

## SAP-C01 Dumps

### AWS Certified Solutions Architect- Professional

<https://www.certleader.com/SAP-C01-dumps.html>



**NEW QUESTION 1**

A company is currently running a production workload on AWS that is very I/O intensive. Its workload consists of a single tier with 10 c4.8xlarge instances, each with 2 TB gp2 volumes. The number of processing jobs has recently increased, and latency has increased as well. The team realizes that they are constrained on the IOPS. For the application to perform efficiently, they need to increase the IOPS by 3,000 for each of the instances. Which of the following designs will meet the performance goal MOST cost effectively?

- A. Change the type of Amazon EBS volume from gp2 to io1 and set provisioned IOPS to 9,000.
- B. Increase the size of the gp2 volumes in each instance to 3 TB.
- C. Create a new Amazon EFS file system and move all the data to this new file system
- D. Mount this file system to all 10 instances.
- E. Create a new Amazon S3 bucket and move all the data to this new bucket
- F. Allow each instance to access this S3 bucket and use it for storage.

**Answer: B**

**NEW QUESTION 2**

A group of Amazon EC2 instances have been configured as high performance computing (HPC) cluster. The instances are running in a placement group, and are able to communicate with each other at network of up to 20 Gbps.

The cluster needs to communicate with a control EC2 instance outside of the placement group. The control instance has the same instance type and AMI as the other instances, and is configured with a public IP address.

How can the Solutions Architect improve the network speeds between the control instance and the instances in the placement group?

- A. Terminate the control instance and relaunch in the placement group.
- B. Ensure that the instances are communicating using the private IP addresses.
- C. Ensure that the control instance is using an Elastic Network Adapter.
- D. Move the control instance inside the placement group.

**Answer: D**

**Explanation:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

**NEW QUESTION 3**

A company receives clickstream data files to Amazon S3 every five minutes. A Python script runs as a cron job once a day on an Amazon EC2 instance to process each file and load it into a database hosted on Amazon RDS. The cron job takes 15 to 30 minutes to process 24 hours of data. The data consumers ask for the data be available as soon as possible.

Which solution would accomplish the desired outcome?

- A. Increase the size of the instance to speed up processing and update the schedule to run once an hour.
- B. Convert the cron job to an AWS Lambda function and trigger this new function using a cron job on an EC2 instance.
- C. Convert the cron job to an AWS Lambda function and schedule it to run once an hour using Amazon CloudWatch events.
- D. Create an AWS Lambda function that runs when a file is delivered to Amazon S3 using S3 event notifications.

**Answer: D**

**Explanation:**

<https://docs.aws.amazon.com/lambda/latest/dg/with-s3.html>

**NEW QUESTION 4**

An organization has two Amazon EC2 instances:

The first is running an ordering application and an inventory application.

The second is running a queuing system.

During certain times of the year, several thousand orders are placed per second. Some orders were lost when the queuing system was down. Also, the organization's inventory application has the incorrect quantity of products because some orders were processed twice.

What should be done to ensure that the applications can handle the increasing number of orders?

- A. Put the ordering and inventory applications into their own AWS Lambda function
- B. Have the ordering application write the messages into an Amazon SQS FIFO queue.
- C. Put the ordering and inventory applications into their own Amazon ECS containers and create an Auto Scaling group for each application
- D. Then, deploy the message queuing server in multiple Availability Zones.
- E. Put the ordering and inventory applications into their own Amazon EC2 instances, and create an Auto Scaling group for each application
- F. Use Amazon SQS standard queues for the incoming orders, and implement idempotency in the inventory application.
- G. Put the ordering and inventory applications into their own Amazon EC2 instance
- H. Write the incoming orders to an Amazon Kinesis data stream. Configure AWS Lambda to poll the stream and update the inventory application.

**Answer: C**

**Explanation:**

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/standard-queues.html>

**NEW QUESTION 5**

A company currently uses Amazon EBS and Amazon RDS for storage purposes. The company intends to use a pilot light approach for disaster recovery in a different AWS Region. The company has an RTO of 6 hours and an RPO of 24 hours.

Which solution would achieve the requirements with MINIMAL cost?

- A. Use AWS Lambda to create daily EBS and RDS snapshots, and copy them to the disaster recovery region
- B. Use Amazon Route 53 with active-passive failover configuration

- C. Use Amazon EC2 in an Auto Scaling group with the capacity set to 0 in the disaster recovery region.
- D. Use AWS Lambda to create daily EBS and RDS snapshots, and copy them to the disaster recovery region.
- E. Use Amazon Route 53 with active-active failover configuration.
- F. Use Amazon EC2 in an AutoScaling group configured in the same way as in the primary region.
- G. Use Amazon ECS to handle long-running tasks to create daily EBS and RDS snapshots, and copy to the disaster recovery region.
- H. Use Amazon Route 53 with active-passive failover configuration.
- I. Use Amazon EC2 in an Auto Scaling group with the capacity set to 0 in the disaster recovery region.
- J. Use EBS and RDS cross-region snapshot copy capability to create snapshots in the disaster recovery region.
- K. Use Amazon Route 53 with active-active failover configuration.
- L. Use Amazon EC2 in an Auto Scaling group with the capacity set to 0 in the disaster recovery region.

**Answer:** A

**Explanation:**

[https://docs.aws.amazon.com/AmazonECS/latest/developerguide/scheduling\\_tasks.html](https://docs.aws.amazon.com/AmazonECS/latest/developerguide/scheduling_tasks.html)

**NEW QUESTION 6**

As a part of building large applications in the AWS Cloud, the Solutions Architect is required to implement the perimeter security protection. Applications running on AWS have the following endpoints:

- Application Load Balancer
- Amazon API Gateway regional endpoint
- Elastic IP address-based EC2 instances.
- Amazon S3 hosted websites.
- Classic Load Balancer

The Solutions Architect must design a solution to protect all of the listed web front ends and provide the following security capabilities:

- DDoS protection
- SQL injection protection
- IP address whitelist/blacklist
- HTTP flood protection
- Bad bot scraper protection

How should the Solutions Architect design the solution?

- A. Deploy AWS WAF and AWS Shield Advanced on all web endpoint
- B. Add AWS WAF rules to enforce the company's requirements.
- C. Deploy Amazon CloudFront in front of all the endpoint
- D. The CloudFront distribution provides perimeter protection
- E. Add AWS Lambda-based automation to provide additional security.
- F. Deploy Amazon CloudFront in front of all the endpoint
- G. Deploy AWS WAF and AWS Shield Advanced
- H. Add AWS WAF rules to enforce the company's requirement
- I. Use AWS Lambda to automate and enhance the security posture.
- J. Secure the endpoints by using network ACLs and security groups and adding rules to enforce the company's requirement
- K. Use AWS Lambda to automatically update the rules.

**Answer:** C

**NEW QUESTION 7**

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 developed 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 in 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
- B. Make sure that the rest of the steps in the runbook are updated to reflect any changes that may come from the AWS migration.
- C. Write a Python script that uses the AWS API to create the VPC, the EC2 instances, and the RDS instance for the application
- D. Write shell scripts that implement the rest of the steps in the runbook
- E. Have the Python script copy and run the shell scripts on the newly created instances to complete the installation.
- F. Write an AWS CloudFormation template that creates the VPC, the EC2 instances, and the RDS instance for the application
- G. Ensure that the rest of the steps in the runbook are updated to reflect any changes that may come from the AWS migration.
- H. Write an AWS CloudFormation template that creates the VPC, the EC2 instances, and the RDS instance for the application
- I. Include EC2 user data in the AWS CloudFormation template to install and configure the software.

