Exam	:	**SAP-C01**
Title	:	AWS Certified Solutions Architect - Professional
Vendor	:	Amazon
Version	:	V27.95

NO.1 A retail company runs a business-critical web service on an Amazon Elastic Container Service (Amazon ECS) cluster that runs on Amazon EC2 instances The web service receives POST requests from end users and writes data to a MySQL database that runs on a separate EC2 instance The company needs to ensure that data loss does not occur.

The current code deployment process includes manual updates of the ECS service During a recent deployment, end users encountered intermittent 502 Bad Gateway errors in response to valid web requests The company wants to implement a reliable solution to prevent this issue from recurring. The company also wants to automate code deployments. The solution must be highly available and must optimize cost-effectiveness Which combination of steps will meet these requirements? (Select THREE.)

(A). Run the web service on an ECS cluster that has a Fargate launch type Use AWS CodePipeline and AWS CodeDeploy to perform a blue/green deployment with validation testing to update the ECS service.

(B). Migrate the MySQL database to run on an Amazon RDS for MySQL Multi-AZ DB instance that uses Provisioned IOPS SSD (io2) storage

(C). Configure an Amazon Simple Queue Service (Amazon SQS) queue as an event source to receive the POST requests from the web service Configure an AWS Lambda function to poll the queue Write the data to the database.

(D). Run the web service on an ECS cluster that has a Fargate launch type Use AWS CodePipeline and AWS CodeDeploy to perform a canary deployment to update the ECS service.

Answer: C,D

NO.2 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 database. Serve the data through a Network Load Balancer (NLB). Authenticate users using the NLB with credentials stored in AWS Secrets Manager.

(B). Store the data in an Amazon S3 bucket. 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.

(C). Store the data in an Amazon Aurora Serverless database. 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.

(D). Store the data in an Amazon S3 bucket. Serve the data through Amazon Athena using AWS PrivateLink to secure the data in transit.

Answer: C

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)."

NO.3 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

NO.4 A company is collecting a large amount of data from a fleet of IoT devices. Data is stored as Optimized Row Columnar (ORC) files in the Hadoop Distributed File System (HDFS) on a persistent Amazon EMR cluster. The company's data analytics team queries the data by using SQL in Apache Presto deployed on the same EMR cluster Queries scan large amounts of data always run for less than 15 minutes, and run only between 5 PM and 10 PM.
The company is concerned about the high cost associated with the current solution A solutions architect must propose the most cost-effective solution that will allow SQL data queries.
Which solution will meet these requirements?
(A). Store data m Amazon S3 Use Amazon Redshift Spectrum to query data.
(B). Store data m Amazon S3 Use the AWS Glue Data Catalog and Amazon Athena to query data.
(C). Store data in EMR File System (EMRFS). Use Presto n Amazon EMR to query data.
(D). Store data m Amazon Redshift Use Amazon Redshift to query data
Answer: B

NO.5 A company has developed a single-page web application in JavaScript. The source code is

stored in a single Amazon S3 bucket in the us-east-1 Region. The company serves the web application to a global user base through Amazon CloudFront.
The company wants to experiment with two versions of the website without informing application users. Each version of the website will reside in its own S3 bucket. The company wants to determine which version is most successful in marketing a new product.
The solution must send application users that are based in Europe to the new website design. The solution must send application users that are based in the United States to the current website design. However, some exceptions exist. The company needs to be able to redirect specific users to the new website design, regardless of the users' location.
Which solution meets these requirements?
(A). Configure two CloudFront distributions. Configure a geolocation routing policy in Amazon Route 53 to route traffic to the appropriate CloudFront endpoint based on the location of clients.
(B). Configure a single CloudFront distribution. Create a behavior with different paths for each version of the site. Configure Lambda@Edge on the default path to generate redirects and send the client to the correct version of the website.
(C). Configure a single CloudFront distribution. Configure an alternate domain name on the distribution. Configure two behaviors to route users to the different S3 origins based on the domain name that the client uses in the HTTP request.

Answer: A
D.
Configure a single CloudFront distribution with Lambda@Edge. Use Lambda@Edge to send user requests to different origins based on request attributes.

NO.6 A solutions architect is importing a VM from an on-premises environment by using the Amazon EC2 VM Import feature of AWS Import/Export The solutions architect has created an AMI and has provisioned an Amazon EC2 instance that is based on that AMI The EC2 instance runs inside a public subnet in a VPC and has a public IP address assigned The EC2 instance does not appear as a managed instance in the AWS Systems Manager console Which combination of steps should the solutions architect take to troubleshoot this issue"? (Select TWO)
(A). Verify that Systems Manager Agent is installed on the instance and is running
(B). Verify that the instance is assigned an appropriate IAM role for Systems Manager
(C). Verify the existence of a VPC endpoint on the VPC
(D). Verify that the AWS Application Discovery Agent is configured
(E). Verify the correct configuration of service-linked roles for Systems Manager

Answer: A,B,D

NO.7 A company needs to create and manage multiple AWS accounts for a number of departments from a central location. The security team requires read-only access to all accounts from its own AWs account. The company is using AWS Organizations and created an account tor the security team.
How should a solutions architect meet these requirements?
(A). Use the OrganizationAccountAccessRole IAM role to create a new IAM policy wilh read-only access in each member account. Establish a trust relationship between the IAM policy in each member account and the security account. Ask the security team lo use the IAM policy to gain access.
(B). Use the OrganizationAccountAccessRole IAM role to create a new IAM role with read-only access in each member account. Establish a trust relationship between the IAM role in each member account and the security account. Ask the security team lo use the IAM role to gain access.

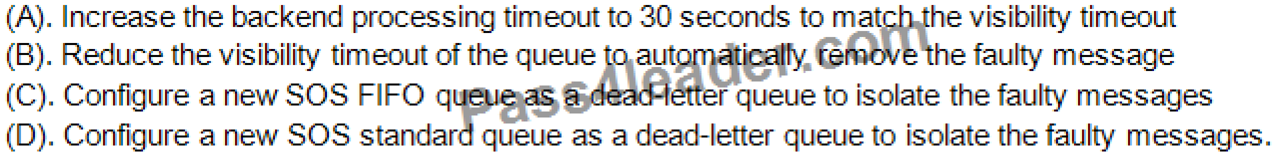
(C). Ask the security team to use AWS Security Token Service (AWS STS) to call the AssumeRole API for the OrganizationAccountAccessRole IAM role in the master account from the security account. Use the generated temporary credentials to gain access.
(D). Ask the security team to use AWS Security Token Service (AWS STS) to call the AssumeRole API for the OrganizationAccountAccessRole IAM role in the member account from the security account. Use the generated temporary credentials to gain access.
Answer: D

NO.8 A company is serving files to Its customers through an SFTP server that is accessible over the internet The SFTP server is running on a single Amazon EC2 instance with an Elastic IP address attached Customers connect to the SFTP server through its Elastic IP address and use SSH (or authentication. The EC2 instance also has an attached security group that allows access from all customer IP addresses.
A solutions architect must implement a solution to improve availability, minimize the complexity of infrastructure management, and minimize the disruption to customers who access files The solution must not change the way customers connect.
Which solution will meet these requirements?
(A). Disassociate the Elastic IP address from the EC2 instance. Create an Amazon S3 bucket to be used for SFTP file hosting. Create an AWS Transfer Family server Configure the Transfer Family server with a publicly accessible endpoint Associate the SFTP Elastic IP address with the new endpoint Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to the S3 bucket.
(B). Disassociate the Elastic IP address from the EC2 instance. Create an Amazon S3 bucket to be used for SFTP file hosting. Create an AWS Transfer Family server. Configure the Transfer Family server with a VPC-hosted. internet-facing endpoint. Associate the SFTP Elastic IP address with the new endpoint. Attach the security group with customer IP addresses to the new endpoint. Point the Transfer Family server to the S3 bucket Sync all files from the SFTP server to the S3 bucket.
(C). Disassociate the Elastic IP address from the EC2 instance. Create a new Amazon Elastic File System {Amazon EFS) file system to be used for SFTP file hosting. Create an AWS Fargate task definition to run an SFTP server. Specify the EFS file system as a mount in the task definition. Create a Fargate service by using the task definition, and place a Network Load Balancer (NLB) in front of the service When configuring the service, attach the security group with customer IP addresses to the tasks that run the SFTP server. Associate the Elastic IP address with the NLB. Sync all files from the SFTP server to the S3 bucket.
(D). Disassociate the Elastic IP address from the EC2 instance. Create a multi-attach Amazon Elastic Block Store (Amazon EBS) volume to be used for SFTP file hosting. Create a Network Load Balancer (NLB) with the Elastic IP address attached. Create an Auto Scaling group with EC2 instances that run an SFTP server Define in the Auto Scaling group that instances that are launched should attach the new multi-attach EBS volume Configure the Auto Scaling group to automatically add instances behind the NLB Configure the Auto Scaling group to use the security group that allows customer IP addresses for the EC2 instances that the Auto Scaling group launches. Sync all files from the SFTP server to the new multi-attach EBS volume.
Answer: B
https://docs.aws.amazon.com/transfer/latest/userguide/create-server-in-vpc.html
https://aws.amazon.com/premiumsupport/knowledge-center/aws-sftp-endpoint-type/

NO.9 A car rental company has built a serverless REST API to provide data to its mobile app. The app

consists of an Amazon API Gateway API with a Regional endpoint, AWS Lambda functions and an Amazon Aurora MySQL Serverless DB cluster The company recently opened the API to mobile apps of partners A significant increase in the number of requests resulted causing sporadic database memory errors Analysis of the API traffic indicates that clients are making multiple HTTP GET requests for the same queries in a short period of time Traffic is concentrated during business hours, with spikes around holidays and other events The company needs to improve its ability to support the additional usage while minimizing the increase in costs associated with the solution.
Which strategy meets these requirements?
(A). Convert the API Gateway Regional endpoint to an edge-optimized endpoint Enable caching in the production stage.
(B). Implement an Amazon ElastiCache for Redis cache to store the results of the database calls Modify the Lambda functions to use the cache
(C). Modify the Aurora Serverless DB cluster configuration to increase the maximum amount of available memory
(D). Enable throttling in the API Gateway production stage Set the rate and burst values to limit the incoming calls
Answer: A

NO.10 A company has implemented an ordering system using an event-dnven architecture. Dunng initial testing, the system stopped processing orders Further tog analysis revealed that one order message in an Amazon Simple Queue Service (Amazon SOS) standard queue was causing an error on the backend and blocking all subsequent order messages The visibility timeout of the queue is set to 30 seconds, and the backend processing timeout is set to 10 seconds. A solutions architect needs to analyze faulty order messages and ensure that the system continues to process subsequent messages Which step should the solutions architect take to meet these requirements?



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

Answer: D

NO.11 A company is creating a sequel for a popular online game. A large number of users from all over the world will play the game within the first week after launch. Currently, the game consists of the following components deployed in a single AWS Region:
* Amazon S3 bucket that stores game assets
* Amazon DynamoDB table that stores player scores
A solutions architect needs to design a Region solution that wifi reduce latency improve reliability, and require the least effort to implement What should the solutions architect do to meet these requirements'
(A). Create an Amazon CloudFront distribution to serve assets from the S3 bucket Configure S3 Cross-Region Replication Create a new DynamoDB able in a new Region Use the new table as a replica target tor DynamoDB global tables.
(B). Create an Amazon CloudFront distribution to serve assets from the S3 bucket. Configure S3 Same-Region Replication. Create a new DynamoDB able m a new Region. Configure asynchronous replication between the DynamoDB tables by using AWS Database Migration Service (AWS DMS) with change data capture (CDC)

(C). Create another S3 bucket in a new Region and configure S3 Cross-Region Replication between the buckets Create an Amazon CloudFront distribution and configure origin failover with two origins accessing the S3 buckets in each Region. Configure DynamoDB global tables by enabling Amazon DynamoDB Streams, and add a replica table in a new Region.
(D). Create another S3 bucket in the same Region, and configure S3 Same-Region Replication between the buckets- Create an Amazon CloudFront distribution and configure origin failover with two origin accessing the S3 buckets Create a new DynamoDB table m a new Region Use the new table as a replica target for DynamoDB global tables.
Answer: B

NO.12 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 servers. Use the AMIs to provision EC2 instances to recreate the applications in the AWS.
Cloud. Place an Application Load Balancer (ALB) in front of the EC2 instances. Use Amazon Route 53 to point the DNS names of the web forms to the ALB.
(B). 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. Create an Amazon Kinesis data stream to receive the data input and store the input in DynamoDB. Use Amazon Route 53 to point the DNS names of the web forms to the Kinesis data stream's endpoint.
(C). Create Docker images for each server of the legacy web form applications. Create an Amazon Elastic Container Service (Amazon ECS) cluster on AWS Fargate. Place an Application Load Balancer in front of the ECS cluster. Use Fargate task storage to store the web form data.
(D). 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.
Answer: D
Provision an Amazon Aurora Serverless cluster. Build multiple schemas for each web forms data storage. Use Amazon API Gateway and an AWS Lambda function to recreate the data input forms. Use Amazon Route 53 to point the DNS names of the web forms to their corresponding API Gateway endpoint.

NO.13 A company stores sales transaction data in Amazon DynamoDB tables. To detect anomalous behaviors and respond quickly, all changes lo the items stored in the DynamoDB tables must be logged within 30 minutes.
Which solution meets the requirements?
(A). Copy the DynamoDB tables into Apache Hive tables on Amazon EMR every hour and analyze them (or anomalous behaviors. Send Amazon SNS notifications when anomalous behaviors are detected.
(B). Use AWS CloudTrail to capture all the APIs that change the DynamoDB tables. Send SNS

notifications when anomalous behaviors are detected using CloudTrail event filtering.
(C). Use Amazon DynamoDB Streams to capture and send updates to AWS Lambda. Create a Lambda function to output records lo Amazon Kinesis Data Streams. Analyze any anomalies with Amazon Kinesis Data Analytics. Send SNS notifications when anomalous behaviors are detected.
(D). Use event patterns in Amazon CloudWatch Events to capture DynamoDB API call events with an AWS Lambda (unction as a target to analyze behavior. Send SNS notifications when anomalous behaviors are detected.
Answer: C
https://aws.amazon.com/blogs/database/dynamodb-streams-use-cases-and-design-patterns/#:~:text=DynamoDB%20Streams%20is%20a%20powerful,for%20up%20to%2024%20hours.
DynamoDb Stream to capture DynamoDB update. And Kinesis Data Analytics for anomaly detection (it uses AWS proprietary Random Cut Forest Algorithm)

NO.14 A company is using AWS Organizations lo manage multiple AWS accounts For security purposes, the company requires the creation of an Amazon Simple Notification Service (Amazon SNS) topic that enables integration with a third-party alerting system in all the Organizations member accounts A solutions architect used an AWS CloudFormation template to create the SNS topic and stack sets to automate the deployment of CloudFormation stacks Trusted access has been enabled in Organizations What should the solutions architect do to deploy the CloudFormation StackSets in all AWS accounts?
(A). Create a stack set in the Organizations member accounts. Use service-managed permissions. Set deployment options to deploy to an organization. Use CloudFormation StackSets drift detection.
(B). Create stacks in the Organizations member accounts. Use self-service permissions. Set deployment options to deploy to an organization. Enable the CloudFormation StackSets automatic deployment.
(C). Create a stack set in the Organizations management account Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets automatic deployment.
(D). Create stacks in the Organizations management account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets drift detection.
Answer: C

NO.15 A company has a data lake in Amazon S3 that needs to be accessed by hundreds of applications across many AWS accounts. The company's information security policy states that the S3 bucket must not be accessed over the public internet and that each application should have the minimum permissions necessary to function.
To meet these requirements, a solutions architect plans to use an S3 access point that is restricted to specific VPCs tor each application.
Which combination of steps should the solutions architect take to implement this solution? (Select TWO.)
(A). Create an S3 access point for each application in the AWS account that owns the S3 bucket. Configure each access point to be accessible only from the application's VPC. Update the bucket policy to require access from an access point.
(B). Create an interface endpoint for Amazon S3 in each application's VPC. Configure the endpoint policy to allow access to an S3 access point. Create a VPC gateway attachment for the S3 endpoint.
(C). Create a gateway endpoint lor Amazon S3 in each application's VPC. Configure the endpoint

policy to allow access to an S3 access point. Specify the route table that is used to access the access point.
(D). Create an S3 access point for each application in each AWS account and attach the access points to the S3 bucket. Configure each access point to be accessible only from the application's VPC. Update the bucket policy to require access from an access point.
(E). Create a gateway endpoint for Amazon S3 in the data lake's VPC. Attach an endpoint policy to allow access to the S3 bucket. Specify the route table that is used to access the bucket.
Answer: A,C
https://joe.blog.freemansoft.com/2020/04/protect-data-in-cloud-with-s3-access.html
https://aws.amazon.com/s3/features/access-points/
https://aws.amazon.com/s3/features/access-points/
& https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/

NO.16 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 VPCs. Create a Route 53 inbound resolver in the shared services VPC. 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.
(B). Associate the private hosted zone to all the VPCs. Deploy an Amazon EC2 conditional forwarder in the shared services VPC. 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.
(C). Associate the private hosted zone to the shared services VPC. Create a Route 53 outbound resolver in the shared services VPC. 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.
(D). Associate the private hosted zone to the shared services VPC. Create a Route 53 inbound resolver in the shared services VPC. 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
https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-dns-management-of-hybrid-cloud-with-amazon-route-53-and-aws-transit-gateway/

NO.17 A company is building a hybrid solution between its existing on-premises systems and a new backend in AWS. The company has a management application to monitor the state of its current IT infrastructure and automate responses to issues. The company wants to incorporate the status of its consumed AWS services into the application. The application uses an HTTPS endpoint to receive updates.
Which approach meets these requirements with the LEAST amount of operational overhead?
(A). Configure AWS Systems Manager OpsCenter to ingest operational events from the on-premises

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

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

NO.18 A company that is developing a mobile game is making game assets available in two AWS Regions. Game assets ate served from a set of Amazon EC2 instances behind an Application Load Balancer (ALB) in each Region. The company requires game assets to be (etched from the closest Region. If game assets become unavailable in the closest Region, they should be fetched from the other Region.
What should a solutions architect do to meet these requirements?
(A). Create an Amazon CloudFront distribution. Create an origin group with one origin for each ALB. Set one of the origins as primary.
(B). Create an Amazon Route 53 health check for each ALB. Create a Route 53 failover routing record pointing to the two ALBs. Set the Evaluate Target Health value to Yes.
(C). Create two Amazon CloudFront distributions, each with one ALB as the origin. Create an Amazon Route 53 failover routing record pointing to the two CloudFront distributions. Set the Evaluate Target Health value to Yes.
(D). Create an Amazon Route 53 health check for each ALB. Create a Route 53 latency alias record pointing to the two ALBs. Set the Evaluate Target Health value to Yes.

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

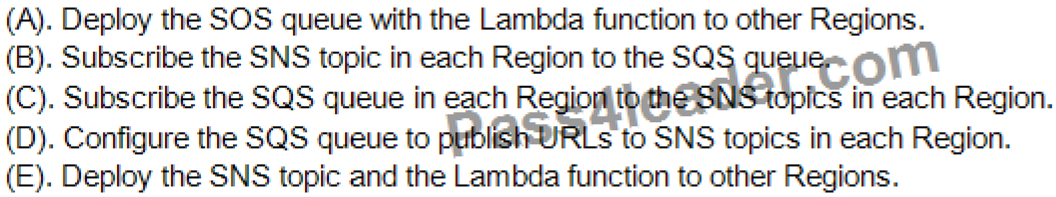
NO.19 An AWS customer has a web application that runs on premises. The web application fetches data from a third-party API that is behind a firewall. The third party accepts only one public CIDR block in each client's allow list.
The customer wants to migrate their web application to the AWS Cloud. The application will be

hosted on a set of Amazon EC2 instances behind an Application Load Balancer (ALB) in a VPC. The ALB is located in public subnets. The EC2 instances are located in private subnets. NAT gateways provide internet access to the private subnets.
How should a solutions architect ensure that the web application can continue to call the third-parly API after the migration?
(A). Associate a block of customer-owned public IP addresses to the VPC. Enable public IP addressing for public subnets in the VPC.
(B). Register a block of customer-owned public IP addresses in the AWS account. Create Elastic IP addresses from the address block and assign them lo the NAT gateways in the VPC.
(C). Create Elastic IP addresses from the block of customer-owned IP addresses. Assign the static Elastic IP addresses to the ALB.
(D). Register a block of customer-owned public IP addresses in the AWS account. Set up AWS Global Accelerator to use Elastic IP addresses from the address block. Set the ALB as the accelerator endpoint.

Answer: B

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

NO.20 A company runs a serverless application in a single AWS Region. The application accesses external URLs and extracts metadata from those sites. The company uses an Amazon Simple Notification Service (Amazon SNS) topic to publish URLs to an Amazon Simple Queue Service (Amazon SQS) queue An AWS Lambda function uses the queue as an event source and processes the URLs from the queue Results are saved to an Amazon S3 bucket The company wants to process each URL other Regions to compare possible differences in site localization URLs must be published from the existing Region. Results must be written to the existing S3 bucket in the current Region.
Which combination of changes will produce multi-Region deployment that meets these requirements? (Select TWO.)



(A). Deploy the SOS queue with the Lambda function to other Regions.
(B). Subscribe the SNS topic in each Region to the SQS queue.
(C). Subscribe the SQS queue in each Region to the SNS topics in each Region.
(D). Configure the SQS queue to publish URLs to SNS topics in each Region.
(E). Deploy the SNS topic and the Lambda function to other Regions.

Answer: C,D

NO.21 A company standardized its method of deploying applications to AWS using AWS CodePipeline and AWS Cloud Formation. The applications are in Typescript and Python. The company has recently acquired another business that deploys applications to AWS using Python scripts.
Developers from the newly acquired company are hesitant to move their applications under CloudFormation because it would require than they learn a new domain-specific language and eliminate their access to language features, such as looping.
How can the acquired applications quickly be brought up to deployment standards while addressing the developers' concerns?
(A). Create CloudFormation templates and re-use parts of the Python scripts as instance user data. Use the AWS Cloud Development Kit (AWS CDK) to deploy the application using these templates.

Incorporate the AWS CDK into CodePipeline and deploy the application to AWS using these templates.
(B). Use a third-party resource provisioning engine inside AWS CodeBuild to standardize the deployment processes of the existing and acquired company. Orchestrate the CodeBuild job using CodePipeline.
(C). Standardize on AWS OpsWorks. Integrate OpsWorks with CodePipeline. Have the developers create Chef recipes to deploy their applications on AWS.
(D). Define the AWS resources using Typescript or Python. Use the AWS Cloud Development Kit (AWS CDK) to create CloudFormation templates from the developers' code, and use the AWS CDK to create CloudFormation stacks. Incorporate the AWS CDK as a CodeBuild job in CodePipeline.
Answer: D

NO.22 A large company has a business-critical application that runs in a single AWS Region The application consists of multiple Amazon EC2 instances and an Amazon RDS Multi-AZ DB instance The EC2 instances run In an Amazon EC2 Auto Scaling group across multiple Availability Zones A solutions architect is implementing a disaster recovery (DR) plan for the application The solutions architect has created a pilot light application deployment in a new Region, which is referred to as the DR Region The DR environment has an Auto Scaling group with a single EC2 instance and a read replica of the RDS DB instance The solutions architect must automate a failover from the primary application environment to the pilot light environment in the DR Region Which solution meets these requirements with the MOST operational efficiency''
(A). Publish an application availability metric to Amazon CloudWatch in the DR Region from the application environment in the primary Region Create a CloudWatch alarm in the DR Region that is invoked when the application availability metric stops being delivered Configure the CloudWatch alarm to send a notification to an Amazon Simple Notification Service (Amazon SNS> topic in the DR Region Add an email subscription to the SNS topic that sends messages to the application owner upon notification, instruct a systems operator to sign in to the AWS Management Console and initiate failover operations for the application
(B). Create a cron task that runs every 5 minutes by using one of the application's EC2 instances in the primary Region Configure the cron task to check whether the application is available Upon failure, the cron task notifies a systems operator and attempts to restart the application services
(C). Create a cron task that runs every 5 minutes by using one of the application's EC2 instances in the primary Region Configure the cron task to check whether the application is available Upon failure, the cron task modifies the DR environment by promoting the read replica and by adding EC2 instances to the Auto Scaling group
(D). Publish an application availability metric to Amazon CloudWatch in the DR Region from the application environment in the primary Region Create a CloudWatch alarm in the DR Region that is invoked when the application availability metric stops being delivered Configure the CloudWatch alarm to send a notification to an Amazon Simple Notification Service (Amazon SNS) topic in the DR Region Use an AWS Lambda function that is invoked by Amazon SNS in the DR Region to promote the read replica and to add EC2 instances to the Auto Scaling group
Answer: D

NO.23 A company hosts a photography website on AWS that has global visitors. The website has experienced steady increases in traffic during the last 12 months, and users have reported a delay in displaying images. The company wants to configure Amazon CloudFront lo deliver photos to visitors

with minimal latency.
Which actions will achieve this goal? (Select TWO.)
(A). Set the Minimum TTL and Maximum TTL to 0 in the CloudFront distribution.
(B). Set the Minimum TTL and Maximum TTL to a high value in the CloudFront distribution.
(C). Set the CloudFront distribution to forward all headers, all cookies, and all query strings to the origin.
(D). Set up additional origin servers that are geographically closer to the requesters. Configure latency-based routing in Amazon Route 53.
(E). Select Price Class 100 on Ihe CloudFront distribution.
Answer: B,D

NO.24 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. Create an AWS WAF web ACL with a rule to block clients "hat submit more than five requests per day. Associate the web ACL with the CloudFront distribution. Configure CloudFront with an origin access identity (OAI) and associate it with the distribution. Configure API Gateway to ensure only the OAI can execute the POST method.
(B). Create an Amazon CloudFront distribution with the API as the origin. Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per day. Associate the web ACL with the CloudFront distribution. Add a custom header to the CloudFront distribution populated with an API key. Configure the API to require an API key on the POST method.
(C). 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. Create a resource policy with a request limit and associate it with the API. Configure the API to require an API key on the POST method.
(D). Associate the web ACL with the API. Create a usage plan with a request limit and associate it with the API. Create an API key and add it to the usage plan.
Answer: D
"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

NO.25 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. Remediate any issues Then use AWS DMS to migrate the data
(C). Use the M5 or CS DMS replication instance type for ongoing replication
(D). Turn off automatic backups and logging of the target database until the migration and cutover processes are complete
Answer: B
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Backups.html

NO.26 A company's site reliability engineer is performing a review of Amazon FSx for Windows File Server deployments within an account that the company acquired Company policy states that all Amazon FSx file systems must be configured to be highly available across Availability Zones.
During the review, the site reliability engineer discovers that one of the Amazon FSx file systems used a deployment type of Single-AZ 2 A solutions architect needs to minimize downtime while aligning this Amazon FSx file system with company policy.
What should the solutions architect do to meet these requirements?
(A). Reconfigure the deployment type to Multi-AZ for this Amazon FSx tile system
(B). Create a new Amazon FSx fie system with a deployment type o(Multi-AZ. Use AWS DataSync to transfer data to the new Amazon FSx file system. Point users to the new location
(C). Create a second Amazon FSx file system with a deployment type of Single-AZ 2. Use AWS DataSync to keep the data n sync. Switch users to the second Amazon FSx fie system in the event of failure
(D). Use the AWS Management Console to take a backup of the Amazon FSx He system Create a new Amazon FSx file system with a deployment type of Multi-AZ Restore the backup
Answer: B
to the new Amazon FSx file system. Point users to the new location.

NO.27 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. 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
(C). Update the existing VPC. and associate an Amazon-provided IPv6 CIDR block with the VPC and ail subnets Create an egress-only internet gateway Update the VPC route tables for all private subnets, and add a route for /0 to the egress-only internet gateway
(D). Update the existing VPC and associate a custom IPv6 CIDR block with the VPC and all subnets Create a new NAT gateway, and enable IPv6 support Update the VPC route tables for all private subnets and add a route for 70 to the IPv6-enabled NAT gateway.

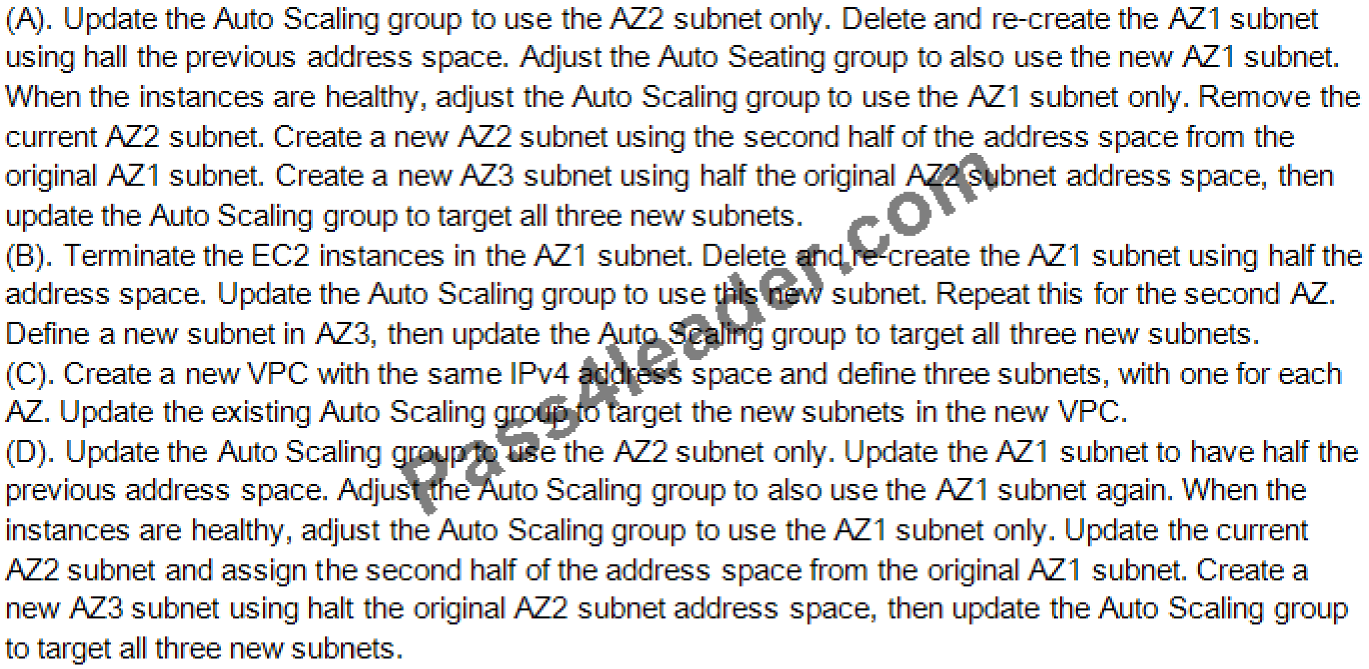
Answer: C

NO.28 A company is running an application distributed over several Amazon EC2 instances in an Auto Seating group behind an Application Load Balancer The security team requires that all application access attempts be made available for analysis information about the client IP address, connection type, and user agent must be included Which solution will meet these requirements?
(A). Enable EC2 detailed monitoring, and include network 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. Send all traffic information through Amazon Kinesis Data Firehose to an Amazon Elasticsearch Service (Amazon ES) cluster that the security team uses for analysis.
Answer: C
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html
https://docs.aws.amazon.com/vpc/latest/mirroring/what-is-traffic-mirroring.html

NO.29 A company manages multiple AWS accounts by using AWS Organizations. Under the root OU. the company has two OUs: Research and DataOps.
Because of regulatory requirements, all resources that the company deploys in the organization must reside in the ap-northeast-1 Region. Additionally. EC2 instances that the company deploys in the DataOps OU must use a predefined list of instance types A solutions architect must implement a solution that applies these restrictions. The solution must maximize operational efficiency and must minimize ongoing maintenance Which combination of steps will meet these requirements? (Select TWO)
(A). Create an IAM role in one account under the DataOps OU Use the ec2 Instance Type condition key in an inline policy on the role to restrict access to specific instance types.
(B). Create an IAM user in all accounts under the root OU Use the aws RequestedRegion condition key in an inline policy on each user to restrict access to all AWS Regions except ap-northeast-1.
(C). Create an SCP Use the aws:RequestedRegion condition key to restrict access to all AWS Regions except ap-northeast-1 Apply the SCP to the root OU.
(D). Create an SCP Use the ec2Region condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root OU. the DataOps OU. and the Research OU.
(E). Create an SCP Use the ec2:InstanceType condition key to restrict access to specific instance types Apply the SCP to the DataOps OU.
Answer: C,E

NO.30 A solutions architect has an operational workload deployed on Amazon EC2 instances in an Auto Scaling group. The VPC architecture spans two Availability Zones (AZ) with a subnet in each that the Auto Scaling group is targeting. The VPC is connected to an on-premises environment and connectivity cannot be interrupted. The maximum size ol the Auto Scaling group is 20 instances in service. The VPC IPv4 addressing is as follows:

VPC CIDR: 10.0.0.0/23
AZ1 subnet CIDR: 10.0.0.0/24
AZ2 subnet CIDR: 10.0.1.0/24
Since deployment, a third AZ has become available in the Region. The solutions architect wants to adopt the new AZ without adding additional IPv4 address space and without service downtime.
Which solution will meet these requirements?



(A). Update the Auto Scaling group to use the AZ2 subnet only. Delete and re-create the AZ1 subnet using hall the previous address space. Adjust the Auto Seating group to also use the new AZ1 subnet. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only. Remove the current AZ2 subnet. Create a new AZ2 subnet using the second half of the address space from the original AZ1 subnet. 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.
(B). Terminate the EC2 instances in the AZ1 subnet. Delete and re-create the AZ1 subnet using half the address space. Update the Auto Scaling group to use this new subnet. Repeat this for the second AZ. Define a new subnet in AZ3, then update the Auto Scaling group to target all three new subnets.
(C). Create a new VPC with the same IPv4 address space and define three subnets, with one for each AZ. Update the existing Auto Scaling group to target the new subnets in the new VPC.
(D). Update the Auto Scaling group to use the AZ2 subnet only. Update the AZ1 subnet to have half the previous address space. Adjust the Auto Scaling group to also use the AZ1 subnet again. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only. Update the current AZ2 subnet and assign the second half of the address space from the original AZ1 subnet. Create a new AZ3 subnet using halt the original AZ2 subnet address space, then update the Auto Scaling group to target all three new subnets.

Answer: A
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.

NO.31 A company is using AWS Organizations lo manage multiple accounts. Due to regulatory requirements, the company wants to restrict specific member accounts to certain AWS Regions, where they are permitted to deploy resources. The resources in the accounts must be tagged, enforced based on a group standard, and centrally managed with minimal configuration.
What should a solutions architect do to meet these requirements?
(A). Create an AWS Config rule in the specific member accounts to limit Regions and apply a tag policy.
(B). From the AWS Billing and Cost Management console, in the master account, disable Regions for the specific member accounts and apply a tag policy on the root.
(C). Associate the specific member accounts with the root. Apply a tag policy and an SCP using conditions to limit Regions.
(D). Associate the specific member accounts with a new OU. Apply a tag policy and an SCP using conditions to limit Regions.
Answer: D

NO.32 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. Use Amazon Cognito federation and Login with Amazon for authentication and authorization.
(C). Create an API layer with Amazon API Gateway. Rehost the microservices on AWS Fargate containers.
(D). Create an API layer with Amazon API Gateway. Rehost the microservices on Amazon Elastic Container Service (Amazon ECS) containers.
(E). Replatform the database to Amazon RDS for MySQL.
(F). Replatform the database to Amazon Aurora MySQL Serverless.
Answer: A,C,E

NO.33 A company wants to control its cost of Amazon Athena usage The company has allocated a specific monthly budget for Athena usage A solutions architect must design a solution that will prevent the company from exceeding the budgeted amount Which solution will moot these requirements?
(A). Use AWS Budgets. Create an alarm (or when the cost of Athena usage reaches the budgeted amount for the month. Configure AWS Budgets actions to deactivate Athena until the end of the month.
(B). Use Cost Explorer to create an alert for when the cost of Athena usage reaches the budgeted amount for the month. Configure Cost Explorer to publish notifications to an Amazon Simple Notification Service (Amazon SNS) topic.
(C). Use AWS Trusted Advisor to track the cost of Athena usage. 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
(D). Use Athena workgroups to set a limit on the amount of data that can be scanned. Set a limit that is appropriate for the monthly budget and the current pricing for Athena.
Answer: D

NO.34 A web application is hosted in a dedicated VPC that is connected to a company's on-premises data center over a Site-to-Site VPN connection. The application is accessible from the company network only. This is a temporary non-production application that is used during business hours. The workload is generally low with occasional surges.
The application has an Amazon Aurora MySQL provisioned database cluster on the backend. The VPC has an internet gateway and a NAT gateways attached. The web servers are in private subnets in an Auto Scaling group behind an Elastic Load Balancer. The web servers also upload data to an Amazon S3 bucket through the internet.
A solutions architect needs to reduce operational costs and simplify the architecture.
Which strategy should the solutions architect use?
(A). Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only. Use 3-year scheduled Reserved Instances for

the web server EC2 instances. Detach the internet gateway and remove the NAT gateways from the VPC. Use an Aurora Servertess database and set up a VPC endpoint for the S3 bucket.
(B). Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only. Detach the internet gateway and remove the NAT gateways from the VPC. Use an Aurora Servertess database and set up a VPC endpoint for the S3 bucket, then update the network routing and security rules and policies related to the changes.
(C). Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only. Detach the internet gateway from the VPC, and use an Aurora Servertess database. Set up a VPC endpoint for the S3 bucket, then update the network routing and security rules and policies related to the changes.
(D). Use 3-year scheduled Reserved Instances for the web server Amazon EC2 instances. Remove the NAT gateways from the VPC, and set up a VPC endpoint for the S3 bucket. Use Amazon
(E). CloudWatch and AWS Lambda to stop and start the Aurora DB cluster so it operates during business hours only. Update the network routing and security rules and policies related to the changes.
Answer: B
The application is accessible from the company network only remove NAT and IGW, application - S3 with VPC endpoint. Non-Production application no need to go for Reserved instances To build site-to-site vpn, you don't need internet gateway. Instead, customer gateway is needed.
https://docs.aws.amazon.com/vpn/latest/s2svpn/SetUpVPNConnections.html#vpn-create-cgw

NO.35 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 an AWS accounts. The company plans to use Amazon Elasticsearch Service (Amazon ES) to perform log analyses in me logging account.
Which strategy should a solutions architect use to meet These requirements?
(A). Configure CloudTrail and VPC Flow Logs m each AWS account to send data to a centralized Amazon S3 Ducket in the fogging account. Create an AWS Lambda function to load data from the S3 bucket to Amazon ES m the togging account
(B). Configure CloudTrail and VPC Flow Logs to send data to a fog group m Amazon CloudWatch Logs n each AWS account Configure a CloudWatch subscription filter m each AWS account to send data to Amazon Kinesis Data Firehose In the fogging account Load data from Kinesis Data Firehose Into Amazon ES in the logging account
(C). Configure CloudTrail and VPC Flow Logs to send data to a separate Amazon S3 bucket In each AWS account. Create an AWS Lambda function triggered by S3 evens to copy the data to a centralized logging bucket. Create another Lambda function lo load data from the S3 bucket to Amazon ES in the logging account.
(D). Configure CloudTrail and VPC Flow Logs to send data to a fog group in Amazon CloudWatch Logs n each AWS account Create AWS Lambda functions in each AWS account to subscribe to the tog groups and stream the data to an Amazon S3 bucket in the togging account. Create another Lambda function to toad data from the S3 bucket to Amazon ES in the logging account.
Answer: A

NO.36 A company is migrating a legacy application from an on-premises data center to AWS. The application uses MangeDB as a key-value database According to the company's technical guidelines, all Amazon EC2 instances must be hosted in a private subnet without an internet connection In

addition, all connectivity between applications and databases must be encrypted. The database must be able to scale based on demand Which solution will meet these requirements?
(A). Create new Amazon DocumentDB (with MangeDB compatibility) tables for the application with Provisioned IOPS volumes Use the instance endpoint to connect to Amazon DocumentDB
(B). Create new Amazon DynamoDB tables for the application with on-demand capacity Use a gateway VPC endpoint for DynamoDB to connect lo the DynamoDB tables
(C). Create new Amazon DynamoDB tables for the application with on-demand capacity Use an interface VPC endpoint for DynamoDB to connect to the DynamoDB tables
(D). Create new Amazon DocumentDB (with MangeDB compatibility) tables for the application with Provisioned IOPS volumes Use the cluster endpoint to connect to Amazon DocumentDB
Answer: C

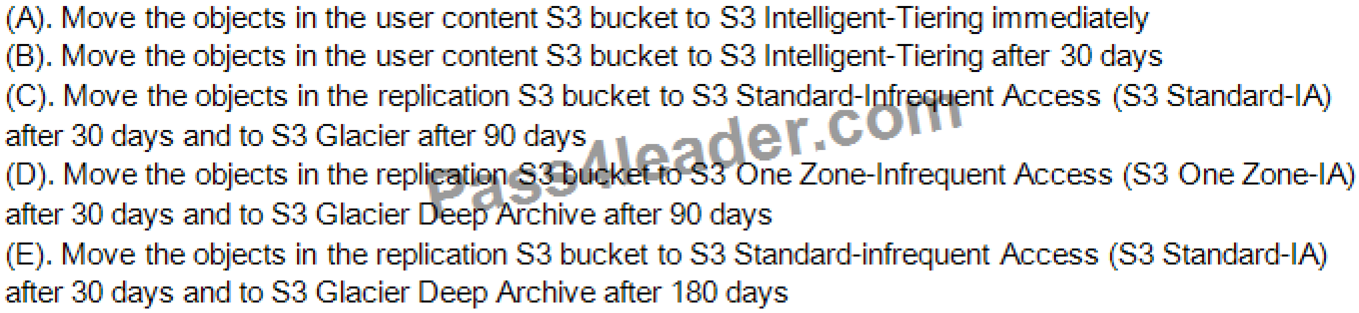
NO.37 A fitness tracking company serves users around the world, with its primary markets in North America and Asi a. The company needs to design an infrastructure for its read-heavy user authorization application with the following requirements:
* Be resilient to problems with the application in any Region.
* Write to a database in a single Region.
* Read from multiple Regions.
* Support resiliency across application tiers in each Region.
* Support the relational database semantics reflected in the application.
Which combination of steps should a solutions architect take? (Select TWO.)
(A). Use an Amazon Route 53 geoproximity routing policy combined with a multivalue answer routing policy.
(B). Deploy web. application, and MySQL database servers to Amazon EC2 instances in each Region. Set up the application so that reads and writes are local to the Region. Create snapshots of the web, application, and database servers and store the snapshots in an Amazon S3 bucket in both Regions. Set up cross-Region replication for the database layer.
(C). Use an Amazon Route 53 geolocation routing policy combined with a failover routing policy.
(D). Set up web, application, and Amazon RDS for MySQL instances in each Region. Set up the application so that reads are local and writes are partitioned based on the user. Set up a Multi-AZ failover for the web, application, and database servers. Set up cross-Region replication for the database layer.
(E). Set up active-active web and application servers in each Region. Deploy an Amazon Aurora global database with clusters in each Region. Set up the application to use the in-Region Aurora database endpoints. Create snapshots of the web and application servers and store them in an Amazon S3 bucket in both Regions.
Answer: C,E
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html Geoproximity routing policy is good to control the user traffic to specific regions. However, a multivalue answer routing policy may cause the users to be randomly sent to other healthy regions that may be far away from the user's location. You can use geolocation routing policy to direct the North American users to your servers on the North America region and configure failover routing to the Asia region in case the North America region fails. You can configure the same for the Asian users pointed to the Asia region servers and have the North America region as its backup.

