 104

- (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 instances
- B. Remove all security group rules attached to EC2 instances that allow inbound TCP on port 22. Advise the engineers to remotely access the instances by using the EC2 Instance Connect CLI.
- C. Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's device
- D. Install the Amazon CloudWatch agent on all EC2 instances and send operating system audit logs to CloudWatch Logs.
- E. Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's device
- F. Enable AWS Config for EC2 security group resource change
- G. Enable AWS Firewall Manager and apply a security group policy that automatically remediates changes to rules.
- H. Create an IAM role with the AmazonSSMManagedInstanceCore managed policy attached
- I. Attach the IAM role to all the EC2 instances
- J. Remove all security group rules attached to the EC2 instances
- 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 109

- (Exam Topic 1)

A company is migrating applications from on-premises to the AWS Cloud. These applications power the company's internal web forms. These web forms collect data for specific events several times each quarter. The web forms use simple SQL statements to save the data to a local relational database.

Data collection occurs for each event, and the on-premises servers are idle most of the time. The company needs to minimize the amount of idle infrastructure that supports the web forms.

Which solution will meet these requirements?

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

Answer: D

Explanation:

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

NEW QUESTION 110

- (Exam Topic 2)

A life sciences company is using a combination of open source tools to manage data analysis workflows and Docker containers running on servers in its on-premises data center to process genomics data. Sequencing data is generated and stored on a local storage area network (SAN), and then the data is processed. The research and development teams are running into capacity issues and have decided to re-architect their genomics analysis platform on AWS to scale based on workload demands and reduce the turnaround time from weeks to days.

The company has a high-speed AWS Direct Connect connection. Sequencers will generate around 200 GB of data for each genome, and individual jobs can take

several hours to process the data with ideal compute capacity. The end result will be stored in Amazon S3. The company is expecting 10-15 job requests each day. Which solution meets these requirements?

- A. Use regularly scheduled AWS Snowball Edge devices to transfer the sequencing data into AWS. When AWS receives the Snowball Edge device and the data is loaded into Amazon S3, use S3 events to trigger an AWS Lambda function to process the data.
- B. Use AWS Data Pipeline to transfer the sequencing data to Amazon S3. Use S3 events to trigger an Amazon EC2 Auto Scaling group to launch custom-AMI EC2 instances running the Docker containers to process the data.
- C. Use AWS DataSync to transfer the sequencing data to Amazon S3. Use S3 events to trigger an AWS Lambda function that starts an AWS Step Functions workflow. Store the Docker images in Amazon Elastic Container Registry (Amazon ECR) and trigger AWS Batch to run the container and process the sequencing data.
- D. Use an AWS Storage Gateway file gateway to transfer the sequencing data to Amazon S3. Use S3 events to trigger an AWS Batch job that runs on Amazon EC2 instances running the Docker containers to process the data.

Answer: C

NEW QUESTION 114

- (Exam Topic 2)

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

GET /posts/{postId} to get post details

GET /users/{userId} to get user details

GET /comments/{commentId} to get comments details

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

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

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

Answer: C

NEW QUESTION 118

- (Exam Topic 2)

A company 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 121

- (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 RDS, and AWS CloudTrail. Load customer records in Amazon RDS MySQL and train users to run queries using the AWS CLI.
- B. 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.
- C. 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 train users to run queries using the CLI via Athena. Analyze CloudTrail events 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 DynamoDB, 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.
- E. 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 125

- (Exam Topic 2)

A company's solution architect is designing a disaster recovery (DR) solution for an application that runs on AWS. The application uses PostgreSQL 11.7 as its database. The company has an RPO of 30 seconds. The solution 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 in us-west-2. Set the managed RPO 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 130

- (Exam Topic 2)

A company wants to migrate its website from an on-premises data center onto AWS At the same time it wants to migrate the website to a containerized microservice-based architecture to improve the availability and cost efficiency The company's security policy states that privileges and network permissions must be configured according to best practice, using least privilege

A solutions architect must create a containerized architecture that meets the security requirements and has deployed the application to an Amazon ECS cluster What steps are required after the deployment to meet the requirements'? (Select TWO.)