**Answer: D**

#### NEW QUESTION 8

A company runs its containerized batch jobs on Amazon ECS. The jobs are scheduled by submitting a container image, a task definition, and the relevant data to an Amazon S3 bucket. Container images may be unique per job. Running the jobs as quickly as possible is of utmost importance, so submitting jobs artifacts to the S3 bucket triggers the job to run immediately. Sometimes there may be no jobs running at all. However, jobs of any size can be submitted with no prior warning to the IT Operations team. Job definitions include CPU and memory resource requirements.

What solution will allow the batch jobs to complete as quickly as possible after being scheduled?

- A. Schedule the jobs on an Amazon ECS cluster using the Amazon EC2 launch type
- B. Use Service Auto Scaling to increase or decrease the number of running tasks to suit the number of running jobs.
- C. Schedule the jobs directly on EC2 instance
- D. Use Reserved Instances for the baseline minimum load, and use On-Demand Instances in an Auto Scaling group to scale up the platform based on demand.
- E. Schedule the jobs on an Amazon ECS cluster using the Fargate launch type
- F. Use Service Auto Scaling to increase or decrease the number of running tasks to suit the number of running jobs.
- G. Schedule the jobs on an Amazon ECS cluster using the Fargate launch type
- H. Use Spot Instances in an Auto Scaling group to scale the platform based on demand
- I. Use Service Auto Scaling to increase or decrease the number of running tasks to suit the number of running jobs.

**Answer: C**

#### NEW QUESTION 9

A large company has increased its utilization of AWS over time in an unmanaged way. As such, they have a large number of independent AWS accounts across different business units, projects, and environments. The company has created a Cloud Center of Excellence team, which is responsible for managing all aspects of the AWS Cloud, including their AWS accounts.

Which of the following should the Cloud Center of Excellence team do to BEST address their requirements in a centralized way? (Select two.)

- A. Control all AWS account root user credentials
- B. Assign AWS IAM users in the account of each user who needs to access AWS resources
- C. Follow the policy of least privilege in assigning permissions to each user.
- D. Tag all AWS resources with details about the business unit, project, and environment
- E. Send all AWS Cost and Usage reports to a central Amazon S3 bucket, and use tools such as Amazon Athena and Amazon QuickSight to collect billing details by business unit.
- F. Use the AWS Marketplace to choose and deploy a Cost Management tool
- G. Tag all AWS resources with details about the business unit, project, and environment
- H. Send all AWS Cost and Usage reports for the AWS accounts to this tool for analysis.
- I. Set up AWS Organization
- J. Enable consolidated billing, and link all existing AWS accounts to a master billing account
- K. Tag all AWS resources with details about the business unit, project and environment
- L. Analyze Cost and Usage reports using tools such as Amazon Athena and Amazon QuickSight to collect billing details by business unit.
- M. Using a master AWS account, create IAM users within the master account
- N. Define IAM roles in the other AWS accounts, which cover each of the required functions in the account
- O. Follow the policy of least privilege in assigning permissions to each role, then enable the IAM users to assume the roles that they need to use.

**Answer: DE**

#### NEW QUESTION 10

A company is migrating a subset of its application APIs from Amazon EC2 instances to run on a serverless infrastructure. The company has set up Amazon API Gateway, AWS Lambda, and Amazon DynamoDB for the new application. The primary responsibility of the Lambda function is to obtain data from a third-party Software as a Service (SaaS) provider. For consistency, the Lambda function is attached to the same virtual private cloud (VPC) as the original EC2 instances. Test users report an inability to use this newly moved functionality, and the company is receiving 5xx errors from API Gateway. Monitoring reports from the SaaS provider shows that the requests never made it to its systems. The company notices that Amazon CloudWatch Logs are being generated by the Lambda functions. When the same functionality is tested against the EC2 systems, it works as expected.

What is causing the issue?

- A. Lambda is in a subnet that does not have a NAT gateway attached to it to connect to the SaaS provider.
- B. The end-user application is misconfigured to continue using the endpoint backed by EC2 instances.
- C. The throttle limit set on API Gateway is too low and the requests are not making their way through.
- D. API Gateway does not have the necessary permissions to invoke Lambda.

**Answer: A**

#### NEW QUESTION 10

A company is running an email application across multiple AWS Regions. The company uses Ohio (us-east-2) as the primary Region and Northern Virginia (us-east-1) as the Disaster Recovery (DR) Region. The data is continuously replicated from the primary Region to the DR Region by a single instance on the public subnet in both Regions. The replication messages between the Regions have a significant backlog during certain times of the day. The backlog clears on its own after a short time, but it affects the application's RPO.

Which of the following solutions should help remediate this performance problem? (Select TWO)

- A. Increase the size of the instances.
- B. Have the instance in the primary Region write the data to an Amazon SQS queue in the primary Region instead, and have the instance in the DR Region poll from this queue.
- C. Use multiple instances on the primary and DR Regions to send and receive the replication data.
- D. Change the DR Region to Oregon (us-west-2) instead of the current DR Region.
- E. Attach an additional elastic network interface to each of the instances in both Regions and set up load balancing between the network interfaces.

**Answer:** AC

#### NEW QUESTION 13

A company had a tight deadline to migrate its on-premises environment to AWS. It moved over Microsoft SQL Servers and Microsoft Windows Servers using the virtual machine import/export service and rebuild other applications native to the cloud. The team created both Amazon EC2 databases and used Amazon RDS. Each team in the company was responsible for migrating their applications, and they have created individual accounts for isolation of resources. The company did not have much time to consider costs, but now it would like suggestions on reducing its AWS spend. Which steps should a Solutions Architect take to reduce costs?

- A. Enable AWS Business Support and review AWS Trusted Advisor's cost check
- B. Create Amazon EC2 Auto Scaling groups for applications that experience fluctuating demand
- C. Save AWS Simple Monthly Calculator reports in Amazon S3 for trend analysis
- D. Create a master account under Organizations and have teams join for consolidating billing.
- E. Enable Cost Explorer and AWS Business Support Reserve Amazon EC2 and Amazon RDS DB instance
- F. Use Amazon CloudWatch and AWS Trusted Advisor for monitoring and to receive cost-savings suggestions
- G. Create a master account under Organizations and have teams join for consolidated billing.
- H. Create an AWS Lambda function that changes the instance size based on Amazon CloudWatch alarms. Reserve instances based on AWS Simple Monthly Calculator suggestion
- I. Have an AWS Well-Architected framework review and apply recommendation
- J. Create a master account under Organizations and have teams join for consolidated billing.
- K. Create a budget and monitor for costs exceeding the budget
- L. Create Amazon EC2 Auto Scaling groups for applications that experience fluctuating demand
- M. Create an AWS Lambda function that changes instance sizes based on Amazon CloudWatch alarm
- N. Have each team upload their bill to an Amazon S3 bucket for analysis of team spending
- O. Use Spot instances on nightly batch processing jobs.

**Answer:** B

#### Explanation:

Import/Export supports importing and exporting data into and out of Amazon S3 buckets. For significant data sets, AWS Import/Export is often faster than Internet transfer and more cost effective than upgrading your connectivity.

#### NEW QUESTION 15

A company runs a public-facing application that uses a Java-based web service via a RESTful API. It is hosted on Apache Tomcat on a single server in a data center that runs consistently at 30% CPU utilization. Use of the API is expected to increase by 10 times with a new product launch. The business wants to migrate the application to AWS with no disruption and needs it to scale to meet demand. The company has already decided to use Amazon Route 53 and CNAME records to redirect traffic. How can these requirements be met with the LEAST amount of effort?

- A. Use AWS Elastic Beanstalk to deploy the Java web service and enable Auto Scaling. Then switch the application to use the new web service.
- B. Lift and shift the Apache server to the cloud using AWS SMS. Then switch the application to direct web service traffic to the new instance.
- C. Create a Docker image and migrate the image to Amazon ECS. Then change the application code to direct web service queries to the ECS container.
- D. Modify the application to call the web service via Amazon API Gateway. Then create a new AWS Lambda Java function to run the Java web service code. After testing, change API Gateway to use the Lambda function.