NO.38 A company runs a popular public-facing ecommerce website. Its user base is growing quickly

from a local market to a national market. The website is hosted in an on-premises data center with web servers and a MySQL database. The company wants to migrate its workload (o AWS. A solutions architect needs to create a solution to:
* Improve security
* Improve reliability
* Improve availability
* Reduce latency
* Reduce maintenance
Which combination of steps should the solutions architect take to meet these requirements? (Select THREE.)
(A). Use Amazon EC2 instances in two Availability Zones for the web servers in an Auto Scaling group behind an Application Load Balancer.
(B). Migrate the database to a Multi-AZ Amazon Aurora MySQL DB cluster.
(C). Use Amazon EC2 instances in two Availability Zones to host a highly available MySQL database cluster.
(D). Host static website content in Amazon S3. Use S3 Transfer Acceleration to reduce latency while serving webpages. Use AWS WAF to improve website security.
(E). Host static website content in Amazon S3. Use Amazon CloudFronl to reduce latency while serving webpages. Use AWS WAF to improve website security
(F). Migrate the database to a single-AZ Amazon RDS for MySQL DB instance.
Answer: A,B,E

NO.39 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 account. Create IAM policies to limit access to non-European Regions Attach the IAM policies to the IAM groups
(B). Enable AWS Organizations, attach the AWS accounts, and create OUs for European Regions and non-European Regions. Create SCPs to limit access to non-European Regions and attach the policies to the OUs.
(C). Set up AWS Single Sign-On and attach AWS accounts. Create permission sets with policies to restrict access to non-European Regions Create IAM users and IAM groups in each account.
(D). Enable AWS Organizations, attach the AWS accounts, and create OUs for European Regions and non-European Regions. Create permission sets with policies to restrict access to non-European Regions. Create IAM users and IAM groups in the primary account.
Answer: B
"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.html#example-scp-deny-region
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition.html

NO.40 A company has a platform that contains an Amazon S3 bucket for user content. The S3 bucket has thousands of terabytes of objects, all in the S3 Standard storage class. The company has an RTO of 6 hours The company must replicate the data from its primary AWS Region to a replication S3 bucket in another Region The user content S3 bucket contains user-uploaded files such as videos and photos. The user content S3 bucket has an unpredictable access pattern. The number of users is increasing quickly, and the company wants to create an S3 Lifecycle policy to reduce storage costs Which combination of steps will meet these requirements MOST cost-effectively'? (Select TWO)



(A). Move the objects in the user content S3 bucket to S3 Intelligent-Tiering immediately
(B). Move the objects in the user content S3 bucket to S3 Intelligent-Tiering after 30 days
(C). Move the objects in the replication S3 bucket to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days and to S3 Glacier after 90 days
(D). Move the objects in the replication S3 bucket to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days and to S3 Glacier Deep Archive after 90 days
(E). Move the objects in the replication S3 bucket to S3 Standard-infrequent Access (S3 Standard-IA) after 30 days and to S3 Glacier Deep Archive after 180 days

Answer: A,D

NO.41 A company requires that all internal application connectivity use private IP addresses. To facilitate this policy, a solutions architect has created interface endpoints to connect to AWS public services. Upon testing, the solutions architect notices that the service names are resolving to public IP addresses, and that internal services cannot connect to the interface endpoints.
Which step should the solutions architect take to resolve this issue?
(A). Update the subnet route table with a route to the interface endpoint.
(B). Enable the private DNS option on the VPC attributes.
(C). Configure the security group on the interface endpoint to allow connectivity to the AWS services.
(D). Configure an Amazon Route 53 private hosted zone with a conditional forwarder for the internal application.

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

NO.42 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. 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
(B). Deploy an organization-wide AWS Conng rule that requires all resources in the selected OUs to associate the AWS WAF rules. 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.
(C). 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
(D). 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

NO.43 A company is building an image service on the web that will allow users to upload and search random photos. At peak usage, up to 10.000 users worldwide will upload their images. The service will then overlay text on the uploaded images, which will then be published on the company website.
Which design should a solutions architect implement?
(A). Store the uploaded images in Amazon Elastic File System (Amazon EFS). Send application log information about each image to Amazon CloudWatch Logs. Create a fleet of Amazon EC2 instances that use CloudWatch Logs to determine which images need to be processed. Place processed images in anolher directory in Amazon EFS. Enable Amazon CloudFront and configure the origin to be the one of the EC2 instances in the fleet.
(B). Store the uploaded images in an Amazon S3 bucket and configure an S3 bucket event notification to send a message to Amazon Simple Notification Service (Amazon SNS). Create a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) to pull messages from Amazon SNS to process the images and place them in Amazon Elastic File System (Amazon EFS). Use Amazon CloudWatch metrics for the SNS message volume to scale out EC2 instances. Enable Amazon CloudFront and configure the origin lo be the ALB in front of the EC2 instances.
(C). Store the uploaded images in an Amazon S3 bucket and configure an S3 bucket event notification to send a message to the Amazon Simple Queue Service (Amazon SOS) queue. Create a fleet of Amazon EC2 instances to pull messages from Ihe SOS queue to process the images and place them in another S3 bucket. Use Amazon CloudWatch metrics for queue depth to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to be the S3 bucket that contains the processed images.
(D). Store the uploaded images on a shared Amazon Elastic Block Store (Amazon EBS) volume mounted to a fleet of Amazon EC2 Spot instances. Create an Amazon DynamoDB table that contains information about each uploaded image and whether it has been processed. Use an Amazon EventBridge (Amazon CloudWatch Events) rule lo scale out EC2 instances. Enable Amazon CloudFront and configure the origin to reference an Elastic Load Balancer in front of the fleet of EC2 instances.
Answer: C

NO.44 A financial services company logs personally identifiable information 10 its application logs stored in Amazon S3. Due to regulatory compliance requirements, the log files must be encrypted at rest. The security team has mandated that the company's on-premises hardware security modules (HSMs) be used to generate the CMK material.
Which steps should the solutions architect take to meet these requirements?
(A). Create an AWS CloudHSM cluster. Create a new CMK in AWS KMS using AWS_CloudHSM as the source (or the key material and an origin of AWS_CLOUDHSM. Enable automatic key rotation on the CMK with a duration of 1 year. Configure a bucket policy on the togging bucket thai disallows uploads of unencrypted data and requires that the encryption source be AWS KMS.

(B). Provision an AWS Direct Connect connection, ensuring there is no overlap of the RFC 1918 address space between on-premises hardware and the VPCs. Configure an AWS bucket policy on the logging bucket that requires all objects to be encrypted. Configure the logging application to query the on-premises HSMs from the AWS environment for the encryption key material, and create a unique CMK for each logging event.
(C). Create a CMK in AWS KMS with no key material and an origin of EXTERNAL. Import the key material generated from the on-premises HSMs into the CMK using the public key and import token provided by AWS. Configure a bucket policy on the logging bucket that disallows uploads of non-encrypted data and requires that the encryption source be AWS KMS.
(D). Create a new CMK in AWS KMS with AWS-provided key material and an origin of AWS_KMS. Disable this CMK. and overwrite the key material with the key material from the on-premises HSM using the public key and import token provided by AWS. Re-enable the CMK. Enable automatic key rotation on the CMK with a duration of 1 year. Configure a bucket policy on the logging bucket that disallows uploads of non-encrypted data and requires that the encryption source be AWS KMS.
Answer: C
https://aws.amazon.com/blogs/security/how-to-byok-bring-your-own-key-to-aws-kms-for-less-than-15-00-a-year-using-aws-cloudhsm/
https://docs.aws.amazon.com/kms/latest/developerguide/importing-keys-create-cmk.html

NO.45 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
Answer: A,D
E, Establish a networking account in the AWS Cloud. 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

NO.46 A company needs to store and process image data that will be uploaded from mobile devices using a custom mobile app. Usage peaks between 8 AM and 5 PM on weekdays, with thousands of uploads per minute. The app is rarely used at any other time A user is notified when image processing is complete.
Which combination of actions should a solutions architect take to ensure image processing can scale to handle the load1? (Select THREE.)
(A). Upload files from the mobile software directly to Amazon S3. Use S3 event notifications to create a message in an Amazon MQ queue.
(B). Upload files from the mobile software directly to Amazon S3. Use S3 event notifications to create a message in an Amazon Simple Queue Service (Amazon SQS) standard queue.

(C). Invoke an AWS Lambda function to perform image processing when a message is available in the queue.
(D). Invoke an S3 Batch Operations job to perform image processing when a message is available in the queue.
(E). Send a push notification to the mobile app by using Amazon Simple Notification Service (Amazon SNS) when processing is complete.
(F). Send a push notification to the mobile app by using Amazon Simple Email Service (Amazon SES) when processing is complete.
Answer: B,C,E
https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-basics.html

NO.47 A company has a media metadata extraction pipeline running on AWS. Notifications containing a reference to a file Amazon S3 are sent to an Amazon Simple Notification Service (Amazon SNS) topic The pipeline consists of a number of AWS Lambda functions that are subscribed to the SNS topic The Lambda functions extract the S3 file and write metadata to an Amazon RDS PostgreSQL DB instance.
Users report that updates to the metadata are sometimes stow to appear or are lost. During these times, the CPU utilization on the database is high and the number of failed Lambda invocations increases.
Which combination of actions should a solutions architect take to r-e'p resolve this issue? (Select TWO.)
(A). Enable massage delivery status on the SNS topic Configure the SNS topic delivery policy to enable retries with exponential backoff
(B). Create an Amazon Simple Queue Service (Amazon SOS) FIFO queue and subscribe the queue to the SNS topic Configure the Lambda functions to consume messages from the SQS queue.
(C). Create an RDS proxy for the RDS instance Update the Lambda functions to connect to the RDS instance using the proxy.
(D). Enable the RDS Data API for the RDS instance. Update the Lambda functions to connect to the RDS instance using the Data API
(E). Create an Amazon Simple Queue Service (Amazon SQS) standard queue for each Lambda function and subscribe the queues to the SNS topic. Configure the Lambda functions to consume messages from their respective SQS queue.
Answer: C,E

NO.48 A medical company is running a REST API on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group behind an Application Load Balancer (ALB). The ALB runs in three public subnets, and the EC2 instances run in three private subnets. The company has deployed an Amazon CloudFront distribution that has the AL8 as the only origin.
Which solution should a solutions architect recommend to enhance the origin security?
(A). Store a random string in AWS Secrets Manager. Create an AWS Lambda (unction for automatic secret rotation. Configure CloudFront to inject the random string as a custom HTTP header for the origin request. Create an AWS WAF web ACL rule with a string match rule for the custom header. Associate the web ACL with the ALB.
(B). Create an AWS WAF web ACL rule with an IP match condition of the CloudFront service IP address ranges. Associate the web ACL with the ALB. Move the ALB into the three private subnets.
(C). Store a random string in AWS Systems Manager Parameter Store. Configure Parameter Store

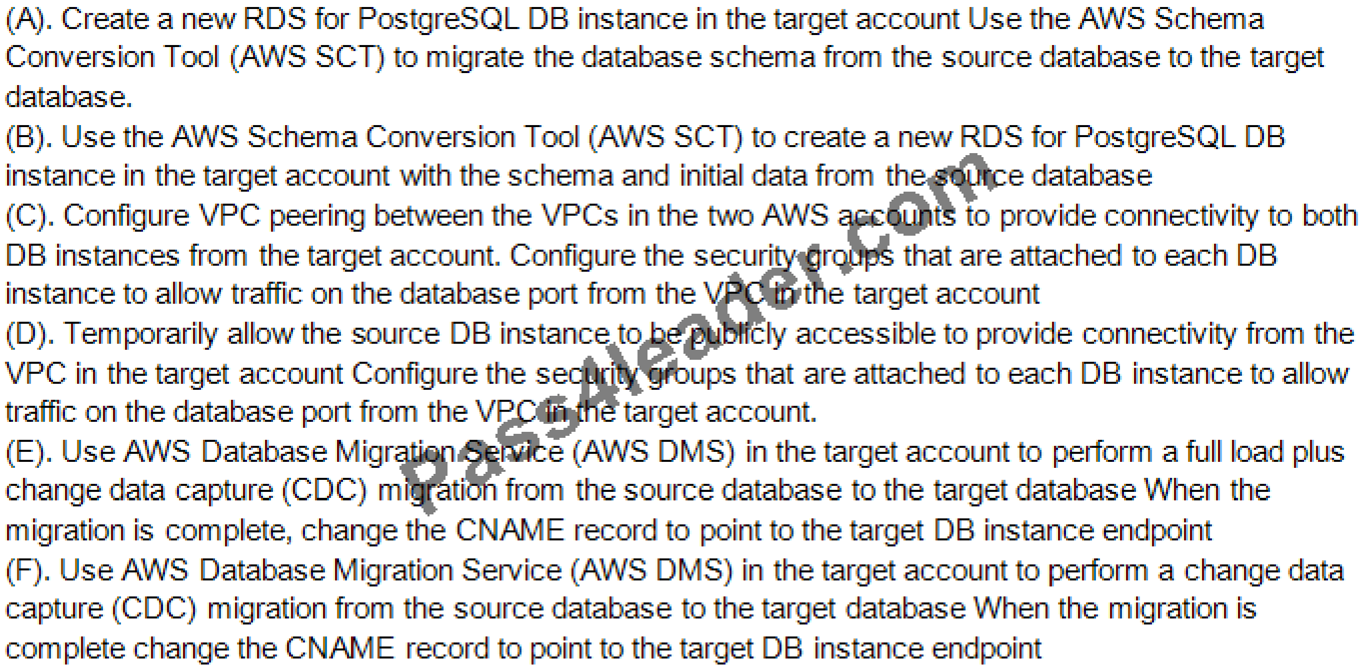
automatic rotation for the string. Configure CloudFront to inject the random siring as a custom HTTP header for the origin request. Inspect the value of the custom HTTP header, and block access in the ALB.
(D). Configure AWS Shield Advanced. Create a security group policy to allow connections from CloudFront service IP address ranges. Add the policy to AWS Shield Advanced, and attach the policy to the ALB.

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

NO.49 A development team has created a new flight tracker application that provides near-real-time data to users. The application has a front end that consists of an Application Load Balancer (ALB) in front of two large Amazon EC2 instances in a single Availability Zone. Data is stored in a single Amazon RDS MySQL DB instance. An Amazon Route 53 DNS record points to the ALB.
Management wants the development team to improve the solution to achieve maximum reliability with the least amount of operational overhead.
Which set of actions should the team take?
(A). Create RDS MySQL read replicas. Deploy the application to multiple AWS Regions. Use a Route 53 latency-based routing policy to route to the application.
(B). Configure the DB instance as Multi-AZ. Deploy the application to two additional EC2 instances in different Availability Zones behind an ALB.
(C). Replace the DB instance with Amazon DynamoDB global tables. Deploy the application in multiple AWS Regions. Use a Route 53 latency-based routing policy to route to the application.
(D). Replace the DB instance with Amazon Aurora with Aurora Replicas. Deploy the application to mulliple smaller EC2 instances across multiple Availability Zones in an Auto Scaling group behind an ALB.

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

NO.50 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. 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

(D). 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.

(E). 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

(F). 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: B,C,E

NO.51 A company is planning on hosting its ecommerce platform on AWS using a multi-tier web application designed for a NoSQL database. The company plans to use the us-west-2 Region as its primary Region. The company want to ensure that copies of the application and data are available in a second Region, us-west-1, for disaster recovery. The company wants to keep the time to fail over as low as possible. Failing back to the primary Region should be possible without administrative interaction after the primary service is restored.

Which design should the solutions architect use?

(A). Use AWS Cloud Formation StackSets lo create the stacks in both Regions with Auto Scaling groups for the web and application tiers. Asynchronously replicate static content between Regions using Amazon S3 cross-Region replication. Use an Amazon Route 53 DNS failover routing policy to direct users to the secondary site in us-west-1 in the event of an outage. Use Amazon DynamoDB global tables for the database tier.

(B). Use AWS Cloud Formation StackSets to create the stacks in both Regions with Auto Scaling groups for the web and application tiers. Asynchronously replicate static content between Regions using Amazon S3 cross-Region replication. Use an Amazon Route 53 DNS failover routing policy to direct users to the secondary site in us-west-1 in the event of an outage. Deploy an Amazon Aurora global database for the database tier.

(C). Use AWS Service Catalog to deploy the web and application servers in both Regions. Asynchronously replicate static content between the two Regions using Amazon S3 cross-Region replication. Use Amazon Route 53 health checks to identify a primary Region failure and update the public DNS entry listing to the secondary Region in the event of an outage. Use Amazon RDS for MySQL with cross-Region replication for the database tier.

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

Answer: A

NO.52 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: B,D
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-to-amazon-rds-for-postgresql.html

NO.53 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 toot to create dashboards to observe events in near-real time.
* Support for semi -structured JSON data and dynamic schemas.
Which combination of components will enabled 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 10 process and transform events
(B). Create an Amazon Kinesis data stream to buffer events Create an AWS Lambda function to process and transform evens
(C). Configure an Amazon Aurora PostgreSQL DB cluster to receive events Use Amazon Quick Sight 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 0 DB instance to receive events Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards
Answer: D,E

NO.54 A solutions architect is responsible (or redesigning a legacy Java application to improve its availability, data durability, and scalability. Currently, the application runs on a single high-memory Amazon EC2 instance. It accepts HTTP requests from upstream clients, adds them to an in-memory queue, and responds with a 200 status. A separate application thread reads items from the queue, processes them, and persists the results to an Amazon RDS MySQL instance. The processing time for each item takes 90 seconds on average, most of which is spent waiting on external service calls, but

the application is written to process multiple items in parallel.
Traffic to this service is unpredictable. During periods of high load, items may sit in the internal queue for over an hour while the application processes the backlog. In addition, the current system has issues with availability and data loss if the single application node fails.
Clients that access this service cannot be modified. They expect to receive a response to each HTTP request they send within 10 seconds before they will time out and retry the request.
Which approach would improve the availability and durability of (he system while decreasing the processing latency and minimizing costs?
(A). Create an Amazon API Gateway REST API that uses Lambda proxy integration to pass requests to an AWS Lambda function. Migrate the core processing code to a Lambda function and write a wrapper class that provides a handler method that converts the proxy events to the internal application data model and invokes the processing module.
(B). Create an Amazon API Gateway REST API that uses a service proxy to put items in an Amazon SOS queue. Extract the core processing code from the existing application and update it to pull items from Amazon SOS instead of an in-memory queue. Deploy the new processing application to smaller EC2 instances within an Auto Scaling group that scales dynamically based on the approximate number of messages in the Amazon SOS queue.
(C). Modify the application to use Amazon DynamoDB instead of Amazon RDS. Configure Auto Scaling for the DynamoDB table. Deploy the application within an Auto Scaling group with a scaling policy based on CPU utilization. Back the in-memory queue with a memory-mapped file to an instance store volume and periodically write that file to Amazon S3.
(D). Update the application to use a Redis task queue instead of the in-memory queue. 8uild a Docker container image for the application. Create an Amazon ECS task definition that includes the application container and a separate container to host Redis. Deploy the new task definition as an ECS service using AWS Fargate, and enable Auto Scaling.

Answer: B

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

NO.55 A digital marketing company has multiple AWS accounts that belong to various teams. The creative team uses an Amazon S3 bucket in its AWS account to securely store images and media files that are used as content for the company's marketing campaigns. The creative team wants to share the S3 bucket with the strategy team so that the strategy team can view the objects.
A solutions architect has created an IAM role that is named strategy_reviewer in the Strategy account. The solutions architect also has set up a custom AWS Key Management Service (AWS KMS) key in the Creative account and has associated the key with the S3 bucket. However, when users from the Strategy account assume the IAM role and try to access objects in the S3 bucket, they receive an Account.
The solutions architect must ensure that users in the Strategy account can access the S3 bucket. The solution must provide these users with only the minimum permissions that they need.
Which combination of steps should the solutions architect take to meet these requirements? (Select THREE.)
(A). Create a bucket policy that includes read permissions for the S3 bucket. Set the principal of the

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

Answer: A,C,E

NO.56 A company is migrating its marketing website and content management system from an on-premises data center to AWS. The company wants the AWS application to be deployed in a VPC with Amazon EC2 instances used for the web servers and an Amazon RDS instance for the database.
The company has a runbook document that describes the installation process of the on-premises system. The company would like to base the AWS system on the processes referenced in the runbook document. The runbook document describes the installation and configuration of the operating systems, network settings, the website, and content management system software on the servers After the migration is complete, the company wants to be able to make changes quickly to take advantage of other AWS features.
How can the application and environment be deployed and automated m AWS. while allowing for future changes?
(A). Update the runbook to describe how to create the VPC. the EC2 instances and the RDS instance for the application by using the AWS Console Make sure that the rest of the steps in the runbook are updated to reflect any changes that may come from the AWS migration
(B). Write a Python script that uses the AWS API to create the VPC. the EC2 instances and the RDS instance for the application Write shell scripts that implement the rest of the steps in the runbook Have the Python script copy and run the shell scripts on the newly created instances to complete the installation
(C). Write an AWS Cloud Formation template that creates the VPC, the EC2 instances, and the RDS instance for the application Ensure that the rest of the steps in the runbook are updated to reflect any changes that may come from the AWS migration
(D). Write an AWS CloudFormation template that creates the VPC the EC2 instances, and the RDS instance for the application Include EC2 user data in the AWS Cloud Formation template to install and configure the software.

Answer: D

NO.57 A company is running a web application on Amazon EC2 instances in a production AWS account. The company requires all logs generated from the web application to be copied to a central AWS account (or analysis and archiving. The company's AWS accounts are currently managed independently. Logging agents are configured on the EC2 instances to upload the tog files to an Amazon S3 bucket in the central AWS account.
A solutions architect needs to provide access for a solution that will allow the production account to store log files in the central account. The central account also needs to have read access to the tog

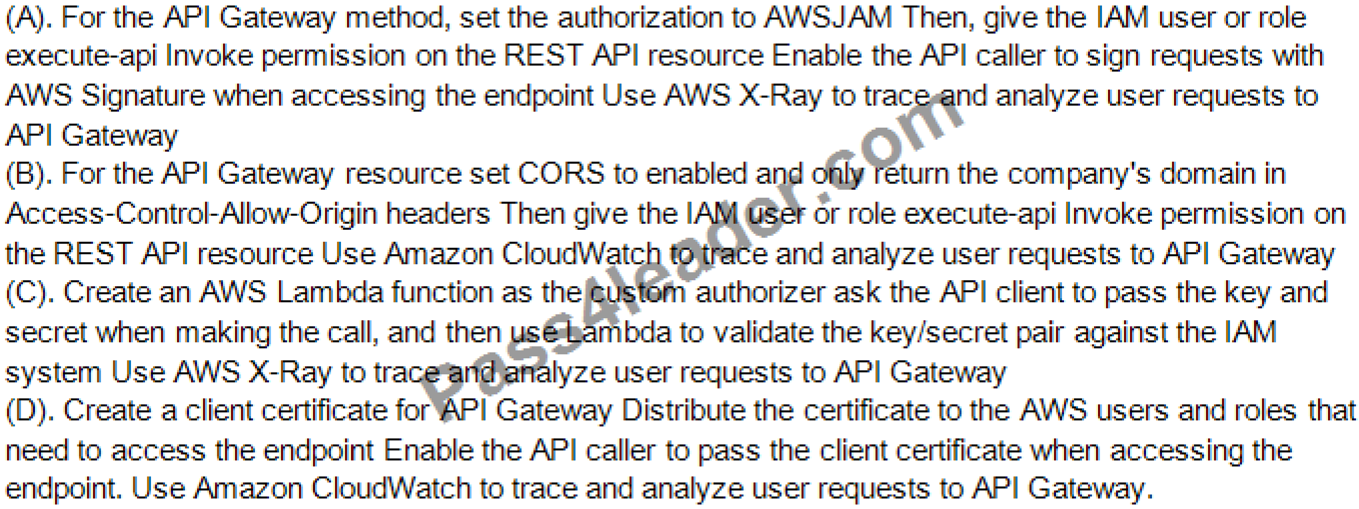
files.
What should the solutions architect do to meet these requirements?
(A). Create a cross-account role in the central account. Assume the role from the production account when the logs are being copied.
(B). Create a policy on the S3 bucket with the production account ID as the principal. Allow S3 access from a delegated user.
(C). Create a policy on the S3 bucket with access from only the CIDR range of the EC2 instances in the production account. Use the production account ID as the principal.
(D). Create a cross-account role in the production account. Assume the role from the production account when the logs are being copied.
Answer: B

NO.58 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 buckets. Use the audit logs S3 bucket as a destination for audit logs
(B). Enable replication between all current S3 buckets and the audit logs S3 bucket Enable S3 Versioning in the audit logs S3 bucket
(C). 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.
(D). Enable AWS CloudTrail. 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

NO.59 A company provides a centralized Amazon EC2 application hosted in a single shared VPC. The centralized application must be accessible from client applications running in the VPCs of other business units. The centralized application front end is configured with a Network Load Balancer (NLB) for scalability.
Up to 10 business unit VPCs will need to be connected to the shared VPC. Some of the business unit VPC CIDR blocks overlap with the shared VPC. and some overlap with each other. Network connectivity to the centralized application in the shared VPC should be allowed from authorized business unit VPCs only.
Which network configuration should a solutions architect use to provide connectivity from the client applications in the business unit VPCs to the centralized application in the shared VPC?
(A). Create an AW5 Transit Gateway. Attach the shared VPC and the authorized business unit VPCs to the transit gateway. Create a single transit gateway route table and associate it with all of the attached VPCs. Allow automatic propagation of routes from the attachments into the route table. Configure VPC routing tables to send traffic to the transit gateway.
(B). Create a VPC endpoint service using the centralized application NLB and enable (he option to require endpoint acceptance. Create a VPC endpoint in each of the business unit VPCs using the service name of the endpoint service. Accept authorized endpoint requests from the endpoint service console.

(C). Create a VPC peering connection from each business unit VPC to Ihe shared VPC. Accept the VPC peering connections from the shared VPC console. Configure VPC routing tables to send traffic to the VPC peering connection.
(D). Configure a virtual private gateway for the shared VPC and create customer gateways for each of the authorized business unit VPCs. Establish a Sile-to-Site VPN connection from the business unit VPCs to the shared VPC. Configure VPC routing tables to send traffic to the VPN connection.
Answer: B
Amazon Transit Gateway doesn't support routing between Amazon VPCs with overlapping CIDRs. If you attach a new Amazon VPC that has a CIDR which overlaps with an already attached Amazon VPC, Amazon Transit Gateway will not propagate the new Amazon VPC route into the Amazon Transit Gateway route table.
https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html#client-ip-preservation

NO.60 A solutions architect wants to make sure that only AWS users or roles with suitable permissions can access a new Amazon API Gateway endpoint The solutions architect wants an end-to-end view of each request to analyze the latency of the request and create service maps How can the solutions architect design the API Gateway access control and perform request inspections''



(A). For the API Gateway method, set the authorization to AWSJAM Then, give the IAM user or role execute-api Invoke permission on the REST API resource Enable the API caller to sign requests with AWS Signature when accessing the endpoint Use AWS X-Ray to trace and analyze user requests to API Gateway
(B). For the API Gateway resource set CORS to enabled and only return the company's domain in Access-Control-Allow-Origin headers Then give the IAM user or role execute-api Invoke permission on the REST API resource Use Amazon CloudWatch to trace and analyze user requests to API Gateway
(C). Create an AWS Lambda function as the custom authorizer ask the API client to pass the key and secret when making the call, and then use Lambda to validate the key/secret pair against the IAM system Use AWS X-Ray to trace and analyze user requests to API Gateway
(D). Create a client certificate for API Gateway Distribute the certificate to the AWS users and roles that need to access the endpoint Enable the API caller to pass the client certificate when accessing the endpoint. Use Amazon CloudWatch to trace and analyze user requests to API Gateway.

Answer: A

NO.61 A company is using AWS CodePipeline for the CI/CO of an application to an Amazon EC2 Auto Scaling group. All AWS resources are defined in AWS CloudFormation templates. The application artifacts are stored in an Amazon S3 bucket and deployed to the Auto Scaling group using instance user data scripts. As the application has become more complex, recent resource changes in the Cloud Formation templates have caused unplanned downtime.
How should a solutions architect improve the CI'CD pipeline to reduce the likelihood that changes in the templates will cause downtime?
(A). Adapt the deployment scripts to detect and report CloudFormation error conditions when performing deployments. Write test plans for a testing team to execute in a non-production environment before approving the change for production.
(B). Implement automated testing using AWS CodeBuild in a test environment. Use CloudFormation change sets to evaluate changes before deployment. Use AWS CodeDeploy to leverage blue/green deployment patterns to allow evaluations and the ability to revert changes, if needed.

(C). Use plugins for the integrated development environment (IDE) to check the templates for errors, and use the AWS CLI to validate that the templates are correct. Adapt the deployment code to check for error conditions and generate notifications on errors. Deploy to a test environment and execute a manual test plan before approving the change for production.
(D). Use AWS CodeDeploy and a blue/green deployment pattern with CloudFormation to replace the user data deployment scripts. Have the operators log in to running instances and go through a manual test plan to verify the application is running as expected.
Answer: B
https://aws.amazon.com/blogs/devops/performing-bluegreen-deployments-with-aws-codedeploy-and-auto-scaling-groups/ When one adopts go infrastructure as code, we need to test the infrastructure code as well via automated testing, and revert to original if things are not performing correctly.

NO.62 A software development company has multiple engineers who are working remotely. The company is running Active Directory Domain Services (AD DS) on an Amazon EC2 instance. The company's security policy states that all internal, nonpublic services that are deployed in a VPC must be accessible through a VPN Multi-factor authentication (MFA) must be used for access to a VPN.
Whet should a solution architect do to meet these requirements?
(A). Create an AWS Site-to-Site VPN connection Configure integration between a VPN and AD DS. Use an Amazon Workspaces client with MFA support enabled to establish a VPN connection.
(B). Create an AWS Client VPN endpoint Create an AD Connector directory for integration with AD DS Enable MFA for AD Connector Use AWS Client VPN to establish a VPN connection.
(C). Create multiple AWS Site-to-Site VPN connections by using AWS VPN CloudHub Configure integration between AWS VPN CloudHub and AD DS Use AWS Cop4ot to establish a VPN connection.
(D). Create an Amazon WorkLink endpoint Configure integration between Amazon WorkLink and AD DS. Enable MFA in Amazon WorkLink Use AWS Client VPN to establish a VPN connection.
Answer: B

NO.63 A financial services company loaded millions of historical stock trades into an Amazon DynamoDB table The table uses on-demand capacity mode Once each day at midnight, a few million new records are loaded into the table Application read activity against the table happens in bursts throughout the day, and a limited set of keys are repeatedly looked up. The company needs to reduce costs associated with DynamoDB.
Which strategy should a solutions architect recommend to meet this requirement?
(A). Deploy an Amazon ElastiCache cluster in front of the DynamoDB table.
(B). Deploy DynamoDB Accelerator (DAX) Configure DynamoDB auto scaling Purchase Savings Plans in Cost Explorer
(C). Use provisioned capacity mode Purchase Savings Plans in Cost Explorer
(D). Deploy DynamoDB Accelerator (DAX) Use provisioned capacity mode Configure DynamoDB auto scaling
Answer: D

NO.64 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. 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
(C). Store the data in a series of Amazon S3 buckets Create an application running m 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
(D). 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
Answer: D

NO.65 A company plans to refactor a monolithic application into a modern application designed deployed or AWS. The CLCD pipeline needs to be upgraded to support the modem 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 Beanstak to sage in a secondary environment as the deployment target for the CI/CD pipeline of the application. To deploy swap the staging and production environment URLs.
(C). Use AWS Systems Manager to re-provision the infrastructure for each deployment Update the Amazon EC2 user data to pull the latest code art-fact from Amazon S3 and use Amazon Route 53 weighted routing to point to the new environment
(D). Roll out At application updates as pan of an Auto Scaling event using prebuilt AMIs. 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
It is the fastest when it comes to rollback and deploying changes every hour

NO.66 A company has multiple AWS accounts as part of an organization created with AWS Organizations. Each account has a VPC in the us-east-2 Region and is used for either production or development workloads. Amazon EC2 instances across production accounts need to communicate with each other, and EC2 instances across development accounts need to communicate with each other, but production and development instances should not be able to communicate with each other.
To facilitate connectivity, the company created a common network account. The company used AWS Transit Gateway to create a transit gateway in the us-east-2 Region in the network account and shared the transit gateway with the entire organization by using AWS Resource Access Manager. Network administrators then attached VPCs in each account to the transit gateway, after which the EC2 instances were able to communicate across accounts. However, production and development accounts were also able to communicate with one another.
Which set of steps should a solutions architect take to ensure production traffic and development traffic are completely isolated?
(A). Modify the security groups assigned to development EC2 instances to block traffic from production EC2 instances. Modify the security groups assigned to production EC2 instances to block traffic from development EC2 instances.
(B). Create a tag on each VPC attachment with a value of either production or development, according to the type of account being attached. Using the Network Manager feature of AWS Transit Gateway, create policies that restrict traffic between VPCs based on the value of this tag.
(C). Create separate route tables for production and development traffic. Delete each account's association and route propagation to the default AWS Transit Gateway route table. Attach development VPCs to the development AWS Transit Gateway route table and production VPCs to the production route table, and enable automatic route propagation on each attachment.
(D). Create a tag on each VPC attachment with a value of either production or development, according to the type of account being attached. Modify the AWS Transit Gateway routing table to route production tagged attachments to one another and development tagged attachments to one another.
Answer: C
https://docs.aws.amazon.com/vpc/latest/tgw/vpc-tgw.pdf

NO.67 A company's security compliance requirements state that all Amazon EC2 images must be scanned for vulnerabilities and must pass a CVE assessment A solutions architect is developing a mechanism to create security-approved AMIs that can be used by developers Any new AMIs should go through an automated assessment process and be marked as approved before developers can use them The approved images must be scanned every 30 days to ensure compliance Which combination of steps should the solutions architect take to meet these requirements while following best practices'? (Select TWO)
(A). Use the AWS Systems Manager EC2 agent to run the CVE assessment on the EC2 instances launched from the AMIs that need to be scanned
(B). Use AWS Lambda to write automatic approval rules Store the approved AMI list in AWS Systems Manager Parameter Store Use Amazon EventBridge to trigger an AWS Systems Manager Automation document on all EC2 instances every 30 days.
(C). Use Amazon Inspector to run the CVE assessment on the EC2 instances launched from the AMIs that need to be scanned

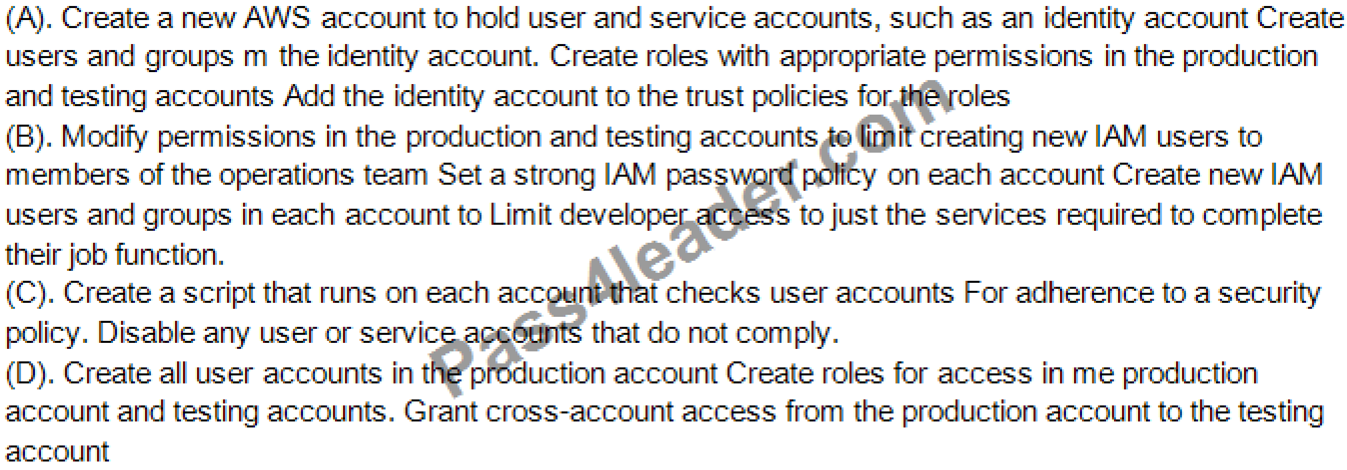
(D). Use AWS Lambda to write automatic approval rules Store the approved AMI list in AWS Systems Manager Parameter Store Use a managed AWS Config rule for continuous scanning on all EC2 instances, and use AWS Systems Manager Automation documents for remediation
(E). Use AWS CloudTrail to run the CVE assessment on the EC2 instances launched from the AMIs that need to be scanned
Answer: B,C

NO.68 A solutions architect at a largo company needs to set up network security for outbound traffic to the internet from all AWS accounts within an organization m AWS Organizations The organization has more than 100 AWS accounts, and the accounts route to each other by using a centralized AWS Transit Gateway. Each account has both an internet gateway and a NAT gateway for outbound traffic to the interne) The company deploys resources only Into a single AWS Region The company needs the ability to add centrally managed rule-based filtering on all outbound traffic to the internet for all AWS accounts in the organization The peak load of outbound traffic will not exceed 25 Gbps in each Availability Zone Which solution meets these requirements?
(A). Creates a new VPC for outbound traffic to the internet Connect the existing transit gateway to the new VPC Configure a new NAT gateway Create an Auto Scaling group of Amazon EC2 Instances that run an open-source internet proxy for rule-based filtering across all Availability Zones in the Region Modify all default routes to point to the proxy's Auto Scaling group
(B). Create a new VPC for outbound traffic to the internet Connect the existing transit gateway to the new VPC Configure a new NAT gateway Use an AWS Network Firewall firewall for rule-based filtering Create Network Firewall endpoints In each Availability Zone Modify all default routes to point to the Network Firewall endpoints
(C). Create an AWS Network Firewall firewal for rule-based filtering in each AWS account Modify all default routes to point to the Network Firewall firewalls in each account.
(D). In each AWS account, create an Auto Scaling group of network-optimized Amazon EC2 instances that run an open-source internet proxy for rule-based filtering Modify all default routes to point to the proxy's Auto Scaling group.
Answer: B
https://aws.amazon.com/blogs/networking-and-content-delivery/deployment-models-for-aws-network-firewall/
https://aws.amazon.com/blogs/networking-and-content-delivery/deploy-centralized-traffic-filtering-using-aws-network-firewall/

NO.69 A company has multiple business units Each business unit has its own AWS account and runs a single website within that account. The company also has a single logging account. Logs from each business unit website are aggregated into a single Amazon S3 bucket in the logging account. The S3 bucket policy provides each business unit with access to write data into the bucket and requires data to be encrypted.
The company needs to encrypt logs uploaded into the bucket using a Single AWS Key Management Service {AWS KMS) CMK The CMK that protects the data must be rotated once every 365 days Which strategy is the MOST operationally efficient for the company to use to meet these requirements?
(A). Create a customer managed CMK ri the logging account Update the CMK key policy to provide access to the logging account only Manually rotate the CMK every 365 days.
(B). Create a customer managed CMK in the logging account. Update the CMK key policy to provide access to the logging account and business unit accounts. Enable automatic rotation of the CMK

(C). Use an AWS managed CMK m the togging account. Update the CMK key policy to provide access to the logging account and business unit accounts Manually rotate the CMK every 365 days.
(D). Use an AWS managed CMK in the togging account Update the CMK key policy to provide access to the togging account only. Enable automatic rotation of the CMK.
Answer: A

NO.70 A company has deployed an application to multiple environments in AWS. including production and testing the company has separate accounts for production and testing, and users are allowed to create additional application users for team members or services. as needed. The security team has asked the operations team tor better isolation between production and testing with centralized controls on security credentials and improved management of permissions between environments Which of the following options would MOST securely accomplish this goal?


(A). Create a new AWS account to hold user and service accounts, such as an identity account Create users and groups m the identity account. Create roles with appropriate permissions in the production and testing accounts Add the identity account to the trust policies for the roles
(B). Modify permissions in the production and testing accounts to limit creating new IAM users to members of the operations team Set a strong IAM password policy on each account Create new IAM users and groups in each account to Limit developer access to just the services required to complete their job function.
(C). Create a script that runs on each account that checks user accounts For adherence to a security policy. Disable any user or service accounts that do not comply.
(D). Create all user accounts in the production account Create roles for access in me production account and testing accounts. Grant cross-account access from the production account to the testing account

Answer: A

NO.71 A startup company recently migrated a large ecommerce website to AWS. The website has experienced a 70% increase in sales. Software engineers are using a private GitHub repository to manage code. The DevOps learn is using Jenkins for builds and unit testing. The engineers need to receive notifications for bad builds and zero downtime during deployments. The engineers also need to ensure any changes to production are seamless for users and can be rolled back in the event of a major issue.
The software engineers have decided to use AWS CodePipeline to manage their build and deployment process.
Which solution will meet these requirements?
(A). Use GitHub websockets to trigger the CodePipeline pipeline. Use the Jenkins plugin for AWS CodeBuild to conduct unit testing. Send alerts to an Amazon SNS topic for any bad builds. Deploy in an in-place. all-at-once deployment configuration using AWS CodeDeploy.
(B). Use GitHub webhooks to trigger the CodePipeline pipeline. Use the Jenkins plugin for AWS CodeBuild to conduct unit testing. Send alerts to an Amazon SNS topic for any bad builds. Deploy in a blue/green deployment using AWS CodeDeploy.
(C). Use GitHub websockets to trigger the CodePipeline pipeline. Use AWS X-Ray for unit testing and static code analysis. Send alerts to an Amazon SNS topic for any bad builds. Deploy in a blue/green deployment using AWS CodeDeploy.
(D). Use GitHub webhooks to trigger the CodePipeline pipeline. Use AWS X-Ray for unit testing and static code analysis. Send alerts to an Amazon SNS topic for any bad builds. Deploy in an in-place, all-

at-once deployment configuration using AWS CodeDeploy.
Answer: B

NO.72 A team collects and routes behavioral data for an entire company. The company runs a Multi-AZ VPC environment with public subnets, private subnets, and in internet gateway Each public subnet also contains a NAT gateway Most of the company's applications read from and write to Amazon Kinesis Data Streams. Most of the workloads run in private subnets.
A solutions architect must review the infrastructure The solutions architect needs to reduce costs and maintain the function of the applications. The solutions architect uses Cost Explorer and notices that the cost in the EC2-Other category is consistently high A further review shows that NatGateway-Bytes charges are increasing the cost in the EC2-Other category.
What should the solutions architect do to meet these requirements?
(A). Enable VPC Flow Logs. Use Amazon Athena to analyze the logs for traffic that can be removed. Ensure that security groups are blocking traffic that is responsible for high costs.
(B). Add an interface VPC endpoint for Kinesis Data Streams to the VPC. Ensure that applications have the correct IAM permissions to use the interface VPC endpoint.
(C). Enable VPC Flow Logs and Amazon Detective. Review Detective findings for traffic that is not related to Kinesis Data Streams Configure security groups to block that traffic
(D). Add an interface VPC endpoint for Kinesis Data Streams to the VPC Ensure that the VPC endpoint policy allows traffic from the applications
Answer: D
https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-access.html
https://aws.amazon.com/premiumsupport/knowledge-center/vpc-reduce-nat-gateway-transfer-costs/ VPC endpoint policies enable you to control access by either attaching a policy to a VPC endpoint or by using additional fields in a policy that is attached to an IAM user, group, or role to restrict access to only occur via the specified VPC endpoint

NO.73 A solutions architect has implemented a SAML 2.0 federated identity solution with their company's on-premises identity provider (IdP) to authenticate users' access to the AWS environment. When the solutions architect tests authentication through the federated identity web portal access to the AWS environment is granted However, when test users attempt to authenticate through the federated identity web portal, they are not able to access the AWS environment.
Which items should the solutions architect check to ensure identity federation is property configured? (Select THREE j
(A). The IAM user's permissions pokey has allowed the use of SAML federation for that user
(B). The IAM roles created for the federated users' or federated groups' trust policy have set the SAML provider as the principle.
(C). Test users are not in the AWSFederatedUsers group in the company's IdP
(D). The web portal calls the AWS STS AssumeRoleWithSAML API with the ARN of the SAML provider the ARN of the IAM role, and the SAML assertion from IdP
(E). The on-premises IdP's DNS hostname is reachable from the AWS environment VPCs.
(F). The company's IdP defines SAML assertions that property map users or groups m the company to IAM roles with appropriate permissions
Answer: B,C,F

NO.74 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

NO.75 A retail company has a small ecommerce web application that uses an Amazon RDS for PostgreSQL DB instance The DB instance is deployed with the Multi-AZ option turned on.
Application usage recently increased exponentially and users experienced frequent HTTP 503 errors Users reported the errors, and the company's reputation suffered The company could not identify a definitive root cause.
The company wants to improve its operational readiness and receive alerts before users notice an incident The company also wants to collect enough information to determine the root cause of any future incident.
Which solution will meet these requirements with the LEAST operational overhead?
(A). Turn on Enhanced Monitoring for the DB instance Modify the corresponding parameter group to turn on query logging for all the slow queries Create Amazon CloudWatch alarms Set the alarms to appropriate thresholds that are based on performance metrics in CloudWatch
(B). Turn on Enhanced Monitoring and Performance Insights for the DB instance Create Amazon CloudWatch alarms Set the alarms to appropriate thresholds that are based on performance metrics in CloudWatch
(C). Turn on log exports to Amazon CloudWatch for the PostgreSQL logs on the DB instance Analyze the logs by using Amazon Elasticsearch Service (Amazon ES) and Kibana Create a dashboard in Kibana Configure alerts that are based on the metrics that are collected
(D). Turn on Performance Insights for the DB instance Modify the corresponding parameter group to turn on query logging for all the slow queries Create Amazon CloudWatch alarms Set the alarms to appropriate thresholds that are based on performance metrics in CloudWatch
Answer: A

NO.76 A solutions architect works for a government agency that has strict disaster recovery requirements All Amazon Elastic Block Store (Amazon EBS) snapshots are required to be saved in at least two additional AWS Regions. The agency also is required to maintain the lowest possible operational overhead.
Which solution meets these requirements?
(A). Configure a policy in Amazon Data Lifecycle Manager (Amazon DLMJ to run once daily to copy the EBS snapshots to the additional Regions.
(B). Use Amazon EventBridge (Amazon CloudWatch Events) to schedule an AWS Lambda function to copy the EBS snapshots to the additional Regions.
(C). Set up AWS Backup to create the EBS snapshots. Configure Amazon S3 cross-Region replication to copy the EBS snapshots to the additional Regions.
(D). Schedule Amazon EC2 Image Builder to run once daily to create an AMI and copy the AMI to the additional Regions.