A. Create tasks using the bridge network mode

B. Create tasks using the awsvpc network mode

C. Apply security groups to Amazon EC2 instances and use IAM roles for EC2 instances to access other resources

D. Apply security groups to the tasks, and pass IAM credentials into the container at launch time to access other resources

E. Apply security groups to the tasks; and use IAM roles for tasks to access other resources

Answer: BE

NEW QUESTION 134

- (Exam Topic 2)

A fleet of Amazon ECS instances is used to poll an Amazon SQS queue and update items in an Amazon DynamoDB database Items in the table are not being updated, and the SQS queue is filling up Amazon CloudWatch Logs are showing consistent 400 errors when attempting to update the table The provisioned write capacity units are appropriately configured, and no throttling is occurring

What is the LIKELY cause of the failure*?

A. The ECS service was deleted

B. The ECS configuration does not contain an Auto Scaling group

C. The ECS instance task execution IAM role was modified

D. The ECS task role was modified

Answer: D

NEW QUESTION 137

- (Exam Topic 2)

A large company has many business units Each business unit has multiple AWS accounts for different purposes. The CIO of the company sees that each business unit has data that would be useful to share with other parts of the company in total there are about 10 PB of data that needs to be shared with users in 1.000 AWS accounts. The data is proprietary so some of it should only be available to users with specific job types Some of the data is used for throughput of intensive workloads such as simulations. The number of accounts changes frequently because of new initiatives acquisitions and divestitures

A solutions architect has been asked to design a system that will allow for sharing data for use in AWS with all of the employees in the company

Which approach will allow for secure data sharing in scalable way?

A. Store the data in a single Amazon S3 bucket Create an IAM role for every combination of job type and business unit that allows for appropriate read/write access based on object prefixes in the S3 bucket The roles should have trust policies that allow the business unit's AWS accounts to assume their roles Use IAM in each business unit's AWS account to prevent them from assuming roles for a different job type Users get credentials to access the data by using AssumeRole from their business unit's AWS account Users can then use those credentials with an S3 client

B. Store the data in a single Amazon S3 bucket Write a bucket policy that uses conditions to grant read and write access where appropriate based on each user's business unit and job type

C. Determine the business unit with the AWS account accessing the bucket and the job type with a prefix in the IAM user's name Users can access data by using IAM credentials from their business unit's AWS account with an S3 client

D. Store the data in a series of Amazon S3 buckets Create an application running on Amazon EC2 that is integrated with the company's identity provider (IdP) that authenticates users and allows them to download or upload data through the application The application uses the business unit and job type information in the IdP to control what users can upload and download through the application The users can access the data through the application's API

E. Store the data in a series of Amazon S3 buckets Create an AWS STS token vending machine that is integrated with the company's identity provider (IdP) When a user logs in: have the token vending machine attach an IAM policy that assumes the role that limits the user's access and/or upload only the data the user is authorized to access Users can get credentials by authenticating to the token vending machine's website or API and then use those credentials with an S3 client

F. D

Answer: E

NEW QUESTION 139

- (Exam Topic 2)

A company has more than 10.000 sensors that send data to an on-premises Apache Kafka server by using the Message Queuing Telemetry Transport (MQTT) protocol . The on-premises Kafka server transforms the data and then stores the results as objects in an Amazon S3 bucket

Recently, the Kafka server crashed. The company lost sensor data while the server was being restored A solutions architect must create a new design on AWS that is highly available and scalable to prevent a similar occurrence

Which solution will meet these requirements?

A. Launch two Amazon EC2 instances to host the Kafka server in an active/standby configuration across two Availability Zone

B. Create a domain name in Amazon Route 53 Create a Route 53 failover policy Route the sensors to send the data to the domain name

C. Migrate the on-premises Kafka server to Amazon Managed Streaming for Apache Kafka (Amazon MSK). Create a Network Load Balancer (NLB) that points to the Amazon MSK broke

D. Enable NLB health checks Route the sensors to send the data to the NLB.

E. Deploy AWS IoT Core, and connect it to an Amazon Kinesis Data Firehose delivery stream Use an AWS Lambda function to handle data transformation Route the sensors to send the data to AWS IoT Core
F. Deploy AWS IoT Core, and launch an Amazon EC2 instance to host the Kafka server Configure AWS IoT Core to send the data to the EC2 instance Route the sensors to send the data to AWS IoT Core.

Answer: A

NEW QUESTION 140

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 144

- (Exam Topic 2)

A development team is Deploying new APIs as serverless applications within a company. The team is currently using the AWS Management Console to provision Amazon API Gateway, AWS Lambda, and Amazon DynamoDB resources A solutions architect has been tasked with automating the future deployments of these serverless APIs
How can this be accomplished?