**Answer:** A

#### NEW QUESTION 16

A company is running a .NET three-tier web application on AWS. The team currently uses XL storage optimized instances to store and serve the website's image and video files on local instance storage. The company has encountered issues with data loss from replication and instance failures. The Solutions Architect has been asked to redesign this application to improve its reliability while keeping costs low. Which solution will meet these requirements?

- A. Set up a new Amazon EFS share, move all image and video files to this share, and then attach this new drive as a mount point to all existing servers.
- B. Create an Elastic Load Balancer with Auto Scaling general purpose instances.
- C. Enable Amazon CloudFront to the Elastic Load Balance.
- D. Enable Cost Explorer and use AWS Trusted Advisor checks to continue monitoring the environment for future savings.
- E. Implement Auto Scaling with general purpose instance types and an Elastic Load Balance.
- F. Enable an Amazon CloudFront distribution to Amazon S3 and move images and video files to Amazon S3. Reserve general purpose instances to meet base performance requirements.
- G. Use Cost Explorer and AWS Trusted Advisor checks to continue monitoring the environment for future savings.
- H. Move the entire website to Amazon S3 using the S3 website hosting feature.
- I. Remove all the web servers and have Amazon S3 communicate directly with the application servers in Amazon VPC.
- J. Use AWS Elastic Beanstalk to deploy the .NET application.
- K. Move all images and video files to Amazon EFS.
- L. Create an Amazon CloudFront distribution that points to the EFS share.
- M. Reserve the m4.xl instances needed to meet base performance requirements.

**Answer:** B

**NEW QUESTION 21**

A company has an Amazon VPC that is divided into a public subnet and a private 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. Only network traffic that is required for the Application Load Balancer to access the web application can be allowed to travel between the public and private subnets.

What collection of rules should be written to ensure that the private subnet's NACL meets the requirement? (Select TWO.)

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

**Answer:** BE

**NEW QUESTION 25**

A company has multiple AWS accounts hosting IT applications. An Amazon CloudWatch Logs agent is installed on all Amazon EC2 instances. The company wants to aggregate all security events in a centralized AWS account dedicated to log storage.

Security Administrators need to perform near-real-time gathering and correlating of events across multiple AWS accounts. Which solution satisfies these requirements?

- A. Create a Log Audit IAM role in each application AWS account with permissions to view CloudWatch Logs, configure an AWS Lambda function to assume the Log Audit role, and perform an hourly export of CloudWatch Logs data to an Amazon S3 bucket in the logging AWS account.
- B. Configure CloudWatch Logs streams in each application AWS account to forward events to CloudWatch Logs in the logging AWS account.
- C. In the logging AWS account, subscribe an Amazon Kinesis Data Firehose stream to Amazon CloudWatch Events, and use the stream to persist log data in Amazon S3.
- D. Create Amazon Kinesis Data Streams in the logging account, subscribe the stream to CloudWatch Logs streams in each application AWS account, configure an Amazon Kinesis Data Firehose delivery stream with the Data Streams as its source, and persist the log data in an Amazon S3 bucket inside the logging AWS account.
- E. Configure CloudWatch Logs agents to publish data to an Amazon Kinesis Data Firehose stream in the logging AWS account, use an AWS Lambda function to read messages from the stream and push messages to Data Firehose, and persist the data in Amazon S3.

**Answer:** C

**Explanation:**

The solution uses Amazon Kinesis Data Streams and a log destination to set up an endpoint in the logging account to receive streamed logs and uses Amazon Kinesis Data Firehose to deliver log data to the Amazon Simple Storage Solution (S3) bucket. Application accounts will subscribe to stream all (or part) of their Amazon CloudWatch logs to a defined destination in the logging account via subscription filters. <https://aws.amazon.com/blogs/architecture/central-logging-in-multi-account-environments/>

**NEW QUESTION 27**

A company wants to ensure that the workloads for each of its business units have complete autonomy and a minimal blast radius in AWS. The Security team must be able to control access to the resources and services in the account to ensure that particular services are not used by the business units.

How can a Solutions Architect achieve the isolation requirements?

- A. Create individual accounts for each business unit and add the account to an OU in AWS Organizations. Modify the OU to ensure that the particular services are blocked.
- B. Federate each account with an IdP, and create separate roles for the business units and the Security team.
- C. Create individual accounts for each business unit.
- D. Federate each account with an IdP and create separate roles and policies for business units and the Security team.
- E. Create one shared account for the entire company.
- F. Create separate VPCs for each business unit.
- G. Create individual IAM policies and resource tags for each business unit.
- H. Federate each account with an IdP, and create separate roles for the business units and the Security team.
- I. Create one shared account for the entire company.
- J. Create individual IAM policies and resource tags for each business unit.
- K. Federate the account with an IdP, and create separate roles for the business units and the Security team.

**Answer:** A

**NEW QUESTION 30**

A company wants to manage the costs associated with a group of 20 applications that are critical, by migrating to AWS. The applications are a mix of Java and Node.js spread across different instance clusters. The company wants to minimize costs while standardizing by using a single deployment methodology. Most of the applications are part of month-end processing routines with a small number of concurrent users, but they are occasionally run at other times. Average application memory consumption is less than 1 GB, though some applications use as much as 2.5 GB of memory during peak processing. The most important application in the group is a billing report written in Java that accesses multiple data sources and often for several hours.

Which is the MOST cost-effective solution?

- A. Deploy a separate AWS Lambda function for each application.
- B. Use AWS CloudTrail logs and Amazon CloudWatch alarms to verify completion of critical jobs.
- C. Deploy Amazon ECS containers on Amazon EC2 with Auto Scaling configured for memory utilization of 75%. Deploy an ECS task for each application being migrated with ECS task scaling.
- D. Monitor services and hosts by using Amazon CloudWatch.
- E. Deploy AWS Elastic Beanstalk for each application with Auto Scaling to ensure that all requests have sufficient resources.
- F. Monitor each AWS Elastic Beanstalk deployment with using CloudWatch alarms.
- G. Deploy a new Amazon EC2 instance cluster that co-hosts all applications by using EC2 Auto Scaling and Application Load Balancer.
- H. Scale cluster size based on a custom metric set on instance memory utilization.
- I. Purchase 3-year Reserved instance reservations equal to the GroupMaxSize parameter of the Auto Scaling group.

**Answer:** C

**NEW QUESTION 33**

A Solutions Architect is designing the storage layer for a recently purchased application. The application will be running on Amazon EC2 instances and has the following layers and requirements:

Data layer: A POSIX file system shared across many systems.

Service layer: Static file content that requires block storage with more than 100k IOPS. Which combination of AWS services will meet these needs? (Choose two.)

- A. Data layer – Amazon S3
- B. Data layer – Amazon EC2 Ephemeral Storage
- C. Data layer – Amazon EFS
- D. Service layer – Amazon EBS volumes with Provisioned IOPS
- E. Service layer – Amazon EC2 Ephemeral Storage

**Answer:** CE

**Explanation:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-instances.html>

**NEW QUESTION 38**

A Solutions Architect must update an application environment within AWS Elastic Beanstalk using a blue/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

**Explanation:**

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMEswap.html>

**NEW QUESTION 41**

A Solutions Architect has created an AWS CloudFormation template for a three-tier application that contains an Auto Scaling group of Amazon EC2 instances running a custom AMI.

The Solutions Architect wants to ensure that future updates to the custom AMI can be deployed to a running stack by first updating the template to refer to the new AMI, and then invoking UpdateStack to replace the EC2 instances with instances launched from the new AMI. How can updates to the AMI be deployed to meet these requirements?