Answer: A

NO.77 An online retail company hosts its stateful web-based application and MySQL database in an on-premises data center on a single server. The company wants to increase its customer base by conducting more marketing campaigns and promotions. In preparation, the company wants to migrate its application and database to AWS to increase the reliability of its architecture.
Which solution should provide the HIGHEST level of reliability?
(A). Migrate the database to an Amazon RDS MySQL Multi-AZ DB instance. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in Amazon Neptune.
(B). Migrate the database to Amazon Aurora MySQL. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in an Amazon ElastiCache for Redis replication group.
(C). Migrate the database to Amazon DocumentDB (with MongoDB compatibility). Deploy the application in an Auto Scaling group on Amazon EC2 instances behind a Network Load Balancer. Store sessions in Amazon Kinesis Data Firehose.
(D). Migrate the database to an Amazon RDS MariaDB Multi-AZ DB instance. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in Amazon ElastiCache for Memcached.
Answer: B

NO.78 A company is planning to migrate an application from on premises to the AWS Cloud. The company will begin the migration by moving the application's underlying data storage to AWS The application data is stored on a shared tie system on premises, and the application servers connect to the shared We system through SMB.
A solutions architect must implement a solution that uses an Amazon S3 bucket tor shared storage Until the application Is fully migrated and code is rewritten to use native Amazon S3 APIs, the application must continue to have access to the data through SMB The solutions architect must migrate the application data to AWS to its new location while still allowing the on-premises application to access the data.
Which solution will meet these requirements?
(A). Create a new Amazon FSx for Windows File Server fie system Configure AWS DataSync with one location tor the on-premises file share and one location for the new Amazon FSx file system Create a new DataSync task to copy the data from the on-premises file share location to the Amazon FSx file system
(B). Create an S3 bucket for the application. Copy the data from the on-premises storage to the S3 bucket
(C). Deploy an AWS Server Migration Service (AWS SMS) VM to the on-premises environment. Use AWS SMS to migrate the file storage server from on premises to an Amazon EC2 instance
(D). Create an S3 bucket for the application. Deploy a new AWS Storage Gateway Me gateway on an on-premises VM. Create a new file share that stores data in the S3 bucket and is associated with the tie gateway. Copy the data from the on-premises storage to the new file gateway endpoint.
Answer: A

NO.79 A company that designs multiplayer online games wants to expand its user base outside of Europe. The company transfers a significant amount of UDP traffic to Keep all the live and interactive sessions of the games The company has plans for rapid expansion and wants to build its architecture to provide an optimized online experience to its users Which architecture will meet these requirements with the LOWEST latency for users''

(A). Set up a Multi-AZ environment in a single AWS Region Use Amazon CloudFront to cache user sessions

(B). Set up environments in multiple AWS Regions Create an accelerator in AWS Global Accelerator, and add endpoints from different Regions to it

(C). Set up environments in multiple AWS Regions Use Amazon Route 53. and select latency-based routing

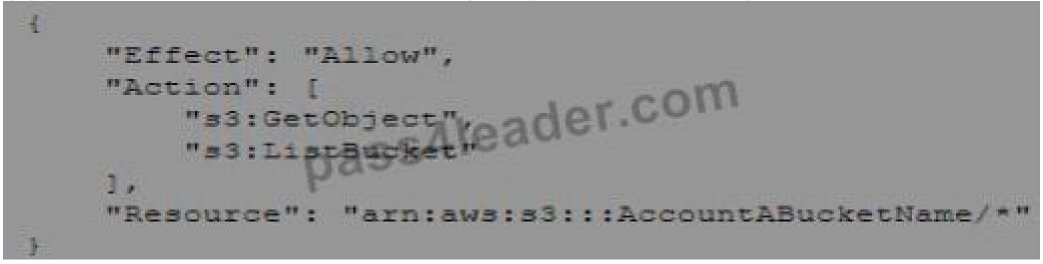
(D). Set up a Multi-AZ environment in a single AWS Region. Use AWS Lambda@Edge to update sessions closer to the users

Answer: B

NO.80 A retail company needs to provide a series of data files to another company. which is its business partner. These files are saved in an Amazon S3 bucket under Account A.
which belongs to the retail company. The business partner company wants one of its IAM users User_DataProcessor to access the files from its own AWS account (Account B) Which combination of steps must the companies take so that User_DataProcessor can access the S3 bucket successfully? (Select TWO.)

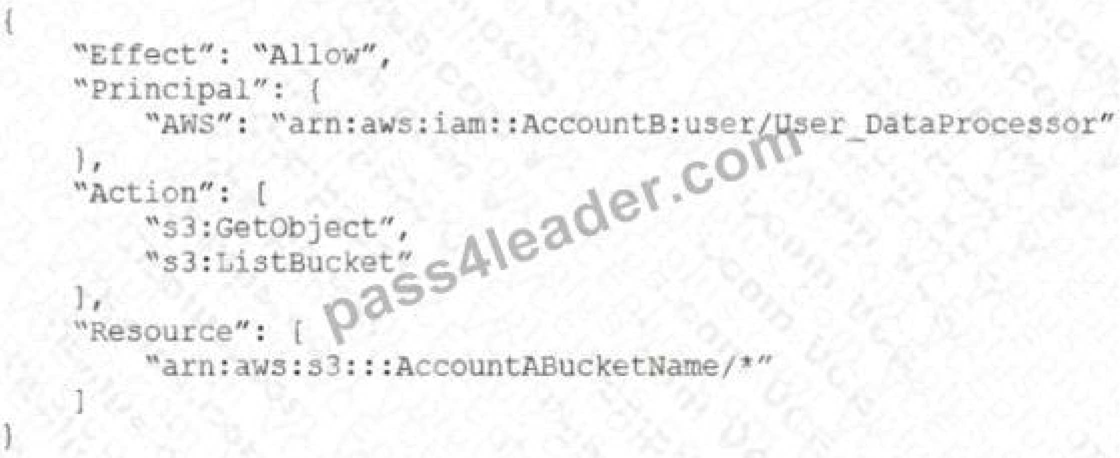
(A). Turn on the cross-origin resource sharing (CORS) feature for the S3 bucket in Account A.

(B). In Account A. set the S3 bucket policy to the following.



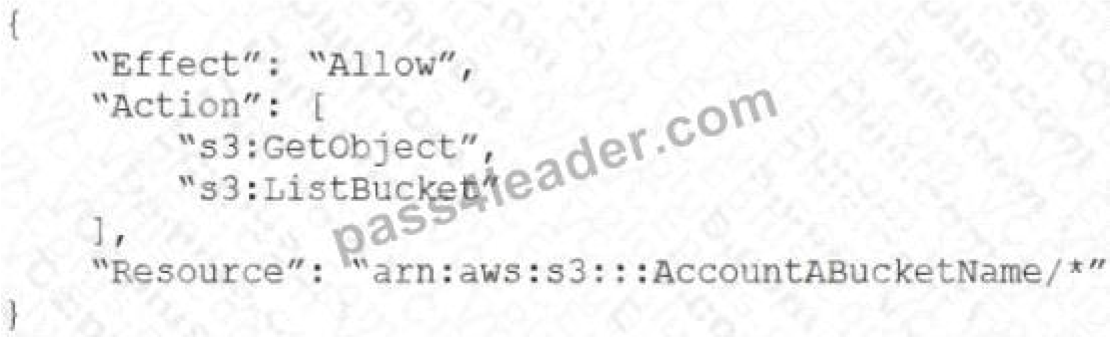
```
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3:::AccountABucketName/*"
}
```

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



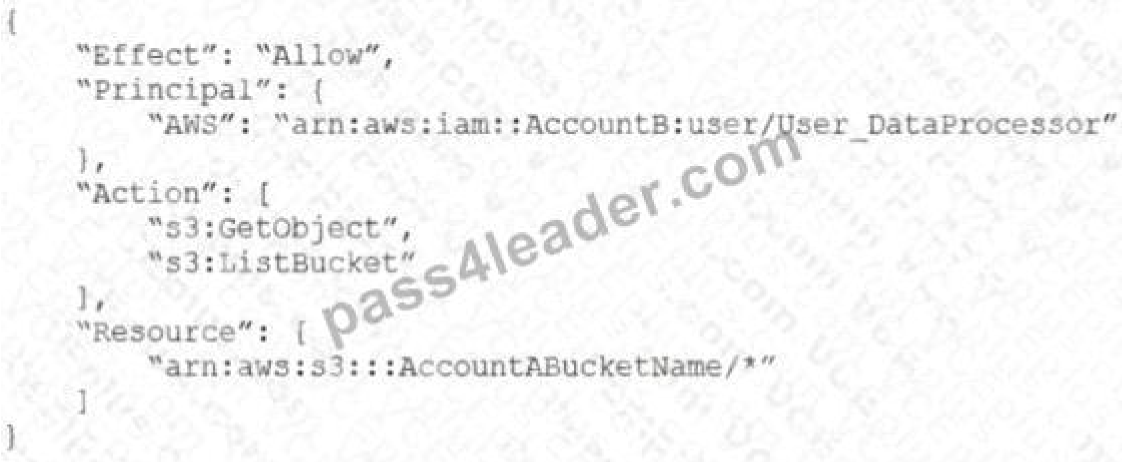
```
{
    “Effect”: “Allow”,
    “Principal”: {
        “AWS”: “arn:aws:iam::AccountB:user/User_DataProcessor”
    },
    “Action”: [
        “s3:GetObject”,
        “s3:ListBucket”
    ],
    “Resource”: [
        “arn:aws:s3:::AccountABucketName/*”
    ]
}
```

(D). InAccount B, set the permissions of User_DataProcessor to the following:



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

(E). InAccount B, set the permissions of User_DataProcessor to the following:



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

Answer: A,D

NO.81 A company is running a web application with On-Demand Amazon EC2 instances in Auto Scaling groups that scale dynamically based on custom metrics After extensive testing, the company determines that the m5.2xlarge instance size is optimal for the workload Application data is stored in db.r4.4xlarge Amazon RDS instances that are confirmed to be optimal. The traffic to the web application spikes randomly during the day.

What other cost-optimization methods should the company implement to further reduce costs without impacting the reliability of the application?

(A). Double the instance count in the Auto Scaling groups and reduce the instance size to m5.large

(B). Reserve capacity for the RDS database and the minimum number of EC2 instances that are constantly running.

(C). Reduce the RDS instance size to db.r4.xlarge and add five equivalent^ sized read replicas to provide reliability.

(D). Reserve capacity for all EC2 instances and leverage Spot Instance pricing for the RDS database.

Answer: B

People are being confused by the term 'reserve capacity'. This is not the same as an on-demand capacity reservation. This article by AWS clearly states that by 'reserving capacity' you are reserving the instances and reducing your costs. See - https://aws.amazon.com/aws-cost-management/aws-cost-optimization/reserved-instances/

NO.82 A company is migrating its infrastructure to the AW5 Cloud. The company must comply with a variety of regulatory standards for different projects. The company needs a multi-account environment.

A solutions architect needs to prepare the baseline infrastructure The solution must provide a

consistent baseline of management and security but it must allow flexibility for different compliance requirements within various AWS accounts. The solution also needs to integrate with the existing on-premises Active Directory Federation Services (AD FS) server.
Which solution meets these requirements with the LEAST amount of operational overhead?
(A). Create an organization In AWS Organizations Create a single SCP for least privilege access across all accounts Create a single OU for all accounts Configure an IAM identity provider tor federation with the on-premises AD FS server Configure a central togging account with a defined process for log generating services to send log events to the central account. Enable AWS Config in the central account with conformance packs for all accounts.
(B). Create an organization In AWS Organizations Enable AWS Control Tower on the organization. Review included guardrails for SCPs. Check AWS Config for areas that require additions Add OUs as necessary Connect AWS Single Sign-On to the on-premises AD FS server
(C). Create an organization in AWS Organizations Create SCPs for least privilege access Create an OU structure, and use it to group AWS accounts Connect AWS Single Sign-On to the on-premises AD FS server. Configure a central logging account with a defined process for tog generating services to send log events to the central account Enable AWS Config in the central account with aggregators and conformance packs.
(D). Create an organization in AWS Organizations Enable AWS Control Tower on the organization Review included guardrails for SCPs. Check AWS Config for areas that require additions Configure an IAM identity provider for federation with the on-premises AD FS server.
Answer: A

NO.83 A company wants to migrate an application to Amazon EC2 from VMware Infrastructure that runs in an on-premises data center. A solutions architect must preserve the software and configuration settings during the migration.
What should the solutions architect do to meet these requirements?
(A). Configure the AWS DataSync agent to start replicating the data store to Amazon FSx for Windows File Server Use the SMB share to host the VMware data store. Use VM Import/Export to move the VMs to Amazon EC2.
(B). Use the VMware vSphere client to export the application as an image in Open Virealization Format (OVF) format Create an Amazon S3 bucket to store the image in the destination AWS Region. Create and apply an IAM role for VM Import Use the AWS CLI to run the EC2 import command.
(C). Configure AWS Storage Gateway for files service to export a Common Internet File System (CIFSJ share. Create a backup copy to the shared folder. Sign in to the AWS Management Console and create an AMI from the backup copy Launch an EC2 instance that is based on the AMI.
(D). Create a managed-instance activation for a hybrid environment in AWS Systems Manager. Download and install Systems Manager Agent on the on-premises VM Register the VM with Systems Manager to be a managed instance Use AWS Backup to create a snapshot of the VM and create an AMI. Launch an EC2 instance that is based on the AMI
Answer: B
https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html
- Export an OVF Template
- Create / use an Amazon S3 bucket for storing the exported images. The bucket must be in the Region where you want to import your VMs.
- Create an IAM role named vmimport.
- You'll use AWS CLI to run the import commands.

https://aws.amazon.com/premiumsupport/knowledge-center/import-instances/

NO.84 A company is running a tone-of-business (LOB) application on AWS to support its users The application runs in one VPC. with a backup copy in a second VPC in a different AWS Region for disaster recovery The company has a single AWS Direct Connect connection between its on-premises network and AWS The connection terminates at a Direct Connect gateway All access to the application must originate from the company's on-premises network, and traffic must be encrypted in transit through the use of Psec. The company is routing traffic through a VPN tunnel over the Direct Connect connection to provide the required encryption.
A business continuity audit determines that the Direct Connect connection represents a potential single point of failure for access to the application The company needs to remediate this issue as quickly as possible.
Which approach will meet these requirements?
(A). Order a second Direct Connect connection to a different Direct Connect location. Terminate the second Direct Connect connection at the same Direct Connect gateway.
(B). Configure an AWS Site-to-Site VPN connection over the internet Terminate the VPN connection at a virtual private gateway in the secondary Region
(C). Create a transit gateway Attach the VPCs to the transit gateway, and connect the transit gateway to the Direct Connect gateway Configure an AWS Site-to-Site VPN connection, and terminate it at the transit gateway
(D). Create a transit gateway. Attach the VPCs to the transit gateway, and connect the transit gateway to the Direct Connect gateway. Order a second Direct Connect connection, and terminate it at the transit gateway.
Answer: C
Create a transit gateway. Attach the VPCs to the transit gateway, and connect the transit gateway to the Direct Connect gateway. Configure an AWS Site-to- Site VPN connection, and terminate it at the transit gateway
https://aws.amazon.com/premiumsupport/knowledge-center/dx-configure-dx-and-vpn-failover-tgw/
All access to the application must originate from the company's on-premises network and traffic must be encrypted in transit through the use of IPsec. = need to use VPN.

NO.85 A company runs a highly available data collection application on Amazon EC2 in the eu-north-1 Region. The application collects data from end-user devices and writes records to an Amazon Kinesis data stream and a set of AWS Lambda functions that process the records The company persists the output of the record processing to an Amazon S3 bucket in eu-north-1. The company uses the data in the S3 bucket as a data source for Amazon Athena
(A). In each of the Iwo new Regions set up the Lambda functions to run in a VPC Set up an S3 gateway endpoint in that VPC
(B). Turn on S3 Transfer Acceleration on the S3 bucket in eu-north-1 Change the application to use the new S3 accelerated endpoint when the application uploads data to the S3 bucket
(C). Create an S3 bucket in each of the two new Regions Set the application in each new Region to upload to its respective S3 bucket Set up S3 Cross-Region Replication to replicate data to the S3 bucket in eu-north-1
(D). Increase the memory requirements of the Lambda functions to ensure that they have multiple cores available Use the multipart upload feature when the application uploads data to Amazon S3 Lambda

Answer: A

NO.86 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. Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs in each Region as part of an Auto Scaling group spanning both VPCs and served by the ALB.
(B). Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. 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.
(C). Create a VPC in the us-west-1 Region. 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 ALB. Create an Amazon Route 53 record that points to the ALB.
(D). Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. Deploy the same solution to the us-west-1 Region. Create separate Amazon Route 53 records in each Region that point to the ALB in the Region. Use Route 53 health checks to provide high availability across both Regions.
Answer: B
A new web application in a active-passive DR mode. a Route 53 record set with a failover routing policy.

NO.87 A company has an application that generates reports and stores them in an Amazon S3 bucket. When a user accesses their report, the application generates a signed URL to allow the user to download the report. The company's security team has discovered that the files are public and that anyone can download them without authentication. The company has suspended the generation of new reports until the problem is resolved.
Which set of actions will immediately remediate the security issue without impacting the application's normal workflow?
(A). Create an AWS Lambda function that applies a deny all policy for users who are not authenticated. Create a scheduled event to invoke the Lambda function.
(B). Review the AWS Trusted Advisor bucket permissions check and implement the recommended actions.
(C). Run a script that puts a private ACL on all of the objects in the bucket.
(D). Use the Block Public Access feature in Amazon S3 to set the IgnorePublicAcls option to TRUE on the bucket.
Answer: D
The S3 bucket is allowing public access and this must be immediately disabled. Setting the IgnorePublicAcls option to TRUE causes Amazon S3 to ignore all public ACLs on a bucket and any

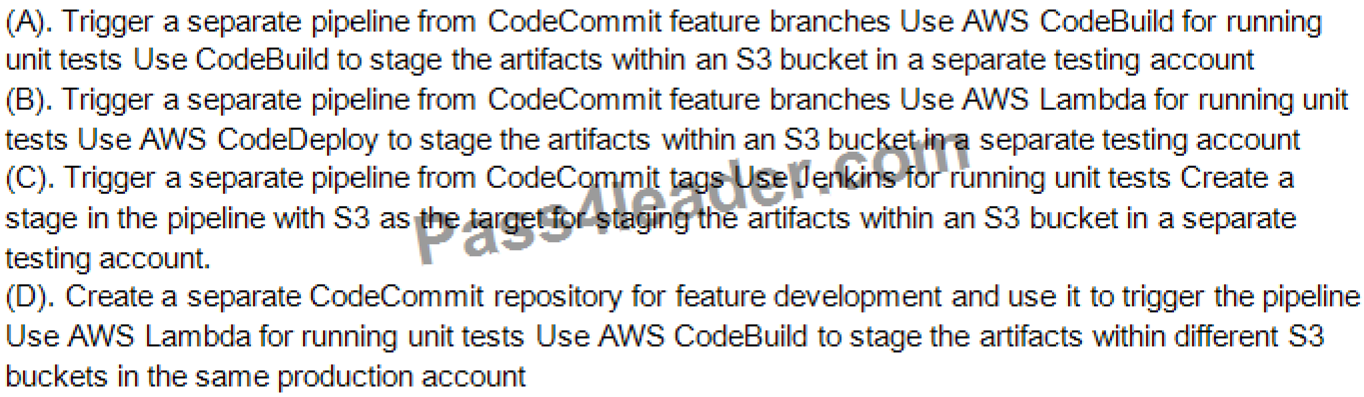
objects that it contains.
The other settings you can configure with the Block Public Access Feature are:
o BlockPublicAcls - PUT bucket ACL and PUT objects requests are blocked if granting public access.
o BlockPublicPolicy - Rejects requests to PUT a bucket policy if granting public access.
o RestrictPublicBuckets - Restricts access to principles in the bucket owners' AWS account.
https://aws.amazon.com/s3/features/block-public-access/

NO.88 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 actions. Move the organization's root SCP to the Production OU. Move the new account to the Production OU when adjustments to AWS Config are complete.
Answer: D

NO.89 A company has a complex web application that leverages Amazon CloudFront for global scalability and performance. Over time, users report that the web application is slowing down.
The company's operations team reports that the CloudFront cache hit ratio has been dropping steadily. The cache metrics report indicates that query strings on some URLs are inconsistently ordered and are specified sometimes in mixed-case letters and sometimes in lowercase letters.
Which set of actions should the solutions architect take to increase the cache hit ratio as quickly as possible?
(A). Deploy a Lambda@Edge function to sort parameters by name and force them to be lowercase. Select the CloudFront viewer request trigger to invoke the function.
(B). Update the CloudFront distribution to disable caching based on query string parameters.
(C). Deploy a reverse proxy after the load balancer to post-process the emitted URLs in the application to force the URL strings to be lowercase.
(D). Update the CloudFront distribution to specify casing-insensitive query string processing.
Answer: A
https://docs.amazonaws.cn/en_us/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html#lambda-examples-query-string-examples Before CloudFront serves content from the cache it will trigger any Lambda function associated with the Viewer Request, in which we can

normalize parameters.
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html#lambda-examples-normalize-query-string-parameters

NO.90 A company is currently using AWS CodeCommit for its source control and AWS CodePipeline for continuous integration The pipeline has a build stage for building the artifacts, which is then staged in an Amazon S3 bucket.
The company has identified various improvement opportunities in the existing process and a solutions architect has been given the following requirements
* Create a new pipeline to support feature development
* Support feature development without impacting production applications
* Incorporate continuous testing with unit tests
* Isolate development and production artifacts
* Support the capability to merge tested code into production code
How should the solutions architect achieve these requirements?


(A). Trigger a separate pipeline from CodeCommit feature branches Use AWS CodeBuild for running unit tests Use CodeBuild to stage the artifacts within an S3 bucket in a separate testing account
(B). Trigger a separate pipeline from CodeCommit feature branches Use AWS Lambda for running unit tests Use AWS CodeDeploy to stage the artifacts within an S3 bucket in a separate testing account
(C). Trigger a separate pipeline from CodeCommit tags Use Jenkins for running unit tests Create a stage in the pipeline with S3 as the target for staging the artifacts within an S3 bucket in a separate testing account.
(D). Create a separate CodeCommit repository for feature development and use it to trigger the pipeline Use AWS Lambda for running unit tests Use AWS CodeBuild to stage the artifacts within different S3 buckets in the same production account

Answer: A

NO.91 A company uses AWS Organizations to manage more than 1.000 AWS accounts. The company has created a new developer organization. There are 540 developer member accounts that must be moved to the new developer organization All accounts are set up with all the required Information so mat each account can be operated as a standalone account Which combination of steps should a solutions architect take to move all of the developer accounts to the new developer organization?
(Select THREE)
(A). Call the MoveAccount operation In the Organizations API from the old organization's management account to migrate the developer accounts to the new developer organization
(B). From the management account remove each developer account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API
(C). From each developer account, remove the account from the old organization using the RemoveAccounrFromOrganization operation in the Organizations API
(D). Sign in to the new developer organization's management account and create a placeholder member account that acts as a target for the developer account migration
(E). Call the InviteAccountToOrganzation operation in the Organizations API from the new developer organization's management account to send invitations to the developer accounts.
(F). Have each developer sign in to their account and confirm to join the new developer organization.
Answer: B,D,E

NO.92 A company has an application that sells tickets online and experiences bursts of demand every 7 days. The application has a stateless presentation layer running on Amazon EC2. an Oracle database to store unstructured data catalog information, and a backend API layer. The front-end layer uses an Elastic Load Balancer to distribute the load across nine On-Demand Instances over three Availability Zones (AZs). The Oracle database is running on a single EC2 instance. The company is experiencing performance issues when running more than two concurrent campaigns. A solutions architect must design a solution that meets the following requirements:
* Address scalability issues.
* Increase the level of concurrency.
* Eliminate licensing costs.
* Improve reliability.
Which set of steps should the solutions architect take?
(A). Create an Auto Scaling group for the front end with a combination of On-Demand and Spot Instances to reduce costs. Convert the Oracle database into a single Amazon RDS reserved DB instance.
(B). Create an Auto Scaling group for the front end with a combination of On-Demand and Spot Instances to reduce costs. Create two additional copies of the database instance, then distribute the databases in separate AZs.
(C). Create an Auto Scaling group for the front end with a combination of On-Demand and Spot Instances to reduce costs. Convert the tables in the Oracle database into Amazon DynamoDB tables.
(D). Convert the On-Demand Instances into Spot Instances to reduce costs for the front end. Convert the tables in the Oracle database into Amazon DynamoDB tables.

Answer: C

Combination of On-Demand and Spot Instances + DynamoDB.

NO.93 A company maintains a restaurant review website. The website is a single-page application where files are stored in Amazon S3 and delivered using Amazon CloudFront. The company receives several fake postings every day that are manually removed.
The security team has identified that most of the fake posts are from bots with IP addresses that have a bad reputation within the same global region. The team needs to create a solution to help restrict the bots from accessing the website.
Which strategy should a solutions architect use?
(A). Use AWS Firewall Manager to control the CloudFront distribution security settings. Create a geographical block rule and associate it with Firewall Manager.
(B). Associate an AWS WAF web ACL with the CloudFront distribution. Select the managed Amazon IP reputation rule group for the web ACL with a deny action.
(C). Use AWS Firewall Manager to control the CloudFront distribution security settings. Select the managed Amazon IP reputation rule group and associate it with Firewall Manager with a deny action.
(D). Associate an AWS WAF web ACL with the CloudFront distribution. Create a rule group for the web ACL with a geographical match statement with a deny action.

Answer: B

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

NO.94 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 group. Ensure that the EC2 instance type supports enhanced networking.
(B). Launch five new EC2 instances into an Auto Scaling group in the same Availability Zone. Attach an extra elastic network interface to each EC2 instance.
(C). Launch five new EC2 instances into a partition placement group. Ensure that the EC2 instance type supports enhanced networking.
(D). Launch five new EC2 instances into a spread placement group. Attach an extra elastic network interface to each EC2 instance.
Answer: A
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.

NO.95 A company used Amazon EC2 instances to deploy a web fleet to host a blog site The EC2 instances are behind an Application Load Balancer (ALB) and are configured in an Auto ScaSng group The web application stores all blog content on an Amazon EFS volume.
The company recently added a feature 'or Moggers to add video to their posts, attracting 10 times the previous user traffic At peak times of day. users report buffering and timeout issues while attempting to reach the site or watch videos Which is the MOST cost-efficient and scalable deployment that win resolve the issues for users?
(A). Reconfigure Amazon EFS to enable maximum I/O.
(B). Update the Nog site to use instance store volumes tor storage. Copy the site contents to the volumes at launch and to Amazon S3 al shutdown.
(C). Configure an Amazon CloudFront distribution. Point the distribution to an S3 bucket, and migrate the videos from EFS to Amazon S3.
(D). Set up an Amazon CloudFront distribution for all site contents, and point the distribution at the ALB.
Answer: C

NO.96 A company has a serverless multi-tenant content management system on AWS. The architecture contains a web-based front end that interacts with an Amazon API Gateway API that uses a custom AWS Lambda authorizes The authorizer authenticates a user to its tenant ID and encodes the information in a JSON Web Token (JWT) token. After authentication, each API call through API Gateway targets a Lambda function that interacts with a single Amazon DynamoOB table to fulfill requests.
To comply with security standards, the company needs a stronger isolation between tenants. The company will have hundreds of customers within the first year.
Which solution will meet these requirements with the LEAST operational?
(A). Create a DynamoDB table for each tenant by using the tenant ID in the table name. Create a

service that uses the JWT token to retrieve the appropriate Lambda execution role that is tenant-specific. Attach IAM policies to the execution role to allow access only to the DynamoDB table for the tenant.
(B). Add tenant ID information to the partition key of the DynamoDB table. Create a service that uses the JWT token to retrieve the appropriate Lambda execution role that is tenant-specific. Attach IAM policies to the execution role to allow access to items in the table only when the key matches the tenant ID.
(C). Create a separate AWS account for each tenant of the application. Use dedicated infrastructure for each tenant. Ensure that no cross-account network connectivity exists.
(D). Add tenant ID as a sort key in every DynamoDB table. Add logic to each Lambda function to use the tenant ID that comes from the JWT token as the sort key in every operation on the DynamoDB table.
Answer: B

NO.97 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. 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.
(B). Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's devices. Install the Amazon CloudWatch agent on all EC2 instances and send operating system audit logs to CloudWatch Logs.
(C). Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's devices. Enable AWS Config for EC2 security group resource changes. Enable AWS Firewall Manager and apply a security group policy that automatically remediates changes to rules.
(D). Create an IAM role with the Ama2onSSMManagedInstanceCore managed policy attached. Attach the IAM role to all the EC2 instances. Remove all security group rules attached to the EC2
(E). 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

NO.98 A group of research institutions and hospitals are in a partnership to study 2 PBs of genomic dat a. The institute that owns the data stores it in an Amazon S3 bucket and updates it regularly. The institute would like to give all of the organizations in the partnership read access to the data. All members of the partnership are extremety cost-conscious, and the institute that owns the account with the S3 bucket is concerned about covering the costs tor requests and data transfers from Amazon S3.

Which solution allows for secure datasharing without causing the institute that owns the bucket to assume all the costs for S3 requests and data transfers'?
(A). Ensure that all organizations in the partnership have AWS accounts. 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. Have the organizations assume and use that read role when accessing the data.
(B). Ensure that all organizations in the partnership have AWS accounts. 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. Enable Requester Pays on the bucket. Have the organizations use their AWS credentials when accessing the data.
(C). Ensure that all organizations in the partnership have AWS accounts. 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 organizations. Have the organizations use their AWS credentials when accessing the data using their accounts
(D). Ensure that all organizations in the partnership have AWS accounts. 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. Enable Requester Pays on the bucket. Have the organizations assume and use that read role when accessing the data.
Answer: B
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

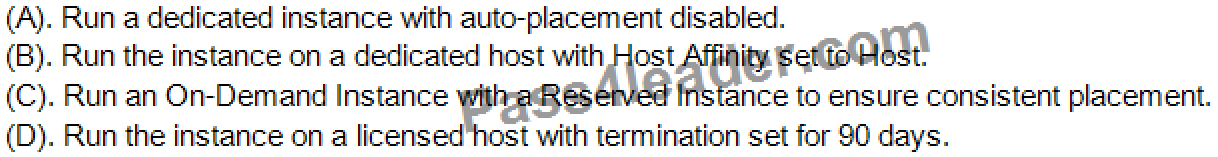
NO.99 An online e-commerce business is running a workload on AWS. The application architecture includes a web tier, an application tier for business logic, and a database tier for user and transactional data management. The database server has a 100 GB memory requirement. The business requires cost-efficient disaster recovery for the application with an RTO of 5 minutes and an RPO of 1 hour. The business also has a regulatory requirement for out-of-region disaster recovery with a minimum distance between the primary and alternate sites of 250 miles.
Which of the following options can the solutions architect design to create a comprehensive solution for this customer that meets the disaster recovery requirements?
(A). Back up the application and database data frequently and copy them to Amazon S3. Replicate the backups using S3 cross-region replication, and use AWS Cloud Formation to instantiate infrastructure for disaster recovery and restore data from Amazon S3.
(B). Employ a pilot light environment in which the primary database is configured with mirroring to build a standby database on m4.large in Ihe alternate region. Use AWS Cloud Formation to instantiate the web servers, application servers, and load balancers in case of a disaster to bring the application up in the alternate region. Vertically resize the database to meet the full production demands, and use Amazon Route 53 to switch traffic to the alternate region.
(C). Use a scaled-down version of the fully functional production environment in the alternate region that includes one instance of the web server, one instance of the application server, and a replicated instance of the database server in standby mode. Place the web and the application tiers in an Auto Scaling group behind a load balancer, which can automatically scale when the load arrives to the application. Use Amazon Route 53 to switch traffic to the alternate region,

(D). Employ a multi-region solution with fully functional web. application, and database tiers in both regions with equivalent capacity. Activate the primary database in one region only and the standby database in the other region. Use Amazon Route 53 to automatically switch traffic from one region to another using health check routing policies.

Answer: C

As RTO is in minutes (https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/plan-for-disaster-recovery-dr.html) Warm standby (RPO in seconds, RTO in minutes): Maintain a scaled-down version of a fully functional environment always running in the DR Region. Business-critical systems are fully duplicated and are always on, but with a scaled down fleet. When the time comes for recovery, the system is scaled up quickly to handle the production load.

NO.100 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

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

NO.101 A company runs a popular web application in an on-premises data center. The application receives four million views weekly. The company expects traffic to increase by 200% because of an advertisement that will be published soon.

The company needs to decrease the load on the origin before the increase of traffic occurs. The company does not have enough time to move the entire application to the AWS Cloud.

Which solution will meet these requirements?

(A). Create an Amazon CloudFront content delivery network (CDN). Enable query forwarding to the origin. Create a managed cache policy that includes query strings. Use an on-premises load balancer as the origin. Offload the DNS querying to AWS to handle CloudFront CDN traffic.

(B). Create an Amazon CloudFront content delivery network (CDN) that uses a Real Time Messaging Protocol (RTMP) distribution. Enable query forwarding to the origin. Use an on-premises load balancer as the origin. Offload the DNS querying to AWS to handle CloudFront CDN traffic.

(C). Create an accelerator in AWS Global Accelerator. Add listeners for HTTP and HTTPS TCP ports. Create an endpoint group. Create a Network Load Balancer (NLB), and attach it to the endpoint group. Point the NLB to the on-premises servers. Offload the DNS querying to AWS to handle AWS

Global Accelerator traffic.
(D). Create an accelerator in AWS Global Accelerator. Add listeners for HTTP and HTTPS TCP ports. Create an endpoint group. Create an Application Load Balancer (ALB), and attach it to the endpoint group. Point the ALB to the on-premises servers. Offload the DNS querying to AWS to handle AWS Global Accelerator traffic.
Answer: D

NO.102 A finance company hosts a data lake in Amazon S3. The company receives financial data records over SFTP each night from several third parties. The company runs its own SFTP server on an Amazon EC2 instance in a public subnet of a VPC. After the files ate uploaded, they are moved to the data lake by a cron job that runs on the same instance. The SFTP server is reachable on DNS sftp.examWe.com through the use of Amazon Route 53.
What should a solutions architect do to improve the reliability and scalability of the SFTP solution?
(A). Move the EC2 instance into an Auto Scaling group. Place the EC2 instance behind an Application Load Balancer (ALB). Update the DNS record sftp.example.com in Route 53 to point to the ALB.
(B). Migrate the SFTP server to AWS Transfer for SFTP. Update the DNS record sftp.example.com in Route 53 to point to the server endpoint hostname.
(C). Migrate the SFTP server to a file gateway in AWS Storage Gateway. Update the DNS record sflp.example.com in Route 53 to point to the file gateway endpoint.
(D). Place the EC2 instance behind a Network Load Balancer (NLB). Update the DNS record sftp.example.com in Route 53 to point to the NLB.
Answer: B

NO.103 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. 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
(B). Deploy an organization-wide AWS Config rule that requires all resources in the selected OUs to associate the AWS WAF rules. 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.
(C). Create AWS WAF rules in the management account of the organization Use AWS Lambda environment variables to store account numbers and OUs to manage Update environment variables as needed to add or remove accounts or OUs Create cross-account IAM roles in member accounts Assume the rotes by using AWS Security Token Service (AWS STS) in the Lambda function to create and update AWS WAF rules in the member accounts.
(D). 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

NO.104 A company is planning to migrate an application from on premises to the AWS Cloud. The company will begin the migration by moving the application's underlying data storage to AWS The application data is stored on a shared tie system on premises, and the application servers connect to the shared We system through SMB.

A solutions architect must implement a solution that uses an Amazon S3 bucket tor shared storage Until the application Is fully migrated and code is rewritten to use native Amazon S3 APIs, the application must continue to have access to the data through SMB The solutions architect must migrate the application data to AWS to its new location while still allowing the on-premises application to access the data.

Which solution will meet these requirements?

(A). Create a new Amazon FSx for Windows File Server fie system Configure AWS DataSync with one location tor the on-premises file share and one location for the new Amazon FSx file system Create a new DataSync task to copy the data from the on-premises file share location to the Amazon FSx file system

(B). Create an S3 bucket for the application. Copy the data from the on-premises storage to the S3 bucket

(C). Deploy an AWS Server Migration Service (AWS SMS) VM to the on-premises environment. Use AWS SMS to migrate the file storage server from on premises to an Amazon EC2 instance

(D). Create an S3 bucket for the application. Deploy a new AWS Storage Gateway Me gateway on an on-premises VM. Create a new file share that stores data in the S3 bucket and is associated with the tie gateway. Copy the data from the on-premises storage to the new file gateway endpoint.

Answer: A

NO.105 A financial company is building a system to generate monthly, immutable bank account statements for its users. Statements are stored in Amazon S3. Users should have immediate access to their monthly statements for up to 2 years. Some users access their statements frequently, whereas others rarely access their statements. The company's security and compliance policy requires that the statements be retained for at least 7 years.

What is the MOST cost-effective solution to meet the company's needs?

(A). Create an S3 bucket with Object Lock disabled. Store statements in S3 Standard. Define an S3 Lifecycle policy to transition the data to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days. Define another S3 Lifecycle policy to move the data to S3 Glacier Deep Archive after 2 years. Attach an S3 Glacier Vault Lock policy with deny delete permissions for archives less than 7 years old.

(B). Create an S3 bucket with versioning enabled. Store statements in S3 Intelligent-Tiering. Use same-Region replication to replicate objects to a backup S3 bucket. Define an S3 Lifecycle policy for the backup S3 bucket to move the data to S3 Glacier. Attach an S3 Glacier Vault Lock policy with deny delete permissions for archives less than 7 years old.

(C). Create an S3 bucket with Object Lock enabled. Store statements in S3 Intelligent-Tiering. Enable compliance mode with a default retention period of 2 years. Define an S3 Lifecycle policy to move the data to S3 Glacier after 2 years. Attach an S3 Glacier Vault Lock policy with deny delete permissions for archives less than 7 years old.

(D). Create an S3 bucket with versioning disabled. Store statements in S3 One Zone-Infrequent Access

(S3 One Zone-IA). Define an S3 Lifecyde policy to move the data to S3 Glacier Deep Archive after 2 years. Attach an S3 Glader Vault Lock policy with deny delete permissions for archives less than 7 years old.

Answer: C

https://aws.amazon.com/about-aws/whats-new/2018/11/s3-object-lock/

Create an S3 bucket with Object Lock enabled. Store statements in S3 Intelligent-Tiering. Enable compliance mode with a default retention period of 2 years. Define an S3 Lifecycle policy to move the data to S3 Glacier after 2 years. Attach an S3 Glacier Vault Lock policy with deny delete permissions for archives less than 7 years old.

https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html

NO.106 A company is using an Amazon EMR cluster to run its big data jobs The cluster's jobs are invoked by AWS Step Functions Express Workflows that consume various Amazon Simple Queue Service (Amazon SQS) queues The workload of this solution is variable and unpredictable Amazon CloudWatch metrics show that the cluster's peak utilization is only 25% at times and that the cluster sits idle the rest of the time A solutions architect must optimize the costs of the cluster without negatively impacting the time it takes to run the various jobs What is the MOST cost-effective solution that meets these requirements?

(A). Modify the EMR cluster by turning on automatic scaling of the core nodes and task nodes with a custom policy that is based on cluster utilization Purchase Reserved Instance capacity to cover the master node.

(B). Modify the EMR cluster to use an instance fleet of Dedicated On-Demand Instances for the master node and core nodes, and to use Spot Instances for the task nodes. Define target capacity for each node type to cover the load.

(C). Purchase Reserved Instances for the master node and core nodes Terminate all existing task nodes in the EMR cluster

(D). Modify the EMR cluster to use capacity-optimized Spot Instances and a diversified task fleet. Define target capacity for each node type with a mix of On-Demand Instances and Spot Instances.

Answer: B

NO.107 A multimedia company needs to deliver its video-on-demand (VOD) content to its subscribers in a cost-effective way. The video files range in size from 1-15 GB and are typically viewed frequently for the first 6 months alter creation, and then access decreases considerably. The company requires all video files to remain immediately available for subscribers. There are now roughly 30.000 files, and the company anticipates doubling that number over time.

What is the MOST cost-effective solution for delivering the company's VOD content?

(A). Store the video files in an Amazon S3 bucket using S3 Intelligent-Tiering. Use Amazon CloudFront to deliver the content with the S3 bucket as the origin.

(B). Use AWS Elemental MediaConvert and store the adaptive bitrate video files in Amazon S3. Configure an AWS Elemental MediaPackage endpoint to deliver the content from Amazon S3.

(C). Store the video files in Amazon Elastic File System (Amazon EFS) Standard. Enable EFS lifecycle management to move the video files to EFS Infrequent Access after 6 months. Create an Amazon EC2 Auto Scaling group behind an Elastic Load Balancer to deliver the content from Amazon EFS.

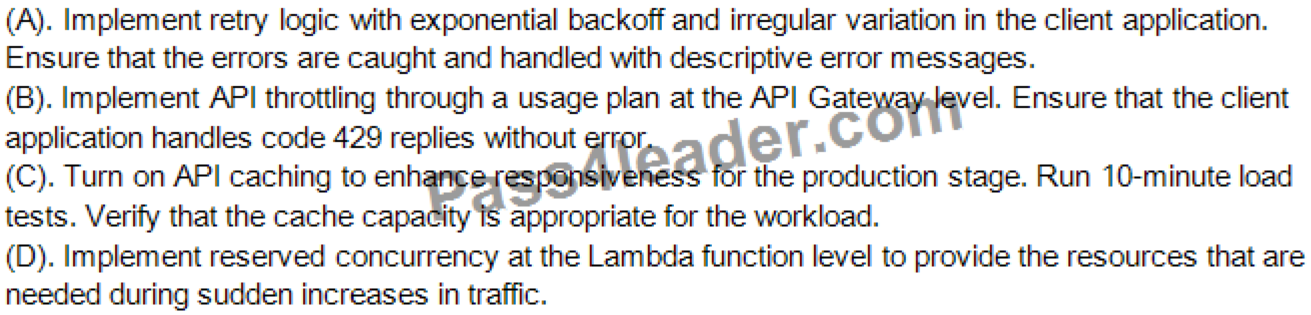
(D). Store the video files in Amazon S3 Standard. Create S3 Lifecycle rules to move the video files to S3 Standard-Infrequent Access (S3 Standard-IA) after 6 months and to S3 Glacier Deep Archive after 1 year. Use Amazon CloudFront to deliver the content with the S3 bucket as the origin.