- A. Use AWS CloudFormation with a Lambda-backed custom resource to provision API Gateway Use the Manifest: :DynamoDB::Table and AWS::Lambda::Function resources to create the Amazon DynamoDB table and Lambda functions Write a script to automate the deployment of the CloudFormation template.
- B. Use the AWS Serverless Application Model to define the resources Upload a YAML template and application files to the code repository Use AWS CodePipeline to connect to the code repository and to create an action to build using AWS CodeBuild
- C. Use the AWS CloudFormation deployment provider in CodePipeline to deploy the solution.
- D. Use AWS CloudFormation to define the serverless application
- E. Implement versioning on the Lambda functions and create aliases to point to the version
- F. When deploying, configure weights to implement shifting traffic to the newest version, and gradually update the weights as traffic moves over
- G. Commit the application code to the AWS CodeCommit code repository
- H. Use AWS CodePipeline and connect to the CodeCommit code repository Use AWS CodeBuild to build and deploy the Lambda functions using AWS CodeDeploy Specify the deployment preference type in CodeDeploy to gradually shift traffic over to the new version.

Answer: B

NEW QUESTION 149

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 154

- (Exam Topic 2)

A company wants to use Amazon Workspaces in combination with thin client devices to replace aging desktops Employees use the desktops to access applications that work with clinical trial data Corporate security policy states that access to the applications must be restricted to only company branch office locations. The company is considering adding an additional branch office in the next 6 months.
Which solution meets these requirements with the MOST operational efficiency?

- A. Create an IP access control group rule with the list of public addresses from the branch offices Associate the IP access control group with the Workspaces directory
- B. Use AWS Firewall Manager to create a web ACL rule with an IPSet with the list of public addresses from the branch office locations Associate the web ACL with the Workspaces directory
- C. Use AWS Certificate Manager (ACM) to issue trusted device certificates to the machines deployed in the branch office locations Enable restricted access on the Workspaces directory

D. Create a custom Workspace image with Windows Firewall configured to restrict access to the public addresses of the branch offices Use the image to deploy the Workspaces.

Answer: C

NEW QUESTION 157

- (Exam Topic 2)

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

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

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

Answer: D

NEW QUESTION 160

- (Exam Topic 2)

A solutions architect uses AWS Organizations to manage several AWS accounts for a company. The full Organizations feature set is activated for the organization. All production AWS accounts exist under an OU that is named "production " Systems operators have full administrative privileges within these accounts by using IAM roles.

The company wants to ensure that security groups in all production accounts do not allow inbound traffic for TCP port 22. All noncompliant security groups must be remediated immediately, and no new rules that allow port 22 can be created.

Which solution will meet these requirements?

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

Answer: D

NEW QUESTION 164

- (Exam Topic 2)

A company has an on-premises monitoring solution using a PostgreSQL database for persistence of events. The database is unable to scale due to heavy ingestion and it frequently runs out of storage.

The company wants to create a hybrid solution and has already set up a VPN connection between its network and AWS. The solution should include the following attributes:

- Managed AWS services to minimize operational complexity
- A buffer that automatically scales to match the throughput of data and requires no on-going administration.
- A visualization tool to create dashboards to observe events in near-real time.
- Support for semi-structured JSON data and dynamic schemas.

Which combination of components will enable the company to create a monitoring solution that will satisfy these requirements" (Select TWO.)

- A. Use Amazon Kinesis Data Firehose to buffer events Create an AWS Lambda function to process and transform events
- B. Create an Amazon Kinesis data stream to buffer events Create an AWS Lambda function to process and transform events
- C. Configure an Amazon Aurora PostgreSQL DB cluster to receive events Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards
- D. Configure Amazon Elasticsearch Service (Amazon ES) to receive events Use the Kibana endpoint deployed with Amazon ES to create near-real-time visualizations and dashboards.
- E. Configure an Amazon Neptune DB instance to receive events Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards

Answer: DE

NEW QUESTION 169

- (Exam Topic 2)

A company is using a lift-and-shift strategy to migrate applications from several on-premises Windows servers to AWS. The Windows servers will be hosted on

Amazon EC2 instances in the us-east-1 Region.

The company's security policy allows the installation of migration tools on servers. The migration data must be encrypted in transit and encrypted at rest. The applications are business critical. The company needs to minimize the cutover window and minimize the downtime that results from the migration. The company wants to use Amazon CloudWatch and AWS CloudTrail for monitoring.

Which solution will meet these requirements?