- A. Create a change set for a new version of the template, view the changes to the running EC2 instances to ensure that the AMI is correctly updated, and then execute the change set.
- B. Edit the AWS::AutoScaling::LaunchConfiguration resource in the template, changing its DeletionPolicy to Replace.
- C. Edit the AWS::AutoScaling::AutoScalingGroup resource in the template, inserting an UpdatePolicy attribute.
- D. Create a new stack from the updated template.
- E. Once it is successfully deployed, modify the DNS records to point to the new stack and delete the old stack.

**Answer: C**

**Explanation:**

References:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-as-launchconfig.html>

**NEW QUESTION 44**

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-premise
- B. Use the MAM solution to extract the videos from the current archive and push them into the file gateway
- C. Use the catalog of faces to build a collection in Amazon Rekognition
- D. 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.
- E. Set up an AWS Storage Gateway, tape gateway appliance on-premise
- F. Use the MAM solution to extract the videos from the current archive and push them into the tape gateway
- G. Use the catalog of faces to build a collection in Amazon Rekognition
- H. 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.
- I. Configure a video ingestion stream by using Amazon Kinesis Video Stream
- J. Use the catalog of faces to build a collection in Amazon Rekognition
- K. Stream the videos from the MAM solution into Kinesis Video Stream
- L. Configure Amazon Rekognition to process the streamed video
- M. Then, use a stream consumer to retrieve the required metadata, and push the metadata into the MAM solution
- N. Configure the stream to store the videos in Amazon S3.
- O. Set up an Amazon EC2 instance that runs the OpenCV libraries
- P. Copy the videos, images, and face catalog from the on-premises library into an Amazon EBS volume mounted on this EC2 instance
- Q. 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.

**Answer: C**

**Explanation:**

<https://docs.aws.amazon.com/rekognition/latest/dg/streaming-video.html>

**NEW QUESTION 47**

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

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

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

**Answer: B**

**Explanation:**

<https://docs.aws.amazon.com/AmazonS3/latest/dev/RequesterPaysBuckets.html>

**NEW QUESTION 50**

A company is creating an account strategy so that they can begin using AWS. The Security team will provide each team with the permissions they need to follow the principle of least privileged access. Teams would like to keep their resources isolated from other groups, and the Finance team would like each team's resource usage separated for billing purposes.

Which account creation process meets these requirements and allows for changes?

- A. Create a new AWS Organizations account
- B. Create groups in Active Directory and assign them to roles in AWS to grant federated access
- C. Require each team to tag their resources, and separate bills based on tag
- D. Control access to resources through IAM granting the minimally required privilege.
- E. Create individual accounts for each team
- F. Assign the security as the master account, and enable consolidated billing for all other accounts
- G. Create a cross-account role for security to manage accounts, and send logs to a bucket in the security account.
- H. Create a new AWS account, and use AWS Service Catalog to provide teams with the required resources. Implement a third-party billing to provide the Finance team with the resource use for each team based on tagging
- I. Isolate resources using IAM to avoid account sprawl
- J. Security will control and monitor logs and permissions.
- K. Create a master account for billing using Organizations, and create each team's account from that master account
- L. Create a security account for logs and cross-account access
- M. Apply service control policies on each account, and grant the Security team cross-account access to all accounts
- N. Security will create IAM policies for each account to maintain least privilege access.

**Answer: B**

**NEW QUESTION 53**

A Solutions Architect has been asked to look at a company's Amazon Redshift cluster, which has quickly become an integral part of its technology and supports key business processes. The Solutions Architect is to increase the reliability and availability of the cluster and provide options to ensure that if an issue arises, the cluster can either operate or be restored within four hours.

Which of the following solution options BEST addresses the business need in the most cost-effective manner?

- A. Ensure that the Amazon Redshift cluster has been set up to make use of Auto Scaling groups with the nodes in the cluster spread across multiple Availability Zones.
- B. Ensure that the Amazon Redshift cluster creation has been templated using AWS CloudFormation so it can easily be launched in another Availability Zone and data populated from the automated Redshift back-ups stored in Amazon S3.
- C. Use Amazon Kinesis Data Firehose to collect the data ahead of ingestion into Amazon Redshift and create clusters using AWS CloudFormation in another region and stream the data to both clusters.
- D. Create two identical Amazon Redshift clusters in different regions (one as the primary, one as the secondary). Use Amazon S3 cross-region replication from the primary to secondary. Use Amazon S3 cross-region replication from the primary to secondary region, which triggers an AWS Lambda function to populate the cluster in the secondary region.

**Answer: B**

**Explanation:**

[https://aws.amazon.com/redshift/faqs/?nc1=h\\_ls](https://aws.amazon.com/redshift/faqs/?nc1=h_ls) Q: What happens to my data warehouse cluster availability and data durability if my data warehouse cluster's Availability Zone (AZ) has an outage? If your Amazon Redshift data warehouse cluster's Availability Zone becomes unavailable, you will not be able to use your cluster until power and network access to the AZ are restored. Your data warehouse cluster's data is preserved so you can start using your Amazon Redshift data warehouse as soon as the AZ becomes available again. In addition, you can also choose to restore any existing snapshots to a new AZ in the same Region. Amazon Redshift will restore your most frequently accessed data first so you can resume queries as quickly as possible.

FROM 37

**NEW QUESTION 57**

The Solutions Architect manages a serverless application that consists of multiple API gateways, AWS Lambda functions, Amazon S3 buckets, and Amazon DynamoDB tables. Customers say that a few application components slow while loading dynamic images, and some are timing out with the "504 Gateway Timeout" error. While troubleshooting the scenario, the Solutions Architect confirms that DynamoDB monitoring metrics are at acceptable levels.

Which of the following steps would be optimal for debugging these application issues? (Choose two.)

- A. Parse HTTP logs in Amazon API Gateway for HTTP errors to determine the root cause of the errors.
- B. Parse Amazon CloudWatch Logs to determine processing times for requested images at specified intervals.
- C. Parse VPC Flow Logs to determine if there is packet loss between the Lambda function and S3.
- D. Parse AWS X-Ray traces and analyze HTTP methods to determine the root cause of the HTTP errors.
- E. Parse S3 access logs to determine if objects being accessed are from specific IP addresses to narrow the scope to geographic latency issues.

**Answer: BD**

**Explanation:**

First "A 504 Gateway Timeout Error means your web server didn't receive a timely response from another server upstream when it attempted to load one of your web pages. Put simply, your web servers aren't communicating with each other fast enough". This specific issue is addressed in the AWS article "Tracing, Logging and Monitoring an API Gateway API". [https://docs.amazonaws.cn/en\\_us/apigateway/latest/developerguide/monitoring\\_overview.html](https://docs.amazonaws.cn/en_us/apigateway/latest/developerguide/monitoring_overview.html)

**NEW QUESTION 62**

A company has been using a third-party provider for its content delivery network and recently decided to switch to Amazon CloudFront. The Development team wants to maximize performance for the global user base. The company uses a content management system (CMS) that serves both static and dynamic content. The CMS is behind an Application Load Balancer (ALB) which is set as the default origin for the distribution. Static assets are served from an Amazon S3 bucket. The Origin Access Identity (OAI) was created properly and the S3 bucket policy has been updated to allow the GetObject action from the OAI, but static assets are receiving a 404 error.

Which combination of steps should the Solutions Architect take to fix the error? (Select TWO.)

- A. Add another origin to the CloudFront distribution for the static assets
- B. Add a path-based rule to the ALB to forward requests for the static assets
- C. Add an RTMP distribution to allow caching of both static and dynamic content

- D. Add a behavior to the CloudFront distribution for the path pattern and the origin of the static assets
- E. Add a host header condition to the ALB listener and forward the header from CloudFront to add traffic to the allow list

**Answer:** AD

### NEW QUESTION 63

A Solutions Architect is migrating a 10 TB PostgreSQL database to Amazon RDS for PostgreSQL. The company's internet link is 50 MB with a VPN in the Amazon VPC, and the Solutions Architect needs to migrate the data and synchronize the changes before the cutover. The cutover must take place within an 8-day period.