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

NO.108 A company hosts its primary API on AWS by using an Amazon API Gateway API and AWS Lambda functions that contain the logic for the API methods. The company s internal applications use the API for core functionality and business logic. The company's customers use the API to access data from their accounts Several customers also have access to a legacy API that is running on a single standalone Amazon EC2 instance.
The company wants to increase the security for these APIs to better prevent denial of service (DoS) attacks, check for vulnerabilities, and guard against common exploits What should a solutions architect do to meet these requirements?
(A). Use AWS WAF to protect both APIs Configure Amazon Inspector to analyze the legacy API Configure Amazon GuardDuty to monitor for malicious attempts to access the APIs
(B). Use AWS WAF to protect the API Gateway API Configure Amazon Inspector to analyze both APIs Configure Amazon GuardDuty to block malicious attempts to access the APIs.
(C). Use AWS WAF to protect the API Gateway API Configure Amazon inspector to analyze the legacy API Configure Amazon GuardDuty to monitor for malicious attempts to access the APIs.
(D). Use AWS WAF to protect the API Gateway API Configure Amazon inspector to protect the legacy API Configure Amazon GuardDuty to block malicious attempts to access the APIs.
Answer: C

NO.109 A company is planning to set up a REST API application on AWS. The application team wants to set up a new identity store on AWS The IT team does not want to maintain any infrastructure or servers for this deployment.
What is the MOST operationally efficient solution that meets these requirements?
(A). Deploy the application as AWS Lambda functions. Set up Amazon API Gateway REST API endpoints for the application Create a Lambda function, and configure a Lambda authorizer
(B). Deploy the application in AWS AppSync, and configure AWS Lambda resolvers Set up an Amazon Cognito user pool, and configure AWS AppSync to use the user pool for authorization
(C). Deploy the application as AWS Lambda functions. Set up Amazon API Gateway REST API endpoints for the application Set up an Amazon Cognito user pool, and configure an Amazon Cognito authorizer
(D). Deploy the application in Amazon Elastic Kubemetes Service (Amazon EKS) clusters. Set up an Application Load Balancer for the EKS pods Set up an Amazon Cognito user pool and service pod for authentication.
Answer: C

NO.110 A software company has deployed an application that consumes a REST API by using Amazon API Gateway. AWS Lambda functions, and an Amazon DynamoDB table. The application is showing an increase in the number of errors during PUT requests. Most of the PUT calls come from a small number of clients that are authenticated with specific API keys.
A solutions architect has identified that a large number of the PUT requests originate from one client. The API is noncritical, and clients can tolerate retries of unsuccessful calls. However, the errors are displayed to customers and are causing damage to the API's reputation.
What should the solutions architect recommend to improve the customer experience?



(A). Implement retry logic with exponential backoff and irregular variation in the client application. Ensure that the errors are caught and handled with descriptive error messages.

(B). Implement API throttling through a usage plan at the API Gateway level. Ensure that the client application handles code 429 replies without error.

(C). Turn on API caching to enhance responsiveness for the production stage. Run 10-minute load tests. Verify that the cache capacity is appropriate for the workload.

(D). Implement reserved concurrency at the Lambda function level to provide the resources that are needed during sudden increases in traffic.

Answer: A

NO.111 A company uses multiple AWS accounts in a single AWS Region A solutions architect is designing a solution to consolidate logs generated by Elastic Load Balancers (ELBs) in the AppDev, AppTest and AppProd accounts. The logs should be stored in an existing Amazon S3 bucket named s3-eib-logs in the central AWS account. The central account is used for log consolidation only and does not have ELBs deployed ELB logs must be encrypted at rest Which combination of steps should the solutions architect take to build the solution'' (Select TWO)

(A). Update the S3 bucket policy for the s3-elb-logs bucket to allow the s3 PutBucketLogging action for the central AWS account ID

(B). Update the S3 bucket policy for the s3-eib-logs bucket to allow the s3 PutObject and s3 DeleteObject actions for the AppDev AppTest and AppProd account IDs

(C). Update the S3 bucket policy for the s3-elb-logs bucket to allow the s3 PutObject action for the AppDev AppTest and AppProd account IDs

(D). Enable access logging for the ELBs. Set the S3 location to the s3-elb-logs bucket

(E). Enable Amazon S3 default encryption using server-side encryption with S3 managed encryption keys (SSE-S3) for the s3-elb-logs S3 bucket

Answer: A,E

NO.112 A large company recently experienced an unexpected increase in Amazon RDS and Amazon DynamoDB costs The company needs to increase visibility into details of AWS Billing and Cost Management There are various accounts associated with AWS Organizations, including many development and production accounts. There is no consistent tagging strategy across the organization, but there are guidelines in place that require all infrastructure to be deployed using AWS Cloud Formation with consistent tagging Management requires cost center numbers and project ID numbers for all existing and future DynamoDB tables and RDS instances Which strategy should the solutions architect provide to meet these requirements?

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

(B). Use an AWS Config rule to alert the finance team of untagged resources Create a centralized AWS Lambda based solution to tag untagged RDS databases and DynamoDB resources every hour using a cross-account rote.

(C). Use Tag Editor to tag existing resources Create cost allocation tags to define the cost center and project ID Use SCPs to restrict resource creation that do not have the cost center and project ID on the resource.

(D). Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources Update existing federated roles to restrict privileges to provision resources that do not include the cost center and project ID on the resource

Answer: C

NO.113 A company is running a critical application that uses an Amazon RDS for MySQL database to store dat a. The RDS DB instance is deployed in Multi-AZ mode.
A recent RDS database failover test caused a 40-second outage to the application A solutions architect needs to design a solution to reduce the outage time to less than 20 seconds.
Which combination of steps should the solutions architect take to meet these requirements? (Select THREE.)
(A). Use Amazon ElastiCache for Memcached in front of the database
(B). Use Amazon ElastiCache for Redis in front of the database.
(C). Use RDS Proxy in front of the database
(D). Migrate the database to Amazon Aurora MySQL
(E). Create an Amazon Aurora Replica
(F). Create an RDS for MySQL read replica
Answer: A,B,F

NO.114 A company runs an application in the cloud that consists of a database and a website Users can post data to the website, have the data processed, and have the data sent back to them in an email. Data is stored in a MySQL database running on an Amazon EC2 instance The database is running in a VPC with two private subnets The website is running on Apache Tomcat in a single EC2 instance in a different VPC with one public subnet There is a single VPC peering connection between the database and website VPC.
The website has suffered several outages during the last month due to high traffic Which actions should a solutions architect take to increase the reliability of the application? (Select THREE)
(A). Place the Tomcat server in an Auto Scaling group with multiple EC2 instances behind an Application Load Balancer
(B). Provision an additional VPC peering connection
(C). Migrate the MySQL database to Amazon Aurora with one Aurora Replica
(D). Provision two NAT gateways in the database VPC
(E). Move the Tomcat server to the database VPC
(F). Create an additional public subnet in a different Availability Zone in the website VPC
Answer: A,C,F

NO.115 A solutions architect needs to advise a company on how to migrate its on-premises data processing application to the AWS Cloud. Currently, users upload input files through a web portal. The web server then stores the uploaded files on NAS and messages the processing server over a message queue. Each media file can take up to 1 hour to process. The company has determined that the number of media files awaiting processing is significantly higher during business hours, with the number of files rapidly declining after business hours.
What is the MOST cost-effective migration recommendation?
(A). Create a queue using Amazon SQS. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the files. Store the processed files in an Amazon S3 bucket.
(B). Create a queue using Amazon MO. Configure the existing web server to publish to the new queue. When there are messages in the queue, create a new Amazon EC2 instance to pull requests from the queue and process the files. Store the processed files in Amazon EFS. Shut down the EC2

instance after the task is complete.
(C). Create a queue using Amazon MO. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the files. Store the processed files in Amazon EFS.
(D). Create a queue using Amazon SOS. Configure the existing web server to publish to the new queue. Use Amazon EC2 instances in an EC2 Auto Scaling group to pull requests from the queue and process the files. Scale the EC2 instances based on the SOS queue length. Store the processed files in an Amazon S3 bucket.
Answer: D
https://aws.amazon.com/blogs/compute/operating-lambda-performance-optimization-part-1/

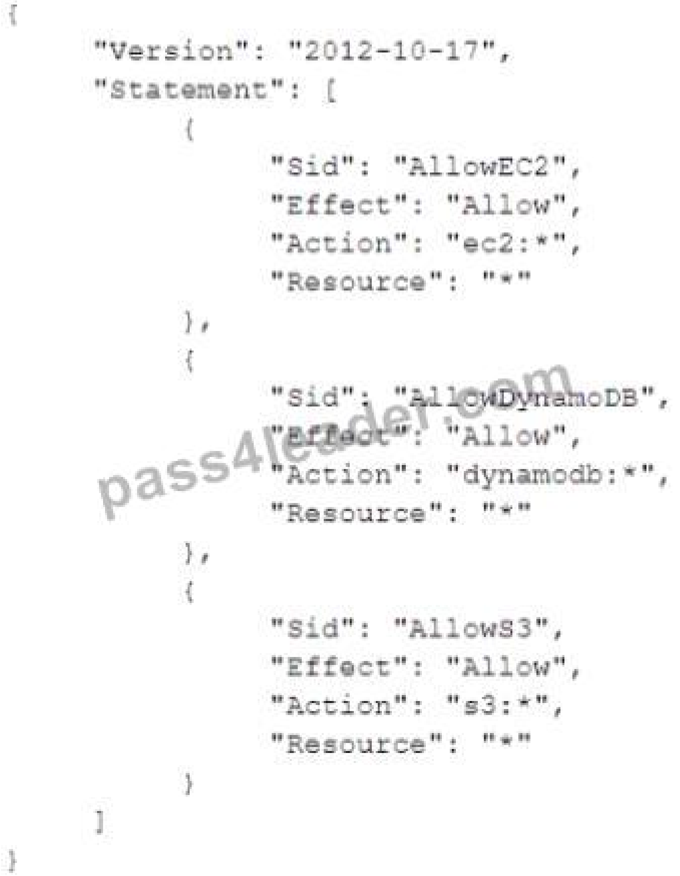
NO.116 A company wants to retire its Oracle Solaris NFS storage arrays. The company requires rapid data migration over its internet network connection to a combination of destinations for Amazon S3. Amazon Elastic File System (Amazon EFS), and Amazon FSx lor Windows File Server. The company also requires a full initial copy, as well as incremental transfers of changes until the retirement of the storage arrays. All data must be encrypted and checked for integrity.
What should a solutions architect recommend to meet these requirements?
(A). Configure CloudEndure. Create a project and deploy the CloudEndure agent and token to the storage array. Run the migration plan to start the transfer.
(B). Configure AWS DataSync. Configure the DataSync agent and deploy it to the local network. Create a transfer task and start the transfer.
(C). Configure the aws S3 sync command. Configure the AWS client on the client side with credentials. Run the sync command to start the transfer.
(D). Configure AWS Transfer (or FTP. Configure the FTP client with credentials. Script the client to connect and sync to start the transfer.
Answer: B

NO.117 A company operates quick-service restaurants. The restaurants follow a predictable model with high sales traffic for -4 hours daily Sates traffic is lower outside of those peak hours.
The point of sale and management platform is deployed in the AWS Cloud and has a backend that is based or Amazon DynamoDB The database table uses provisioned throughput mode with 100.000 RCUs and 80.000 WCUs to match Known peak resource consumption.
The company wants to reduce its DynamoDB cost and minimize the operational overhead for the IT staff.
Which solution meets these requirements MOST cost-effectively?
(A). Reduce the provisioned RCUs and WCUs
(B). Change the DynamoDB table to use on-demand capacity
(C). Enable Dynamo DB auto seating for the table.
(D). Purchase 1-year reserved capacity that is sufficient to cover the peak load for 4 hours each day.
Answer: C

NO.118 A solutions architect must update an application environment within AWS Elastic Beanstalk using a With green deployment methodology. The solutions architect creates an environment that is identical to the existing application environment and deploys the application to the new environment.
What should be done next to complete the update?

(A). Redirect to the new environment using Amazon Route 53
(B). Select the Swap Environment URLs option.
(C). Replace the Auto Scaling launch configuration
(D). Update the DNS records to point to the green environment
Answer: B

NO.119 A company is in the process of implementing AWS Organizations to constrain its developers to use only Amazon EC2. Amazon S3 and Amazon DynamoDB. The developers account resides In a dedicated organizational unit (OU). The solutions architect has implemented the following SCP on the developers account:



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

When this policy is deployed, IAM users in the developers account are still able to use AWS services that are not listed in the policy. What should the solutions architect do to eliminate the developers' ability to use services outside the scope of this policy?
(A). Create an explicit deny statement for each AWS service that should be constrained
(B). Remove the Full AWS Access SCP from the developer account's OU
(C). Modify the Full AWS Access SCP to explicitly deny all services
(D). Add an explicit deny statement using a wildcard to the end of the SCP
Answer: B

NO.120 An online magazine will launch Its latest edition this month. This edition will be the first to be distributed globally. The magazine's dynamic website currently uses an Application Load Balancer in front of the web tier a fleet of Amazon EC2 instances for web and application servers, and Amazon Aurora MySQL. Portions of the website include static content and almost all traffic is read-only The magazine is expecting a significant spike m internet traffic when the new edition is launched Optimal

performance is a top priority for the week following the launch Which combination of steps should a solutions architect take to reduce system response antes for a global audience? (Select TWO)
(A). Use logical cross-Region replication to replicate the Aurora MySQL database to a secondary Region Replace the web servers with Amazon S3 Deploy S3 buckets in cross-Region replication mode
(B). Ensure the web and application tiers are each m Auto Scaling groups. Introduce an AWS Direct Connect connection Deploy the web and application tiers in Regions across the world
(C). Migrate the database from Amazon Aurora to Amazon RDS for MySQL. Ensure all three of the application tiers-web. application, and database-are in private subnets.
(D). Use an Aurora global database for physical cross-Region replication. Use Amazon S3 with cross-Region replication for static content and resources. Deploy the web and application tiers in Regions across the world
(E). Introduce Amazon Route 53 with latency-based routing and Amazon CloudFront distributions. Ensure me web and application tiers are each in Auto Scaling groups
Answer: D,E

NO.121 A company is migrating an on-premises content management system (CMS) to AWS Fargate. The company uses the CMS for blog posts that include text, images, and videos. The company has observed that traffic to blog posts drops by more than 80% after the posts are more than 30 days old The CMS runs on multiple VMs and stores application state on disk This application state is shared across all instances across multiple Availability Zones Images and other media are stored on a separate NFS file share. The company needs to reduce the costs of the existing solution while minimizing the impact on performance.
Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO.)
(A). Store media in an Amazon S3 Standard bucket Create an S3 Lifecycle configuration that transitions objects that are older than 30 days to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class.
(B). Store media on an Amazon Elastic File System (Amazon EFS) volume Attach the EFS volume to all Fargate instances.
(C). Store application state on an Amazon Elastic File System (Amazon EFS) volume Attach the EFS volume to all Fargate instances.
(D). Store application state on an Amazon Elastic Block Store (Amazon EBS) volume Attach the EBS volume to all Fargate instances.
(E). Store media in an Amazon S3 Standard bucket Create an S3 Lifecycle configuration that transitions objects that are older than 30 days to the S3 Glacier storage class
Answer: A,C

NO.122 A company is developing and hosting several projects in the AWS Cloud. The projects are developed across multiple AWS accounts under the same organization in AWS Organizations. The company requires the cost lor cloud infrastructure to be allocated to the owning project. The team responsible for all of the AWS accounts has discovered that several Amazon EC2 instances are lacking the Project tag used for cost allocation.
Which actions should a solutions architect take to resolve the problem and prevent it from happening in the future? (Select THREE.)
(A). Create an AWS Config rule in each account to find resources with missing tags.
(B). Create an SCP in the organization with a deny action for ec2:RunInstances if the Project tag is missing.

(C). Use Amazon Inspector in the organization to find resources with missing tags.
(D). Create an IAM policy in each account with a deny action for ec2:RunInstances if the Project tag is missing.
(E). Create an AWS Config aggregator for the organization to collect a list of EC2 instances with the missing Project tag.
(F). Use AWS Security Hub to aggregate a list of EC2 instances with the missing Project tag.
Answer: B,D,E

NO.123 A company is developing a gene reporting device that will collect genomic information to assist researchers with collecting large samples of data from a diverse population. The device will push 8 KB of genomic data every second to a data platform that will need to process and analyze the data and provide information back to researchers The data platform must meet the following requirements:
* Provide near-real-time analytics of the inbound genomic data
* Ensure the data is flexible, parallel, and durable
* Deliver results of processing to a data warehouse
Which strategy should a solutions architect use to meet these requirements?
(A). Use Amazon Kinesis Data Firehose to collect the inbound sensor data analyze the data with Kinesis clients. and save the results to an Amazon RDS instance
(B). Use Amazon Kinesis Data Streams to collect the inbound sensor data analyze the data with Kinesis clients and save the results to an Amazon Redshift duster using Amazon EMR
(C). Use Amazon S3 to collect the inbound device data analyze the data from Amazon SOS with Kinesis and save the results to an Amazon Redshift duster
(D). Use an Amazon API Gateway to put requests into an Amazon SQS queue analyze the data with an AWS Lambda function and save the results an Amazon Redshift duster using Amazon EMR
Answer: A

NO.124 A company wants to deploy an API to AWS. The company plans to run the API on AWS Fargate behind a load balancer. The API requires the use of header-based routing and must be accessible from on-premises networks through an AWS Direct Connect connection and a private VIF. The company needs to add the client IP addresses that connect to the API to an allow list in AWS. The company also needs to add the IP addresses of the API to the allow list. The company's security team will allow /27 CIDR ranges to be added to the allow list. The solution must minimize complexity and operational overhead.
Which solution will meet these requirements?
(A). Create a new Network Load Balancer (NLB) in the same subnets as the Fargate task deployments. Create a security group that includes only the client IP addresses that need access to the API. Attach the new security group to the Fargate tasks. Provide the security team with the NLB's IP addresses for the allow list.
(B). Create two new /27 subnets. Create a new Application Load Balancer (ALB) that extends across the new subnets. Create a security group that includes only the client IP addresses that need access to the API. Attach the security group to the ALB. Provide the security team with the new subnet IP ranges for the allow list.
(C). Create two new '27 subnets. Create a new Network Load Balancer (NLB) that extends across the new subnets. Create a new Application Load Balancer (ALB) within the new subnets. Create a security group that includes only the client IP addresses that need access to the API. Attach the security group

to the ALB. Add the ALB's IP addresses as targets behind the NLB. Provide the security team with the NLB's IP addresses for the allow list.
(D). Create a new Application Load Balancer (ALB) in the same subnets as the Fargate task deployments. Create a security group that includes only the client IP addresses that need access to the API. Attach the security group to the ALB. Provide the security team with the ALB's IP addresses for the allow list.
Answer: A

NO.125 A new startup is running a serverless application using AWS Lambda as the primary source of compute New versions of the application must be made available to a subset of users before deploying changes to all users Developers should also have the ability to stop the deployment and have access to an easy rollback mechanism A solutions architect decides to use AWS CodeDeploy to deploy changes when a new version is available.
Which CodeDeploy configuration should the solutions architect use?
(A). A blue/green deployment
(B). A linear deployment
(C). A canary deployment
(D). An all-at-once deployment
Answer: C

NO.126 A company is migrating an application to AWS. It wants to use fully managed services as much as possible during the migration. The company needs to store large, important documents within the application with the following requirements:
1. The data must be highly durable and available.
2. The data must always be encrypted at rest and in transit.
3. The encryption key must be managed by the company and rotated periodically.
Which of the following solutions should the solutions architect recommend?
(A). Deploy the storage gateway to AWS in file gateway mode. Use Amazon EBS volume encryption using an AWS KMS key to encrypt the storage gateway volumes.
(B). Use Amazon S3 with a bucket policy to enforce HTTPS for connections to the bucket and to enforce server-side encryption and AWS KMS for object encryption.
(C). Use Amazon DynamoDB with SSL to connect to DynamoDB. Use an AWS KMS key to encrypt DynamoDB objects at rest.
(D). Deploy instances with Amazon EBS volumes attached to store this data. Use E8S volume encryption using an AWS KMS key to encrypt the data.
Answer: B
Use Amazon S3 with a bucket policy to enforce HTTPS for connections to the bucket and to enforce server-side encryption and AWS KMS for object encryption.

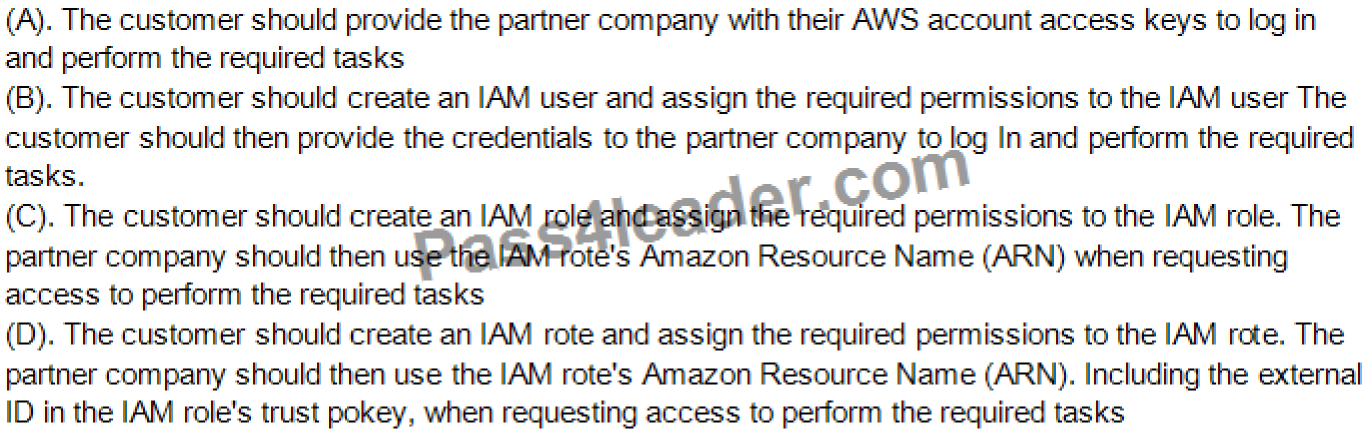
NO.127 A company's AWS architecture currently uses access keys and secret access keys stored on each instance to access AWS services. Database credentials are hard-coded on each instance. SSH keys for command-tine remote access are stored in a secured Amazon S3 bucket. The company has asked its solutions 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 (or remote access.
(E). Use AWS KMS to store database credentials.
(F). Use AWS Systems Manager Session Manager tor remote access
Answer: A,C,F
https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html

NO.128 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 toots.
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 me AWS Lambda function will trigger to crawl objects in me S3 bucket
(F). Create an AWS Glue crawler that the Amazon EventBridge (Amazon CloudWatCh Events) rule will trigger to crawl objects m the S3 bucket
Answer: B,D,F

NO.129 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: B,E

NO.130 An AWS partner company is building a service in AWS Organizations using Its organization named org. This service requires the partner company to have access to AWS resources in a customer account, which is in a separate organization named org2 The company must establish least privilege security access using an API or command line tool to the customer account What is the MOST secure way to allow org1 to access resources h org2?



(A). The customer should provide the partner company with their AWS account access keys to log in and perform the required tasks

(B). The customer should create an IAM user and assign the required permissions to the IAM user The customer should then provide the credentials to the partner company to log In and perform the required tasks.

(C). The customer should create an IAM role and assign the required permissions to the IAM role. The partner company should then use the IAM rote's Amazon Resource Name (ARN) when requesting access to perform the required tasks

(D). The customer should create an IAM rote and assign the required permissions to the IAM rote. The partner company should then use the IAM rote's Amazon Resource Name (ARN). Including the external ID in the IAM role's trust pokey, when requesting access to perform the required tasks

Answer: D

NO.131 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. Delete the existing private virtual interface from the existing connection. Create the second Direct Connect connection. Create a new private virtual interlace on each connection, and connect both private victual interfaces to the Direct Connect gateway. Connect the Direct Connect gateway to the single VPC.

(B). Keep the existing private virtual interface. Create the second Direct Connect connection. Create a new private virtual interface on the new connection, and connect the new private virtual interface to the single VPC.

(C). Keep the existing private virtual interface. Create the second Direct Connect connection. Create a new public virtual interface on the new connection, and connect the new public virtual interface to the single VPC.

(D). Provision a transit gateway. Delete the existing private virtual interface from the existing connection. Create the second Direct Connect connection. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the transit gateway. Associate the transit gateway with the single VPC.

Answer: A

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

NO.132 A company hosts a web application on AWS in the us-east-1 Region. The application servers are distributed across three Availability Zones behind an Application Load Balancer The database is hosted in a MySQL database on an Amazon EC2 instance A solutions architect needs to design a cross-Region data recovery solution using AWS services with an RTO of less than 5 minutes and an RPO of less than 1 minute. The solutions architect is deploying application servers in us-west-2 and

has configured Amazon Route 53 health checks and DNS failover to us-west-2.
Which additional step should the solutions architect take?
(A). Migrate the database to an Amazon RDS for MySQL instance with a cross-Region read replica in us-west-2
(B). Migrate the database to an Amazon Aurora global database with the primary in us-east-1 and the secondary in us-west-2
(C). Migrate the database to an Amazon RDS for MySQL instance with a Multi-AZ deployment
(D). Create a MySQL standby database on an Amazon EC2 instance in us-west-2
Answer: C

NO.133 An e-commerce company is revamping its IT infrastructure and is planning to use AWS services. The company's CIO has asked a solutions architect to design a simple, highly available, and loosely coupled order processing application. The application is responsible (or receiving and processing orders before storing them in an Amazon DynamoDB table. The application has a sporadic traffic pattern and should be able to scale during markeling campaigns to process the orders with minimal delays.
Which of the following is the MOST reliable approach to meet the requirements?
(A). Receive the orders in an Amazon EC2-hosted database and use EC2 instances to process them.
(B). Receive the orders in an Amazon SOS queue and trigger an AWS Lambda function lo process them.
(C). Receive the orders using the AWS Step Functions program and trigger an Amazon ECS container lo process them.
(D). Receive the orders in Amazon Kinesis Data Streams and use Amazon EC2 instances to process them.
Answer: B
Q: How does Amazon Kinesis Data Streams differ from Amazon SQS?
Amazon Kinesis Data Streams enables real-time processing of streaming big data. It provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications. The Amazon Kinesis Client Library (KCL) delivers all records for a given partition key to the same record processor, making it easier to build multiple applications reading from the same Amazon Kinesis data stream (for example, to perform counting, aggregation, and filtering).
https://aws.amazon.com/kinesis/data-streams/faqs/
https://aws.amazon.com/blogs/big-data/unite-real-time-and-batch-analytics-using-the-big-data-lambda-architecture-without-servers/

NO.134 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 VPC. and ensure that network access control and security group rules allow the relevant inbound and outbound traffic.

(D). Attach a NAT gateway to the VPC. and ensure that network access control and security group rules allow the relevant inbound and outbound traffic.
Answer: A

NO.135 A company runs applications on Amazon EC2 instances. The company plans to begin using an Auto Scaling group for the instances. As part of this transition, a solutions architect must ensure that Amazon CloudWatch Logs automatically collects logs from all new instances The new Auto Scaling group will use a launch template that includes the Amazon Linux 2 AMI and no key pair Which solution meets these requirements?
(A). Create an Amazon CloudWatch agent configuration for the workload Store the CloudWatch agent configuration in an Amazon S3 bucket Write an EC2 user data script to fetch the configuration He from Amazon S3. Configure the cloudWatch agent on the instance during Initial boot.
(B). Create an Amazon CloudWatch agent configuration for the workload In AWS Systems Manager Parameter Store Create a Systems Manager document that Installs and configures the CloudWatch agent by using the configuration Create an Amazon EventBridge (Amazon CloudWatch Events) rule on the default event bus with a Systems Manager Run Command target that runs the document whenever an instance enters the running state.
(C). Create an Amazon CloudWatch agent configuration for the workload Create an AWS Lambda function to Install and configure CloudWatch agent by using AWS Systems Manager Session Manager. 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
(D). Create an Amazon CloudWatch agent configuration for the workload. Save the CloudWatch agent configuration as pan of an AWS Lambda deployment package. Use AWS CloudTrail to capture EC2 tagging events and initiate agent installation. Use AWS CodeBuild to configure the CloudWatch agent on the instances that run the workload.
Answer: B

NO.136 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/Jpostld) to get post details
GET /users/{userld}. to get user details
GET /comments/{commentld}: 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{commentld} 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

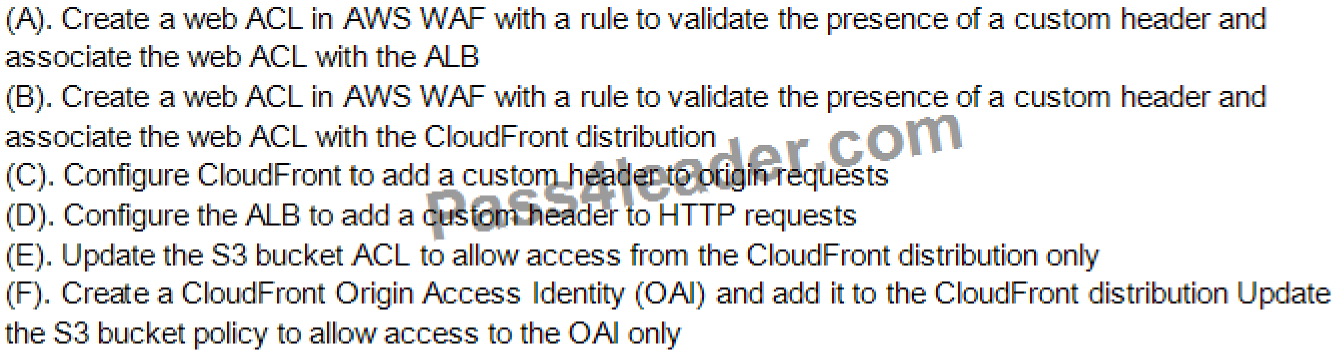
NO.137 A large company with hundreds of AWS accounts has a newly established centralized internal process for purchasing new or modifying existing Reserved Instances. This process requires all business units that want to purchase or modify Reserved Instances to submit requests to a dedicated team for procurement or execution. Previously, business units would directly purchase or

modify Reserved Instances in their own respective AWS accounts autonomously.
Which combination of steps should be taken to proactively enforce the new process in the MOST secure way possible? (Select TWO.)
(A). Ensure all AWS accounts are part of an AWS Organizations structure operating in all features mode.
(B). Use AWS Contig lo report on the attachment of an IAM policy that denies access to the ec2:PurchaseReservedInstancesOffering and ec2:ModifyReservedInstances actions.
(C). In each AWS account, create an IAM policy with a DENY rule to the ec2:PurchaseReservedInstancesOffering and ec2:ModifyReservedInstances actions.
(D). Create an SCP that contains a deny rule to the ec2:PurchaseReservedInstancesOffering and ec2: Modify Reserved Instances actions. Attach the SCP to each organizational unit (OU) of the AWS Organizations structure.
(E). Ensure that all AWS accounts are part of an AWS Organizations structure operating in consolidated billing features mode.
Answer: A,D
https://docs.aws.amazon.com/organizations/latest/APIReference/API_EnableAllFeatures.html
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp-strategies.html

NO.138 A company is developing a new service that will be accessed using TCP on a static port A solutions architect must ensure that the service is highly available, has redundancy across Availability Zones, and is accessible using the DNS name myservice.com, which is publicly accessible The service must use fixed address assignments so other companies can add the addresses to their allow lists.
Assuming that resources are deployed in multiple Availability Zones in a single Region, which solution will meet these requirements?
(A). Create Amazon EC2 instances with an Elastic IP address for each instance Create a Network Load Balancer (NLB) and expose the static TCP port Register EC2 instances with the NLB Create a new name server record set named my service com, and assign the Elastic IP addresses of the EC2 instances to the record set Provide the Elastic IP addresses of the EC2 instances to the other companies to add to their allow lists
(B). Create an Amazon ECS cluster and a service definition for the application Create and assign public IP addresses for the ECS cluster Create a Network Load Balancer (NLB) and expose the TCP port Create a target group and assign the ECS cluster name to the NLB Create a new A record set named my service com and assign the public IP addresses of the ECS cluster to the record set Provide the public IP addresses of the ECS cluster to the other companies to add to their allow lists
(C). Create Amazon EC2 instances for the service Create one Elastic IP address for each Availability Zone Create a Network Load Balancer (NLB) and expose the assigned TCP port Assign the Elastic IP addresses to the NLB for each Availability Zone Create a target group and register the EC2 instances with the NLB Create a new A (alias) record set named my service com, and assign the NLB DNS name to the record set.
(D). Create an Amazon ECS cluster and a service definition for the application Create and assign public IP address for each host in the cluster Create an Application Load Balancer (ALB) and expose the static TCP port Create a target group and assign the ECS service definition name to the ALB Create a new CNAME record set and associate the public IP addresses to the record set Provide the Elastic IP addresses of the Amazon EC2 instances to the other companies to add to their allow lists
Answer: C

NO.139 A company deploys a new web application As part of the setup, the company configures AWS WAF to log to Amazon S3 through Amazon Kinesis Data Firehose. The company develops an Amazon Athena query that runs once daily to return AWS WAF log data from the previous 24 hours. The volume of daily logs is constant However over time, the same query is taking more time to run A solutions architect needs to design a solution to prevent the query time from continuing to increase. The solution must minimize operational overhead Which solution will meet these requirements?
(A). Create an AWS Lambda function that consolidates each day's AWS WAF logs into one log file
(B). Reduce the amount of data scanned by configuring AWS WAF to send logs to a different S3 bucket each day
(C). Update the Kinesis Data Firehose configuration to partition the data in Amazon S3 by date and time Create external tables for Amazon Redshift Configure Amazon Redshift Spectrum to query the data source
(D). Modify the Kinesis Data Firehose configuration and Athena table definition to partition the data by date and time. Change the Athena query to view the relevant partitions
Answer: D

NO.140 A company is launching a web-based application in multiple regions around the world The application consists of both static content stored in a private Amazon S3 bucket and dyna ECS containers behind an Application Load Balancer (ALB) The company requires that the static and dynamic application content be accessible through Amazon CloudFront only Which combination of steps should a solutions architect recommend to restrict direct content access to CloudFront? (Select THREE)



(A). Create a web ACL in AWS WAF with a rule to validate the presence of a custom header and associate the web ACL with the ALB
(B). Create a web ACL in AWS WAF with a rule to validate the presence of a custom header and associate the web ACL with the CloudFront distribution
(C). Configure CloudFront to add a custom header to origin requests
(D). Configure the ALB to add a custom header to HTTP requests
(E). Update the S3 bucket ACL to allow access from the CloudFront distribution only
(F). Create a CloudFront Origin Access Identity (OAI) and add it to the CloudFront distribution Update the S3 bucket policy to allow access to the OAI only

Answer: A,C,F

NO.141 A solutions architect is building a web application that uses an Amazon RDS for PostgreSQL DB instance The DB instance is expected to receive many more reads than writes The solutions architect needs to ensure that the large amount of read traffic can be accommodated and that the DB instance is highly available.
Which steps should the solutions architect take to meet these requirements? (Select THREE.)
(A). Create multiple read replicas and put them into an Auto Scaling group
(B). Create multiple read replicas in different Availability Zones.
(C). Create an Amazon Route 53 hosted zone and a record set for each read replica with a TTL and a weighted routing policy
(D). Create an Application Load Balancer (ALBJ and put the read replicas behind the ALB.
(E). Configure an Amazon CloudWatch alarm to detect a failed read replica Set the alarm to directly invoke an AWS Lambda function to delete its Route 53 record set.

(F). Configure an Amazon Route 53 health check for each read replica using its endpoint

Answer: B,C,F

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

NO.142 A company has used infrastructure as code (IaC) to provision a set of two Amazon EC2 instances. The instances have remained the same tor several years.

The company's business has grown rapidly in the past few months. In response, the company's operations team has implemented an Auto Scaling group to manage the sudden increases in traffic Company policy requires a monthly installation of security updates on all operating systems that are running.

The most recent security update required a reboot. As a result the Auto Scaling group terminated the instances and replaced them with new, unpatched instances.

Which combination of steps should a sol-tons architect recommend to avoid a recurrence of this issue? (Select TWO)

(A). Modify the Auto Scaling group by setting the Update policy to target the oldest launch configuration for replacement.

(B). Create a new Auto Scaling group before the next patch maintenance During the maintenance window patch both groups and reboot the instances.

(C). Create an Elastic Load Balancer in front of the Auto Scaling group Configure monitoring to ensure that target group health checks return healthy after the Auto Scaling group replaces the terminated instances

(D). Create automation scripts to patch an AMI. update the launch configuration, and invoke an Auto Scaling instance refresh.

(E). Create an Elastic Load Balancer in front of the Auto Scaling group Configure termination protection on the instances.

Answer: A,C

NO.143 A company is finalizing the architecture for its backup solution for applications running on AWS. All of the applications run on AWS and use at least two Availability Zones in each tier.

Company policy requires IT to durably store nightly backups of all its data in at least two locations: production and disaster recovery. The locations must be m different geographic regions. The company also needs the backup to be available to restore immediately at the production data center, and within 24 hours at the disaster recovery location backup processes must be fully automated.

What is the MOST cost-effective backup solution that will meet all requirements?

(A). Back up all the data to a large Amazon EBS volume attached to the backup media server m the production region. Run automated scripts to snapshot these volumes nightly. and copy these snapshots to the disaster recovery region.

(B). Back up all the data to Amazon S3 in the disaster recovery region Use a Lifecycle policy to move this data to Amazon Glacier in the production region immediately Only the data is replicated: remove the data from the S3 bucket in the disaster recovery region.

(C). Back up all the data to Amazon Glacier in the production region. Set up cross-region replication of

this data to Amazon Glacier in the disaster recovery region. Set up a lifecycle policy to delete any data o der than 60 days.
(D). Back up all the data to Amazon S3 in the production region. Set up cross-region replication of this S3 bucket to another region and set up a lifecycle policy in the second region to immediately move this data to Amazon Glacier
Answer: D

NO.144 A company has many AWS accounts and uses AWS Organizations to manage all of them. A solutions architect must implement a solution that the company can use to share a common network across multiple accounts.
The company's infrastructure team has a dedicated infrastructure account that has a VPC. The infrastructure team must use this account to manage the network. Individual accounts cannot have the ability to manage their own networks. However, individual accounts must be able to create AWS resources within subnets.
Which combination of actions should the solutions architect perform to meet these requirements? (Select TWO.)
(A). Create a transit gateway in the infrastructure account.
(B). Enable resource sharing from the AWS Organizations management account.
(C). Create VPCs in each AWS account within the organization in AWS Organizations. Configure the VPCs to share the same CIDR range and subnets as the VPC in the infrastructure account. Peer the VPCs in each individual account with the VPC in the infrastructure account,
(D). Create a resource share in AWS Resource Access Manager in the infrastructure account. Select the specific AWS Organizations OU that will use the shared network. Select each subnet to associate with the resource share.
(E). Create a resource share in AWS Resource Access Manager in the infrastructure account. Select the specific AWS Organizations OU that will use the shared network. Select each prefix list to associate with the resource share.
Answer: C,E
https://docs.aws.amazon.com/vpc/latest/userguide/sharing-managed-prefix-lists.html

NO.145 A company is planning to migrate its on-premises data analysis application to AWS. The application is hosted across a fleet of servers and requires consistent system time.
The company has established an AWS Direct Connect connection from its on-premises data center to AWS. The company has a high-precision stratum-0 atomic dock network appliance that acts as an NTP source for all on-premises servers.
After the migration to AWS is complete, the clock on all Amazon EC2 instances that host the application must be synchronized with the on-premises atomic clock network appliance.
Which solution will meet these requirements with the LEAST administrative overhead?
(A). Configure a DHCP options set with the on-premises NTP server address Assign the options set to the VPC. Ensure that NTP traffic is allowed between AWS and the on-premises networks.
(B). Create a custom AMI to use the Amazon Time Sync Service at 169.254.169.123 Use this AMI for the application Use AWS Config to audit the NTP configuration.
(C). Deploy a third-party time server from the AWS Marketplace. Configure the time server to synchronize with the on-premises atomic clock network appliance. Ensure that NTP traffic is allowed inbound in the network ACLs for the VPC that contains the third-party server.
(D). Create an IPsec VPN tunnel from the on-premises atomic clock network appliance to the VPC to

encrypt the traffic over the Direct Connect connection. Configure the VPC route tables to direct NTP traffic over the tunnel.

Answer: B

NO.146 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 job. Configure a server in the company items 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.