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

Answer: A

NEW QUESTION 170

- (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 172

- (Exam Topic 2)

A solutions architect has been assigned to migrate a 50 TB Oracle data warehouse that contains sales data from on-premises to Amazon Redshift Major updates to the sales data occur on the final calendar day of the month For the remainder of the month, the data warehouse only receives minor daily updates and is primarily used for reading and reporting Because of this the migration process must start on the first day of the month and must be complete before the next set of updates occur. This provides approximately 30 days to complete the migration and ensure that the minor daily changes have been synchronized with the Amazon Redshift data warehouse Because the migration cannot impact normal business network operations, the bandwidth allocated to the migration for moving data over the internet is 50 Mbps The company wants to keep data migration costs low

Which steps will allow the solutions architect to perform the migration within the specified timeline?

- A. Install Oracle database software on an Amazon EC2 instance Configure VPN connectivity between AWS and the company's data center Configure the Oracle database running on Amazon EC2 to join the Oracle Real Application Clusters (RAC) When the Oracle database on Amazon EC2 finishes synchronizing, create an AWS DMS ongoing replication task to migrate the data from the Oracle database on Amazon EC2 to Amazon Redshift Verify the data migration is complete and perform the cut over to Amazon Redshift.
- B. Create an AWS Snowball import job Export a backup of the Oracle data warehouse Copy the exported data to the Snowball device Return the Snowball device to AWS Create an Amazon RDS for Oracle database and restore the backup file to that RDS instance Create an AWS DMS task to migrate the data from the RDS for Oracle database to Amazon Redshift Copy daily incremental backups from Oracle in the data center to the RDS for Oracle database over the internet Verify the data migration is complete and perform the cut over to Amazon Redshift.
- C. Install Oracle database software on an Amazon EC2 instance To minimize the migration time configure VPN connectivity between AWS and the company's data center by provisioning a 1 Gbps AWS Direct Connect connection Configure the Oracle database running on Amazon EC2 to be a read replica of the data center Oracle database Start the synchronization process between the company's on-premises data center and the Oracle database on Amazon EC2 When the Oracle database on Amazon EC2 is synchronized with the on-premises database create an AWS DMS ongoing replication task from the Oracle database read replica that is running on Amazon EC2 to Amazon Redshift Verify the data migration is complete and perform the cut over to Amazon Redshift.
- D. Create an AWS Snowball import jo
- E. Configure a server in the company's data center with an extraction agen
- F. Use AWS SCT to manage the extraction agent and convert the Oracle schema to an Amazon Redshift schem
- G. Create a new project in AWS SCT using the registered data extraction agen
- H. Create a local task and an AWS DMS task in AWS SCT with replication of ongoing change
- I. Copy data to the Snowball device and return the Snowball device to AW
- J. Allow AWS DMS to copy data from Amazon S3 to Amazon Redshif
- K. Verify that the data migration is complete and perform the cut over to Amazon Redshift.

Answer: D

Explanation:

Create an AWS Snowball import job. Configure a server in the company's data center with an extraction agent. Use AWS SCT to manage the extraction agent and convert the Oracle schema to an Amazon Redshift schema. Create a new project in AWS SCT using the registered data extraction agent. Create a local task

and an AWS DMS task in AWS SCT with replication of ongoing changes. Copy data to the Snowball device and return the Snowball device to AWS. Allow AWS DMS to copy data from Amazon S3 to Amazon Redshift. Verify that the data migration is complete and perform the cut over to Amazon Redshift.
<https://aws.amazon.com/getting-started/hands-on/migrate-oracle-to-amazon-redshift/>

NEW QUESTION 176

- (Exam Topic 2)

A company is running a workload that consists of thousands of Amazon EC2 instances. The workload is running in a VPC that contains several public subnets and private subnets. The public subnets have a route for 0.0.0.0/0 to an existing internet gateway. The private subnets have a route for 0.0.0.0/0 to an existing NAT gateway.

A solutions architect needs to migrate the entire fleet of EC2 instances to use IPv6. The EC2 instances that are in private subnets must not be accessible from the public internet.

What should the solutions architect do to meet these requirements?

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

Answer: C

NEW QUESTION 179

- (Exam Topic 2)

A large company recently experienced an unexpected increase in Amazon RDS and Amazon DynamoDB costs. The company needs to increase visibility into details of AWS Billing and Cost Management. There are various accounts associated with AWS Organizations, including many development and production accounts. There is no consistent tagging strategy across the organization, but there are guidelines in place that require all infrastructure to be deployed using AWS CloudFormation with consistent tagging. Management requires cost center numbers and project ID numbers for all existing and future DynamoDB tables and RDS instances.