What is the LEAST complex method of migrating the database securely and reliably?

- A. Order an AWS Snowball device and copy the database using the AWS DM
- B. When the database is available in Amazon S3, use AWS DMS to load it to Amazon RDS, and configure a job to synchronize changes before the cutover.
- C. Create an AWS DMS job to continuously replicate the data from on premises to AW
- D. Cutover to Amazon RDS after the data is synchronized.
- E. Order an AWS Snowball device and copy a database dump to the devic
- F. After the data has been copied to Amazon S3, import it to the Amazon RDS instanc
- G. Set up log shipping over a VPN to synchronize changes before the cutover.
- H. Order an AWS Snowball device and copy the database by using the AWS Schema Conversion Tool. When the data is available in Amazon S3, use AWS DMS to load it to Amazon RDS, and configure a job to synchronize changes before the cutover.

**Answer:** B

### NEW QUESTION 64

A company is adding a new approved external vendor that only supports IPv6 connectivity. The company's backend systems sit in the private subnet of an Amazon VPC. The company uses a NAT gateway to allow these systems to communicate with external vendors over IPv4. Company policy requires systems that communicate with external vendors use a security group that limits access to only approved external vendors. The virtual private cloud (VPC) uses the default network ACL.

The Systems Operator successfully assigns IPv6 addresses to each of the backend systems. The Systems Operator also updates the outbound security group to include the IPv6 CIDR of the external vendor (destination). The systems within the VPC are able to ping one another successfully over IPv6. However, these systems are unable to communicate with the external vendor.

What changes are required to enable communication with the external vendor?

- A. Create an IPv6 NAT instanc
- B. Add a route for destination 0.0.0.0/0 pointing to the NAT instance.
- C. Enable IPv6 on the NAT gatewa
- D. Add a route for destination ::/0 pointing to the NAT gateway.
- E. Enable IPv6 on the internet gatewa
- F. Add a route for destination 0.0.0.0/0 pointing to the IGW.
- G. Create an egress-only internet gatewa
- H. Add a route for destination ::/0 pointing to the gateway.

**Answer:** D

### Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html>

### NEW QUESTION 69

A company that provides wireless services needs a solution to store and analyze log files about user activities. Currently, log files are delivered daily to Amazon Linux on Amazon EC2 instance. A batch script is run once a day to aggregate data used for analysis by a third-party tool. The data pushed to the third-party tool is used to generate a visualization for end users. The batch script is cumbersome to maintain, and it takes several hours to deliver the ever-increasing data volumes to the third-party tool. The company wants to lower costs, and is open to considering a new tool that minimizes development effort and lowers administrative overhead. The company wants to build a more agile solution that can store and perform the analysis in near-real time, with minimal overhead. The solution needs to be cost effective and scalable to meet the company's end-user base growth.

Which solution meets the company's requirements?

- A. Develop a Python script to failure the data from Amazon EC2 in real time and store the data in Amazon S3. Use a copy command to copy data from Amazon S3 to Amazon Redshif
- B. Connect a business intelligence tool running on Amazon EC2 to Amazon Redshift and create the visualizations.
- C. Use an Amazon Kinesis agent running on an EC2 instance in an Auto Scaling group to collect and send the data to an Amazon Kinesis Data Firehose delivery strea
- D. The Kinesis Data Firehose delivery stream will deliver the data directly to Amazon E
- E. Use Kibana to visualize the data.
- F. Use an in-memory caching application running on an Amazon EBS-optimized EC2 instance to capture the log data in near real-tim
- G. Install an Amazon ES cluster on the same EC2 instance to store the log files as they are delivered to Amazon EC2 in near real-tim
- H. Install a Kibana plugin to create the visualizations.
- I. Use an Amazon Kinesis agent running on an EC2 instance to collect and send the data to an Amazon Kinesis Data Firehose delivery strea
- J. The Kinesis Data Firehose delivery stream will deliver the data to Amazon S3. Use an AWS Lambda function to deliver the data from Amazon S3 to Amazon E
- K. Use Kibana to visualize the data.

**Answer:** B

### Explanation:

<https://docs.aws.amazon.com/firehose/latest/dev/writing-with-agents.html>

### NEW QUESTION 73

A company manages more than 200 separate internet-facing web applications. All of the applications are deployed to AWS in a single AWS Region. The fully qualified domain names (FQDNs) of all of the applications are made available through HTTPS using Application Load Balancers (ALBs). The ALBs are configured to use public SSL/TLS certificates.

A Solutions Architect needs to migrate the web applications to a multi-region architecture. All HTTPS services should continue to work without interruption. Which approach meets these requirements?

- A. Request a certificate for each FQDN using AWS KM
- B. Associate the certificates with the ALBs in the primary AWS Region
- C. Enable cross-region availability in AWS KMS for the certificates and associate the certificates with the ALBs in the secondary AWS Region.
- D. Generate the key pairs and certificate requests for each FQDN using AWS KM
- E. Associate the certificates with the ALBs in both the primary and secondary AWS Regions.
- F. Request a certificate for each FQDN using AWS Certificate Manage
- G. Associate the certificates with the ALBs in both the primary and secondary AWS Regions.
- H. Request certificates for each FQDN in both the primary and secondary AWS Regions using AWS Certificate Manage
- I. Associate the certificates with the corresponding ALBs in each AWS Region.

**Answer:** D

**Explanation:**

<https://docs.aws.amazon.com/acm/latest/userguide/acm-regions.html>

Certificates in ACM are regional resources. To use a certificate with Elastic Load Balancing for the same fully qualified domain name (FQDN) or set of FQDNs in more than one AWS region, you must request or import a certificate for each region. For certificates provided by ACM, this means you must revalidate each domain name in the certificate for each region. You cannot copy a certificate between regions.

**NEW QUESTION 77**

A company's data center is connected to the AWS Cloud over a minimally used 10-Gbps AWS Direct Connect connection with a private virtual interface to its virtual private cloud (VPC). The company internet connection is 200 Mbps and the company has a 150-TB dataset that is created each Friday. The data must be transferred and available in Amazon S3 on Monday morning.

Which is the LEAST expensive way to meet the requirements while allowing for data transfer growth?

- A. Order two 80-GB AWS Snowball appliances. Offload the data to the appliances and ship them to AWS. AWS will copy the data from the Snowball appliances to Amazon S3.
- B. Create a VPC endpoint for Amazon S3. Copy the data to Amazon S3 by using the VPC endpoint, forcing the transfer to use the Direct Connect connection.
- C. Create a VPC endpoint for Amazon S3. Set up a reverse proxy farm behind a Classic Load Balancer in the VPC. Copy the data to Amazon S3 using the proxy.
- D. Create a public virtual interface on a Direct Connect connection and copy the data to Amazon S3 over the connection.

**Answer:** D

**NEW QUESTION 78**

The company Security team requires that all data uploaded into an Amazon S3 bucket must be encrypted. The encryption keys must be highly available and the company must be able to control access on a per-user basis, with different users having access to different encryption keys.

Which of the following architectures will meet these requirements? (Choose two.)

- A. Use Amazon S3 server-side encryption with Amazon S3-managed key.
- B. Allow Amazon S3 to generate an AWS/S3 master key, and use IAM to control access to the data keys that are generated.
- C. Use Amazon S3 server-side encryption with AWS KMS-managed keys, create multiple customer master keys, and use key policies to control access to them.
- D. Use Amazon S3 server-side encryption with customer-managed keys, and use AWS CloudHSM to manage the key.
- E. Use CloudHSM client software to control access to the keys that are generated.
- F. Use Amazon S3 server-side encryption with customer-managed keys, and use two AWS CloudHSM instances configured in high-availability mode to manage the key.
- G. Use the Cloud HSM client software to control access to the keys that are generated.
- H. Use Amazon S3 server-side encryption with customer-managed keys, and use two AWS CloudHSM instances configured in high-availability mode to manage the key.
- I. Use IAM to control access to the keys that are generated in CloudHSM.