Answer: D

Create an AWS Snowball import job. Configure a server in the company items 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/

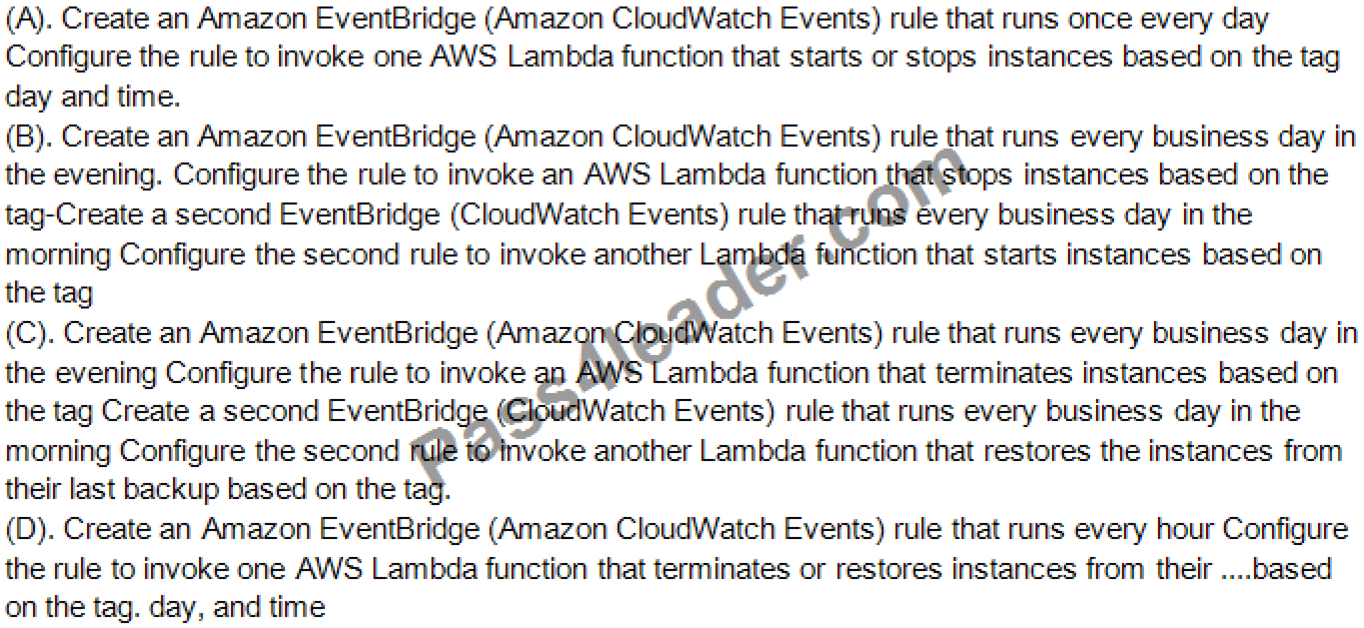
NO.147 To abide by industry regulations, a solutions architect must design a solution that will store a company's critical data in multiple public AWS Regions, including in the United States, where the company's headquarters is located. The solutions architect is required to provide access to the data stored in AWS to the company's global WAN network. The security team mandates that no traffic accessing this data should traverse the public internet.
How should the solutions architect design a highly available solution that meets the requirements and is cost-effective?
(A). Establish AWS Direct Connect connections from the company headquarters to all AWS Regions in use. Use the company WAN lo send traffic over to the headquarters and then to the respective DX connection to access the data.
(B). Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use inter-region VPC peering to access the data in other AWS Regions.
(C). Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use an AWS transit VPC solution to access data in other AWS Regions.
(D). Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use Direct Connect Gateway to access data in other AWS Regions.
Answer: D
This feature also allows you to connect to any of the participating VPCs from any Direct Connect location, further reducing your costs for making using AWS services on a cross-region basis.
https://aws.amazon.com/blogs/aws/new-aws-direct-connect-gateway-inter-region-vpc-access/
https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway.html

NO.148 A company has implemented a global multiplayer gaming platform The platform requires gaming clients to have reliable, low-latency access to the server infrastructure that is hosted on a fleet of Amazon EC2 instances in a single AWS Region The gaming clients use a custom TCP protocol to connect to the server infrastructure The application architecture requires client IP addresses to be available to the server software Which solution meets these requirements?
(A). Create a Network Load Balancer (NLB), and add the EC2 instances to a target group Create an Amazon CloudFront Real Time Messaging Protocol (RTMP) distribution and configure the origin to point to the DNS endpoint of the NLB Use proxy protocol version 2 headers to preserve client IP addresses
(B). Use an AWS Direct Connect gateway to connect multiple Direct Connect locations in different Regions globally Configure Amazon Route 53 with geolocation routing to send traffic to the nearest Direct Connect location Associate the VPC that contains the EC2 instances with the Direct Connect gateway
(C). Create an accelerator in AWS Global Accelerator and configure the listener to point to a single

endpoint group Add each of the EC2 instances as endpoints to the endpoint group Configure the endpoint group weighting equally across all of the EC2 endpoints
(D). Create an Application Load Balancer (ALB) and add the EC2 instances to a target group Create a set of Amazon Route 53 latency-based alias records that point to the DNS endpoint of the ALB Use X-Forwarded-For headers to preserve client IP addresses
Answer: B

NO.149 A company is using AWS CloudFormation to deploy its infrastructure. The company is concerned that if a production CloudFormation stack is deleted, important data stored in Amazon RD5 databases or Amazon EBS volumes might also be deleted.
now can the company prevent users from accidentally deleting data m this way?
(A). Modify the CloudFormation templates to add a DeletionPolicy attribute to RDS and EBS resources.
(B). Configure a stack policy that disallows the deletion of RDS and EBS resources.
(C). Modify IAM policies to deny deleting RDS and EBS resources that ate lagged with an "aws:cloudformation:stack-name'' tag.
(D). Use AWS Config rules to prevent deleting RDS and EBS resources.
Answer: A

NO.150 A company runs its application in the eu-west-1 Region and has one account for each of its environments development, testing, and production All the environments are running 24 hours a day 7 days a week by using stateful Amazon EC2 instances and Amazon RDS for MySQL databases The databases are between 500 GB and 800 GB in size The development team and testing team work on business days during business hours, but the production environment operates 24 hours a day. 7 days a week. The company wants to reduce costs AH resources are tagged with an environment tag with either development, testing, or production as the key.
What should a solutions architect do to reduce costs with the LEAST operational effort?



(A). Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs once every day Configure the rule to invoke one AWS Lambda function that starts or stops instances based on the tag day and time.
(B). Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs every business day in the evening. Configure the rule to invoke an AWS Lambda function that stops instances based on the tag-Create a second EventBridge (CloudWatch Events) rule that runs every business day in the morning Configure the second rule to invoke another Lambda function that starts instances based on the tag
(C). Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs every business day in the evening Configure the rule to invoke an AWS Lambda function that terminates instances based on the tag Create a second EventBridge (CloudWatch Events) rule that runs every business day in the morning Configure the second rule to invoke another Lambda function that restores the instances from their last backup based on the tag.
(D). Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs every hour Configure the rule to invoke one AWS Lambda function that terminates or restores instances from their ....based on the tag. day, and time

Answer: C

NO.151 A company has a policy that all Amazon EC2 instances that are running a database must exist within the same subnets in a shared VPC Administrators must follow security compliance requirements and are not allowed to directly log in to the shared account All company accounts are members of the same organization in AWS Organizations. The number of accounts will rapidly increase as the company grows.

A solutions architect uses AWS Resource Access Manager to create a resource share in the shared account What is the MOST operationally efficient configuration to meet these requirements?

(A). Add the VPC to the resource share. Add the account IDs as principals

(B). Add all subnets within the VPC to the resource share. Add the account IDs as principals

(C). Add all subnets within the VPC to the resource share. Add the organization as a principal.

(D). Add the VPC to the resource share. Add the organization as a principal

Answer: C

https://docs.aws.amazon.com/ram/latest/userguide/getting-started-sharing.html#getting-started-sharing-create To restrict resource sharing to only principals in your organization, choose Allow sharing with principals in your organization only.

https://docs.aws.amazon.com/ram/latest/userguide/ram-ug.pdf

NO.152 A financial services company in North America plans to release a new online web application to its customers on AWS . The company will launch the application in the us-east-1 Region on Amazon EC2 instances. The application must be highly available and must dynamically scale to meet user traffic. The company also wants to implement a disaster recovery environment for the application in the us-west-1 Region by using active-passive failover.

Which solution will meet these requirements?

(A). Create a VPC in us-east-1 and a VPC in us-west-1 Configure VPC peering In the us-east-1 VPC. create an Application Load Balancer (ALB) that extends across multiple Availability Zones in both VPCs Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in both VPCs Place the Auto Scaling group behind the ALB.

(B). Create a VPC in us-east-1 and a VPC in us-west-1. In the us-east-1 VPC. create an Application Load Balancer (ALB) that extends across multiple Availability Zones in that VPC. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in the us-east-1 VPC Place the Auto Scaling group behind the ALB Set up the same configuration in the us-west-1 VPC. Create an Amazon Route 53 hosted zone Create separate records for each ALB Enable health checks to ensure high availability between Regions.

(C). Create a VPC in us-east-1 and a VPC in us-west-1 In the us-east-1 VPC. create an Application Load Balancer (ALB) that extends across multiple Availability Zones in that VPC Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in the us-east-1 VPC Place the Auto Scaling group behind the ALB Set up the same configuration in the us-west-1 VPC Create an Amazon Route 53 hosted zone. Create separate records for each ALB Enable health checks and configure a failover routing policy for each record.

(D). Create a VPC in us-east-1 and a VPC in us-west-1 Configure VPC peering In the us-east-1 VPC. create an Application Load Balancer (ALB) that extends across multiple Availability Zones in Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in both VPCs Place the Auto Scaling group behind the ALB Create an Amazon Route 53 host.. Create a record for the ALB.

Answer: C

NO.153 A new application is running on Amazon Elastic Container Service (Amazon ECS) with AWS

Fargate The application uses an Amazon Aurora MySQL database The application and the database run m the same subnets of a VPC with distinct security groups that are configured.
The password (or the database is stored m AWS Secrets Manager and is passed to the application through the D8_PASSWORD environment variable The hostname of the database is passed to the application through the DB_HOST environment variable The application Is failing to access the database.
Which combination of actions should a solutions architect take to resolve this error? (Select THREE)
(A). Ensure that the container has the environment variable with name "DB_PASSWORD" specified with a "ValueFrom" and the ARN of the secret
(B). Ensure that the container has the environment variable with name *D8_PASSWORD" specified with a "ValueFrom" and the secret name of the secret.
(C). Ensure that the Fargate service security group allows inbound network traffic from the Aurora MySQL database on the MySQL TCP port 3306.
(D). Ensure that the Aurora MySQL database security group allows inbound network traffic from the Fargate service on the MySQL TCP port 3306.
(E). Ensure that the container has the environment variable with name "D8_HOST" specified with the hostname of a DB instance endpoint.
(F). Ensure that the container has the environment variable with name "DB_HOST" specified with the hostname of the OB duster endpoint.
Answer: A,D,E

NO.154 A company wants to migrate its corporate data center from on premises to the AWS Cloud. The data center includes physical servers and VMs that use VMware and Hyper-V. An administrator needs to select the correct services to collect data (or the initial migration discovery process. The data format should be supported by AWS Migration Hub. The company also needs the ability to generate reports from the data.
Which solution meets these requirements?
(A). Use the AWS Agentless Discovery Connector for data collection on physical servers and all VMs. Store the collected data in Amazon S3. Query the data with S3 Select. Generate reports by using Kibana hosted on Amazon EC2.
(B). Use the AWS Application Discovery Service agent for data collection on physical servers and all VMs. Store the collected data in Amazon Elastic File System (Amazon EFS). Query the data and generate reports with Amazon Athena.
(C). Use the AWS Application Discovery Service agent for data collection on physical servers and Hyper-V. Use the AWS Agentless Discovery Connector for data collection on VMware. Store the collected data in Amazon S3. Query the data with Amazon Athena. Generate reports by using Amazon QuickSight.
(D). Use the AWS Systems Manager agent for data collection on physical servers. Use the AWS Agentless Discovery Connector for data collection on all VMs. Store, query, and generate reports from the collected data by using Amazon Redshift.
Answer: C
https://docs.aws.amazon.com/application-discovery/latest/userguide/discovery-agent.html
https://docs.aws.amazon.com/application-discovery/latest/userguide/discovery-connector.html

NO.155 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 interne: gateway Host the Lambda functions m 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. Update the Neptune security group to allow access from the IP ranges of the Lambda functions.
(D). Host the Lambda functions outside the VPC. Create a VPC endpoint for the Neptune database, and have the Lambda functions access Neptune over the VPC endpoint
(E). Create three private subnets in the Neptune VPC. Host the Lambda functions m the three new isolated subnets. Create a VPC endpoint for DynamoDB. and route DynamoDB traffic to the VPC endpoint
Answer: A,C

NO.156 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 Zones. 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
(B). 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 broker. Enable NLB health checks Route the sensors to send the data to the NLB.
(C). 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
(D). 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 AWSIoT Core.
Answer: A

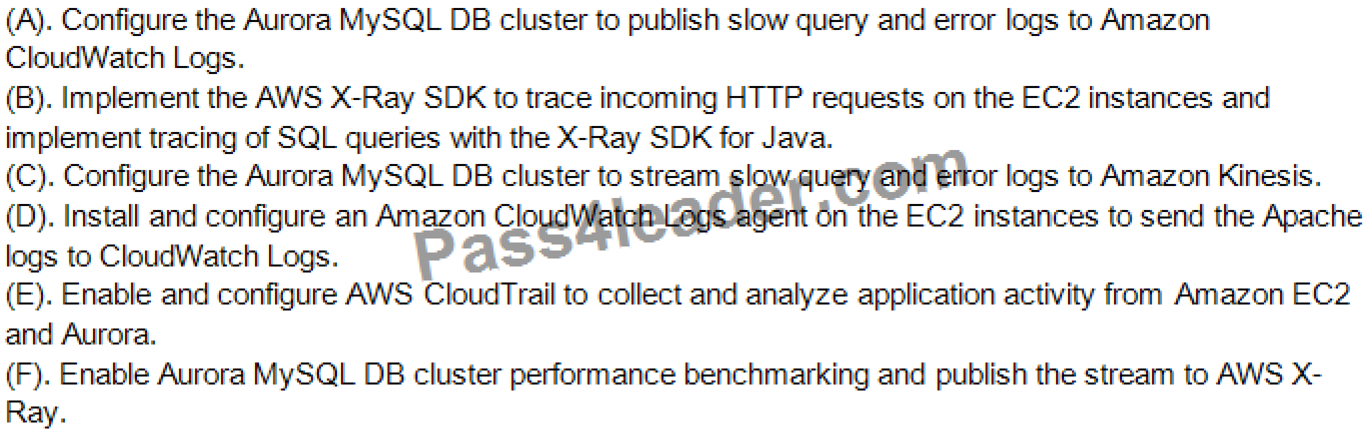
NO.157 A company is running an application in the AWS Cloud. The application runs on containers in an Amazon Elastic Container Service (Amazon ECS) cluster. The ECS tasks use the Fargate launch type. The application's data is relational and is stored in Amazon Aurora MySQL. To meet regulatory requirements, the application must be able to recover to a separate AWS Region in the event of an application failure. In case of a failure, no data can be lost. Which solution will meet these requirements with the LEAST amount of operational overhead?
(A). Provision an Aurora Replica in a different Region.
(B). Set up AWS DataSync for continuous replication of the data to a different Region.
(C). Set up AWS Database Migration Service (AWS DMS) to perform a continuous replication of the

data to a different Region.
(D). Use Amazon Data Lifecycle Manager {Amazon DLM) to schedule a snapshot every 5 minutes.
Answer: B

NO.158 A company's solution architect is designing a diasaster recovery (DR) solution for an application that runs on AWS. The application uses PostgreSQL 11.7 as its database. The company has an PRO of 30 seconds. The solutions architect must design a DR solution with the primary database in the us-east-1 Region and the database in the us-west-2 Region.
What should the solution architect do to meet these requirements with minimum application change?
(A). Migrate the database to Amazon RDS for PostgreSQL in us-east-1. Set up a read replica up a read replica in us-west-2. Set the managed PRO for the RDS database to 30 seconds.
(B). Migrate the database to Amazon for PostgreSQL in us-east-1. Set up a standby replica in an Availability Zone in us-west-2, Set the managed PRO for the RDS database to 30 seconds.
(C). Migrate the database to an Amazon Aurora PostgreSQL global database with the primary Region as us-east-1 and the secondary Region as us-west-2. Set the managed PRO for the Aurora database to 30 seconds.
(D). Migrate the database to Amazon DynamoDB in us-east-1. Set up global tables with replica tables that are created in us-west-2.
Answer: A

NO.159 A company uses AWS Transit Gateway for a hub-and-spoke model to manage network traffic between many VPCs. The company is developing a new service that must be able to send data at 100 Gbps. The company needs a faster connection to other VPCs in the same AWS Region.
Which solution will meet these requirements?
(A). Establish VPC peering between the necessary VPCs. Ensure that all route tables are updated as required.
(B). Attach an additional transit gateway to the VPCs. Update the route tables accordingly.
(C). Create AWS Site-to-Site VPN connections that use equal-cost multi-path (ECMP) routing between the necessary VPCs.
(D). Create an additional attachment from the necessary VPCs to the existing transit gateway.
Answer: D

NO.160 A company built an ecommerce website on AWS using a three-tier web architecture. The application is Java-based and composed of an Amazon CloudFront distribution, an Apache web server layer of Amazon EC2 instances in an Auto Scaling group, and a backend Amazon Aurora MySQL database.
Last month, during a promotional sales event, users reported errors and timeouts while adding items to their shopping carts. The operations team recovered the logs created by the web servers and reviewed Aurora DB cluster performance metrics. Some of the web servers were terminated before logs could be collected and the Aurora metrics were not sufficient for query performance analysis.
Which combination of steps must the solutions architect take to improve application performance visibility during peak traffic events? (Select THREE.)



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

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

NO.161 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 dat a. 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 field. 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.
(B). Configure an S3 Lifecycle object expiration rule that is based on the contract's expiration date
(C). Write a script to perform a conditional delete on all the affected DynamoDB records
(D). Temporarily suspend versioning on the S3 bucket. Create and invoke an AWS Lambda function that deletes affected objects Reactivate versioning when the operation is complete
(E). Write a script to delete objects from Amazon S3 Specify in each request a NoncurrentVersionExpiration property with a NoncurrentDays attribute set to 0.
Answer: C,E

NO.162 A company recently deployed a new application that runs on a group of Amazon EC2 Linux instances in a VPC In a peered VPC the company launched an EC2 Linux instance that serves as a bastion host The security group of the application instances allows access only on TCP port 22 from the private IP of the bastion host The security group of the bastion host allows access to TCP port 22

from 0 0 0.0/0 so that system administrators can use SSH to remotely log in to the application instances from several branch offices While looking through operating system logs on the bastion host, a cloud engineer notices thousands of failed SSH logins to the bastion host from locations around the world The cloud engineer wants to change how remote access is granted to the application instances and wants to meet the following requirements:
* Eliminate brute-force SSH login attempts
* Retain a log of commands run during an SSH session
* Retain the ability to forward ports
Which solution meets these requirements for remote access to the application instances?
(A). Configure the application instances to communicate with AWS Systems Manager Grant access to the system administrators to use Session Manager to establish a session with the application instances Terminate the bastion host
(B). Update the security group of the bastion host to allow traffic from only the public IP addresses of the branch offices
(C). Configure an AWS Client VPN endpoint and provision each system administrator with a certificate to establish a VPN connection to the application VPC Update the security group of the application instances to allow traffic from only the Client VPN IPv4 CIDR. Terminate the bastion host.
(D). Configure the application instances to communicate with AWS Systems Manager. Grant access to the system administrators to issue commands to the application instances by using Systems Manager Run Command. Terminate the bastion host.
Answer: A
"Session Manager removes the need to open inbound ports, manage SSH keys, or use bastion hosts"
Ref: https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html

NO.163 A company is running an application on several Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer. The load on the application varies throughout the day, and EC2 instances are scaled in and out on a regular basis. Log files from the EC2 instances are copied to a central Amazon S3 bucket every 15 minutes. The security team discovers that log files are missing from some of the terminated EC2 instances.
Which set of actions will ensure that log files are copied to the central S3 bucket from the terminated EC2 instances?
(A). Create a script to copy log files to Amazon S3, and store the script in a file on the EC2 instance. Create an Auto Scaling lifecycle hook and an Amazon EventBridge (Amazon CloudWatch Events) rule to detect lifecycle events from the Auto Scaling group. Invoke an AWS Lambda function on the autoscaling:EC2_INSTANCE_TERMINATING transition to send ABANDON to the Auto Scaling group to prevent termination, run the script to copy the log files, and terminate the instance using the AWS SDK.
(B). Create an AWS Systems Manager document with a script to copy log files to Amazon S3. Create an Auto Scaling lifecycle hook and an Amazon EventBridge (Amazon CloudWatch Events) rule to detect lifecycle events from the Auto Scaling group. Invoke an AWS Lambda function on the autoscaling:EC2_INSTANCE_TERMINATING transition to call the AWS Systems Manager API SendCommand operation to run the document to copy the log files and send CONTINUE to the Auto Scaling group to terminate the instance.
(C). Change the log delivery rate to every 5 minutes. Create a script to copy log files to Amazon S3, and add the script to EC2 instance user data. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to detect EC2 instance termination. Invoke an AWS Lambda function from the

EventBridge (CloudWatch Events) rule that uses the AWS CLI to run the user-data script to copy the log files and terminate the instance.
(D). Create an AWS Systems Manager document with a script to copy log files to Amazon S3. Create an Auto Scaling lifecycle hook that publishes a message to an Amazon Simple Notification Service (Amazon SNS) topic. From the SNS notification, call the AWS Systems Manager API SendCommand operation to run the document to copy the log files and send ABANDON to the Auto Scaling group to terminate the instance.
Answer: B
https://docs.aws.amazon.com/autoscaling/ec2/userguide/adding-lifecycle-hooks.html
- Refer to Default Result section - If the instance is terminating, both abandon and continue allow th e instance to terminate. However, abandon stops any remaining actions, such as other lifecycle hooks, and continue allows any other lifecycle hooks to complete.
https://aws.amazon.com/blogs/infrastructure-and-automation/run-code-before-terminating-an-ec2-auto-scaling-instance/
https://github.com/aws-samples/aws-lambda-lifecycle-hooks-function
https://github.com/aws-samples/aws-lambda-lifecycle-hooks-function/blob/master/cloudformation/template.yaml

NO.164 A company has an organization in AWS Organizations. The organization consists of a large number of AWS accounts that belong to separate business units. The company requires all Amazon EC2 instances to be provisioned with custom, hardened AMIs. The company wants a solution that provides each AWS account access to the AMIs Which solution will meet these requirements with the MOST operational efficiency?
(A). Create the AMIs with EC2 Image Builder Create an AWS CodePipeline pipeline to share the AMIs across all AWS accounts.
(B). Deploy Jenkins on an EC2 instance Create jobs to create and share the AMIs across all AWS accounts.
(C). Create and share the AMIs with EC2 Image Builder Use AWS Service Catalog to configure a product that provides access to the AMIs across all AWS accounts.
(D). Create the AMIs with EC2 Image Builder Create an AWS Lambda function to share the AMIs across all AWS accounts.
Answer: C

NO.165 A solutions architect is designing the data storage and retrieval architecture for a new application that a company will be launching soon. The application is designed to ingest millions of small records per minute from devices all around the world. Each record is less than 4 KB in size and needs to be stored in a durable location where it can be retrieved with low latency. The data is ephemeral and the company is required to store the data for 120 days only, after which the data can be deleted.
The solutions architect calculates that, during the course of a year, the storage requirements would be about 10-15 TB.
Which storage strategy is the MOST cost-effective and meets the design requirements?
(A). Design the application to store each incoming record as a single .csv file in an Amazon S3 bucket to allow for indexed retrieval. Configure a lifecycle policy to delete data older than 120 days.
(B). Design the application to store each incoming record in an Amazon DynamoDB table properly configured for the scale. Configure the DynamoOB Time to Live (TTL) feature to delete records older

than 120 days.
(C). Design the application to store each incoming record in a single table in an Amazon RDS MySQL database. Run a nightly cron job that executes a query to delete any records older than 120 days.
(D). Design the application to batch incoming records before writing them to an Amazon S3 bucket. Update the metadata for the object to contain the list of records in the batch and use the Amazon S3 metadata search feature to retrieve the data. Configure a lifecycle policy to delete the data after 120 days.
Answer: B
DynamoDB with TTL, cheaper for sustained throughput of small items + suited for fast retrievals. S3 cheaper for storage only, much higher costs with writes. RDS not designed for this use case.

NO.166 A company is migrating an application to the AWS Cloud. The application runs in an on-premises data center and writes thousands of images into a mounted NFS file system each night After the company migrates the application, the company will host the application on an Amazon EC2 instance with a mounted Amazon Elastic File System (Amazon EFS) file system.
The company has established an AWS Direct Connect connection to AWS Before the migration cutover. a solutions architect must build a process that will replicate the newly created on-premises images to the EFS file system What is the MOST operationally efficient way to replicate the images?
(A). Configure a periodic process to run the aws s3 sync command from the on-premises file system to Amazon S3 Configure an AWS Lambda function to process event notifications from Amazon S3 and copy the images from Amazon S3 to the EFS file system
(B). Deploy an AWS Storage Gateway file gateway with an NFS mount point. Mount the file gateway file system on the on-premises server. Configure a process to periodically copy the images to the mount point
(C). Deploy an AWS DataSync agent to an on-premises server that has access to the NFS file system Send data over the Direct Connect connection to an S3 bucket by using a public VIF Configure an AWS Lambda function to process event notifications from Amazon S3 and copy the images from Amazon S3 to the EFS file system
(D). Deploy an AWS DataSync agent to an on-premises server that has access to the NFS file system Send data over the Direct Connect connection to an AWS PrivateLink interface VPC endpoint for Amazon EFS by using a private VIF Configure a DataSync scheduled task to send the images to the EFS file system every 24 hours.
Answer: A

NO.167 A company has introduced a new policy that allows employees to work remotely from their homes if they connect by using a VPN The company Is hosting Internal applications with VPCs in multiple AWS accounts Currently the applications are accessible from the company's on-premises office network through an AWS Site-to-Site VPN connection The VPC in the company's main AWS account has peering connections established with VPCs in other AWS accounts.
A solutions architect must design a scalable AWS Client VPN solution for employees to use while they work from home What is the MOST cost-effective solution that meets these requirements?
(A). Create a Client VPN endpoint in each AWS account Configure required routing that allows access to internal applications
(B). Create a Client VPN endpoint in the mam AWS account Configure required routing that allows access to internal applications
(C). Create a Client VPN endpoint in the main AWS account Provision a transit gateway that is

connected to each AWS account Configure required routing that allows access to internal applications
(D). Create a Client VPN endpoint in the mam AWS account Establish connectivity between the Client VPN endpoint and the AWS Site-to-Site VPN
Answer: C

NO.168 A company is moving a business-critical multi-tier application to AWS. The architecture consists of a desktop client application and server infrastructure. The server infrastructure resides in an on-premises data center that frequently fails to maintain the application uptime SLA of 99.95%. A solutions architect must re-architect the application to ensure that it can meet or exceed the SLA.
The application contains a PostgreSQL database running on a single virtual machine. The business logic and presentation layers are load balanced between multiple virtual machines. Remote users complain about slow load times while using this latency-sensitive application.
Which of the following will meet the availability requirements with little change to the application while improving user experience and minimizing costs?
(A). Migrate the database to a PostgreSQL database in Amazon EC2. Host the application and presentation layers in automatically scaled Amazon ECS containers behind an Application Load Balancer. Allocate an Amazon Workspaces Workspace for each end user to improve the user experience.
(B). Migrate the database to an Amazon RDS Aurora PostgreSQL configuration. Host the application and presentation layers in an Auto Scaling configuration on Amazon EC2 instances behind an Application Load Balancer. Use Amazon AppStream 2.0 to improve the user experience.
(C). Migrate the database to an Amazon RDS PostgreSQL Mulli-AZ configuration. Host the application and presentation layers in automatically scaled AWS Fargate containers behind a Network Load Balancer. Use Amazon ElastiCache to improve the user experience.
(D). Migrate the database to an Amazon Redshift cluster with at least two nodes. Combine and host the application and presentation layers in automatically scaled Amazon ECS containers behind an Application Load Balancer. Use Amazon CloudFront to improve the user experience.
Answer: B
Aurora would improve availability that can replicate to multiple AZ (6 copies). Auto scaling would improve the performance together with a ALB. AppStream is like Citrix that deliver hosted Apps to users.

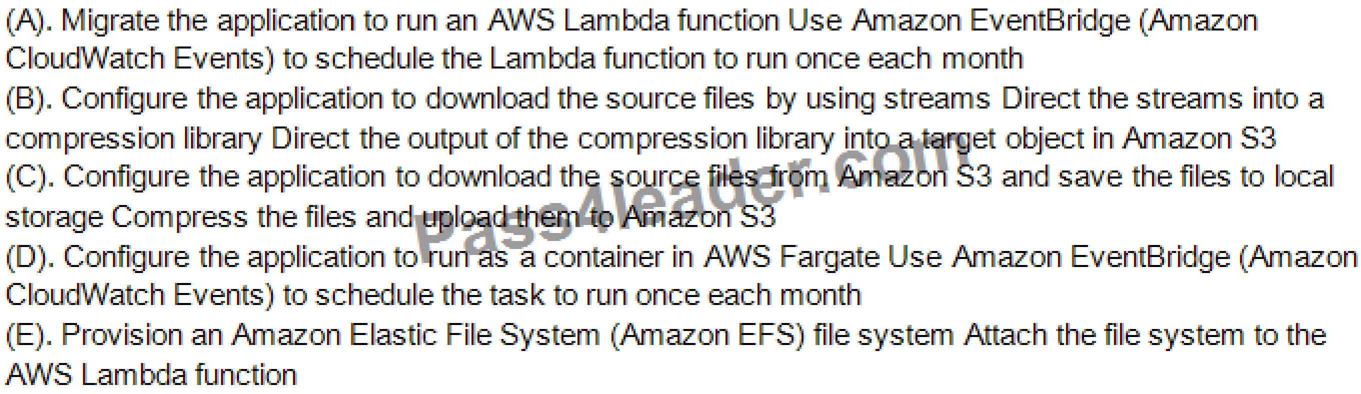
NO.169 A company runs a proprietary stateless ETL application on an Amazon EC2 Linux instance. The application is a Linux binary, and the source code cannot be modified. The application is single-threaded, uses 2 GB of RAM. and is highly CPU intensive The application is scheduled to run every 4 hours and runs for up to 20 minutes A solutions architect wants to revise the architecture for the solution.
Which strategy should the solutions architect use?
(A). Use AWS Lambda to run the application. Use Amazon CloudWatch Logs to invoke the Lambda function every 4 hours
(B). Use AWS Batch to run the application Use an AWS Step Functions state machine to invoke the AWS Batch job every 4 hours
(C). Use AWS Fargate to run the application Use Amazon EventBridge (Amazon CloudWatch Events) to invoke the Fargate task every 4 hours
(D). Use Amazon 6C2 Spot Instances to run the application Use AWS CodeDeptoy to deploy and run

the application every 4 hours.

Answer: C

NO.170 A company has an application Once a month, the application creates a compressed file that contains every object within an Amazon S3 bucket The total size of the objects before compression is 1 TB.

The application runs by using a scheduled cron job on an Amazon EC2 instance that has a 5 TB Amazon Elastic Block Store (Amazon EBS) volume attached The application downloads all the files from the source S3 bucket to the EBS volume, compresses the file, and uploads the file to a target S3 bucket Every invocation of the application takes 2 hours from start to finish Which combination of actions should a solutions architect take to OPTIMIZE costs for this application? (Select TWO.)



(A). Migrate the application to run an AWS Lambda function Use Amazon EventBridge (Amazon CloudWatch Events) to schedule the Lambda function to run once each month

(B). Configure the application to download the source files by using streams Direct the streams into a compression library Direct the output of the compression library into a target object in Amazon S3

(C). Configure the application to download the source files from Amazon S3 and save the files to local storage Compress the files and upload them to Amazon S3

(D). Configure the application to run as a container in AWS Fargate Use Amazon EventBridge (Amazon CloudWatch Events) to schedule the task to run once each month

(E). Provision an Amazon Elastic File System (Amazon EFS) file system Attach the file system to the AWS Lambda function

Answer: C,D

NO.171 An enterprise runs 103 line-of-business applications on virtual machines in an on-premises data center. Many of the applications are simple PHP. Java, or Ruby web applications, are no longer actively developed, and serve little traffic.

Which approach should be used to migrate these applications to AWS with the LOWEST infrastructure costs?

(A). Deploy the applications lo single-instance AWS Elastic Beanstalk environments without a load balancer.

(B). Use AWS SMS to create AMIs for each virtual machine and run them in Amazon EC2.

(C). Convert each application to a Docker image and deploy to a small Amazon ECS cluster behind an Application Load Balancer.

(D). Use VM Import/Export to create AMIs for each virtual machine and run them in single-instance AWS Elastic Beanstalk environments by configuring a custom image.

Answer: C

NO.172 A company is using an Amazon CloudFront distribution to distribute both static and dynamic content from a web application running behind an Application Load Balancer The web application requires user authorization and session tracking tor dynamic content The CloudFront distribution has a single cache behavior configured to forward the Authorization, Host, and Agent HTTP allow list headers and a session cookie to the origin All other cache behavior settings are set to their default value A valid ACM certificate is applied to the CloudFront distribution with a matching CNAME in the distribution settings The ACM certificate is also applied to the HTTPS listener for the Application Load Balancer The CloudFront origin protocol policy is set to HTTPS only Analysis of the cache statistics report shows that the miss rate for this distribution is very high What can the solutions architect do

to improve the cache hit rate for this distribution without causing the SSL/TLS handshake between CloudFront and the Application Load Balancer to fail?
(A). Create two cache behaviors for static and dynamic content Remove the user-Agent and Host HTTP headers from the allow list headers section on both of the cache behaviors Remove the session cookie from the allow list cookies section and the Authorization HTTP header from the allow list headers section for cache behavior configured for static content
(B). Remove the user-Agent and Authorization HTTP headers from the allow list headers section of the cache behaviour. Then update the cache behaviour to use resigned cookies for authorization
(C). Remove the Host HTTP header from the allow list headers section and remove the session cookie from the allow list cookies section for the default cache behaviour Enable automatic object compression and use Lambda@Edge viewer request events for user authorization
(D). Create two cache behaviours for static and dynamic content Remove the User-Agent HTTP header from the allow list headers section on both of the cache behaviours
Answer: D
Remove the session cookie from the allow list cookies section and the Authorization HTTP header from the allow list headers section for cache behaviour configured for static content Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/understanding-the-cache-key.html Removing the host header will result in failed flow between CloudFront and ALB, because they have same certificate.

NO.173 A software company is using three AWS accounts for each of its 1 0 development teams The company has developed an AWS CloudFormation standard VPC template that includes three NAT gateways The template is added to each account for each team The company is concerned that network costs will increase each time a new development team is added A solutions architect must maintain the reliability of the company's solutions and minimize operational complexity What should the solutions architect do to reduce the network costs while meeting these requirements?
(A). Create a single VPC with three NAT gateways in a shared services account Configure each account VPC with a default route through a transit gateway to the NAT gateway in the shared services account VPC Remove all NAT gateways from the standard VPC template
(B). Create a single VPC with three NAT gateways in a shared services account Configure each account VPC with a default route through a VPC peering connection to the NAT gateway in the shared services account VPC Remove all NAT gateways from the standard VPC template
(C). Remove two NAT gateways from the standard VPC template Rely on the NAT gateway SLA to cover reliability for the remaining NAT gateway.
(D). Create a single VPC with three NAT gateways in a shared services account Configure a Site-to-Site VPN connection from each account to the shared services account Remove all NAT gateways from the standard VPC template
Answer: A

NO.174 A team collects and routes behavioral data for an entire company The company runs a Multi-AZ VPC environment with public subnets, private subnets, and in internet gateway Each public subnet also contains a NAT gateway Most of the company's applications read from and write to Amazon Kinesis Data Streams. Most of the workloads am in private subnets.
A solutions architect must review the infrastructure The solutions architect needs to reduce costs and maintain the function of the applications The solutions architect uses Cost Explorer and notices that the cost in the EC2-Other category is consistently high A further review shows that NatGateway-Bytes

charges are increasing the cost in the EC2-Other category.
What should the solutions architect do to meet these requirements?
(A). Enable VPC Flow Logs. Use Amazon Athena to analyze the logs for traffic that can be removed. Ensure that security groups are Mocking traffic that is responsible for high costs.
(B). Add an interface VPC endpoint for Kinesis Data Streams to the VPC. Ensure that applications have the correct IAM permissions to use the interface VPC endpoint.
(C). Enable VPC Flow Logs and Amazon Detective Review Detective findings for traffic that is not related to Kinesis Data Streams Configure security groups to block that traffic
(D). Add an interface VPC endpoint for Kinesis Data Streams to the VPC. Ensure that the VPC endpoint policy allows traffic from the applications.
Answer: D
https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-access.html
https://aws.amazon.com/premiumsupport/knowledge-center/vpc-reduce-nat-gateway-transfer-costs/ VPC endpoint policies enable you to control access by either attaching a policy to a VPC endpoint or by using additional fields in a policy that is attached to an IAM user, group, or role to restrict access to only occur via the specified VPC endpoint

NO.175 A company is refactoring its on-premises order-processing platform in the AWS Cloud. The platform includes a web front end that is hosted on a fleet of VMs RabbitMQ to connect the front end to the backend, and a Kubernetes cluster to run a containerized backend system to process the orders. The company does not want to make any major changes to the application Which solution will meet these requirements with the LEAST operational overhead?
(A). Create an AMI of the web server VM Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer Set up Amazon MQ to replace the on-premises messaging queue Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend
(B). Create a custom AWS Lambda runtime to mimic the web server environment Create an Amazon API Gateway API to replace the front-end web servers Set up Amazon MQ to replace the on-premises messaging queue Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend
(C). Create an AMI of the web server VM Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer Set up Amazon MQ to replace the on-premises messaging queue Install Kubernetes on a fleet of different EC2 instances to host the order-processing backend
(D). Create an AMI of the web server VM Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer Set up an Amazon Simple Queue Service (Amazon SQS) queue to replace the on-premises messaging queue Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend
Answer: A

NO.176 A company needs to implement a patching process for its servers. The on-premises servers and Amazon EC2 instances use a variety of tools to perform patching. Management requires a single report showing the patch status of all the servers and instances.
Which set of actions should a solutions architect take to meet these requirements?
(A). Use AWS Systems Manager to manage patches on the on-premises servers and EC2 instances. Use Systems Manager to generate patch compliance reports.
(B). Use AWS OpsWorks to manage patches on the on-premises servers and EC2 instances. Use Amazon OuickSight integration with OpsWorks to generate patch compliance reports.

(C). Use an Amazon EventBridge (Amazon CloudWatch Events) rule to apply patches by scheduling an AWS Systems Manager patch remediation job. Use Amazon Inspector to generate patch compliance reports.
(D). Use AWS OpsWorks to manage patches on the on-premises servers and EC2 instances. Use AWS X-Ray to post the patch status to AWS Systems Manager OpsCenter to generate patch compliance reports.
Answer: A
https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html

NO.177 A company runs an IoT platform on AWS IoT sensors in various locations send data to the company's Node js API servers on Amazon EC2 instances running behind an Application Load Balancer The data is stored in an Amazon RDS MySQL DB instance that uses a 4 TB General Purpose SSD volume The number of sensors the company has deployed in the field has increased over time and is expected to grow significantly The API servers are consistently overloaded and RDS metrics show high write latency Which of the following steps together will resolve the issues permanently and enable growth as new sensors are provisioned, while keeping this platform cost-efficient? {Select TWO.)
(A). Resize the MySQL General Purpose SSD storage to 6 TB to improve the volume's IOPS
(B). Re-architect the database tier to use Amazon Aurora instead of an RDS MySQL DB instance and add read replicas
(C). Leverage Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data
(D). Use AWS X-Ray to analyze and debug application issues and add more API servers to match the load
(E). Re-architect the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance
Answer: C,E

NO.178 A video streaming company recently launched a mobile app for video sharing. The app uploads various files to an Amazon S3 bucket in the us-east-1 Region. The files range in size from 1 GB to 1 0 GB Users who access the app from Australia have experienced uploads that take long periods of time Sometimes the files fail to completely upload for these users . A solutions architect must improve the app' performance for these uploads Which solutions will meet these requirements? (Select TWO.)
(A). Enable S3 Transfer Acceleration on the S3 bucket Configure the app to use the Transfer Acceleration endpoint for uploads
(B). Configure an S3 bucket in each Region to receive the uploads. Use S3 Cross-Region Replication to copy the files to the distribution S3 bucket.
(C). Set up Amazon Route 53 with latency-based routing to route the uploads to the nearest S3 bucket Region.
(D). Configure the app to break the video files into chunks Use a multipart upload to transfer files to Amazon S3.
(E). Modify the app to add random prefixes to the files before uploading
Answer: A,C

NO.179 A company is deploying a distributed in-memory database on a fleet of Amazon EC2 instances. The fleet consists of a primary node and eight worker nodes. The primary node is responsible for monitoring cluster health, accepting user requests, distributing user requests to worker nodes and sending an aggregate response back to a client. Worker nodes communicate with each other to replicate data partitions.

The company requires the lowest possible networking latency to achieve maximum performance.

Which solution will meet these requirements?

(A). Launch memory optimized EC2 instances in a partition placement group

(B). Launch compute optimized EC2 instances in a partition placement group

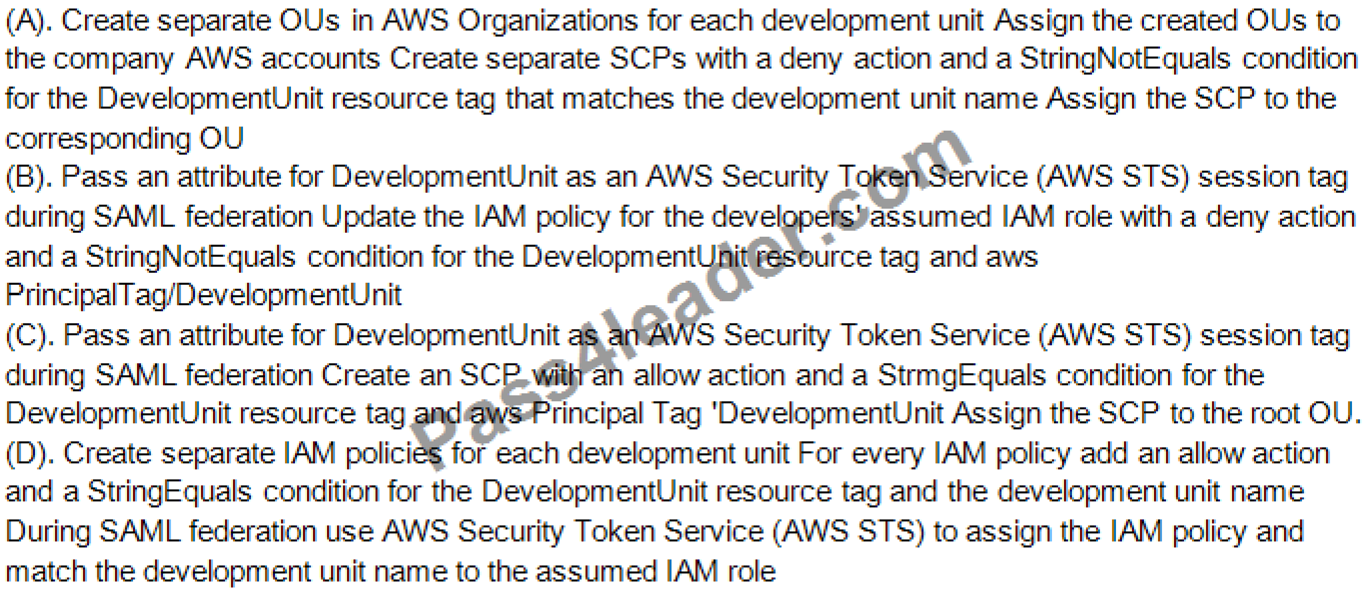
(C). Launch memory optimized EC2 instances in a cluster placement group

(D). Launch compute optimized EC2 instances in a spread placement group.

Answer: A

NO.180 A company is running multiple workloads in the AWS Cloud The company has separate units for software development The company uses AWS Organizations and federation with SAML to give permissions to developers to manage resources in their AWS accounts The development units each deploy their production workloads into a common production account Recently, an incident occurred in the production account in which members of a development unit terminated an EC2 instance that belonged to a different development unit. A solutions architect must create a solution that prevents a similar incident from happening in the future. The solution also must a low developers the possibilityy to manage the instances used for their workloads.

Which strategy will meet these requirements?



(A). Create separate OUs in AWS Organizations for each development unit Assign the created OUs to the company AWS accounts Create separate SCPs with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag that matches the development unit name Assign the SCP to the corresponding OU

(B). Pass an attribute for DevelopmentUnit as an AWS Security Token Service (AWS STS) session tag during SAML federation Update the IAM policy for the developers' assumed IAM role with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag and aws PrincipalTag/DevelopmentUnit

(C). Pass an attribute for DevelopmentUnit as an AWS Security Token Service (AWS STS) session tag during SAML federation Create an SCP with an allow action and a StrmgEquals condition for the DevelopmentUnit resource tag and aws Principal Tag 'DevelopmentUnit Assign the SCP to the root OU.

(D). Create separate IAM policies for each development unit For every IAM policy add an allow action and a StringEquals condition for the DevelopmentUnit resource tag and the development unit name During SAML federation use AWS Security Token Service (AWS STS) to assign the IAM policy and match the development unit name to the assumed IAM role

Answer: A

NO.181 A solutions architect is building a web application that uses an Amazon RDS for PostgreSQL DB instance The DB instance is expected to receive many more reads than writes. The solutions architect needs to ensure that the large amount of read traffic can be accommodated and that the DB instance is highly available.

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

(A). Create multiple read replicas and put them into an Auto Scaling group.

(B). Create multiple read replicas in different Availability Zones.

(C). Create an Amazon Route 53 hosted zone and a record set for each read replica with a TTL and a weighted routing policy.

(D). Create an Application Load Balancer (ALB) and put the read replicas behind the ALB.