Which strategy should the solutions architect provide to meet these requirements?

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

Answer: B

NEW QUESTION 180

- (Exam Topic 2)

A solutions architect needs to provide AWS Cost and Usage Report data from a company's AWS Organizations management account. The company already has an Amazon S3 bucket to store the reports. The reports must be automatically ingested into a database that can be visualized with other tools.

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

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that a new object creation in the S3 bucket will trigger.
- B. Create an AWS Cost and Usage Report configuration to deliver the data into the S3 bucket.
- C. Configure an AWS Glue crawler that a new object creation in the S3 bucket will trigger.
- D. Create an AWS Lambda function that a new object creation in the S3 bucket will trigger.
- E. Create an AWS Glue crawler that the AWS Lambda function will trigger to crawl objects in the S3 bucket.
- F. Create an AWS Glue crawler that the Amazon EventBridge (Amazon CloudWatch Events) rule will trigger to crawl objects in the S3 bucket.

Answer: BDF

NEW QUESTION 185

- (Exam Topic 2)

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

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

- A. Configure CloudTrail and VPC Flow Logs in each AWS account to send data to a centralized Amazon S3 bucket in the logging account.
- B. Create an AWS Lambda function to load data from the S3 bucket to Amazon ES in the logging account.
- C. Configure CloudTrail and VPC Flow Logs to send data to a log group in Amazon CloudWatch Logs in each AWS account. Configure a CloudWatch subscription filter in each AWS account to send data to Amazon Kinesis Data Firehose in the logging account. Load data from Kinesis Data Firehose into Amazon ES in the logging account.
- D. Configure CloudTrail and VPC Flow Logs to send data to a separate Amazon S3 bucket in each AWS account.
- E. Create an AWS Lambda function triggered by S3 events to copy the data to a centralized logging bucket.
- F. Create another Lambda function to load data from the S3 bucket to Amazon ES in the logging account.
- G. Configure CloudTrail and VPC Flow Logs to send data to a log group in Amazon CloudWatch Logs in each AWS account. Create AWS Lambda functions in each AWS account to subscribe to the log groups and stream the data to an Amazon S3 bucket in the logging account.
- H. Create another Lambda function to load data from the S3 bucket to Amazon ES in the logging account.

Answer: A

NEW QUESTION 186

- (Exam Topic 2)

A company is planning to migrate an Amazon RDS for Oracle database to an RDS for PostgreSQL DB instance in another AWS account. A solutions architect needs to design a migration strategy that will require no downtime and that will minimize the amount of time necessary to complete the migration. The migration strategy must replicate all existing data and any new data that is created during the migration. The target database must be identical to the source database at completion of the migration process.

All applications currently use an Amazon Route 53 CNAME record as their endpoint for communication with the RDS for Oracle DB instance. The RDS for Oracle DB instance is in a private subnet.

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

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

Answer: BCE

NEW QUESTION 191

- (Exam Topic 2)

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

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

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule.
- B. Define a pattern with the detail-type value set to AWS API Call via CloudTrail and an eventName of CreateUser.
- C. Configure CloudTrail to send a notification for the CreateUser event to an Amazon Simple Notification Service (Amazon SNS) topic.
- D. Invoke a container that runs in Amazon Elastic Container Service (Amazon ECS) with AWS Fargate technology to remove access.
- E. Invoke an AWS Step Functions state machine to remove access.
- F. Use Amazon Simple Notification Service (Amazon SNS) to notify the security team.
- G. Use Amazon Pinpoint to notify the security team.

Answer: ABE

NEW QUESTION 194

- (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 Cloud.
- 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 195

- (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 200

- (Exam Topic 2)

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

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

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

Answer: ACF

NEW QUESTION 203

- (Exam Topic 2)

A company runs a software-as-a-service (SaaS) application on AWS. The application consists 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 handler function.
- C. Migrate the database to Amazon Aurora and add a read replica
- D. Use Amazon Route 53 weighted records
- E. Migrate the database to Amazon Aurora and add an Aurora Replica
- F. Configure Amazon RDS Proxy to manage database connection pools.

Answer: D

NEW QUESTION 205

- (Exam Topic 2)

A company is running a serverless application that consists of several AWS Lambda functions and Amazon DynamoDB tables. The company has created new functionality that requires the Lambda functions to access an Amazon Neptune DB cluster The Neptune DB cluster is located in three subnets in a VPC.