**Answer:** BD

**Explanation:**

<http://websecuritypatterns.com/blogs/2018/03/01/encryption-and-key-management-in-aws-kms-vs-cloudhsm-mys/>

**NEW QUESTION 83**

An internal security audit of AWS resources within a company found that a number of Amazon EC2 instances running Microsoft Windows workloads were missing several important operating system-level patches. A Solutions Architect has been asked to fix existing patch deficiencies, and to develop a workflow to ensure that future patching requirements are identified and taken care of quickly. The Solutions Architect has decided to use AWS Systems Manager. It is important that EC2 instance reboots do not occur at the same time on all Windows workloads to meet organizational uptime requirements.

Which workflow will meet these requirements in an automated manner?

- A. Add a Patch Group tag with a value of Windows Servers to all existing EC2 instances.
- B. Ensure that all Windows EC2 instances are assigned this tag.
- C. Associate the AWS-DefaultPatchBaseline to the Windows Servers patch group.
- D. Define an AWS Systems Manager maintenance window, conduct patching within it, and associate it with the Windows Servers patch group.
- E. Register instances with the maintenance window using associated subnet ID.
- F. Assign the AWS-RunPatchBaseline document as a task within each maintenance window.
- G. Add a Patch Group tag with a value of Windows Servers to all existing EC2 instances.
- H. Ensure that all Windows EC2 instances are assigned this tag.
- I. Associate the AWS-WindowsPatchBaseline document as a task associated with the Windows Servers patch group.
- J. Create an Amazon CloudWatch Events rule configured to use a cron expression to schedule the execution of patching using the AWS Systems Manager run command.
- K. Create an AWS Systems Manager State Manager document to define commands to be executed during patch execution.
- L. Add a Patch Group tag with a value of either Windows Servers1 or Windows Servers2 to all existing EC2 instances.
- M. Ensure that all Windows EC2 instances are assigned this tag.
- N. Associate the AWS-DefaultPatchBaseline with both Windows Servers patch groups.
- O. Define two non-overlapping AWS Systems Manager maintenance windows, conduct patching within them, and associate each with a different patch group.

- P. Register targets with specific maintenance windows using the Patch Group tag
- Q. Assign the AWS-RunPatchBaseline document as a task within each maintenance window.
- R. Add a Patch Group tag with a value of either Windows servers1 or Windows Server2 to all existing EC2 instance
- S. Ensure that all Windows EC2 instances are assigned this ta
- T. Associate theAWS-WindowsPatchBaseline with both Windows Servers patch group
- . Define two non-overlappingAWS Systems Manager maintenance windows, conduct patching within them, and associate each with a different patch group
- . Assign the AWS-RunWindowsPatchBaseline document as a task within each maintenance windo
- . Create an AWS Systems Manager State Manager document to define commands to be executed during patch execution.

**Answer: C**

#### NEW QUESTION 86

A company operating a website on AWS requires high levels of scalability, availability and performance. The company is running a Ruby on Rails application on Amazon EC2. It has a data tier on MySQL 5.6 on Amazon EC2 using 16 TB of Amazon EBS storage. Amazon CloudFront is used to cache application content. The Operations team is reporting continuous and unexpected growth of EBS volumes assigned to the MySQL database. The Solutions Architect has been asked to design a highly scalable, highly available, and high-performing solution. Which solution is the MOST cost-effective at scale?

- A. Implement Multi-AZ and Auto Scaling for all EC2 instances in the current configuratio
- B. Ensure that all EC2 instances are purchased as reserved instance
- C. Implement new elastic Amazon EBS volumes for the data tier.
- D. Design and implement the Docker-based containerized solution for the application using Amazon EC
- E. Migrate to an Amazon Aurora MySQL Multi-AZ cluste
- F. Implement storage checks for Aurora MySQL storage utilization and an AWS Lambda function to grow the Aurora MySQL storage, as necessar
- G. Ensure that Multi-AZ architectures are implemented.
- H. Ensure that EC2 instances are right-sized and behind an Elastic Load Balancing load balancer. Implement Auto Scaling with EC2 instance
- I. Ensure that the reserved instances are purchased for fixed capacity and that Auto Scaling instances run on deman
- J. Migrate to an Amazon Aurora MySQLMulti-AZ cluste
- K. Ensure that Multi-AZ architectures are implemented.
- L. Ensure that EC2 instances are right-sized and behind an Elastic Load Balance
- M. Implement Auto Scaling with EC2 instance
- N. Ensure that Reserved instances are purchased for fixed capacity and that Auto Scaling instances run on deman
- O. Migrate to an Amazon Aurora MySQL Multi-AZ cluste
- P. Implement storage checks for Aurora MySQL storage utilization and an AWS Lambda function to grow Aurora MySQL storage, as necessar
- Q. Ensure Multi-AZ architectures are implemented.

**Answer: C**

#### NEW QUESTION 91

A company has a large on-premises Apache Hadoop cluster with a 20 PB HDFS database. The cluster is growing every quarter by roughly 200 instances and 1 PB. The company's goals are to enable resiliency for its Hadoop data, limit the impact of losing cluster nodes, and significantly reduce costs. The current cluster runs 24/7 and supports a variety of analysis workloads, including interactive queries and batch processing. Which solution would meet these requirements with the LEAST expense and down time?

- A. Use AWS Snowmobile to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster initially sized to handle the interactive workload based on historical data from the on-premises cluste
- B. Store the data on EMRF
- C. Minimize costs using Reserved Instances for master and core nodes and Spot Instances for task nodes, and auto scale task nodes based on Amazon CloudWatch metric
- D. Create job-specific, optimized clusters for batch workloads that are similarly optimized.
- E. Use AWS Snowmobile to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster of similar size and configuration to the current cluste
- F. Store the data on EMRF
- G. Minimize costs by using Reserved Instance
- H. As the workload grows each quarter, purchase additional Reserved Instances and add to the cluster.
- I. Use AWS Snowball to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster initially sized to handle the interactive workloads based on historical data from the on-premises cluste
- J. Store the on EMRF
- K. Minimize costs using Reserved Instances for master and core nodes and Spot Instances for task nodes, and auto scale task nodes based on Amazon CloudWatch metric
- L. Create job-specific, optimized clusters for batch workloads that are similarly optimized.
- M. Use AWS Direct Connect to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster initially sized to handle the interactive workload based on historical data from the on-premises cluste
- N. Store the data on EMRF
- O. Minimize costs using Reserved Instances for master and core nodes and Spot Instances for task nodes, and auto scale task nodes based on Amazon CloudWatch metric
- P. Create job-specific, optimized clusters for batch workloads that are similarly optimized.

**Answer: A**

#### Explanation:

Q: How should I choose between Snowmobile and Snowball?

To migrate large datasets of 10PB or more in a single location, you should use Snowmobile. For datasets less than 10PB or distributed in multiple locations, you should use Snowball. In addition, you should evaluate the amount of available bandwidth in your network backbone. If you have a high speed backbone with hundreds of Gb/s of spare throughput, then you can use Snowmobile to migrate the large datasets all at once. If you have limited bandwidth on your backbone, you should consider using multiple Snowballs to migrate the data incrementally.

#### NEW QUESTION 96

A company has an internal AWS Elastic Beanstalk worker environment inside a VPC that must access an external payment gateway API available on an HTTPS endpoint the public internet. Because of security policies, the payment gateway's Application team can grant access to only one public IP address.

Which architecture will set up an Elastic Beanstalk environment to access the company's application without making multiple changes on the company's end?