(E). Configure an Amazon CloudWatch alarm to detect a failed read replica. Set the alarm to directly invoke an AWS Lambda function to delete its Route 53 record set.
(F). Configure an Amazon Route 53 health check for each read replica using its endpoint
Answer: B,C,F
https://aws.amazon.com/premiumsupport/knowledge-center/requests-rds-read-replicas/ You can use Amazon Route 53 weighted record sets to distribute requests across your read replicas. Within a Route 53 hosted zone, create individual record sets for each DNS endpoint associated with your read replicas and give them the same weight. Then, direct requests to the endpoint of the record set. You can incorporate Route 53 health checks to be sure that Route 53 directs traffic away from unavailable read replicas

NO.182 A data analytics company has an Amazon Redshift cluster that consists of several reserved nodes. The duster is experiencing unexpected bursts of usage because a team of employees is compiling a deep audit analysis report The queries to generate the report are complex read queries and are CPU intensive.
Business requirements dictate that the cluster must be able to service read and write queries at at) times A solutions architect must devise a solution that accommodates the bursts of usage Which solution meets these requirements MOST cost-effectively?
(A). Provision an Amazon EMR duster Offload the complex data processing tasks
(B). Deploy an AWS Lambda function to add capacity to the Amazon Redshift cluster by using a classic resize operation when the duster's CPU metrics in Amazon CloudWatch reach 80%.
(C). Deploy an AWS Lambda function to add capacity to the Amazon Redshift duster by using an elastic resize operation when the duster's CPU metrics in Amazon CloudWatch leach 80%.
(D). Turn on the Concurrency Scaling feature for the Amazon Redshift duster
Answer: D

NO.183 A company is running an application on Amazon EC2 instances in three environments; development, testing, and production. The company uses AMIs to deploy the EC2 instances. The company builds the AMIs by using custom deployment scripts and infrastructure orchestration tools for each release in each environment.
The company is receiving errors in its deployment process. Errors appear during operating system package downloads and during application code installation from a third-party Git hosting service. The company needs deployments to become more reliable across all environments.
Which combination of steps will meet these requirements? (Select THREE).
(A). Mirror the application code to an AWS CodeCommit Git repository. Use the repository to build EC2 AMIs.
(B). Produce multiple EC2 AMIs. one for each environment, for each release.
(C). Produce one EC2 AMI for each release for use across all environments.
(D). Mirror the application code to a third-party Git repository that uses Amazon S3 storage. Use the repository for deployment.
(E). Replace the custom scripts and tools with AWS CodeBuild. Update the infrastructure deployment process to use EC2 Image Builder.
Answer: A,C,E

NO.184 A company has developed an application that is running Windows Server on VMware vSphere VMs that the company hosts or premises. The application data is stored in a proprietary

format that must be read through the application. The company manually provisioned the servers and the application.
As pan of us disaster recovery plan, the company warns the ability to host its application on AWS temporarily me company's on-premises environment becomes unavailable The company wants the application to return to on-premises hosting after a disaster recovery event is complete The RPO 15 5 minutes.
Which solution meets these requirements with the LEAST amount of operational overhead?
(A). Configure AWS DataSync. Replicate the data lo Amazon Elastic Block Store (Amazon EBS) volumes When the on-premises environment is unavailable, use AWS CloudFormation templates to provision Amazon EC2 instances and attach the EBS volumes
(B). Configure CloudEndure Disaster Recovery Replicate the data to replication Amazon EC2 instances that are attached to Amazon Elastic Block Store (Amazon EBS) volumes When the on-premises environment is unavailable, use CloudEndure to launch EC2 instances that use the replicated volumes.
(C). Provision an AWS Storage Gateway We gateway. Recreate the data lo an Amazon S3 bucket. When the on-premises environment is unavailable, use AWS Backup to restore the data to Amazon Elastic Block Store (Amazon EBS) volumes and launch Amazon EC2 instances from these EBS volumes
(D). Provision an Amazon FS* for Windows File Server file system on AWS Replicate :ne data to the system When the on-premoes environment is unavailable, use AWS CloudFormation templates to provision Amazon EC2 instances and use AWS :CloudFofmation::lnit commands to mount the Amazon FSx file shares
Answer: D

NO.185 A company is configuring connectivity to a multi-account AWS environment to support application workloads fiat serve users in a single geographic region. The workloads depend on a highly available, on-premises legacy system deployed across two locations It is critical for the AWS workloads to manias connectivity to the legacy system, and a minimum of 5 Gbps of bandwidth is required All application workloads within AWS must have connectivity with one another.
Which solution will meet these requirements?
(A). Configure multiple AWS Direct Connect (OX) 10 Gbps dedicated connections from a DX partner for each on-premises location Create private virtual interfaces on each connection for each AWS account VPC Associate me private virtual interface with a virtual private gateway attached to each VPC
(B). Configure multiple AWS Direct Connect (DX) 10 Gbps dedicated connections from two DX partners for each on-premises location Create and attach a virtual private gateway for each AWS account VPC. Create a DX gateway m a central network account and associate it with the virtual private gateways Create a public virtual interface on each DX connection and associate the interface with me DX gateway.
(C). 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. Create a transit virtual interface for each DX interlace and associate them with the DX gateway. Create a gateway association between the DX gateway and the transit gateway
(D). 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. 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

NO.186 A company's CI SO 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 m-place deployments Monitor the newly deployed code and. if there are any issues, push another code update
Answer: B

NO.187 A company has its cloud infrastructure on AWS A solutions architect needs to define the infrastructure as code. The infrastructure is currently deployed in one AWS Region. The company's business expansion plan includes deployments in multiple Regions across multiple AWS accounts
What should the solutions architect do to meet these requirements?
(A). Use AWS CloudFormation templates Add IAM policies to control the various accounts Deploy the templates across the multiple Regions
(B). Use AWS Organizations Deploy AWS CloudFormation templates from the management account Use AWS Control Tower to manage deployments across accounts
(C). Use AWS Organizations and AWS CloudFormation StackSets Deploy a CloudFormation template from an account that has the necessary IAM permissions
(D). Use nested stacks with AWS CloudFormation templates Change the Region by using nested stacks
Answer: B

NO.188 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. Configure Amazon CloudWatch alarms to notify administrators when the site fails.

(C). 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. Configure Amazon CloudWatch alarms to notify administrators when the site fails.

(D). Configure an Amazon CloudWatch alarm for Amazon RDS with an action to recover a high-load, impaired RDS instance in the database tier.

(E). 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: B,E

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

NO.189 A company runs an application on AWS. An AWS Lambda function uses credentials to authenticate to an Amazon RDS tor MySQL DB instance. A security risk assessment identified that these credentials are not frequently rotated. Also, encryption at rest is not enabled for the DB instance. The security team requires that both of these issues be resolved.

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

(A). Configure the Lambda function to store and retrieve the database credentials in AWS Secrets Manager and enable rotation of the credentials. Take a snapshot ol the DB instance and encrypt a copy of that snapshot. Replace the DB instance with a new DB instance that is based on the encrypted snapshot.

(B). Enable IAM DB authentication on the DB instance. Grant the Lambda execution role access to the DB instance. Modify the DB instance and enable encryption.

(C). Enable IAM DB authentication on the DB instance. Grant the Lambda execution role access to the DB instance. Create an encrypted read replica of the DB instance. Promote Ihe encrypted read replica to be the new primary node.

(D). Configure the Lambda function to store and retrieve the database credentials as encrypted AWS Systems Manager Parameter Store parameters. Create another Lambda function to automatically rotate the credentials. Create an encrypted read replica of the DB instance. Promote the encrypted read replica to be the new primary node.

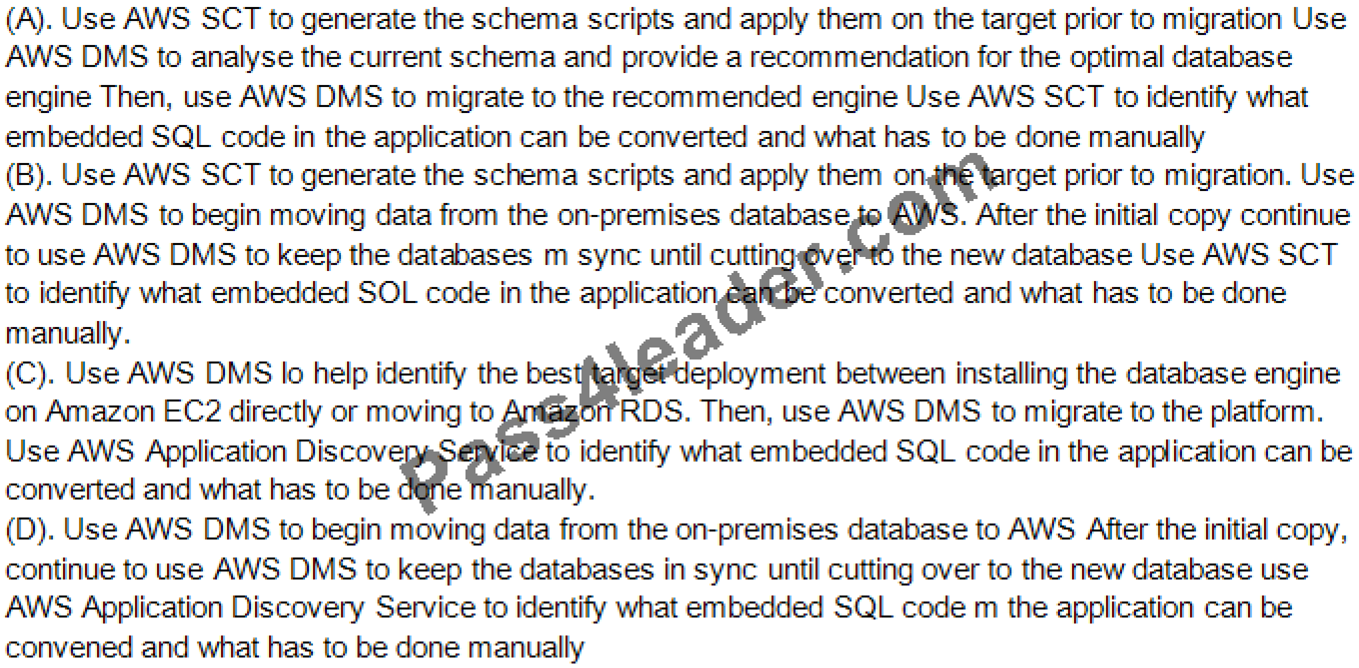
Answer: A

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-manager/#:~:text=Secrets%20Manager%20offers%20built%2Din%20integrations%20for%20rotating

%20credentials%20for,rotate%20other%20types%20of%20secrets.
Encrypting a unencrypted instance of DB or creating a encrypted replica of an un encrypted DB instance are not possible Hence A is the only solution possible.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html#Overview.Encryption.Limitations

NO.190 A company is planning to migrate an application from on premises to AWS. The application currently uses an Oracle database and the company can tolerate a brief downtime of 1 hour when performing the switch to the new infrastructure As part of the migration. the database engine will be changed to MySQL. A solutions architect needs to determine which AWS services can be used to perform the migration while minimizing the amount of work and time required.
Which of the following will meet the requirements?



(A). Use AWS SCT to generate the schema scripts and apply them on the target prior to migration Use AWS DMS to analyse the current schema and provide a recommendation for the optimal database engine Then, use AWS DMS to migrate to the recommended engine Use AWS SCT to identify what embedded SQL code in the application can be converted and what has to be done manually
(B). Use AWS SCT to generate the schema scripts and apply them on the target prior to migration. Use AWS DMS to begin moving data from the on-premises database to AWS. After the initial copy continue to use AWS DMS to keep the databases m sync until cutting over to the new database Use AWS SCT to identify what embedded SOL code in the application can be converted and what has to be done manually.
(C). Use AWS DMS lo help identify the best target deployment between installing the database engine on Amazon EC2 directly or moving to Amazon RDS. Then, use AWS DMS to migrate to the platform. Use AWS Application Discovery Service to identify what embedded SQL code in the application can be converted and what has to be done manually.
(D). Use AWS DMS to begin moving data from the on-premises database to AWS After the initial copy, continue to use AWS DMS to keep the databases in sync until cutting over to the new database use AWS Application Discovery Service to identify what embedded SQL code m the application can be convened and what has to be done manually

Answer: B

NO.191 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: B,D
https://prismatic.io/blog/why-we-moved-from-lambda-to-ecs/

NO.192 A company has a three-tier application running on AWS with a web server, an application server, and an Amazon RDS MySQL DB instance. A solutions architect is designing a disaster recovery (OR) solution with an RPO of 5 minutes.
Which solution will meet the company's requirements?
(A). Configure AWS Backup to perform cross-Region backups of all servers every 5 minutes. Reprovision the three tiers in the DR Region from the backups using AWS CloudFormation in the event of a disaster.
(B). Maintain another running copy of the web and application server stack in the DR Region using AWS CloudFormation drill detection. Configure cross-Region snapshots ol the DB instance to the DR Region every 5 minutes. In the event of a disaster, restore the DB instance using the snapshot in the DR Region.
(C). Use Amazon EC2 Image Builder to create and copy AMIs of the web and application server to both the primary and DR Regions. Create a cross-Region read replica of the DB instance in the DR Region. In the event of a disaster, promote the read replica to become the master and reprovision the servers with AWS CloudFormation using the AMIs.
(D). Create AMts of the web and application servers in the DR Region. Use scheduled AWS Glue jobs to synchronize the DB instance with another DB instance in the DR Region. 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
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.

NO.193 What should the solutions architect do to meet this requirement7
(A). / Use Amazon CloudWatch to monitor the Sample Count statistic for each service in the ECS cluster Se: an alarm for when the math expression sample Notification SERVICE_QUOTA(service)"100 is greater than 80 Notify the development team by using Amazon Simple Notification Service (Amazon SNS)
(B). Use Amazon CloudWatch to monitor service quotas that are published under the AWS-'Usage metric namespace Set an alarm for when the math expression metricSERVlCE QUOTA(metric)"100 is greater than 80 Notify the development team by using Amazon Simple Notification Service (Amazon SNS).
(C). Create an AWS Lambda function to poll detailed metrics from the ECS cluster. When the number running Fargate tasks is greater than 80. invoke Amazon Simple Email Service (Amazon SES) to notify the development team
(D). Create an AWS Config rule to evaluate whether the Fargate SERVICE_QUOTA is greater than 80. Use Amazon Simple Email Service (Amazon SES) to notify the development team when the AWS Config rule is not compliant.
Answer: B

NO.194 A company is planning to host a web application on AWS and works to load balance the

traffic across a group of Amazon EC2 instances. One of the security requirements is to enable end-to-end encryption in transit between the client and the web server.
Which solution will meet this requirement?
(A). Place the EC2 instances behind an Application Load Balancer (ALB) Provision an SSL certificate using AWS Certificate Manager (ACM), and associate the SSL certificate with the ALB. Export the SSL certificate and install it on each EC2 instance. Configure the ALB to listen on port 443 and to forward traffic to port 443 on the instances.
(B). Associate the EC2 instances with a target group. Provision an SSL certificate using AWS Certificate Manager (ACM). Create an Amazon CloudFront distribution and configure It to use the SSL certificate. Set CloudFront to use the target group as the origin server
(C). Place the EC2 instances behind an Application Load Balancer (ALB). Provision an SSL certificate using AWS Certificate Manager (ACM), and associate the SSL certificate with the ALB. Provision a third-party SSL certificate and install it on each EC2 instance. Configure the ALB to listen on port 443 and to forward traffic to port 443 on the instances.
(D). Place the EC2 instances behind a Network Load Balancer (NLB). Provision a third-party SSL certificate and install it on the NLB and on each EC2 instance. Configure the NLB to listen on port 443 and to forward traffic to port 443 on the instances.
Answer: C

NO.195 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 stat c 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. Replace the custom software with Amazon Recognition to categorize the videos.
(B). Store the uploaded videos n Amazon EFS and mount the file system to the EC2 instances for Te web application. Process the SOS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos.
(C). 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.
(D). 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

NO.196 A company has an organization that has many AWS accounts in AWS Organizations A solutions architect must improve how the company manages common security group rules for the AWS accounts in the organization.
The company has a common set of IP CIDR ranges in an allow list in each AWS account lo allow access to and from the company's on-premises network Developers within each account are responsible for

adding new IP CIDR ranges to their security groups. The security team has its own AWS account. Currently, the security team notifies the owners of the other AWS accounts when changes are made to the allow list.
The solutions architect must design a solution that distributes the common set of CIDR ranges across all accounts Which solution meets these requirements with the LEAST amount of operational overhead.
(A). Set up an Amazon Simple Notification Service (Amazon SNS) topic in the security team's AWS account Deploy an AWS Lambda function in each AWS account Configure the Lambda function to run every time an SNS topic receives a message Configure the Lambda function to take an IP address as input and add it to a list of security groups in the account Instruct the security team to distribute changes by publishing messages to its SNS topic
(B). Create new customer-managed prefix lists in each AWS account within the organization Populate the prefix lists in each account with all internal CIDR ranges Notify the owner of each AWS account to allow the new customer-managed prefix list IDs in their accounts in their security groups Instruct the security team to share updates with each AWS account owner.
(C). Create a new customer-managed prefix list in the security team's AWS account Populate the customer-managed prefix list with all internal CIDR ranges. Share the customer-managed prefix list.... organization by using AWS Resource Access Manager Notify the owner of each AWS account to allow the new customer-managed prefix list ID in their security groups
Answer: A

NO.197 A company has an application that runs on Amazon EC2 instances in an Amazon EC2 Auto Scaling group. The company uses AWS CodePipeline to deploy the application. The instances that run in the Auto Scaling group are constantly changing because of scaling events When the company deploys new application code versions the company Installs the AWS CodeDeploy agent on any new target EC2 instances and associates the instances with the CodeDeploy deployment group The application is set to go live within the next 24 hours What should a solutions architect recommend to automate the application deployment process with the LEAST amount of operational overhead?
(A). Configure Amazon EventBridge (Amazon CloudWatch Events) to invoke an AWS Lambda function when a new EC2 instance is launched into the Auto Scaling group. Code the Lambda function to associate the EC2 instances with the CodeDeploy deployment group.
(B). Write a script to suspend Amazon EC2 Auto Scaling operations before the deployment of new code. When the deployment is complete, create a new AMI and configure the Auto Scaling group's launch template to use the new AMI for new launches. Resume Amazon EC2 Auto Scaling operations
(C). Create a new AWS CodeBuild project that creates a new AMI that contains the new code Configure CodeBuild to update the Auto Scaling group's launch template to the new AMI Run an Amazon EC2 Auto Scaling instance refresh operation.
(D). Create a new AMI that has the CodeDeploy agent installed Configure the Auto Scaling group's launch template to use the new AMI Associate the CodeDeploy deployment group with the Auto Scaling group instead of the EC2 instances.
Answer: C

NO.198 A travel company built a web application that uses Amazon Simple Email Service (Amazon SES) to send email notifications to users. The company needs to enable logging to help troubleshoot email delivery issues. The company also needs the ability to do searches that are based on recipient, subject, and time sent.

Which combination of steps should a solutions architect take to meet these requirements? (Select TWO.)
(A). Create an Amazon SES configuration set with Amazon Kinesis Data Firehose as the destination. Choose to send logs to an Amazon S3 bucket.
(B). Enable AWS CloudTrail logging. Specify an Amazon S3 bucket as the destination for the logs.
(C). Use Amazon Athena to query the fogs in the Amazon S3 bucket for recipient, subject, and time sent.
(D). Create an Amazon CloudWatch log group. Configure Amazon SES to send logs to the log group
(E). Use Amazon Athena to query the logs in Amazon CloudWatch for recipient, subject, and time sent.

Answer: A,C
https://docs.aws.amazon.com/ses/latest/dg/event-publishing-retrieving-firehose.html To enable you to track your email sending at a granular level, you can set up Amazon SES to publish email sending events to Amazon CloudWatch, Amazon Kinesis Data Firehose, or Amazon Simple Notification Service based on characteristics that you define. https://docs.aws.amazon.com/ses/latest/dg/monitor-using-event-publishing.html
https://aws.amazon.com/getting-started/hands-on/build-serverless-real-time-data-processing-app-lambda-kinesis-s3-dynamodb-cognito-athena/4/#:~:text=Amazon%20Athena%20allows%20us%20to,to%20an%20Amazon%20S3%20bucket.

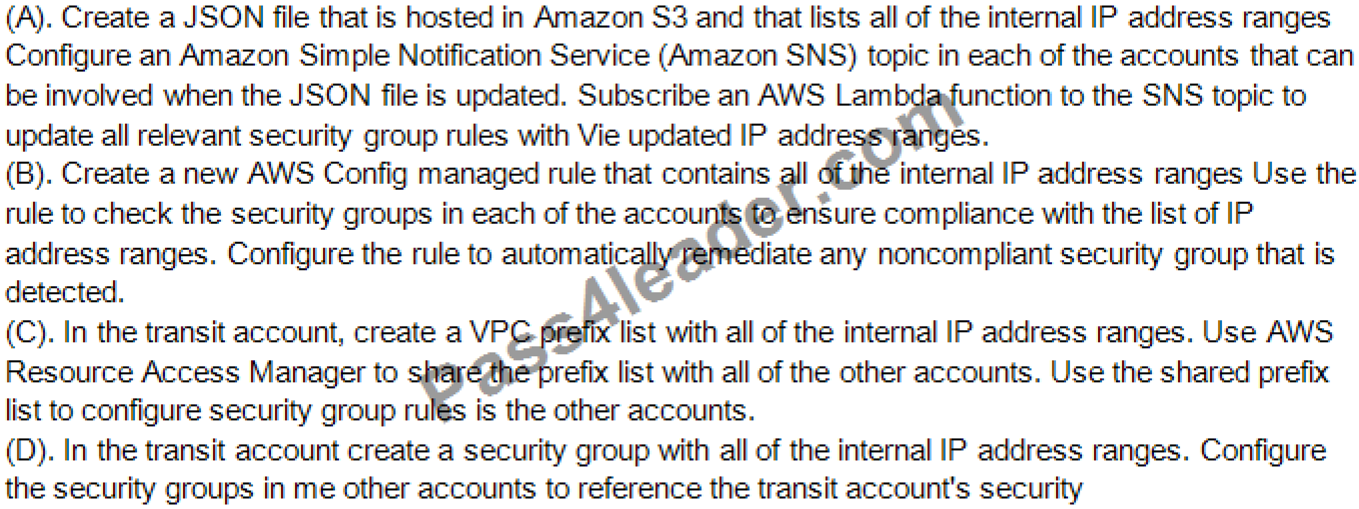
NO.199 A company has a website that enables users to upload videos. Company policy states the uploaded videos must be analyzed for restricted content. An uploaded video is placed in Amazon S3, and a message is pushed to an Amazon SOS queue with the video's location. A backend application pulls this location from Amazon SOS and analyzes the video.
The video analysis is compute-intensive and occurs sporadically during the day The website scales with demand. The video analysis application runs on a fixed number of instances. Peak demand occurs during the holidays, so the company must add instances to the application dunng this time. All instances used are currently on-demand Amazon EC2 T2 instances. The company wants to reduce the cost of the current solution.
Which of the following solutions is MOST cost-effective?
(A). Keep the website on T2 instances. Determine the minimum number of website instances required during off-peak times and use Spot Instances to cover them while using Reserved Instances to cover peak demand. Use Amazon EC2 R4 and Amazon EC2 R5 Reserved Instances in an Auto Scaling group for the video analysis application
(B). Keep the website on T2 instances. Determine the minimum number of website instances required during off-peak times and use Reserved Instances to cover them while using On-Demand Instances to cover peak demand. Use Spot Fleet for the video analysis application comprised of Amazon EC2 C4 and Amazon EC2 C5 Spot Instances.
(C). Migrate the website to AWS Elastic Beanstalk and Amazon EC2 C4 instances. Determine the minimum number of website instances required during off-peak times and use On-Demand Instances to cover them while using Spot capacity to cover peak demand Use Spot Fleet for the video anarysis application comprised of C4 and Amazon EC2 C5 instances.
(D). Migrate the website to AWS Elastic Beanstalk and Amazon EC2 R4 instances. Determine the minimum number of website instances required during off-peak times and use Reserved Instances to cover them while using On-Demand Instances to cover peak demand Use Spot Fleet for the video

analysis application comprised of R4 and Amazon EC2 R5 instances

Answer: B

NO.200 A company has an organization in AWS Organizations that has a large number of AWS accounts. One of the AWS accounts is designated as a transit account and has a transit gateway that is shared with all of the other AWS accounts AWS Site-to-Site VPN connections are configured between ail of the company's global offices and the transit account The company has AWS Config enabled on all of its accounts.

The company's networking team needs to centrally manage a list of internal IP address ranges that belong to the global offices Developers Will reference this list to gain access to applications securely. Which solution meets these requirements with the LEAST amount of operational overhead?



(A). Create a JSON file that is hosted in Amazon S3 and that lists all of the internal IP address ranges Configure an Amazon Simple Notification Service (Amazon SNS) topic in each of the accounts that can be involved when the JSON file is updated. Subscribe an AWS Lambda function to the SNS topic to update all relevant security group rules with Vie updated IP address ranges.

(B). Create a new AWS Config managed rule that contains all of the internal IP address ranges Use the rule to check the security groups in each of the accounts to ensure compliance with the list of IP address ranges. Configure the rule to automatically remediate any noncompliant security group that is detected.

(C). In the transit account, create a VPC prefix list with all of the internal IP address ranges. Use AWS Resource Access Manager to share the prefix list with all of the other accounts. Use the shared prefix list to configure security group rules is the other accounts.

(D). In the transit account create a security group with all of the internal IP address ranges. Configure the security groups in me other accounts to reference the transit account's security

Answer: C

group by using a nested security group reference of *<transit-account-id>./sg-1a2b3c4d".

NO.201 A company wants to improve cost awareness for its Amazon EMR platform The company has aWocated budgets for each team's Amazon EMR usage When a budgetary threshold is reached a notification should be sent by email to the budget office's distribution list Teams should be able lo view their EMR cluster expenses to date A solutions architect needs to create a solution that ensures this policy is proactively and centrally enforced in a multi-account environment Which combination of steps should the solutions architect take to meet these requirements? (Select TWO.)

(A). Update the AWS CloudFormation template to include the AWS Budgets Budget resource with the NotificationsWithSubscnbers property

(B). Implement Amazon CloudWatch dashboards for Amazon EMR usage

(C). Create an EMR bootstrap action that runs at startup that calls the Cost Explorer API to set the budget on the cluster with the GetCostForecast and NotificationsWithSubscnbers actions

(D). Create an AWS Service Catalog portfolio for each team. Add each team's Amazon EMR cluster as an AWS CloudFormation template to their Service Catalog portfolio as a Product

(E). Create an Amazon CloudWatch metric for billing Create a custom alert when costs exceed the budgetary threshold.

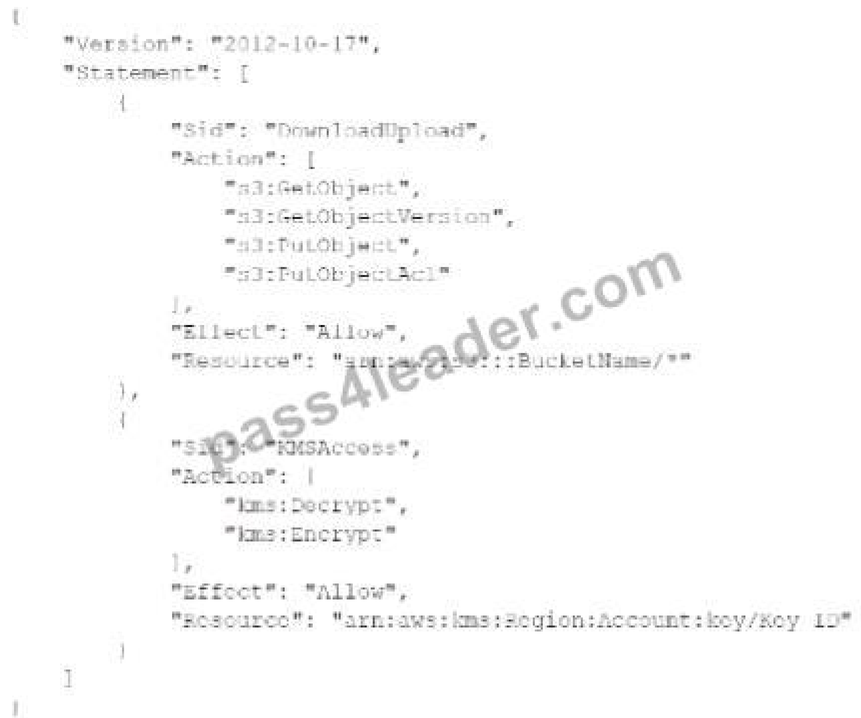
Answer: B,E

NO.202 During an audit, a security team discovered that a development team was putting IAM user secret access keys in their code and then committing it to an AWS CodeCommit repository . The

security team wants to automatically find and remediate instances of this security vulnerability
Which solution will ensure that the credentials are appropriately secured automatically?
(A). Run a script nightly using AWS Systems Manager Run Command to search for credentials on the development instances If found use AWS Secrets Manager to rotate the credentials.
(B). Use a scheduled AWS Lambda function to download and scan the application code from CodeCommit If credentials are found, generate new credentials and store them in AWS KMS
(C). Configure Amazon Macie to scan for credentials in CodeCommit repositories If credentials are found, trigger an AWS Lambda function to disable the credentials and notify the user
(D). Configure a CodeCommit trigger to invoke an AWS Lambda function to scan new code submissions for credentials If credentials are found, disable them in AWS IAM and notify the user.
Answer: A

NO.203 A solutions architect must analyze a company's Amazon EC2 Instances and Amazon Elastic Block Store (Amazon EBS) volumes to determine whether the company is using resources efficiently The company is running several large, high-memory EC2 instances lo host database dusters that are deployed in active/passive configurations The utilization of these EC2 instances varies by the applications that use the databases, and the company has not identified a pattern The solutions architect must analyze the environment and take action based on the findings.
Which solution meets these requirements MOST cost-effectively?
(A). Create a dashboard by using AWS Systems Manager OpsConter Configure visualizations tor Amazon CloudWatch metrics that are associated with the EC2 instances and their EBS volumes Review the dashboard periodically and identify usage patterns Rightsize the EC2 instances based on the peaks in the metrics
(B). Turn on Amazon CloudWatch detailed monitoring for the EC2 instances and their EBS volumes Create and review a dashboard that is based on the metrics Identify usage patterns Rightsize the FC? instances based on the peaks In the metrics
(C). Install the Amazon CloudWatch agent on each of the EC2 Instances Turn on AWS Compute Optimizer, and let it run for at least 12 hours Review the recommendations from Compute Optimizer, and rightsize the EC2 instances as directed
(D). Sign up for the AWS Enterprise Support plan Turn on AWS Trusted Advisor Wait 12 hours Review the recommendations from Trusted Advisor, and rightsize the EC2 instances as directed
Answer: C
(https://aws.amazon.com/compute-optimizer/pricing/ , https://aws.amazon.com/systems-manager/pricing/).
https://aws.amazon.com/compute-optimizer/