Which of the possible solutions will allow the Lambda functions to access the Neptune DB cluster and DynamoDB tables? (Select TWO)

- A. Create three public subnets in the Neptune VPC and route traffic through an internet gateway Host the Lambda functions in the three new public subnets
- B. Create three private subnets in the Neptune VPC and route internet traffic through a NAT gateway Host the Lambda functions in the three new private subnets.
- C. Host the Lambda functions outside the VPC
- D. Update the Neptune security group to allow access from the IP ranges of the Lambda functions.
- E. Host the Lambda functions outside the VPC
- F. Create a VPC endpoint for the Neptune database, and have the Lambda functions access Neptune over the VPC endpoint
- G. Create three private subnets in the Neptune VPC
- H. Host the Lambda functions in the three new isolated subnet
- I. Create a VPC endpoint for DynamoDB
- J. and route DynamoDB traffic to the VPC endpoint

Answer: AC

NEW QUESTION 210

- (Exam Topic 2)

A company is configuring connectivity to a multi-account AWS environment to support application workloads that serve users in a single geographic region. The workloads depend on a highly available, on-premises legacy system deployed across two locations It is critical for the AWS workloads to maintain connectivity to the legacy system, and a minimum of 5 Gbps of bandwidth is required All application workloads within AWS must have connectivity with one another.

Which solution will meet these requirements?

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

Answer: B

NEW QUESTION 211

- (Exam Topic 2)

A company runs applications on Amazon EC2 instances. The company plans to begin using an Auto Scaling group for the instances. As part of this transition, a

solutions architect must ensure that Amazon CloudWatch Logs automatically collects logs from all new instances. The new Auto Scaling group will use a launch template that includes the Amazon Linux 2 AMI and no key pair. Which solution meets these requirements?

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

Answer: B

NEW QUESTION 214

- (Exam Topic 2)

A company plans to refactor a monolithic application into a modern application designed to be deployed on AWS. The CI/CD pipeline needs to be upgraded to support the modern design for the application with the following requirements:

- It should allow changes to be released several times every hour.
- * It should be able to roll back the changes as quickly as possible. Which design will meet these requirements?

- A. Deploy a CI-CD pipeline that incorporates AMIs to contain the application and their configurations. Deploy the application by replacing Amazon EC2 instances.
- B. Specify AWS Elastic Beanstalk to serve as a secondary environment as the deployment target for the CI/CD pipeline of the application.
- C. To deploy, swap the staging and production environment URLs.
- D. Use AWS Systems Manager to re-provision the infrastructure for each deployment. Update the Amazon EC2 user data to pull the latest code artifact from Amazon S3 and use Amazon Route 53 weighted routing to point to the new environment.
- E. Roll out application updates as part of an Auto Scaling event using a prebuilt AMI.
- F. Use new versions of the AMIs to add instances, and phase out all instances that use the previous AMI version with the configured termination policy during a deployment event.

Answer: B

Explanation:

It is the fastest when it comes to rollback and deploying changes every hour.

NEW QUESTION 215

- (Exam Topic 2)

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

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

What CI/CD configuration meets all of the requirements?

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

Answer: B

NEW QUESTION 216

- (Exam Topic 2)

A large education company recently introduced Amazon Workspaces to provide access to internal applications across multiple universities. The company is storing user proxies on an Amazon FSx for Windows File Server file system. The file system is configured with a DNS alias and is connected to a self-managed Active Directory. As more users begin to use the Workspaces, login time increases to unacceptable levels.

An investigation reveals a degradation in performance of the file system. The company created the file system on HDD storage with a throughput of 16 MBps. A solutions architect must improve the performance of the file system during a defined maintenance window.

What should the solutions architect do to meet these requirements with the LEAST administrative effort?

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

the file system Choose to restore previous versions Create a new FSx for Windows File Server file system with SSD storage and 32 MBps of throughput When the copy job is completed, adjust the DNS alias Delete the original file system

Answer: D

NEW QUESTION 218

- (Exam Topic 2)

A news company wants to implement an AWS Lambda function that calls an external API to receive new press releases every 10 minutes. The API provider is planning to use an IP address allow list to protect the API. so the news company needs to provide any public IP addresses that access the API. The company's current architecture includes a VPC with an internet gateway and a NAT gateway. A solutions architect must implement a static IP address for the Lambda function.

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

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

Answer: AC

NEW QUESTION 222

.....

Relate Links

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

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

Contact us

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

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