- A. Configure the Elastic Beanstalk application to place Amazon EC2 instances in a private subnet with an outbound route to a NAT gateway in a public subnet Associate an Elastic IP address to the NAT gateway that can be whitelisted on the payment gateway application side
- B. Configure the Elastic Beanstalk application to place Amazon EC2 instances in a public subnet with an internet gateway Associate an Elastic IP address to the internet gateway that can be whitelisted on the payment gateway application side
- C. Configure the Elastic Beanstalk application to place Amazon EC2 instances in a private subnet Set an `https_proxy` application parameter to send outbound HTTPS connections to an EC2 proxy server deployed in a public subnet Associate an Elastic IP address to the EC2 proxy host that can be whitelisted on the payment gateway application side
- D. Configure the Elastic Beanstalk application to place Amazon EC2 instances in a public subnet Set the `https_proxy` and `no_proxy` application parameters to send non-VPC outbound HTTPS connections to an EC2 proxy server deployed in a public subnet Associate an Elastic IP address to the EC2 proxy host that can be whitelisted on the payment gateway application side

**Answer: C**

#### NEW QUESTION 100

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 SQS queue with the video's location A backend application pulls this location from Amazon SQS 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 during 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 12 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 analysis 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**

#### NEW QUESTION 101

A company's main intranet page has experienced degraded response times as its user base has increased although there are no reports of users seeing error pages. The application uses Amazon DynamoDB in read-only mode.

Amazon DynamoDB latency metrics for successful requests have been in a steady state even during times when users have reported degradation The Development team has correlated the issue to ProvisionedThroughput Exceeded exceptions in the application logs when doing Scan and read operations The team also identified an access pattern of steady spikes of read activity on a distributed set of individual data items

The Chief Technology Officer wants to improve the user experience

Which solutions will meet these requirements with the LEAST amount of changes to the application? (Select TWO )

- A. Change the data model of the DynamoDB tables to ensure that all Scan and read operations meet DynamoDB best practices of uniform data access, reaching the full request throughput provisioned for the DynamoDB tables
- B. Enable DynamoDB auto scaling to manage the throughput capacity as table traffic increases Set the upper and lower limits to control costs and set a target utilization given the peak usage and how quickly the traffic changes.
- C. Provision Amazon ElastiCache for Redis with cluster mode enabled The cluster should be provisioned with enough shards to spread the application load and provision at least one read replica node for each shard
- D. Implement the DynamoDB Accelerator (DAX) client and provision a DAX cluster with the appropriate node types to sustain the application load
- E. Tune the item and query cache configuration for an optimal user experience
- F. Remove error retries and exponential backoffs in the application code to handle throttling errors

**Answer: AE**

#### NEW QUESTION 104

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 requirement:

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 branche
- B. Use AWS CodeBuild for running unit test
- C. Use CodeBuild to stage the artifacts within an S3 bucket in a separate testing account.
- D. Trigger a separate pipeline from CodeCommit feature branche
- E. Use AWS Lambda for running unit test
- F. Use AWS CodeDeploy to stage the artifacts within an S3 bucket in a separate testing account.
- G. Trigger a separate pipeline from CodeCommit tags Use Jenkins for running unit test
- H. Create a stage in the pipeline with S3 as the target for staging the artifacts with an S3 bucket in a separate testing account.
- I. Create a separate CodeCommit repository for feature development and use it to trigger the pipelin
- J. Use AWS Lambda for running unit test
- K. Use AWS CodeBuild to stage the artifacts within different S3 buckets in the same production account.

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/codebuild/latest/userguide/how-to-create-pipeline.html>

**NEW QUESTION 105**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 110**

A retail company is running an application that stores invoice files in Amazon S3 bucket and metadata about the files in an Amazon. 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 tabl
- C. 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.
- D. Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable versioning on the S3 bucke
- E. Implement strict ACLs on the S3 bucket.
- F. 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:** A

**Explanation:**

<https://aws.amazon.com/blogs/aws/new-cross-region-replication-for-amazon-s3/>

**NEW QUESTION 114**

An online retailer needs to regularly process large product catalogs, which are handled in batches. These are sent out to be processed by people using the Amazon Mechanical Turk service, but the retailer has asked its Solutions Architect to design a workflow orchestration system that allows it to handle multiple concurrent Mechanical Turk operations, deal with the result assessment process, and reprocess failures.

Which of the following options gives the retailer the ability to interrogate the state of every workflow with the LEAST amount of implementation effort?

- A. Trigger Amazon CloudWatch alarms based upon message visibility in multiple Amazon SQS queues (one queue per workflow stage) and send messages via Amazon SNS to trigger AWS Lambda functions to process the next ste
- B. Use Amazon ES and Kibana to visualize Lambda processing logs to see the workflow states.
- C. Hold workflow information in an Amazon RDS instance with AWS Lambda functions polling RDS for status change
- D. Worker Lambda functions then process the next workflow step
- E. Amazon QuickSight will visualize workflow states directly out of Amazon RDS.
- F. Build the workflow in AWS Step Functions, using it to orchestrate multiple concurrent workflow
- G. The status of each workflow can be visualized in the AWS Management Console, and historical data can be written to Amazon S3 and visualized using Amazon QuickSight.
- H. Use Amazon SWF to create a workflow that handles a single batch of catalog records with multiple worker tasks to extract the data, transform it, and send it through Mechanical Tur
- I. Use Amazon ES and Kibana to visualize AWS Lambda processing logs to see the workflow states.

**Answer:** C

**Explanation:**

AWS Step Functions is a fully managed service that makes it easy to coordinate the components of distributed applications and microservices using visual workflows. Instead of writing a Decider program, you define state machines in JSON. AWS customers should consider using Step Functions for new applications. If Step Functions does not fit your needs, then you should consider Amazon Simple Workflow (SWF). Amazon SWF provides you complete control over your orchestration logic, but increases the complexity of developing applications. You may write decider programs in the programming language of your choice, or you may use the Flow framework to use programming constructs that structure asynchronous interactions for you. AWS will continue to provide the Amazon SWF service, Flow framework, and support all Amazon SWF customers. <https://aws.amazon.com/swf/faqs/>

**NEW QUESTION 119**

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 master account and the secondary accounts.  
Minimize the effort required to add additional secondary accounts.  
Which combination of steps should be included in the solution? (Choose two.)

- A. Create an organization from the master account
- B. Send invitations to the secondary accounts from the master account
- C. Accept the invitations and create an OU.
- D. Create an organization from the master account
- E. Send a join request to the master account from each secondary account
- F. Accept the requests and create an OU.
- G. Create a VPC peering connection between the master account and the secondary account
- H. Accept the request for the VPC peering connection.
- I. Create a service control policy (SCP) that enables full EC2 access, and attach the policy to the OU.
- J. Create a full EC2 access policy and map the policy to a role in each account
- K. Trust every other account to assume the role.

**Answer:** AD

**Explanation:**

There is a concept of Permission Boundary vs Actual IAM Policies That is, we have a concept of "Allow" vs "Grant". In terms of boundaries, we have the following three boundaries: 1. SCP 2. User/Role boundaries 3. Session boundaries (ex. AssumeRole ... ) In terms of actual permission granting, we have the following: 1. Identity Policies 2. Resource Policies

**NEW QUESTION 123**

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 equivalents sized read replicas to provide reliability
- D. Reserve capacity for all EC2 instances and leverage Spot Instance pricing for the RDS database

**Answer: B**

#### NEW QUESTION 127

A company has an application behind a load balancer with enough Amazon EC2 instances to satisfy peak demand. Scripts and third-party deployment solutions are used to configure EC2 instances when demand increases or an instance fails. The team must periodically evaluate the utilization of the instance types to ensure that the correct sizes are deployed.

How can this workload be optimized to meet these requirements?