NO.204 A solutions architect needs to implement a client-side encryption mechanism for objects that will be stored in a new Amazon S3 bucket. The solutions architect created a CMK that is stored in AWS Key Management Service (AWS KMS) for this purpose.
The solutions architect created the following IAM policy and attached it to an IAM role:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DownloadUpload",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::BucketName/*"
        },
        {
            "Sid": "KMSAccess",
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:kms:Region:Account:key/Key ID"
        }
    ]
}
```

During tests, me solutions architect was able to successfully get existing test objects m the S3 bucket However, attempts to upload a new object resulted in an error message. The error message stated that me action was forbidden.

Which action must me solutions architect add to the IAM policy to meet all the requirements?

(A). Kms:GenerateDataKey

(B). KmsGetKeyPolpcy

(C). kmsGetPubKKey

(D). kms:SKjn

Answer: A

NO.205 A company is hosting a single-page web application in the AWS Cloud. The company is using Amazon CloudFront to reach its goal audience. The CloudFront distribution has an Amazon S3 bucket that is configured as its origin. The static files for the web application are stored in this S3 bucket.

The company has used a simple routing policy to configure an Amazon Route 53 A record The record points to the CloudFront distribution The company wants to use a canary deployment release strategy for new versions of the application.

What should a solutions architect recommend to meet these requirements?

(A). Create a second CloudFront distribution for the new version of the application. Update the Route 53 record to use a weighted routing policy.

(B). Create a Lambda@Edge function. Configure the function to implement a weighting algorithm and rewrite the URL to direct users to a new version of the application.

(C). Create a second S3 bucket and a second CloudFront origin for the new S3 bucket Create a CloudFront origin group that contains both origins Configure origin weighting for the origin group.

(D). Create two Lambda@Edge functions. Use each function to serve one of the application versions Set up a CloudFront weighted Lambda@Edge invocation policy

Answer: A

NO.206 A company is running an application in the AWS Cloud. The application consists of

microservices that run on a fleet of Amazon EC2 instances in multiple Availability Zones behind an Application Load Balancer. The company recently added a new REST API that was implemented in Amazon API Gateway. Some of the older microservices that run on EC2 instances need to call this new API The company does not want the API to be accessible from the public internet and does not want proprietary data to traverse the public internet What should a solutions architect do to meet these requirements?
(A). Create an AWS Site-to-Site VPN connection between the VPC and the API Gateway Use API Gateway to generate a unique API key for each microservice. Configure the API methods to require the key.
(B). Create an interface VPC endpoint for API Gateway, and set an endpoint policy to only allow access to the specific API Add a resource policy to API Gateway to only allow access from the VPC endpoint Change the API Gateway endpoint type to private.
(C). Modify the API Gateway to use IAM authentication Update the IAM policy for the IAM role that is assigned to the EC2 instances to allow access to the API Gateway Move the API Gateway into a new VPC Deploy a transit gateway and connect the VPCs.
(D). Create an accelerator in AWS Global Accelerator and connect the accelerator to the API Gateway. Update the route table for all VPC subnets with a route to the created Global Accelerator endpoint IP address. Add an API key for each service to use for authentication.
Answer: B

NO.207 A solutions architect works for a government agency that has strict disaster recovery requirements All Amazon Elastic Block Store (Amazon EBS) snapshots are required to be saved in at least two additional AWS Regions. The agency also is required to maintain the lowest possible operational overhead.
Which solution meets these requirements?
(A). Configure a policy in Amazon Data Lifecycle Manager (Amazon DLMJ to run once daily to copy the EBS snapshots to the additional Regions.
(B). Schedule Amazon EC2 Image Builder to run once daily to create an AMI and copy the AMI to the additional Regions.
(C). Set up AWS Backup to create the EBS snapshots. Configure Amazon S3 cross-Region replication to copy the EBS snapshots to the additional Regions.
(D). Use Amazon EventBridge (Amazon CloudWatch Events) to schedule an AWS Lambda function to copy the EBS snapshots to the additional Regions.
Answer: A

NO.208 A company has several applications running in an on-premises data center. The data center runs a mix of Windows and Linux VMs managed by VMware vCenter. A solutions architect needs to create a plan to migrate the applications to AWS However, the solutions architect discovers that the documentation for the applications is not up to date and that mere are no complete infrastructure diagrams The company's developers lack time to discuss their applications and current usage with the solutions architect What should the solutions architect do to gather the required information?
(A). Deploy the AWS Server Migration Service (AWS SMS) connector using the OVA image on the VMware cluster to collect configuration and utilization data from the VMs
(B). Use the AWS Migration Portfolio Assessment (MPA) tool to connect to each of the VMs to collect the configuration and utilization data.
(C). Install the AWS Application Discovery Service on each of the VMs to collect the configuration and

utilization data
(D). Register the on-premises VMs with the AWS Migration Hub to collect configuration and utilization data
Answer: A

NO.209 A company wants to change its internal cloud billing strategy for each of its business units. Currently, the cloud governance team shares reports for overall cloud spending with the head of each business unit. The company uses AWS Organizations lo manage the separate AWS accounts for each business unit. The existing tagging standard in Organizations includes the application, environment, and owner. The cloud governance team wants a centralized solution so each business unit receives monthly reports on its cloud spending. The solution should also send notifications for any cloud spending that exceeds a set threshold.
Which solution is the MOST cost-effective way to meet these requirements?
(A). Configure AWS Budgets in each account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in each account to create monthly reports for each business unit.
(B). Configure AWS Budgets in the organization's master account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in the organization's master account to create monthly reports for each business unit.
(C). Configure AWS Budgets in each account and configure budget alerts lhat are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use the AWS Billing and Cost Management dashboard in each account to create monthly reports for each business unit.
(D). Enable AWS Cost and Usage Reports in the organization's master account and configure reports grouped by application, environment, and owner. Create an AWS Lambda function that processes AWS Cost and Usage Reports, sends budget alerts, and sends monthly reports to each business unit's email list.
Answer: B
Configure AWS Budgets in the organization items master account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in the organization items master account to create monthly reports for each business unit.
https://aws.amazon.com/about-aws/whats-new/2019/07/introducing-aws-budgets-reports/#:~:text=AWS%20Budgets%20gives%20you%20the,below%20the%20threshold%20you%20define.

NO.210 A solutions architect uses AWS Organizations to manage several AWS accounts for a company. The full Organizations feature set is activated for the organization. All production AWS accounts exist under an OU that is named "production '' Systems operators have full administrative privileges within these accounts by using IAM roles.
The company wants to ensure that security groups in all production accounts do not allow inbound traffic for TCP port 22. All noncompliant security groups must be remediated immediately, and no new rules that allow port 22 can be created.
Winch solution will meet these requirements?
(A). Write an SCP that denies the CreateSecurityGroup action with a condition o(ec2:tngress rule

with value 22. Apply the SCP to the 'production' OU.
(B). Configure an AWS CloudTrail trail for all accounts Send CloudTrail logs to an Amazon S3 bucket In the Organizations management account. Configure an AWS Lambda function on the management account with permissions to assume a role in all production accounts to describe and modify security groups. 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.
(C). Create an Amazon EvertBridge (Amazon CloudWatch Events) event bus in the Organizations management account. Create an AWS Cloud Formation template to deploy configurations that send CreateSecurityGroup events to the even! bus from an production accounts Configure an AWS Lambda function in the management account with permissions to assume a role all production accounts to describe and modify security groups. Configure the event bus to invoke the Lambda function Configure the Lambda function to analyse each event for noncompliant security group actions and to automatically remediate any issues.
(D). 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. Apply an SCP to the OU to deny modification of the resources that the CloudFormation template provisions.
Answer: D

NO.211 A company is using multiple AWS accounts The DNS records are stored in a private hosted zone for Amazon Route 53 in Account A The company's applications and databases are running in Account B.
A solutions architect win deploy a two-net application In a new VPC To simplify the configuration, the db.example com CNAME record set tor the Amazon RDS endpoint was created in a private hosted zone for Amazon Route 53.
During deployment, the application failed to start. Troubleshooting revealed that db.example com is not resolvable on the Amazon EC2 instance The solutions architect confirmed that the record set was created correctly in Route 53.
Which combination of steps should the solutions architect take to resolve this issue? (Select TWO J
(A). Deploy the database on a separate EC2 instance in the new VPC Create a record set for the instance's private IP in the private hosted zone
(B). Use SSH to connect to the application tier EC2 instance Add an RDS endpoint IP address to the /eto/resolv.conf file
(C). Create an authorization lo associate the private hosted zone in Account A with the new VPC In Account B
(D). Create a private hosted zone for the example.com domain m Account B Configure Route 53 replication between AWS accounts
(E). Associate a new VPC in Account B with a hosted zone in Account A. Delete the association authorization In Account A.
Answer: C,E

NO.212 A company has application services that have been containerized and deployed on multiple Amazon EC2 instances with public IPs. An Apache Kafka cluster has been deployed to the EC2 instances. A PostgreSQL database has been migrated to Amazon RDS lor PostgreSQL. The company

expects a significant increase of orders on its platform when a new version of its flagship product is released.
What changes to the current architecture will reduce operational overhead and support the product release?
(A). Create an EC2 Auto Scaling group behind an Application Load Balancer. Create additional read replicas for the DB instance. Create Amazon Kinesis data streams and configure the application services lo use the data streams. Store and serve static content directly from Amazon S3.
(B). Create an EC2 Auto Scaling group behind an Application Load Balancer. Deploy the DB instance in Multi-AZ mode and enable storage auto scaling. Create Amazon Kinesis data streams and configure the application services to use the data streams. Store and serve static content directly from Amazon S3.
(C). Deploy the application on a Kubernetes cluster created on the EC2 instances behind an Application Load Balancer. Deploy the DB instance in Multi-AZ mode and enable storage auto scaling. Create an Amazon Managed Streaming for Apache Kafka cluster and configure the application services to use the cluster. Store static content in Amazon S3 behind an Amazon CloudFront distribution.
(D). Deploy the application on Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate and enable auto scaling behind an Application Load Balancer. Create additional read replicas for the DB instance. Create an Amazon Managed Streaming for Apache Kafka cluster and configure the application services to use the cluster. Store static content in Amazon S3 behind an Amazon CloudFront distribution.

Answer: D

Deploy the application on Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate and enable auto scaling behind an Application Load Balancer. Create additional read replicas for the DB instance. Create an Amazon Managed Streaming for Apache Kafka cluster and configure the application services to use the cluster. Store static content in Amazon S3 behind an Amazon CloudFront distribution.

NO.213 A company's solution architect is designing a diasaster recovery (DR) solution for an application that runs on AWS. The application uses PostgreSQL 11.7 as its database. The company has an PRO of 30 seconds. The solutions architect must design a DR solution with the primary database in the us-east-1 Region and the database in the us-west-2 Region.
What should the solution architect do to meet these requirements with minimum application change?
(A). Migrate the database to Amazon RDS for PostgreSQL in us-east-1. Set up a read replica up a read replica in us-west-2. Set the managed PRO for the RDS database to 30 seconds.
(B). Migrate the database to Amazon for PostgreSQL in us-east-1. Set up a standby replica in an Availability Zone in us-west-2, Set the managed PRO for the RDS database to 30 seconds.
(C). Migrate the database to an Amazon Aurora PostgreSQL global database with the primary Region as us-east-1 and the secondary Region as us-west-2. Set the managed PRO for the Aurora database to 30 seconds.
(D). Migrate the database to Amazon DynamoDB in us-east-1. Set up global tables with replica tables that are created in us-west-2.

Answer: A

NO.214 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 repository. 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)

(B). Configure scan on push on the repository Configure scan results to be pushed to an Amazon Simple Queue Service (Amazon SQS) queue Invoke an AWS Lambda function when a new message is added to the SOS queue Use the Lambda function to delete the image tag for images that have Critical or High seventy findings. Notify the development team by using Amazon Simple Email Service (Amazon SES).

(C). 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 complete. Use the second Lambda function to delete the image tag for images that have Cnocal or High severity findings. Notify the development team by using Amazon Simple Notification Service (Amazon SNS)

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

Answer: C

NO.215 An education company is running a web application used by college students around the world. The application runs in an Amazon Elastic Container Service {Amazon ECS) cluster in an Auto Scaling group behind an Application Load Balancer (ALB). A system administrator detects a weekly spike in the number of failed login attempts, which overwhelm the application's authentication service. All the failed login attempts originate from about 500 different IP addresses that change each week, A solutions architect must prevent the failed login attempts from overwhelming the authentication service.

Which solution meets these requirements with the MOST operational efficiency?

(A). Use AWS Firewall Manager to create a security group and security group policy to deny access from the IP addresses.

(B). Create an AWS WAF web ACL with a rate-based rule, and set the rule action to Block. Connect the web ACL to the ALB.

(C). Use AWS Firewall Manager to create a security group and security group policy to allow access only to specific CIOR ranges.

(D). Create an AWS WAF web ACL with an IP set match rule, and set the rule action to Block. Connect the web ACL to the ALB.

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

NO.216 A company has created an OU in AWS Organizations for each of its engineering teams Each OU owns multiple AWS accounts. The organization has hundreds of AWS accounts A solutions architect must design a solution so that each OU can view a breakdown of usage costs across its AWS accounts. Which solution meets these requirements?
(A). Create an AWS Cost and Usage Report (CUR) for each OU by using AWS Resource Access Manager Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
(B). Create an AWS Cost and Usage Report (CUR) from the AWS Organizations management account-Allow each team to visualize the CUR through an Amazon QuickSight dashboard
(C). Create an AWS Cost and Usage Report (CUR) in each AWS Organizations member account Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
(D). Create an AWS Cost and Usage Report (CUR) by using AWS Systems Manager Allow each team to visualize the CUR through Systems Manager OpsCenter dashboards
Answer: B

NO.217 A company hosts a large on-premises MySQL database at its main office that supports an issue tracking system used by employees around the world. The company already uses AWS for some workloads and has created an Amazon Route 53 entry for the database endpoint that points to the on-premises database. Management is concerned about the database being a single point of failure and wants a solutions architect to migrate the database to AWS without any data loss or downtime. Which set of actions should the solutions architect implement?
(A). Create an Amazon Aurora DB cluster. Use AWS Database Migration Service (AWS DMS) to do a full load from the on-premises database lo Aurora. Update the Route 53 entry for the database to point to the Aurora cluster endpoint. and shut down the on-premises database.
(B). During nonbusiness hours, shut down the on-premises database and create a backup. Restore this backup to an Amazon Aurora DB cluster. When the restoration is complete, update the Route 53 entry for the database to point to the Aurora cluster endpoint, and shut down the on-premises database.
(C). Create an Amazon Aurora DB cluster. Use AWS Database Migration Service (AWS DMS) to do a full load with continuous replication from the on-premises database to Aurora. When the migration is complete, update the Route 53 entry for the database to point to the Aurora cluster endpoint, and shut down the on-premises database.
(D). Create a backup of the database and restore it to an Amazon Aurora multi-master cluster. This Aurora cluster will be in a master-master replication configuration with the on-premises database. Update the Route 53 entry for the database to point to the Aurora cluster endpoint. and shut down the on-premises database.
Answer: C
"Around the world" eliminates possibility for the maintenance window at night. The other difference

is ability to leverage continuous replication in MySQL to Aurora case.

NO.218 A company Is serving files to its customers through an SFTP server that Is accessible over the internet The SFTP server Is running on a single Amazon EC2 instance with an Elastic IP address attached Customers connect to the SFTP server through its Elastic IP address and use SSH for authentication The EC2 instance also has an attached security group that allows access from all customer IP addresses.

A solutions architect must implement a solution to improve availability minimize the complexity ot infrastructure management and minimize the disruption to customers who access files. The solution must not change the way customers connect.

Which solution will meet these requirements?

(A). Disassociate the Elastic IP address from me EC2 instance Create an Amazon S3 bucket to be used for sftp file hosting Create an AWS Transfer Family server Configure the Transfer Family server with a publicly accessible endpoint. Associate the SFTP Elastic IP address with the new endpoint. Point the Transfer Family server to the S3 bucket Sync all files from the SFTP server to the S3 bucket.

(B). Disassociate the Elastic IP address from the EC2 instance. Create an Amazon S3 bucket to be used for SFTP file hosting Create an AWS Transfer Family server. Configure the Transfer Family server with a VPC-hosted. internet-facing endpoint. Associate the SFTP Elastic IP address with the new endpoint. Attach the security group with customer IP addresses to the new endpoint. Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to The S3 bucket

(C). Disassociate the Elastic IP address from the EC2 instance. Create a new Amazon Elastic File System (Amazon EFS) file system to be used for SFTP file hosting. Create an AWS Fargate task definition to run an SFTP server. Specify the EFS file system as a mount in the task definition Create a Fargate service by using the task definition, and place a Network Load Balancer (NLB) front of the service When configuring the service, attach the security group with customer IP addresses to the tasks that run the SFTP server Associate the Elastic IP address with the Nl B Sync all files from the SFTP server to the S3 bucket

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

Answer: B

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

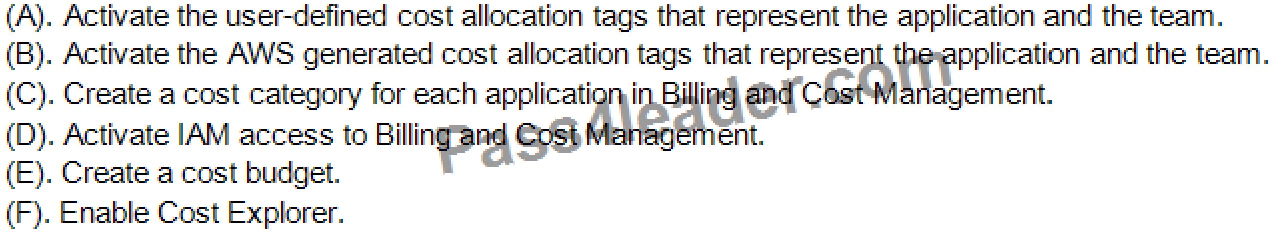
NO.219 A large company is running a popular web application. The application runs on several Amazon EC2 Linux Instances in an Auto Scaling group in a private subnet. An Application Load Balancer is targeting the Instances In the Auto Scaling group in the private subnet. AWS Systems Manager Session Manager Is configured, and AWS Systems Manager Agent is running on all the EC2 instances.

The company recently released a new version of the application Some EC2 instances are now being

marked as unhealthy and are being terminated As a result, the application is running at reduced capacity A solutions architect tries to determine the root cause by analyzing Amazon CloudWatch logs that are collected from the application, but the logs are inconclusive How should the solutions architect gain access to an EC2 instance to troubleshoot the issue1?
(A). Suspend the Auto Scaling group's HealthCheck scaling process. Use Session Manager to log in to an instance that is marked as unhealthy
(B). Enable EC2 instance termination protection Use Session Manager to log In to an instance that is marked as unhealthy.
(C). Set the termination policy to Oldestinstance on the Auto Scaling group. Use Session Manager to log in to an instance that is marked as unhealthy
(D). Suspend the Auto Scaling group's Terminate process. Use Session Manager to log in to an instance that is marked as unhealthy

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

NO.220 The company needs to determine which costs on the monthly AWS bill are attributable to each application or team. The company also must be able to create reports to compare costs from the last 12 months and to help forecast costs for the next 12 months. A solutions architect must recommend an AWS Billing and Cost Management solution that provides these cost reports.
Which combination of actions will meet these requirements? (Select THREE.)


(A). Activate the user-defined cost allocation tags that represent the application and the team.
(B). Activate the AWS generated cost allocation tags that represent the application and the team.
(C). Create a cost category for each application in Billing and Cost Management.
(D). Activate IAM access to Billing and Cost Management.
(E). Create a cost budget.
(F). Enable Cost Explorer.

Answer: A,C,F
https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/manage-cost-categories.html
https://aws.amazon.com/premiumsupport/knowledge-center/cost-explorer-analyze-spending-and-usage/
https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/manage-cost-categories.html
https://docs.aws.amazon.com/cost-management/latest/userguide/ce-enable.html

NO.221 A company wants to use Amazon S3 to back up its on-premises file storage solution. The company s on-premises file storage solution supports NFS and the company wants its new solution to support NFS The company wants to archive the backup Files after 5 days If the company needs

archived files for disaster recovery, the company is willing to wait a few days for the retrieval of those Files.
Which solution meets these requirements MOST cost-effectively?
(A). Deploy an AWS Storage Gateway file gateway that is associated with an S3 bucket Move the files from the on-premises file storage solution to the file gateway Create an S3 Lifecycle rule to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) after 5 days
(B). Deploy an AWS Storage Gateway volume gateway that is associated with an S3 bucket Move the files from the on-premises file storage solution to the volume gateway Create an S3 Lifecycle rule to move the files to S3 Glacier Deep Archive after 5 days
(C). Deploy an AWS Storage Gateway tape gateway that is associated with an S3 bucket Move the files from the on-premises file storage solution to the tape gateway Create an S3 Lifecycle rule to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) after 5 days
(D). Deploy an AWS Storage Gateway file gateway that is associated with an S3 bucket Move the files from the on-premises file storage solution to the file gateway Create an S3 Lifecycle rule to move the files to S3 Glacier Deep Archive after 5 days
Answer: D

NO.222 A company wants to migrate its on-premises data center to the AWS Cloud. This includes thousands of virtualized Linux and Microsoft Windows servers SAN storage, Java and PHP applications with MySQL, and Oracle databases. There are many dependent services hosted either in the same data center or externally. The technical documentation is incomplete and outdated A solutions architect needs to understand the current environment and estimate the cloud resource costs after the migration Which tools or services should the solutions architect use to plan the cloud migration? (Select THREE.)
(A). AWS Application Discovery Service
(B). AWS SMS
(C). AWS X-Ray
(D). AWS Cloud Adoption Readiness Tool (CART)
(E). Amazon Inspector
(F). AWS Migration Hub
Answer: A,D,F

NO.223 A solutions architect is designing a multi-account structure that has 10 existing accounts.
The design must meet the following requirements
* Consolidate all accounts into one organization
* Allow full access to the Amazon EC2 service from the management account and the secondary accounts
* Minimize the effort required to add additional secondary accounts
Which combination of steps should be included in the solution? (Select TWO)
(A). Create an organization from the management account Send invitations to the secondary accounts from the management account Accept the invitations and create an OU
(B). Create an organization from the management account. Send a join request to the management account from each secondary account Accept the requests and create an OU
(C). Create a VPC peering connection between the management account and the secondary accounts Accept the request for the VPC peering connection
(D). Create a service control policy (SCP) that enables full EC2 access, and attach the policy to the OU

(E). Create a full EC2 access policy and map the policy to a role in each account Trust every other account to assume the role

Answer: A,E

NO.224 A company wants to move a web application to AWS. The application stores session information locally on each web server, which will make auto scaling difficult As part of the migration, the application will be rewritten to decouple the session data from the web servers. The company requires low latency, scalability, and availability.

Which service will meet the requirements for storing the session information in the MOST cost-effective way?

(A). Amazon ElastiCache with the Memcached engine

(B). Amazon S3

(C). Amazon RDS MySQL

(D). Amazon ElastiCache with the Redis engine

Answer: D

https://aws.amazon.com/caching/session-management/

Building real-time apps across versatile use cases like gaming, geospatial service, caching, session stores, or queuing, with advanced data structures, replication, and point-in-time snapshot support.

Memcached: Building a simple, scalable caching layer for your data-intensive apps.

https://aws.amazon.com/elasticache/

NO.225 A company is using an existing orchestration tool to manage thousands of Amazon EC2 instances. A recent penetration test found a vulnerability in the company's software stack. This vulnerability has prompted the company to perform a full evaluated of its current production environment The analysts determined that the following vulnerabilities exist within the environment:

* Operating systems with outdated libraries and known vulnerabilities are being used in production

* Relational databases hosted and managed by the company are running unsupported versions with known vulnerabilities

* Data stored in databases Is not encrypted.

The solutions architect intends to use AWS Config to continuously audit and assess the compliance of the company's AWS resource configurations with the company's polices and guidelines What additional steps will enable the company to secure its environments and track resources while adhering to best practices?

(A). Use AWS Application Discovery Service to evaluate at running EC2 instances Use the AWS CLI lo modify each instance, and use EC2 user data to install the AWS Systems Manager Agent during boot Schedule patching to run as a Systems Manager Maintenance Windows task. Migrate all relational databases lo Amazon RDS and enable AWS KMS encryption

(B). Create an AWS CloudFormation template for the EC2 instances Use EC2 user data in the CloudFormation template to install the AWS Systems Manager Agent, and enable AWS KMS encryption on all Amazon EBS volumes. Have CloudFormation replace al running instances. Use Systems Manager Patch Manager to establish a patch baseline and deploy a Systems Manager Maintenance Windows task to run AWS-RunPatchBaseline using the patch baseline

(C). Install the AWS Systems Manager Agent on all existing instances using the company's current orchestration tool Use the Systems Manager Run Command to run a list of commands to upgrade software on each instance using operating system-specific tools. Enable AWS KMS encryption on all Amazon EBS volumes.

(D). install the AWS Systems Manager Agent on all existing instances using the company's current orchestration tool. Migrate al relational databases to Amazon RDS and enable AWS KMS encryption Use Systems Manager Patch Manager to establish a patch baseline and deploy a Systems Manager Maintenance Windows task to run AWS-RunPatchBaseline using the patch baseline.
Answer: D

NO.226 A large company runs workloads in VPCs that are deployed across hundreds of AWS accounts Each VPC consists of public subnets and private subnets that span across multiple Availability Zones NAT gateways are deployed in the public subnets and allow outbound connectivity to the internet from the private subnets.
A solutions architect is working on a hub-and-spoke design. All private subnets in the spoke VPCs must route traffic to the internet through an egress VPC The solutions architect already has deployed a NAT gateway in an egress VPC in a central AWS account Which set of additional steps should the solutions architect take to meet these requirements?
(A). Create peering connections between the egress VPC and the spoke VPCs Configure the required routing to allow access to the internet
(B). Create a transit gateway and share it with the existing AWS accounts Attach existing VPCs to the transit gateway Configure the required routing to allow access to the internet
(C). Create a transit gateway in every account Attach the NAT gateway to the transit gateways Configure the required routing to allow access to the internet
(D). Create an AWS PrivateLink connection between the egress VPC and the spoke VPCs Configure the required routing to allow access to the internet
Answer: B

NO.227 A company is migrating its three-tier web application from on-premises to the AWS Cloud. The company has the following requirements for the migration process:
* Ingest machine images from the on-premises environment.
* Synchronize changes from the on-premises environment to the AWS environment until the production cutover.
* Minimize downtime when executing the production cutover.
* Migrate the virtual machines' root volumes and data volumes.
Which solution will satisfy these requirements with minimal operational overhead?
(A). Use AWS Server Migration Service (SMS) to create and launch a replication job for each tier of the application. Launch instances from the AMIs created by AWS SMS. After initial testing, perform a final replication and create new instances from the updated AMIs.
(B). Create an AWS CLIVM Import/Export script to migrate each virtual machine. Schedule the script to run incrementally to maintain changes in the application. Launch instances from the AMIs created by VM Import/Export. Once testing is done, rerun the script to do a final import and launch the instances from the AMIs.
(C). Use AWS Server Migration Service (SMS) to upload the operating system volumes. Use the AWS CLI import-snaps hot command 'or the data volumes. Launch instances from the AMIs created by AWS SMS and attach the data volumes to the instances. After initial testing, perform a final replication, launch new instances from the replicated AMIs. and attach the data volumes to the instances.
(D). Use AWS Application Discovery Service and AWS Migration Hub to group the virtual machines as an application. Use the AWS CLI VM Import/Export script to import the virtual machines as AMIs.

Schedule the script to run incrementally to maintain changes in the application. Launch instances from the AMIs. After initial testing, perform a final virtual machine import and launch new instances from the AMIs.

Answer: A

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

NO.228 A scientific organization requires the processing of text and picture data stored in an Amazon S3 bucket. The data is gathered from numerous radar stations during a mission's live, time-critical phase. The data is uploaded by the radar stations to the source S3 bucket. The data is preceded with the identification number of the radar station.

In a second account, the business built a destination S3 bucket. To satisfy a compliance target, data must be transferred from the source S3 bucket to the destination S3 bucket. Replication is accomplished by using an S3 replication rule that covers all items in the source S3 bucket.

A single radar station has been recognized as having the most precise dat a. At this radar station, data replication must be completed within 30 minutes of the radar station uploading the items to the source S3 bucket.

What actions should a solutions architect take to ensure that these criteria are met?

(A). Set up an AWS DataSync agent to replicate the prefixed data from the source S3 bucket to the destination S3 bucket. Select to use at available bandwidth on the task, and monitor the task to ensure that it is in the TRANSFERRING status. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an alert if this status changes.

(B). In the second account, create another S3 bucket to receive data from the radar station with the most accurate data Set up a new replication rule for this new S3 bucket to separate the replication from the other radar stations Monitor the maximum replication time to the destination. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an alert when the time exceeds the desired threshold

(C). Enable Amazon S3 Transfer Acceleration on the source S3 bucket, and configure the radar station with the most accurate data to use the new endpoint Monitor the S3 destination bucket's TotalRequestLatency metric Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an alert if this status changes

(D). Create a new S3 replication rule on the source S3 bucket that filters for the keys that use the prefix of the radar station with the most accurate data Enable S3 Replication Time Control (S3 RTC) Monitor the maximum replication time to the destination Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an alert when the time exceeds the desired threshold

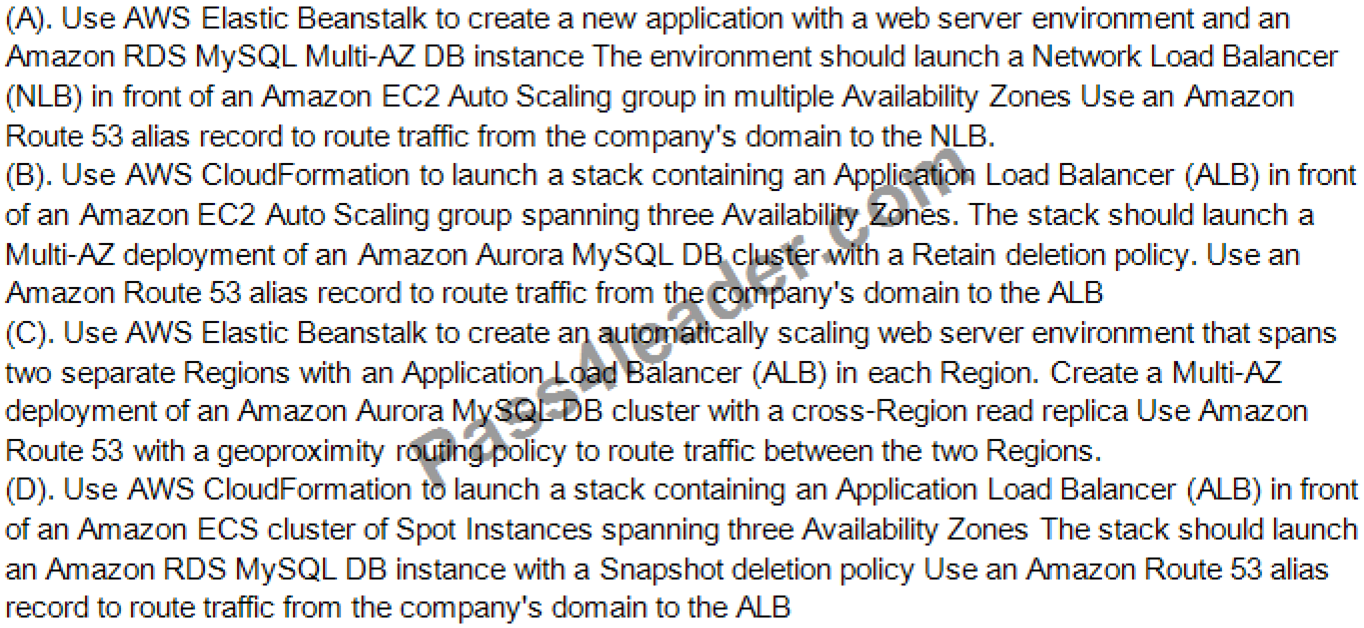
Answer: D

https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-time-control.html

NO.229 A large education company recently introduced Amazon Workspaces to provide access to internal applications across multiple universities. The company is storing user proxies on an Amazon FSx for Windows File Server tile system. The Me system is configured with a DNS alias and is connected to a self-managed Active Directory As more users begin to use the Workspaces login time increases to unacceptable levels An investigation reveals a degradation in performance of the file system. The company created the file system on HDD storage with a throughput of 16 MBps A solutions architect must improve the performance of the file system during a defined maintenance window What should the solutions architect do to meet these requirements with the LEAST

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

NO.230 A company is hosting a three-tier web application in an on-premises environment. Due to a recent surge in traffic that resulted in downtime and a significant financial impact, company management has ordered that the application be moved to AWS. The application is written in .NET and has a dependency on a MySQL database A solutions architect must design a scalable and highly available solution to meet the demand of 200000 daily users.
Which steps should the solutions architect take to design an appropriate solution?



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

Answer: B

NO.231 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. 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
(B). Apply a service control policy (SCP) that denies access to all services except IAM Amazon Athena Amazon S3 and AWS CloudTrail Store customer record files in Amazon S3 and tram users to run queries using the CLI via Athena Analyze CloudTrail events to audit and alarm on queries against personal data
(C). 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
(D). 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

NO.232 A Solutions Architect is constructing a containerized.NET Core application for AWS Fargate. The application's backend needs a high-availability version of Microsoft SQL Server. All application levels must be extremely accessible. The credentials associated with the SQL Server connection string should not be saved to disk inside the.NET Core front-end containers.
Which tactics should the Solutions Architect use to achieve these objectives?
(A). Set up SQL Server to run in Fargate with Service Auto Scaling. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to SQL Server running in Fargate. Specify the ARN of the secret in AWS Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string. Set up the .NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.
(B). Create a Multi-AZ deployment of SQL Server on Amazon RDS. Create a secret in AWS Secrets Manager for the credentials to the RDS database. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to the RDS database in Secrets Manager. Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string. Set up the .NET Core service in Fargate using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.
(C). Create an Auto Scaling group to run SQL Server on Amazon EC2. Create a secret in AWS Secrets Manager for the credentials to SQL Server running on EC2. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to SQL Server on EC2. Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task

definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string. Set up the .NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.
(D). Create a Multi-AZ deployment of SQL Server on Amazon RDS. Create a secret in AWS Secrets Manager for the credentials to the RDS database. Create non- persistent empty storage for the .NET Core containers in the Fargate task definition to store the sensitive information. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to the RDS database in Secrets Manager. Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be written to the non-persistent empty storage on startup for reading into the application to construct the connection string. Set up the .NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.
Answer: B
Secrets Manager natively supports SQL Server on RDS. No real need to create additional 'ephemeral storage' to fetch credentials, as these can be injected to containers as environment variables.
https://aws.amazon.com/premiumsupport/knowledge-center/ecs-data-security-container-task/

NO.233 A developer reports receiving an Error 403: Access Denied message when they try to download an object from an Amazon S3 bucket. The S3 bucket is accessed using an S3 endpoint inside a VPC. and is encrypted with an AWS KMS key. A solutions architect has verified that (he developer is assuming the correct IAM role in the account that allows the object to be downloaded. The S3 bucket policy and the NACL are also valid.
Which additional step should the solutions architect take to troubleshoot this issue?
(A). Ensure that blocking all public access has not been enabled in the S3 bucket.
(B). Verify that the IAM rote has permission to decrypt the referenced KMS key.
(C). Verify that the IAM role has the correct trust relationship configured.
(D). Check that local firewall rules are not preventing access to the S3 endpoint.
Answer: B

NO.234 A company is planning a large event where a promotional offer will be introduced The company's website is hosted on AWS and backed by an Amazon RDS for PostgreSQL DB instance The website explains the promotion and includes a sign-up page that collects user information and preferences Management expects large and unpredictable volumes of traffic periodically which will create many database writes A solutions architect needs to build a solution that does not change the underlying data model and ensures that submissions are not dropped before they are committed to the database Which solutions meets these requirements'?
(A). Immediately before the event, scale up the existing DB instance to meet the anticipated demand. Then scale down after the event
(B). Use Amazon SQS to decouple the application and database layers Configure an AWS Lambda function to write items from the queue into the database
(C). Migrate to Amazon DynamoDB and manage throughput capacity with automatic scaling
(D). Use Amazon ElastiCache for Memcached to increase write capacity to the DB instance
Answer: D

NO.235 A gaming company created a game leaderboard by using a Multi-AZ deployment of an Amazon RDS database. The number of users is growing, and the queries to get individual player

rankings are getting slower over time. The company expects a surge in users for an upcoming version and wants to optimize the design for scalability and performance.
Which solution will meet these requirements?
(A). Migrate the database to Amazon DynamoDB. Store the leader different tables. Use Apache HiveQL JOIN statements to build the leaderboard
(B). Keep the leaderboard data in the RDS DB instance. Provision a Multi-AZ deployment of an Amazon ElastiCache for Redis cluster.
(C). Stream the leaderboard data by using Amazon Kinesis Data Firehose with an Amazon S3 bucket as the destination. Query the S3 bucket by using Amazon Athena for the leaderboard.
(D). Add a read-only replica to the RDS DB instance. Add an RDS Proxy database proxy.
Answer: A

NO.236 A company wants to migrate its data analytics environment from on premises to AWS The environment consists of two simple Node js applications One of the applications collects sensor data and loads it into a MySQL database The other application aggregates the data into reports When the aggregation jobs run. some of the load jobs fail to run correctly The company must resolve the data loading issue The company also needs the migration to occur without interruptions or changes for the company's customers What should a solutions architect do to meet these requirements'?
(A). Set up an Amazon Aurora MySQL database as a replication target for the on-premises database Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica Set up collection endpomts as AWS Lambda functions behind a Network Load Balancer (NLB). and use Amazon RDS Proxy to wnte to the Aurora MySQL database When the databases are synced disable the replication job and restart the Aurora Replica as the primary instance. Point the collector DNS record to the NLB.
(B). Set up an Amazon Aurora MySQL database Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora Move the aggregation jobs to run against the Aurora MySQL database Set up collection endpomts behind an Application Load Balancer (ALB) as Amazon EC2 instances in an Auto Scaling group When the databases are synced, point the collector DNS record to the ALB Disable the AWS DMS sync task after the cutover from on premises to AWS
(C). Set up an Amazon Aurora MySQL database Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora Create an Aurora Replica for the Aurora MySQL database and move the aggregation jobs to run against the Aurora Replica Set up collection endpoints as AWS Lambda functions behind an Application Load Balancer (ALB) and use Amazon RDS Proxy to write to the Aurora MySQL database When the databases are synced, point the collector DNS record to the ALB Disable the AWS DMS sync task after the cutover from on premises to AWS
(D). Set up an Amazon Aurora MySQL database Create an Aurora Replica for the Aurora MySQL database and move the aggregation jobs to run against the Aurora Replica Set up collection endpoints as an Amazon Kinesis data stream Use Amazon Kinesis Data Firehose to replicate the data to the Aurora MySQL database When the databases are synced disable the replication job and restart the Aurora Replica as the primary instance Point the collector DNS record to the Kinesis data stream.
Answer: C

NO.237 A solutions architect is working with a company that is extremely sensitive to its IT costs and wishes to implement controls that will result in a predictable AWS spend each month Which

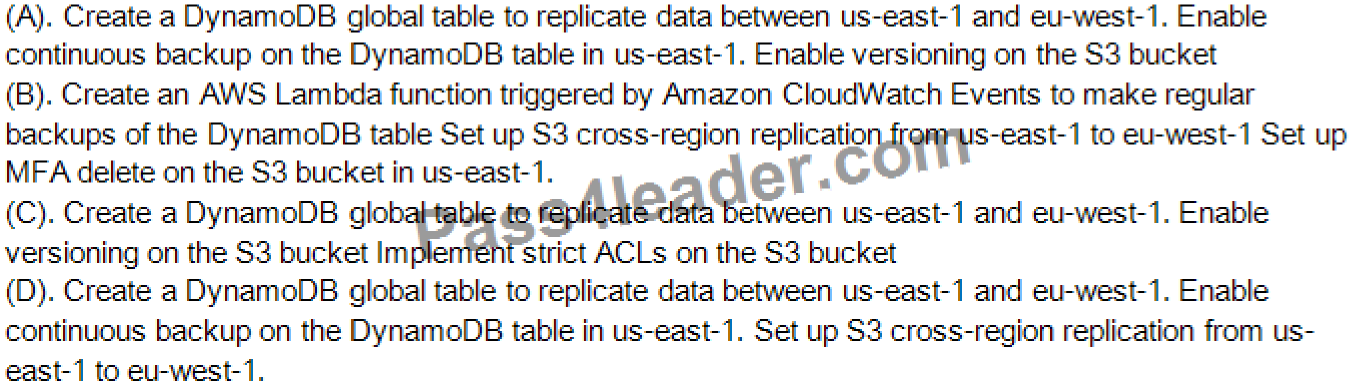
combination ot steps can help the company control and monitor its monthly AWS usage to achieve a cost that is as close as possible to the target amount? (Select THREE.)
(A). Implement an IAM policy that requires users to specify a 'workload' tag for cost allocation when launching Amazon EC2 instances
(B). Contact AWS Support and ask that they apply limits to the account so that users are not able to launch more than a certain number of instance types
(C). Purchase all upfront Reserved Instances that cover 100% of the account's expected Amazon EC2 usage
(D). Place conditions in the users' IAM policies that limit the number of instances they are able to launch
(E). Define 'workload' as a cost allocation tag in the AWS Billing and Cost Management console
(F). Set up AWS Budgets to alert and notify when a given workload is expected to exceed a defined cost
Answer: A,E,F

NO.238 A company has developed a new release of a popular video game and wants to make it available for public download. The new release package is approximately 5 GB in size. The company provides downloads for existing releases from a Linux-based, publicly facing FTP site hosted in an on-premises data center. The company expects the new release will be downloaded by users worldwide The company wants a solution that provides improved download performance and low transfer costs, regardless of a user's location.
Which solutions will meet these requirements?
(A). Store the game files on Amazon EBS volumes mounted on Amazon EC2 instances within an Auto Scaling group Configure an FTP service on the EC2 instances Use an Application Load Balancer in front of the Auto Scaling group. Publish the game download URL for users to download the package.
(B). Store the game files on Amazon EFS volumes that are attached to Amazon EC2 instances within an Auto Scaling group Configure an FTP service on each of the EC2 instances Use an Application Load Balancer in front of the Auto Scaling group Publish the game download URL for users to download the package
(C). Configure Amazon Route 53 and an Amazon S3 bucket for website hosting Upload the game files to the S3 bucket Use Amazon CloudFront for the website Publish the game download URL for users to download the package.
(D). Configure Amazon Route 53 and an Amazon S3 bucket for website hosting Upload the game files to the S3 bucket Set Requester Pays for the S3 bucket Publish the game download URL for users to download the package
Answer: C

NO.239 A company is processing videos in the AWS Cloud by using Amazon EC2 instances in an Auto Scaling group. It takes 30 minutes to process a video. Several EC2 instances scale in and out depending on the number of videos in an Amazon Simple Queue Service (Amazon SQS) queue.
The company has configured the SQS queue with a redrive policy that specifies a target dead-letter queue and a maxReceiveCount of 1. The company has set the visibility timeout for the SQS queue to 1 hour. The company has set up an Amazon CloudWatch alarm to notify the development team when there are messages in the dead-letter queue.
Several times during the day, the development team receives notification that messages are in the dead-letter queue and that videos have not been processed properly. An investigation finds no errors

in the application logs.
How can the company solve this problem?
(A). Turn on termination protection for the EC2 instances.
(B). Update the visibility timeout for the SOS queue to 3 hours.
(C). Configure scale-in protection for the instances during processing.
(D). Update the redrive policy and set maxReceiveCount to 0.
Answer: A

NO.240 A retail company is running an application that stores invoice files in an Amazon S3 bucket and metadata about the files in an Amazon DynamoDB table. The application software runs in both us-east-1 and eu-west-1 The S3 bucket and DynamoDB table are in us-east-1. The company wants to protect itself from data corruption and loss of connectivity to either Region Which option meets these requirements?



(A). Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable continuous backup on the DynamoDB table in us-east-1. Enable versioning on the S3 bucket
(B). Create an AWS Lambda function triggered by Amazon CloudWatch Events to make regular backups of the DynamoDB table Set up S3 cross-region replication from us-east-1 to eu-west-1 Set up MFA delete on the S3 bucket in us-east-1.
(C). Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable versioning on the S3 bucket Implement strict ACLs on the S3 bucket
(D). Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable continuous backup on the DynamoDB table in us-east-1. Set up S3 cross-region replication from us-east-1 to eu-west-1.

Answer: B

NO.241 A medical company is running an application in the AWS Cloud. The application simulates the effect of medical drugs in development.
The application consists of two parts configuration and simulation The configuration part runs in AWS Fargate containers in an Amazon Elastic Container Service (Amazon ECS) cluster. The simulation part runs on large, compute optimized Amazon EC2 instances Simulations can restart if they are interrupted The configuration part runs 24 hours a day with a steady load. The simulation part runs only for a few hours each night with a variable load. The company stores simulation results in Amazon S3, and researchers use the results for 30 days. The company must store simulations for 10 years and must be able to retrieve the simulations within 5 hours Which solution meets these requirements MOST cost-effectively?
(A). Purchase an EC2 Instance Savings Plan to cover the usage for the configuration part Run the simulation part by using EC2 Spot Instances Create an S3 Lifecycle policy to transition objects that are older than 30 days to S3 Intelligent-Tiering
(B). Purchase an EC2 Instance Savings Plan to cover the usage for the configuration part and the simulation part Create an S3 Lifecycle policy to transition objects that are older than 30 days to S3 Glacier
(C). Purchase Compute Savings Plans to cover the usage for the configuration part Run the simulation part by using EC2 Spot instances Create an S3 Lifecycle policy to transition objects that are older than 30 days to S3 Glacier
(D). Purchase Compute Savings Plans to cover the usage for the configuration part Purchase EC2 Reserved Instances for the simulation part Create an S3 Lifecycle policy to transition objects that are

older than 30 days to S3 Glacier Deep Archive
Answer: C

NO.242 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. Outbound internet traffic will be controlled by firewall appliances.
(B). A centralized shared VPC with a subnet for each account. Outbound internet traffic will controlled through a fleet of proxy servers.
(C). 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.
(D). A shared transit gateway to which each VPC will be attached. Outbound internet access will route through a fleet of VPN-attached firewalls.
Answer: D
https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/centralized-egress-to-internet.html
https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/centralized-egress-to-internet.html 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.

NO.243 A solution architect is designing an AWS account structure for a company that consists of multiple terms. All the team will work in the same AWS Region. The company needs a VPC that is connected to the on-premises network. The company expects less than 50 Mbps of total to and from the on-premises network.
Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO)
(A). Create an AWS CloudFormation template that provisions a VPC and the required subnets. Deploy the template to each AWS account
(B). Create an AWS CloudFormabon template that provisions a VPC and the required subnets. Deploy the template to a shared services account. Share the subnets by using AWS Resource Access Manage
r
(C). Use AWS Transit Gateway along with an AWS Site-to-Site VPN for connectivity to the on-premises network. Share the transit gateway by using AWS Resource Access Manager
(D). Use AWS Site-to-Site VPN for connectivity to the on-premises network
(E). Use AWS Direct Connect for connectivity to the on-premises network.
Answer: B,D

NO.244 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 RDS. and creating several additional read replicas to handle the load during end of month

(C). Using Amazon CioudWatch with AWS Lambda to change the type. size, or IOPS of Amazon EBS volumes in the cluster based on a specific CloudWatch metric

(D). 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

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.

NO.245 A company has a project that is launching Amazon EC2 instances that are larger than required. The project's account cannot be part of the company's organization in AWS Organizations due to policy restrictions to keep this activity outside of corporate IT. The company wants to allow only the launch of t3.small EC2 instances by developers in the project's account. These EC2 instances must be restricted to the us-east-2 Region.

What should a solutions architect do to meet these requirements?

(A). Create a new developer account. Move all EC2 instances, users, and assets into us-east-2. Add the account to the company's organization in AWS Organizations. Enforce a tagging policy that denotes Region affinity.

(B). Create an SCP that denies the launch of all EC2 instances except I3.small EC2 instances in us-east-2. Attach the SCP to the project's account.

(C). Create and purchase a t3.small EC2 Reserved Instance for each developer in us-east-2. Assign each developer a specific EC2 instance with their name as the tag.

(D). Create an IAM policy than allows the launch of only t3.small EC2 instances in us-east-2. Attach the policy to the roles and groups that the developers use in the project's account.

Answer: D

NO.246 A company that runs applications on AWS recently subscribed to a new software-as-a-service (SaaS) data vendor. The vendor provides the data by way of a REST API that the vendor hosts in its AWS environment The vendor offers multiple options for connectivity to the API and Is working with the company to find the best way to connect.

The company's AWS account does not allow outbound internet access from Its AWS environment The vendor's services run on AWS in the same AWS Region as the company's applications A solutions architect must Implement connectivity to the vendor's API so that the API is highly available In the company's VPC.

Which solution will meet these requirements?

(A). Connect to the vendor's public API address for the data service.

(B). Connect to the vendor by way of a VPC peering connection between the vendor's VPC and the company's VPC

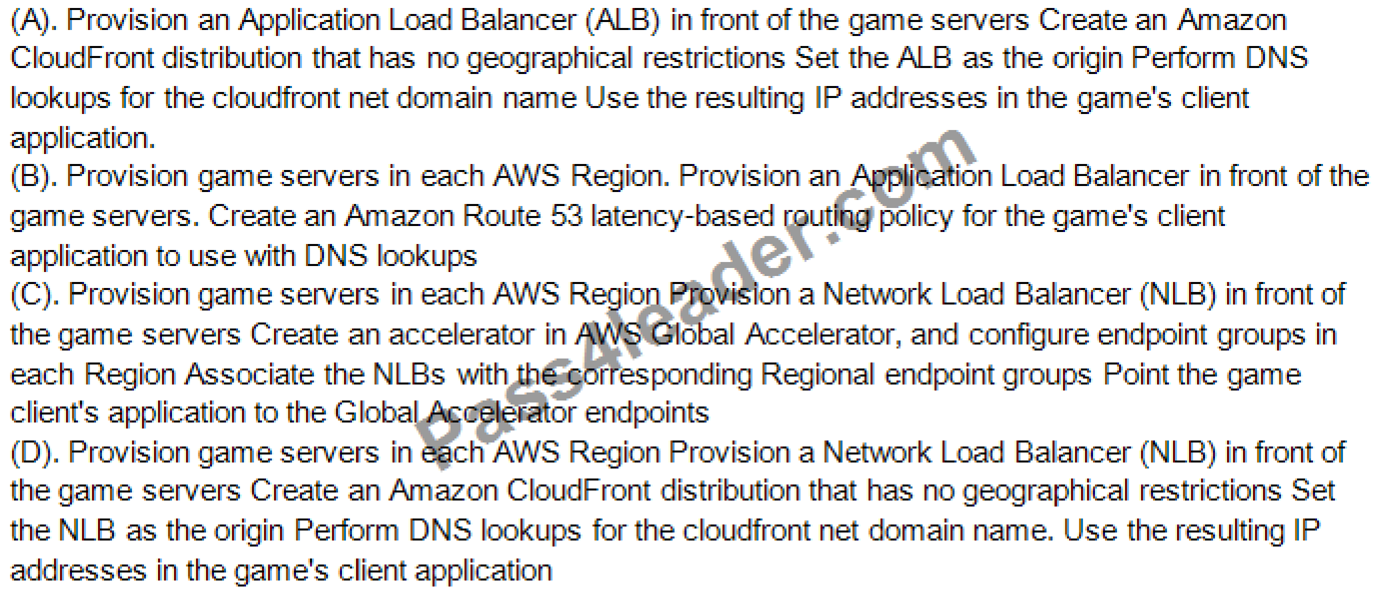
(C). Connect to the vendor by way of a VPC endpoint service that uses AWS PrivateLink
(D). Connect to a public bastion host that the vendor provides Tunnel the API traffic.
Answer: C

NO.247 A company is running a data-intensive application on AWS. The application runs on a cluster of hundreds of Amazon EC2 instances. A shared file system also runs on several EC2 instances that store 200 TB of dat a. The application reads and modifies the data on the shared file system and generates a report. The job runs once monthly, reads a subset of the files from the shared file system, and takes about 72 hours to complete. The compute instances scale in an Auto Scaling group, but the instances that host the shared file system run continuously. The compute and storage instances are all in the same AWS Region.
A solutions architect needs to reduce costs by replacing the shared file system instances. The file system must provide high performance access to the needed data for the duration of the 72-hour run.
Which solution will provide the LARGEST overall cost reduction while meeting these requirements?
(A). Migrate the data from the existing shared file system to an Amazon S3 bucket that uses the S3 Intelligent-Tiering storage class. Before the job runs each month, use Amazon FSx for Lustre to create a new file system with the data from Amazon S3 by using lazy loading. Use the new file system as the shared storage for the duration of the job. Delete the file system when the job is complete.
(B). Migrate the data from the existing shared file system to a large Amazon Elastic Block Store (Amazon EBS) volume with Multi-Attach enabled. Attach the EBS volume to each of the instances by using a user data script in the Auto Scaling group launch template. Use the EBS volume as the shared storage for the duration of the job. Detach the EBS volume when the job is complete.
(C). Migrate the data from the existing shared file system to an Amazon S3 bucket that uses the S3 Standard storage class. Before the job runs each month, use Amazon FSx for Lustre to create a new file system with the data from Amazon S3 by using batch loading. Use the new file system as the shared storage for the duration of the job. Delete the file system when the job is complete.
(D). Migrate the data from the existing shared file system to an Amazon S3 bucket. Before the job runs each month, use AWS Storage Gateway to create a file gateway with the data from Amazon S3. Use the file gateway as the shared storage for the job. Delete the file gateway when the job is complete.
Answer: B

NO.248 A company has built a high performance computing (HPC) cluster in AWS for a tightly coupled workload that generates a large number of shared files stored in Amazon EFS. The cluster was performing well when the number of Amazon EC2 instances in the cluster was 100. However, when the company increased the cluster size to 1,000 EC2 instances, overall performance was well below expectations Which collection of design choices should a solutions architect make to achieve the maximum performance from the HPC cluster? (Select THREE.)
(A). Ensure the HPC cluster is launched within a single Availability Zone.
(B). Launch the EC2 instances and attach elastic network interfaces in multiples of four.
(C). Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled
(D). Ensure the cluster is launched across multiple Availability Zones.
(E). Replace Amazon EFS with multiple Amazon EBS volumes in a RAID array.
(F). Replace Amazon EFS with Amazon FSx for Lustre.
Answer: A,C,E

NO.249 A finance company is storing financial records in an Amazon S3 bucket. The company persists a record for every financial transaction. According to regulatory requirements, the records cannot be modified for at least 1 year after they are written. The records are read on a regular basis and must be immediately accessible.
Which solution will meet these requirements?
(A). Create a new S3 bucket. Turn on S3 Object Lock, set a default retention period of 1 year, and set the retention mode to compliance mode. Store all records in the new S3 bucket.
(B). Create an S3 Lifecycle rule to immediately transfer new objects to the S3 Glacier storage tier Create an S3 Glacier Vault Lock policy that has a retention period of 1 year.
(C). Create an S3 Lifecycle rule to immediately transfer new objects to the S3 Intelligent-Tiering storage tier. Set a retention period of 1 year.
(D). Create an S3 bucket policy with a Deny action for PutObject operations with a condition where the s3:x-amz-object-retention header is not equal to 1 year.
Answer: A

NO.250 A mobile gaming company is expanding into the global market. The company's game servers run in the us-east-1 Region. The game's client application uses UDP to communicate with the game servers and needs to be able to connect to a set of static IP addresses.
The company wants its game to be accessible on multiple continents. The company also wants the game to maintain its network performance and global availability.
Which solution meets these requirements?



(A). Provision an Application Load Balancer (ALB) in front of the game servers Create an Amazon CloudFront distribution that has no geographical restrictions Set the ALB as the origin Perform DNS lookups for the cloudfront net domain name Use the resulting IP addresses in the game's client application.
(B). Provision game servers in each AWS Region. Provision an Application Load Balancer in front of the game servers. Create an Amazon Route 53 latency-based routing policy for the game's client application to use with DNS lookups
(C). Provision game servers in each AWS Region Provision a Network Load Balancer (NLB) in front of the game servers Create an accelerator in AWS Global Accelerator, and configure endpoint groups in each Region Associate the NLBs with the corresponding Regional endpoint groups Point the game client's application to the Global Accelerator endpoints
(D). Provision game servers in each AWS Region Provision a Network Load Balancer (NLB) in front of the game servers Create an Amazon CloudFront distribution that has no geographical restrictions Set the NLB as the origin Perform DNS lookups for the cloudfront net domain name. Use the resulting IP addresses in the game's client application

Answer: A

NO.251 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 complexly.
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: A,C,F

NO.252 An ecommerce website running on AWS uses an Amazon RDS for MySQL DB instance with General Purpose SSD storage. The developers chose an appropriate instance type based on demand, and configured 100 GB of storage with a sufficient amount of free space.
The website was running smoothly for a few weeks until a marketing campaign launched. On the second day of the campaign, users reported long wait times and time outs. Amazon CloudWatch metrics indicated that both reads and writes to the DB instance were experiencing long response times. The CloudWatch metrics show 40% to 50% CPU and memory utilization, and sufficient free storage space is still available. The application server logs show no evidence of database connectivity issues.
What could be the root cause of the issue with the marketing campaign?
(A). It exhausted the I/O credit balance due to provisioning low disk storage during the setup phase.
(B). It caused the data in the tables to change frequently, requiring indexes to be rebuilt to optimize queries.
(C). It exhausted the maximum number of allowed connections to the database instance.
(D). It exhausted the network bandwidth available to the RDS for MySQL DB instance.

Answer: A

"When using General Purpose SSD storage, your DB instance receives an initial I/O credit balance of 5.4 million I/O credits. This initial credit balance is enough to sustain a burst performance of 3,000 IOPS for 30 minutes."
https://aws.amazon.com/blogs/database/how-to-use-cloudwatch-metrics-to-decide-between-general-purpose-or-provisioned-iops-for-your-rds-database/

NO.253 A greeting card company recently advertised that customers could send cards to their favourite celebrities through the company's platform Since the advertisement was published, the platform has received constant traffic from 10.000 unique users each second.
The platform runs on m5.xlarge Amazon EC2 instances behind an Application Load Balancer (ALB) The instances run in an Auto Scaling group and use a custom AMI that is based on Amazon Linux. The platform uses a highly available Amazon Aurora MySQL DB cluster that uses primary and reader endpoints The platform also uses an Amazon ElastiCache for Redis cluster that uses its cluster endpoint The platform generates a new process for each customer and holds open database connections to MySQL for the duration of each customer's session However, resource usage for the platform is low.
Many customers are reporting errors when they connect to the platform Logs show that connections to the Aurora database are failing Amazon CloudWatch metrics show that the CPU load is tow across the platform and that connections to the platform are successful through the ALB.
Which solution will remediate the errors MOST cost-effectively?
(A). Set up an Amazon CloudFront distribution Set the ALB as the origin Move all customer traffic to the CloudFront distribution endpoint
(B). Use Amazon RDS Proxy Reconfigure the database connections to use the proxy

(C). Increase the number of reader nodes in the Aurora MySQL cluster
(D). Increase the number of nodes in the ElastiCache for Redis cluster
Answer: C

NO.254 A company is launching a new web application on Amazon EC2 instances. Development and production workloads exist in separate AWS accounts.
According to the company's security requirements, only automated configuration tools are allowed to access the production account. The company's security team wants to receive immediate notification if any manual access to the production AWS account or EC2 instances occurs Which combination of actions should a solutions architect take in the production account to meet these requirements? (Select THREE.)
(A). Turn on AWS CloudTrail logs in the application's primary AWS Region Use Amazon Athena to queiy the logs for AwsConsoleSignln events.
(B). Configure Amazon Simple Email Service (Amazon SES) to send email to the security team when an alarm is activated.
(C). Deploy EC2 instances in an Auto Scaling group Configure the launch template to deploy instances without key pairs Configure Amazon CloudWatch Logs to capture system access logs Create an Amazon CloudWatch alarm that is based on the logs to detect when a user logs in to an EC2 instance
(D). Configure an Amazon Simple Notification Service (Amazon SNS) topic to send a message to the security team when an alarm is activated
(E). Turn on AWS CloudTrail logs for all AWS Regions. Configure Amazon CloudWatch alarms to provide an alert when an AwsConsoleSignin event is detected.
(F). Deploy EC2 instances in an Auto Scaling group. Configure the launch template to delete the key pair after launch. Configure Amazon CloudWatch Logs for the system access logs Create an Amazon CloudWatch dashboard to show user logins over time.
Answer: C,D,E

NO.255 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. Include the necessary IAM roles for each administrator.
(B). Create the OrganizationAccountAccessPolicy IAM policy in each member account. Connect the member accounts to the management account by using cross-account access.
(C). Create the OrganizationAccountAccessRole IAM role in each member account. Grant permission to the management account to assume the IAM role.
(D). Create the OrganizationAccountAccessRole IAM role in the management account Attach the Administrator Access AWS managed policy to the IAM role. Assign the IAM role to the administrators in each member account.
Answer: C

NO.256 A company wants to migrate a 30 TB Oracle data warehouse from on premises to Amazon Redshift The company used the AWS Schema Conversion Tool (AWS SCT) to convert the schema of the existing data warehouse to an Amazon Redshift schema The company also used a migration assessment report to identify manual tasks to complete.

The company needs to migrate the data to the new Amazon Redshift cluster during an upcoming data freeze period of 2 weeks The only network connection between the on-premises data warehouse and AWS is a 50 Mops internet connection Which migration strategy meets these requirements?

(A). Create an AWS Database Migration Service (AWS DMS) replication instance. 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.

(B). Install the AWS SCT extraction agents on the on-premises servers. Define the extract, upload, and copy tasks to send the data to an Amazon S3 bucket. Copy the data into the Amazon Redshift cluster. Run the tasks at the beginning of the data freeze period.

(C). install the AWS SCT extraction agents on the on-premises servers. 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

(D). 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

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

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

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

NO.257 A solutions architect is designing an application to accept timesheet entries from employees on their mobile devices. Timesheets will be submitted weekly, with most of the submissions occurring on Friday. The data must be stored in a format that allows payroll administrators to run monthly reports. The infrastructure must be highly available and scale to match the rate of incoming data and reporting requests.

Which combination of steps meets these requirements while minimizing operational overhead? (Select TWO.)

(A). Deploy the application to Amazon EC2 On-Demand Instances With load balancing across multiple Availability Zones. Use scheduled Amazon EC2 Auto Scaling to add capacity before the high volume of submissions on Fridays.

(B). Deploy the application in a container using Amazon Elastic Container Service (Amazon ECS) with load balancing across multiple Availability Zones. Use scheduled Service Auto Scaling to add capacity before the high volume of submissions on Fridays.

(C). Deploy the application front end to an Amazon S3 bucket served by Amazon CloudFront. Deploy the application backend using Amazon API Gateway with an AWS Lambda proxy integration.

(D). Store the timesheet submission data in Amazon Redshift. Use Amazon OuickSight to generate the reports using Amazon Redshift as the data source.

(E). Store the timesheet submission data in Amazon S3. Use Amazon Athena and Amazon OuickSight to generate the reports using Amazon S3 as the data source.

Answer: A,E

NO.258 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

NO.259 A company is deploying a third-party firewall appliance solution from AWS Marketplace to monitor and protect traffic that leaves the company's AWS environments. The company wants to deploy this appliance into a shared services VPC and route all outbound internet-bound traffic through the appliances.

A solutions architect needs to recommend a deployment method that prioritizes reliability and minimizes failover time between firewall appliances within a single AWS Region. The company has set up routing from the shared services VPC to other VPCs.

Which steps should the solutions architect recommend to meet these requirements? (Select THREE)

(A). Deploy two firewall appliances into the shared services VPC. each in a separate Availability Zone

(B). Create a new Network Load Balancer in the shared services VPC Create a new target group, and attach it to the new Network Load Balancer Add each of the firewall appliance instances to the target group.

(C). Create a new Gateway Load Balancer in the shared services VPC Create a new target group, and attach it to the new Gateway Load Balancer Add each of the firewall appliance instances to the target group

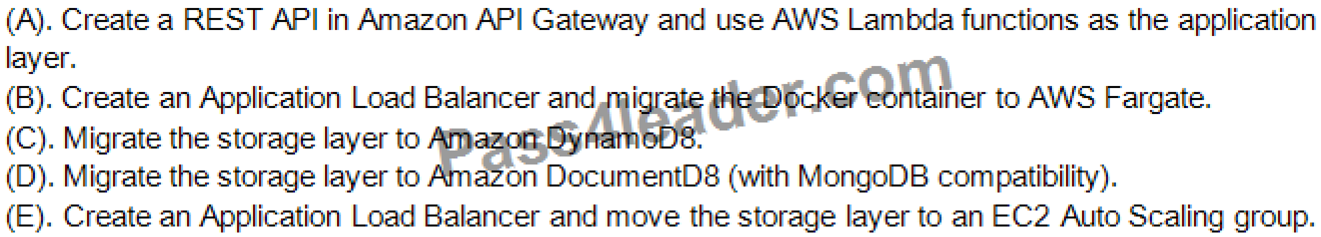
(D). Create a VPC interface endpoint Add a route to the route table in the shared services VPC. Designate the new endpoint as the next hop for traffic that enters the shared services VPC from other VPCs.

(E). Deploy two firewall appliances into the shared services VPC. each in the same Availability Zone

Answer: A,C

NO.260 A solutions architect is evaluating the reliability of a recently migrated application running on AWS. The front end is hosted on Amazon S3 and accelerated by Amazon CloudFront. The application layer is running in a stateless Docker container on an Amazon EC2 On-Demand Instance with an Elastic IP address. The storage layer is a MongoDB database running on an EC2 Reserved Instance in the same Availability Zone as the application layer.

Which combination of steps should the solutions architect take to eliminate single points of failure with minimal application code changes? (Select TWO.)



(A). Create a REST API in Amazon API Gateway and use AWS Lambda functions as the application layer.
(B). Create an Application Load Balancer and migrate the Docker container to AWS Fargate.
(C). Migrate the storage layer to Amazon DynamoD8.
(D). Migrate the storage layer to Amazon DocumentD8 (with MongoDB compatibility).
(E). Create an Application Load Balancer and move the storage layer to an EC2 Auto Scaling group.

Answer: B,D
https://aws.amazon.com/documentdb/?nc1=h_ls
https://aws.amazon.com/blogs/containers/using-alb-ingress-controller-with-amazon-eks-on-fargate/

NO.261 An enterprise company wants to allow its developers to purchase third-party software through AWS Marketplace. The company uses an AWS Organizations account structure with full features enabled, and has a shared services account in each organizational unit (OU) that will be used by procurement managers. The procurement team's policy indicates that developers should be able to obtain third-party software from an approved list only and use Private Marketplace in AWS Marketplace to achieve this requirement . The procurement team wants administration of Private Marketplace to be restricted to a role named procurement-manager-role, which could be assumed by procurement managers Other IAM users groups, roles, and account administrators in the company should be denied Private Marketplace administrative access What is the MOST efficient way to design an architecture to meet these requirements?
(A). Create an IAM role named procurement-manager-role in all AWS accounts in the organization Add the PowerUserAccess managed policy to the role Apply an inline policy to all IAM users and roles in every AWS account to deny permissions on the AWSPrivateMarketplaceAdminFullAccess managed policy.
(B). Create an IAM role named procurement-manager-role in all AWS accounts in the organization Add the AdministratorAccess managed policy to the role Define a permissions boundary with the AWSPrivateMarketplaceAdminFullAccess managed policy and attach it to all the developer roles.
(C). Create an IAM role named procurement-manager-role in all the shared services accounts in the organization Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role Create an organization root-level SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role Create another organization root-level SCP to deny permissions to create an IAM role named procurement-manager-role to everyone in the organization.
(D). Create an IAM role named procurement-manager-role in the AWS accounts that will be used by developers Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role. Create ....Organizations to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role Apply the SCP to all the shared services accounts in the.......
Answer: C

NO.262 A company is creating a sequel for a popular online game. A large number of users from all over the world will play the game within the first week after launch. Currently, the game consists of the following components deployed in a single AWS Region:
* Amazon S3 bucket that stores game assets
* Amazon DynamoDB table that stores player scores
A solutions architect needs to design a multi-Region solution that will reduce latency improve reliability, and require the least effort to implement What should the solutions architect do to meet

these requirements?
(A). Create an Amazon CloudFront distribution to serve assets from the S3 bucket Configure S3 Cross-Region Replication Create a new DynamoDB able in a new Region Use the new table as a replica target tor DynamoDB global tables.
(B). Create an Amazon CloudFront distribution to serve assets from the S3 bucket. Configure S3 Same-Region Replication. Create a new DynamoDB able m a new Region. Configure asynchronous replication between the DynamoDB tables by using AWS Database Migration Service (AWS DMS) with change data capture (CDC)
(C). Create another S3 bucket in a new Region and configure S3 Cross-Region Replication between the buckets Create an Amazon CloudFront distribution and configure origin failover with two origins accessing the S3 buckets in each Region. Configure DynamoDB global tables by enabling Amazon DynamoDB Streams, and add a replica table in a new Region.
(D). Create another S3 bucket in the same Region, and configure S3 Same-Region Replication between the buckets- Create an Amazon CloudFront distribution and configure origin failover with two origin accessing the S3 buckets Create a new DynamoDB table m a new Region Use the new table as a replica target for DynamoDB global tables.
Answer: C

NO.263 A company is running an application distributed over several Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer The security team requires that all application access attempts be made available for analysis Information about the client IP address, connection type, and user agent must be included.
Which solution will meet these requirements?
(A). Enable EC2 detailed monitoring, and include network logs Send all logs through Amazon Kinesis Data Firehose to an Amazon ElasDcsearch Service (Amazon ES) cluster that the security team uses for analysis.
(B). Enable VPC Flow Logs for all EC2 instance network interfaces Publish VPC Flow Logs to an Amazon S3 bucket Have the security team use Amazon Athena to query and analyze the logs
(C). Enable access logs for the Application Load Balancer, and publish the logs to an Amazon S3 bucket Have the security team use Amazon Athena to query and analyze the logs
(D). Enable Traffic Mirroring and specify all EC2 instance network interfaces as the source. 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
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html

NO.264 A company is running a two-tier web-based application in an on-premises data center. The application layer consists of a single server running a stateful application. The application connects to a PostgreSQL database running on a separate server The application's user base is expected to grow significantly, so the company is migrating the application and database to AWS The solution will use Amazon Aurora PostgreSQL. Amazon EC2 Auto Scaling, and Elastic Load Balancing.
Which solution will provide a consistent user experience that will allow the application and database tiers to scale?
(A). Enable Aurora Auto Scaling for Aurora Replicas. Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled

(B). Enable Aurora Auto Scaling for Aurora writers. Use an Application Load Balancer with the round robin routing algorithm and sticky sessions enabled
(C). Aurora Auto Scaling for Aurora Replicas. Use an Application Load Balancer with the round robin routing algorithm and sticky sessions enabled.
(D). Aurora Auto Scaling for Aurora writers. Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled.
Answer: C

NO.265 A company hosts a web application that tuns on a group of Amazon EC2 instances that ate behind an Application Load Balancer (ALB) in a VPC. The company wants to analyze the network payloads lo reverse-engineer a sophisticated attack of the application.
Which approach should the company take to achieve this goal?
(A). Enable VPC Flow Logs. Store the flow logs in an Amazon S3 bucket for analysis.
(B). Enable Traffic Mirroring on the network interface of the EC2 instances. Send the mirrored traffic lo a target for storage and analysis.
(C). Create an AWS WAF web ACL. and associate it with the ALB. Configure AWS WAF logging.
(D). Enable logging for the ALB. Store the logs in an Amazon S3 bucket for analysis.
Answer: A

NO.266 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 addresses Ensure that security groups for EC2 instances allow outbound access to port 53 on those DNS server IP addresses.
(B). Launch an EC2 instance that has DNS BIND installed and configured. 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.
(C). Create a new outbound endpoint in Route 53. and attach me endpoint to the VPC. 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 the on-premises DNS server.
(D). 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: C

NO.267 A company wants to host a new global website that consists of static content. A solutions architect is working on a solution that uses Amazon CloudFront with an origin access identity <OAI) to access website content that is stored in a private Amazon S3 bucket.
During testing, the solutions architect receives 404 errors from the S3 bucket. Error messages appear only for attempts to access paths that end with a forward slash. such as example.com/path/. These

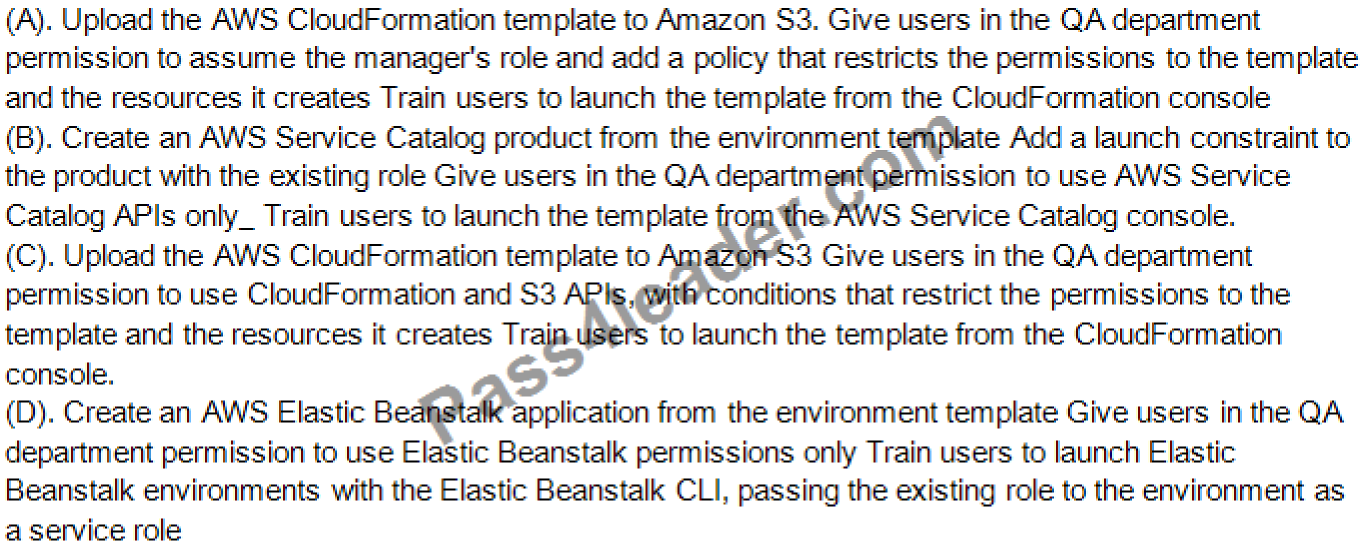
requests should return the existing S3 object path/index.html. Any potential solution must not prevent CloudFront from caching the content.
What should the solutions architect do to resolve this problem?
(A). Change the CloudFront origin to an Amazon API Gateway proxy endpoint. Rewrite the S3 request URL by using an AWS Lambda function.
(B). Change the CloudFront origin to an Amazon API Gateway endpoint. Rewrite the S3 request URL in an AWS service integration.
(C). Change the CloudFront configuration to use an AWS Lambda@Edge function that is invoked by a viewer request event to rewrite the S3 request URL.
(D). Change the CloudFront configuration to use an AWS Lambda@Edge function that is invoked by an origin request event to rewrite the S3 request URL.
Answer: C

NO.268 A financial services company receives a regular data feed from its credit card servicing partner Approximately 5.000 records are sent every 15 minutes in plaintext, delivered over HTTPS directly into an Amazon S3 bucket with server-side encryption. This feed contains sensitive credit card primary account number (PAN) data The company needs to automatically mask the PAN before sending the data to another S3 bucket for additional internal processing. The company also needs to remove and merge specific fields, and then transform the record into JSON format Additionally, extra feeds are likely to be added in the future, so any design needs to be easily expandable.
Which solutions will meet these requirements?
(A). Trigger an AWS Lambda function on file delivery that extracts each record and writes it to an Amazon SQS queue. Trigger another Lambda function when new messages arrive in the SOS queue to process the records, writing the results to a temporary location in Amazon S3. Trigger a final Lambda function once the SOS queue is empty to transform the records into JSON format and send the results to another S3 bucket for internal processing.
(B). Tigger an AWS Lambda function on file delivery that extracts each record and wntes it to an Amazon SOS queue. Configure an AWS Fargate container application to
(C). automatically scale to a single instance when the SOS queue contains messages. Have the application process each record, and transform the record into JSON format. When the queue is empty, send the results to another S3 bucket for internal processing and scale down the AWS Fargate instance.
(D). Create an AWS Glue crawler and custom classifier based on the data feed formats and build a table definition to match Trigger an AWS Lambda function on file delivery to start an AWS Glue ETL job to transform the entire record according to the processing and transformation requirements. Define the output format as JSON. Once complete, have the ETL job send the results to another S3 bucket for internal processing.
(E). Create an AWS Glue crawler and custom classifier based upon the data feed formats and build a table definition to match. Perform an Amazon Athena query on file delivery to start an Amazon EMR ETL job to transform the entire record according to the processing and transformation requirements. Define the output format as JSON. Once complete, send the results to another S3 bucket for internal processing and scale down the EMR cluster.
Answer: C
You can use a Glue crawler to populate the AWS Glue Data Catalog with tables. The Lambda function can be triggered using S3 event notifications when object create events occur. The Lambda function will then trigger the Glue ETL job to transform the records masking the sensitive data and modifying

the output format to JSON. This solution meets all requirements.
Create an AWS Glue crawler and custom classifier based on the data feed formats and build a table definition to match. Trigger an AWS Lambda function on file delivery to start an AWS Glue ETL job to transform the entire record according to the processing and transformation requirements. Define the output format as JSON. Once complete, have the ETL job send the results to another S3 bucket for internal processing.
https://docs.aws.amazon.com/glue/latest/dg/trigger-job.html
https://d1.awsstatic.com/Products/product-name/diagrams/product-page-diagram_Glue_Event-driven-ETL-Pipelines.e24d59bb79a9e24cdba7f43ffd234ec0482a60e2.png

NO.269 A company has an internal application running on AWS that is used to track and process shipments in the company's warehouse. Currently, after the system receives an order, it emails the staff the information needed to ship a package. Once the package is shipped, the staff replies to the email and the order is marked as shipped.
The company wants to stop using email in the application and move to a serverless application model.
Which architecture solution meets these requirements?
(A). Use AWS Batch to configure the different tasks required lo ship a package. Have AWS Batch trigger an AWS Lambda function that creates and prints a shipping label. Once that label is scanned. as it leaves the warehouse, have another Lambda function move the process to the next step in the AWS Batch job.B.
(B). When a new order is created, store the order information in Amazon SQS. Have AWS Lambda check the queue every 5 minutes and process any needed work. When an order needs to be shipped, have Lambda print the label in the warehouse. Once the label has been scanned, as it leaves the warehouse, have an Amazon EC2 instance update Amazon SOS.
(C). Update the application to store new order information in Amazon DynamoDB. 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. 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.
(D). Store new order information in Amazon EFS. Have instances pull the new information from the NFS and send that information to printers in the warehouse. 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

NO.270 A company has an application that uses Amazon EC2 instances in an Auto Scaling group. The quality assurance (QA) department needs to launch a large number of short-lived environments to test the application. The application environments are currently launched by the manager of the department using an AWS CloudFormation template To launch the stack, the manager uses a role with permission to use CloudFormation EC2. and Auto Scaling APIs. The manager wants to allow testers to launch their own environments, but does not want to grant broad permissions to each user
Which set up would achieve these goals?



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

Answer: B

NO.271 A company runs a software-as-a-service (SaaS) application on AWS. The application comets of AWS Lambda function and an Amazon RDS for MySQL Multi-AZ database During market events the application has a much higher workload than normal Users notice slow response times during the peak periods because of many database connections. The company needs to improve the scalable performance and availability of the database.
Which solution meets these requirements?
(A). Create an Amazon CloudWatch alarm action that triggers a Lambda function to add an Amazon RDS for MySQL read replica when resource utilization hits a threshold.
(B). Migrate the database to Amazon Aurora and add a read replica Add a database connection pool outside of the Lambda hardier function.
(C). Migrate the database to Amazon Aurora and add a read replica. Use Amazon Route 53 weighted records
(D). Migrate the database to Amazon Aurora and add an Aurora Replica. Configure Amazon RDS Proxy to manage database connection pools.

Answer: D

NO.272 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 bucket. Mount the NFS file share on each EC2 instance In the cluster.
(B). Provision a new Amazon Elastic File System (Amazon EFS) file system that uses General Purpose performance mode. Mount the EFS file system on each EC2 instance in the cluster.
(C). 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.
(D). Provision a new Amazon Elastic File System (Amazon EFS) file system that uses Max I/O performance mode. Mount the EFS file system on each EC2 instance in the cluster.

Answer: D

NO.273 A company runs an e-commerce platform with front-end and e-commerce tiers. Both tiers run on LAMP stacks with the front-end instances running behind a load balancing appliance that has a virtual offering on AWS Current*/, the operations team uses SSH to log in to the instances to maintain patches and address other concerns. The platform has recently been the target of multiple attacks, including.
* A DDoS attack.
* An SOL injection attack
* Several successful dictionary attacks on SSH accounts on the web servers The company wants to improve the security of the e-commerce platform by migrating to AWS. The company's solutions architects have decided to use the following approach;
* Code review the existing application and fix any SQL injection issues.
* Migrate the web application to AWS and leverage the latest AWS Linux AMI to address initial security patching.
* Install AWS Systems Manager to manage patching and allow the system administrators to run commands on all instances, as needed.
What additional steps will address all of the identified attack types while providing high availability and minimizing risk?
(A). Enable SSH access to the Amazon EC2 instances using a security group that limits access to specific IPs. Migrate on-premises MySQL to Amazon RDS Multi-AZ Install the third-party load balancer from the AWS Marketplace and migrate the existing rules to the load balancer's AWS instances Enable AWS Shield Standard for DDoS protection
(B). Disable SSH access to the Amazon EC2 instances. Migrate on-premises MySQL to Amazon RDS Multi-AZ Leverage an Elastic Load Balancer to spread the load and enable AWS Shield Advanced for protection. Add an Amazon CloudFront distribution in front of the website Enable AWS WAF on the distribution to manage the rules.
(C). Enable SSH access to the Amazon EC2 instances through a bastion host secured by limiting access to specific IP addresses. Migrate on-premises MySQL to a self-managed EC2 instance. Leverage an AWS Elastic Load Balancer to spread the load, and enable AWS Shield Standard for DDoS protection Add an Amazon CloudFront distribution in front of the website.
(D). Disable SSH access to the EC2 instances. Migrate on-premises MySQL to Amazon RDS Single-AZ. Leverage an AWS Elastic Load Balancer to spread the load Add an Amazon CloudFront distribution in front of the website Enable AWS WAF on the distribution to manage the rules.
Answer: B

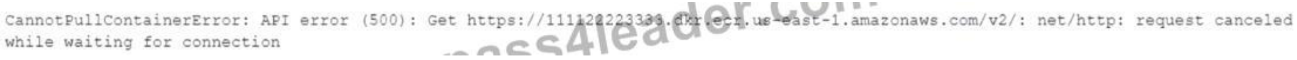
NO.274 A company has an Amazon VPC that is divided into a public subnet and a pnvate subnet. A web application runs in Amazon VPC. and each subnet has its own NACL The public subnet has a CIDR of 10.0.0 0/24 An Application Load Balancer is deployed to the public subnet The private subnet has a CIDR of 10.0.1.0/24. Amazon EC2 instances that run a web server on port 80 are launched into the private subnet Onty network traffic that is required for the Application Load Balancer to access the web application can be allowed to travel between the public and private subnets What collection of rules should be written to ensure that the private subnet's NACL meets the requirement? (Select TWO.)
(A). An inbound rule for port 80 from source 0.0 0.0/0
(B). An inbound rule for port 80 from source 10.0 0 0/24

(C). An outbound rule for port 80 to destination 0.0.0.0/0
(D). An outbound rule for port 80 to destination 10.0.0.0/24
(E). An outbound rule for ports 1024 through 65535 to destination 10.0.0.0/24

Answer: B,E

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

NO.275 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

NO.276 A large multinational company runs a timesheet application on AWS that is used by staff across the world The application runs on Amazon EC2 instances in an Auto Scaling group behind an Elastic Load Balancing (ELB) load balancer, and stores data in an Amazon RDS MySQL Multi-AZ database instance.

The CFO is concerned about the impact on the business if the application is not available The application must not be down for more than two hours, but the solution must be as cost-effective as possible How should the solutions architect meet the CFO's requirements while minimizing data loss?
(A). In another region, configure a read replica and create a copy of the infrastructure When an issue occurs, promote the read replica and configure as an Amazon RDS Multi-AZ database instance Update the DNS record to point to the other region's ELB
(B). Configure a 1-day window of 60-minute snapshots of the Amazon RDS Multi-AZ database instance Create an AWS CloudFormation template of the application infrastructure that uses the latest snapshot When an issue occurs use the AWS CloudFormation template to create the environment in another region Update the DNS record to point to the other region's ELB.
(C). Configure a 1-day window of 60 minute snapshots of the Amazon RDS Multi-AZ database instance which is copied to another region Create an AWS CloudFormation template of the application infrastructure that uses the latest copied snapshot When an issue occurs, use the AWS CloudFormation template to create the environment in another region Update the DNS record to point to the other region's ELB
(D). Configure a read replica in another region Create an AWS CloudFormation template of the application infrastructure When an issue occurs, promote the read replica and configure as an Amazon RDS Multi-AZ database instance and use the AWS CloudFormation template to create the environment in another region using the promoted Amazon RDS instance Update the DNS record to point to the other region's ELB

Answer: D

NO.277 A media company has a 30-TB repository of digital news videos These videos are stored on tape in an on-premises tape library and referenced by a Media Asset Management (MAM) system The company wants to enrich the metadata for these videos in an automated fashion and put them into a searchable catalog by using a MAM feature The company must be able to search based on information in the video such as objects scenery items or people's faces A catalog is available that contains faces of people who have appeared in the videos that include an image of each person The company would like to migrate these videos to AWS The company has a high-speed AWS Direct Connect connection with AWS and would like to move the MAM solution video content directly from its current file system How can these requirements be met by using the LEAST amount of ongoing management overhead and causing MINIMAL disruption to the existing system"'

(A). Set up an AWS Storage Gateway file gateway appliance on-premises. Use the MAM solution to extract the videos from the current archive and push them into the file gateway Use the catalog of faces to build a collection in Amazon Rekognition Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Rekognition pull the video from the Amazon S3 files backing the file gateway, retrieve the required metadata and push the metadata into the MAM solution

(B). Set up an AWS Storage Gateway tape gateway appliance on-premises Use the MAM solution to extract the videos from the current archive and push them into the tape gateway Use the catalog of faces to build a collection in Amazon Rekognition Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Amazon Rekognition process the video in the tape gateway retrieve the required metadata, and push the metadata into the MAM solution

(C). Configure a video ingestion stream by using Amazon Kinesis Video Streams Use the catalog of faces to build a collection in Amazon Rekognition Stream the videos from the MAM solution into Kinesis Video Streams Configure Amazon Rekognition to process the streamed videos Then, use a stream consumer to retrieve the required metadata and push the metadata into the MAM solution Configure the stream to store the videos in Amazon S3

(D). Set up an Amazon EC2 instance that runs the OpenCV libranes Copy the videos, images, and face catalog from the on-premises library into an Amazon EBS volume

Answer: C

mounted on this EC2 instance Process the videos to retrieve the required metadata, and push the metadata into the MAM solution, while also copying the video files to an Amazon S3 bucket

NO.278 A company has an on-premises Microsoft SQL Server database that writes a nightly 200 GB export to a local drive. The company wants to move the backups to more robust cloud storage on Amazon S3. The company has set up a 10 Gbps AWS Direct Connect connection between the on-premises data center and AWS. Which solution meets these requirements Most cost effectively?

(A). Create a new S3 bucket Deploy an AWS Storage Gateway file gateway within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to the new SMB file share.

(B). Create an Amzon FSx for Windows File Server Single-AZ file system within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to an SMB file share on the Amazon FSx file system Enable backups.

(C). Create an Amazon FSx for Windows File Server Multi-AZ system within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to an SMB file share on the Amazon FSx file system. Enable nightly backups.

(D). Create a new S3 buckets. Deploy an AWS Storage Gateway volume gateway within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to the new SMB file share on the volume gateway, and automate copies of this data to an S3 bucket.

Answer: A

NO.279 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

NO.280 A company has developed a web application. The company is hosting the application on a group of Amazon EC2 instances behind an Application Load Balancer. The company wants to improve the security posture of the application and plans to use AWS WAF web ACLs. The solution must not adversely affect legitimate traffic to the application.
How should a solutions architect configure the web ACLs to meet these requirements?
(A). Set the action of the web ACL rules to Count. Enable AWS WAF logging Analyze the requests for false positives Modify the rules to avoid any false positive Over time change the action of the web ACL rules from Count to Block.
(B). Use only rate-based rules in the web ACLs. and set the throttle limit as high as possible Temporarily block all requests that exceed the limit. Define nested rules to narrow the scope of the rate tracking.
(C). Set the action o' the web ACL rules to Block. Use only AWS managed rule groups in the web ACLs Evaluate the rule groups by using Amazon CloudWatch metrics with AWS WAF sampled requests or AWS WAF logs.
(D). Use only custom rule groups in the web ACLs. and set the action to Allow Enable AWS WAF logging Analyze the requests tor false positives Modify the rules to avoid any false positive Over time, change the action of the web ACL rules from Allow to Block.

Answer: B

NO.281 A solutions architect has deployed a web application that serves users across two AWS Regions under a custom domain The application uses Amazon Route 53 latency-based routing The solutions architect has associated weighted record sets with a pair of web servers in separate Availability Zones for each Region The solutions architect runs a disaster recovery scenario When all the web servers in one Region are stopped Route 53 does not automatically redirect users to the other Region Which of the following are possible root causes of this issue? (Select TWO.)
(A). The weight for the Region where the web servers were stopped is higher than the weight for the other Region
(B). One of the web servers in the secondary Region did not pass its HTTP health check
(C). Latency resource record sets cannot be used in combination with weighted resource record sets
(D). The setting to evaluate target health is not turned on for the latency alias resource record set that is associated with the domain in the Region where the web servers were stopped
(E). An HTTP health check has not been set up for one or more of the weighted resource record sets associated with the stopped web servers
Answer: A,E

NO.282 A company has 50 AWS accounts that are members of an organization in AWS Organizations Each account contains multiple VPCs The company wants to use AWS Transit Gateway to establish connectivity between the VPCs in each member account Each time a new member account is created, the company wants to automate the process of creating a new VPC and a transit gateway attachment.
Which combination of steps will meet these requirements? (Select TWO)
(A). From the management account, share the transit gateway with member accounts by using AWS Resource Access Manager
(B). Prom the management account, share the transit gateway with member accounts by using an AWS Organizations SCP
(C). Launch an AWS CloudFormation stack set from the management account that automatical^/ creates a new VPC and a VPC transit gateway attachment in a member account. Associate the attachment with the transit gateway in the management account by using the transit gateway ID.
(D). Launch an AWS CloudFormation stack set from the management account that automatical^ creates a new VPC and a peering transit gateway attachment in a member account. Share the attachment with the transit gateway in the management account by using a transit gateway service-linked role.
(E). From the management account, share the transit gateway with member accounts by using AWS Service Catalog
Answer: A,C

NO.283 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 dat a. 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 EMR. Allow data access patterns to remain the same.
(B). 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.

(C). Move the data to Amazon S3 and use Amazon Athena to query the data for reports. Allow the data scientists to access the data directly in Amazon S3.
(D). Migrate the data to Amazon DynamoDB and modify the reports to fetch data from DynamoDB. Allow the data scientists to access the data directly in DynamoDB.

Answer: C

"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 tit will be: "occasional access for data scientists to retrieve data"

NO.284 A company is storing data on premises on a Windows file server. The company produces 5 GB of new data daily.
The company migrated part of its Windows-based workload to AWS and needs the data to be available on a file system in the cloud. The company already has established an AWS Direct Connect connection between the on-premises network and AWS.
Which data migration strategy should the company use?
(A). Use the file gateway option in AWS Storage Gateway to replace the existing Windows file server, and point the existing file share to the new file gateway.
(B). Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon FSx.
(C). Use AWS Data Pipeline to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS).
(D). Use AWS DataSync to schedule a daily task lo replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS),

Answer: B

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

NO.285 A solutions architect is designing a solution to connect a company's on-premises network with all the company's current and future VPCs on AWS The company is running VPCs in five different AWS Regions and has at least 15 VPCs in each Region.
The company's AWS usage is constantly increasing and will continue to grow Additionally, all the VPCs throughout all five Regions must be able to communicate with each other The solution must maximize scalability and ease of management Which solution meets these requirements'?
(A). Set up a transit gateway in each Region Establish a redundant AWS Site-to-Site VPN connection between the on-premises firewalls and the transit gateway in the Region that is closest to the on-premises network Peer all the transit gateways with each other Connect all the VPCs to the transit gateway in their Region

(B). Create an AWS CloudFormation template for a redundant AWS Site-to-Site VPN tunnel to the on-premises network Deploy the CloudFormation template for each VPC Set up VPC peering between all the VPCs for VPC-to-VPC communication
(C). Set up a transit gateway in each Region Establish a redundant AWS Site-to-Site VPN connection between the on-premises firewalls and each transit gateway Route traffic between the different Regions through the company's on-premises firewalls Connect all the VPCs to the transit gateway in their Region
(D). Create an AWS CloudFormation template for a redundant AWS Site-to-Site VPN tunnel to the on-premises network Deploy the CloudFormation template for each VPC Route traffic between the different Regions through the company's on-premises firewalls
Answer: A

NO.286 A solutions architect is designing a publicly accessible web application that is on an Amazon CloudFront distribution with an Amazon S3 website endpoint as the origin. When the solution is deployed, the website returns an Error 403: Access Denied message.
Which steps should the solutions architect take to correct the issue? (Select TWO.)
(A). Remove the S3 block public access option from the S3 bucket.
(B). Remove the requester pays option trom the S3 bucket.
(C). Remove the origin access identity (OAI) from the CloudFront distribution.
(D). Change the storage class from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA).
(E). Disable S3 object versioning.
Answer: A,C
See using S3 to host a static website with Cloudfront:
https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/
- Using a REST API endpoint as the origin, with access restricted by an origin access identity (OAI)
- Using a website endpoint as the origin, with anonymous (public) access allowed
- Using a website endpoint as the origin, with access restricted by a Referer header

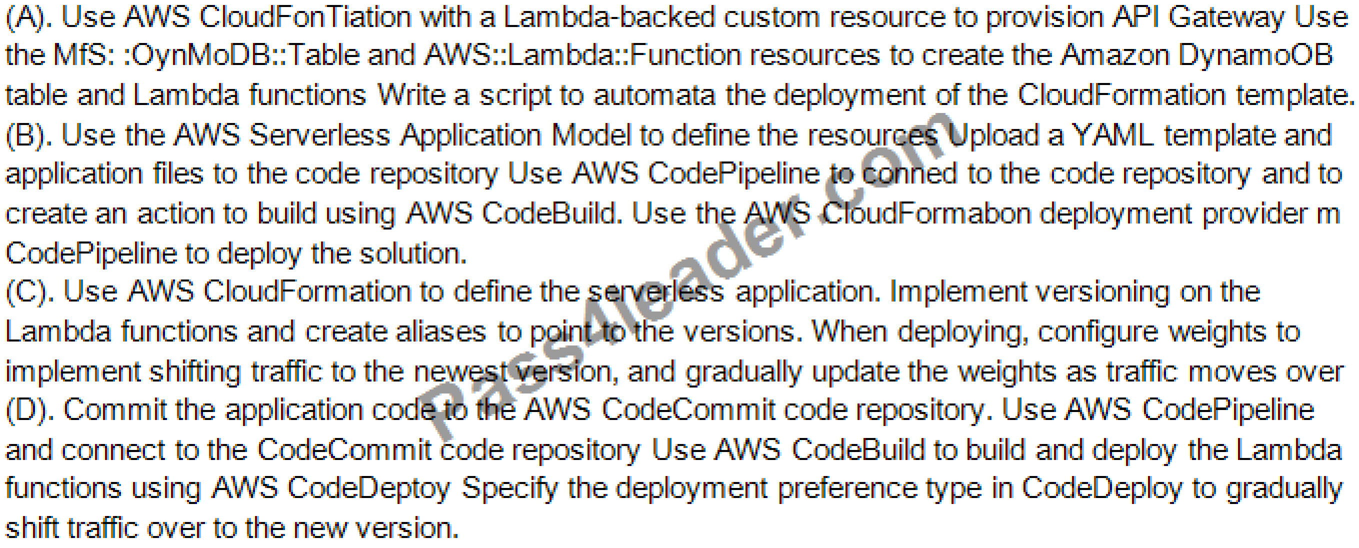
NO.287 A company has a web application that securely uploads pictures and videos to an Amazon S3 bucket The company requires that only authenticated users are allowed to post content T.he application generates a presigned URL that is used to upload objects through a browser interface. Most users are reporting slow upload times for objects larger than 100 MB What can a solutions architect do to improve the performance of these uploads while ensuring only authenticated users are allowed to post content?
(A). Set up an Amazon API Gateway with an edge-optimized API endpoint that has a resource as an S3 service proxy Configure the PUT method for this resource to expose the S3 Putobject operation Secure the API Gateway using a cognito_user_pools authonzer Have the browser interface use API Gateway instead of the presigned URL to upload objects
(B). Set up an Amazon API Gateway with a regional API endpoint that has a resource as an S3 service proxy Configure the PUT method for this resource to expose the S3 Putobject operation Secure the API Gateway using an AWS Lambda authonzer Have the browser interface use API Gateway instead of the presigned URL to upload objects
(C). Enable an S3 Transfer Acceleration endpoint on the S3 bucket Use the endpoint when generating the presigned URL Have the browser interface upload the objects to this URL using the S3 multipart upload API
(D). Configure an Amazon CloudFront distribution for the destination S3 bucket Enable PUT and POST

methods for the CloudFront cache behavior Update the CloudFront origin to use an origin access identity (OAI) Give the OAI user s 3: Putobject permissions in the bucket policy Have the browser interface upload objects using the CloudFront distribution
Answer: D

NO.288 An ecommerce company runs its infrastructure on AWS. The company exposes its APIs to its web and mobile clients through an Application Load Balancer (ALB) in front of an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The EKS cluster runs thousands of pods that provide the APIs.
After extending delivery to a new continent, the company adds an Amazon CloudFront distribution and sets the ALB as the origin. The company also adds AWS WAF to its architecture.
After implementation of the new architecture, API calls are significantly. However, there is a sudden increase in HTTP status code 504 (Gateway Timeout) errors and HTTP status code 502 (Bad Gateway) errors. This increase in errors seems to be for a specific domain. Which factors could be a cause of these errors? (Select TWO.)
(A). AWS WAF is blocking suspicious requests.
(B). The origin is not properly configured in CloudFront.
(C). There is an SSL/TLS handshake issue between CloudFront and the origin.
(D). EKS Kubernetes pods are being cycled.
(E). Some pods are taking more than 30 seconds to answer API calls.
Answer: A,E

NO.289 An auction website enables users to bid on collectible items The auction rules require that each bid is processed only once and in the order it was received The current implementation is based on a fleet of Amazon EC2 web servers that write bid records into Amazon Kinesis Data Streams A single 12 large instance has a cron job that runs the bid processor, which reads incoming bids from Kinesis Data Streams and processes each bid The auction site is growing in popularity, but users are complaining that some bids are not registering Troubleshooting indicates that the bid processor is too slow during peak demand hours sometimes crashes while processing and occasionally loses track of which record is being processed What changes should make the bid processing more reliable?
(A). Refactor the web application to use the Amazon Kinesis Producer Library (KPL) when posting bids to Kinesis Data Streams Refactor the bid processor to flag each record in Kinesis Data Streams as being unread processing and processed At the start of each bid processing run; scan Kinesis Data Streams for unprocessed records
(B). Refactor the web application to post each incoming bid to an Amazon SNS topic in place of Kinesis Data Streams Configure the SNS topic to trigger an AWS Lambda function that B. processes each bid as soon as a user submits it
(C). Refactor the web application to post each incoming bid to an Amazon SQS FIFO queue in place of Kinesis Data Streams Refactor the bid processor to continuously consume the SQS queue Place the bid processing EC2 instance in an Auto Scaling group with a minimum and a maximum size of 1
(D). Switch the EC2 instance type from t2 large to a larger general compute instance type Put the bid processor EC2 instances in an Auto Scaling group that scales out the number of EC2 instances running the bid processor based on the incomingRecords metric in Kinesis Data Streams
Answer: C
https://aws.amazon.com/sqs/faqs/#:~:text=A%20single%20Amazon%20SQS%20message,20%2C000%20for%20a%20FIFO%20queue.

NO.290 A development team s Deploying new APIs as serverless applications within a company. The team is currently using the AWS Maragement 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 serveriess APIs How can this be accomplished?



(A). Use AWS CloudFonTiation with a Lambda-backed custom resource to provision API Gateway Use the MfS: :OynMoDB::Table and AWS::Lambda::Function resources to create the Amazon DynamoOB table and Lambda functions Write a script to automata 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 conned to the code repository and to create an action to build using AWS CodeBuild. Use the AWS CloudFormabon deployment provider m CodePipeline to deploy the solution.
(C). Use AWS CloudFormation to define the serverless application. Implement versioning on the Lambda functions and create aliases to point to the versions. When deploying, configure weights to implement shifting traffic to the newest version, and gradually update the weights as traffic moves over
(D). Commit the application code to the AWS CodeCommit code repository. Use AWS CodePipeline and connect to the CodeCommit code repository Use AWS CodeBuild to build and deploy the Lambda functions using AWS CodeDeptoy Specify the deployment preference type in CodeDeploy to gradually shift traffic over to the new version.

Answer: B