- A. Use CloudFormer to create AWS CloudFormation stacks from the current resource
- B. Deploy that stack by using AWS CloudFormation in the same regio
- C. Use Amazon CloudWatch alarms to send notifications about underutilized resources to provide cost-savings suggestions.
- D. Create an Auto Scaling group to scale the instances, and use AWS CodeDeploy to perform the configuratio
- E. Change from a load balancer to an Application Load Balance
- F. Purchase a third-party product that provides suggestions for cost savings on AWS resources.
- G. Deploy the application by using AWS Elastic Beanstalk with default option
- H. Register for an AWS Support Developer pla
- I. Review the instance usage for the application by using Amazon CloudWatch, and identify less expensive instances that can handle the loa
- J. Hold monthly meetings to review new instance types and determine whether Reserved instances should be purchased.
- K. Deploy the application as a Docker image by using Amazon EC
- L. Set up Amazon EC2 Auto Scaling and Amazon ECS scalin
- M. Register for AWS Business Support and use Trusted Advisor checks to provide suggestions on cost savings.

**Answer: D**

#### NEW QUESTION 128

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? (Choose two.)

- A. Create tasks using the bridge network mode.
- B. Create tasks using the awsvpc network mode.
- C. Apply security groups to Amazon EC2 instances, and use IAM roles for EC2 instances to access other resources.
- D. Apply security groups to the tasks, and pass IAM credentials into the container at launch time to access other resources.
- E. Apply security groups to the tasks, and use IAM roles for tasks to access other resources.

**Answer: BE**

#### Explanation:

<https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-ecs-introduces-awsvpc-networking-mode-for-c>

<https://amazonaws-china.com/blogs/compute/introducing-cloud-native-networking-for-ecs-containers/>

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task-iam-roles.html>

#### NEW QUESTION 132

A large company is migrating its entire IT portfolio to AWS. Each business unit in the company has a standalone AWS account that supports both development and test environments. New accounts to support production workloads will be needed soon.

The Finance department requires a centralized method for payment but must maintain visibility into each group's spending to allocate costs.

The Security team requires a centralized mechanism to control IAM usage in all the company's accounts. What combination of the following options meet the company's needs with LEAST effort? (Choose two.)

- A. Use a collection of parameterized AWS CloudFormation templates defining common IAM permissions that are launched into each accoun
- B. Require all new and existing accounts to launch the appropriate stacks to enforce the least privilege model.
- C. Use AWS Organizations to create a new organization from a chosen payer account and define an organizational unit hierarch
- D. Invite the existing accounts to join the organization and create new accounts using Organizations.
- E. Require each business unit to use its own AWS account
- F. Tag each AWS account appropriately and enable Cost Explorer to administer chargebacks.
- G. Enable all features of AWS Organizations and establish appropriate service control policies that filter IAM permissions for sub-accounts.
- H. Consolidate all of the company's AWS accounts into a single AWS accoun
- I. Use tags for billing purposes and IAM's Access Advice feature to enforce the least privilege model.

**Answer: BD**

#### NEW QUESTION 137

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 The 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 authorize
- B. Have the browser interface use API Gateway instead of the presigned URL to upload objects
- C. 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 authorizer Have the browser interface use API Gateway instead of the presigned URL lo upload objects
- D. 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 the URL using the S3 multipart upload API.
- E. 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 s3:PutObject permissions in the bucket policy Have the browser interface upload

objects using the CloudFront distribution.

**Answer:** A

#### NEW QUESTION 138

A company is building an AWS landing zone and has asked a Solutions Architect to design a multi-account access strategy that will allow hundreds of users to use corporate credentials to access the AWS Console. The company is running a Microsoft Active Directory and users will use an AWS Direct Connect connection to connect to AWS. The company also wants to be able to federate to third-party services and providers, including custom applications. Which solution meets the requirements by using the LEAST amount of management overhead?

- A. Connect the Active Directory to AWS by using single sign-on and an Active Directory Federation Services (AD FS) with SAML 2.0, and then configure the identity Provider (IdP) system to use form-based authentication
- B. Build the AD FS portal page with corporate branding, and integrate third-party applications that support SAML 2.0 as required.
- C. Create a two-way Forest trust relationship between the on-premises Active Directory and the AWS Directory Service
- D. Set up AWS Single Sign-On with AWS Organization
- E. Use single sign-on integrations for connections with third-party applications.
- F. Configure single sign-on by connecting the on-premises Active Directory using the AWS Directory Service AD Connector
- G. Enable federation to the AWS services and accounts by using the IAM applications and services linking function
- H. Leverage third-party single sign-on as needed.
- I. Connect the company's Active Directory to AWS by using AD FS and SAML 2.0. Configure the AD FS claim rule to leverage Regex and a common Active Directory naming convention for the security group to allow federation of all AWS accounts
- J. Leverage third-party single sign-on as needed, and add it to the AD FS server.

**Answer:** D

#### Explanation:

<https://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directory-federation-services-a>

#### NEW QUESTION 140

A company wants to move a web application to AWS. The application stores session information locally on each web server, which will make auto scaling difficult. As part of the migration, the application will be rewritten to decouple the session data from the web servers. The company requires low latency, scalability, and availability.

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

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

**Answer:** D

#### Explanation:

<https://aws.amazon.com/caching/session-management/> <https://aws.amazon.com/elasticache/redis-vs-memcached/>

#### NEW QUESTION 144

A company is having issues with a newly deployed serverless infrastructure that uses Amazon API Gateway, Amazon Lambda, and Amazon DynamoDB. In a steady state, the application performs as expected. However, during peak load, tens of thousands of simultaneous invocations are needed and user requests fail multiple times before succeeding. The company has checked the logs for each component, focusing specifically on Amazon CloudWatch Logs for Lambda. There are no errors logged by the services or applications. What might cause this problem?

- A. Lambda has very little memory assigned, which causes the function to fail at peak load.
- B. Lambda is in a subnet that uses a NAT gateway to reach out to the internet, and the function instance does not have sufficient Amazon EC2 resources in the VPC to scale with the load.
- C. The throttle limit set on API Gateway is very low during peak load, the additional requests are not making their way through to Lambda
- D. DynamoDB is set up in an auto scaling mode
- E. During peak load, DynamoDB adjusts capacity and through successfully.

**Answer:** A

#### NEW QUESTION 148

During a security audit of a Service team's application a Solutions Architect discovers that a username and password for an Amazon RDS database and a set of AWS IAM user credentials can be viewed in the AWS Lambda function code. The Lambda function uses the username and password to run queries on the database and it uses the IAM credentials to call AWS services in a separate management account. The Solutions Architect is concerned that the credentials could grant inappropriate access to anyone who can view the Lambda code. The management account and the Service team's account are in separate AWS Organizations organizational units (OUs). Which combination of changes should the Solutions Architect make to improve the solution's security? (Select TWO)

- A. Configure Lambda to assume a role in the management account with appropriate access to AWS
- B. Configure Lambda to use the stored database credentials in AWS Secrets Manager and enable automatic rotation
- C. Create a Lambda function to rotate the credentials every hour by deploying a new Lambda version with the updated credentials
- D. Use an SCP on the management account OU to prevent IAM users from accessing resources in the Service team's account
- E. Enable AWS Shield Advanced on the management account to shield sensitive resources from unauthorized IAM access

**Answer:** BD

#### NEW QUESTION 149

A company has an application that runs a web service on Amazon EC2 instances and stores .jpg images in Amazon S3. The web traffic has a predictable

baseline, but often demand spikes unpredictably for short periods of time. The application is loosely coupled and stateless. The .jpg images stored in Amazon S3 are accessed frequently for the first 15 to 20 days, they are seldom accessed thereafter but always need to be immediately available. The CIO has asked to find ways to reduce costs.

Which of the following options will reduce costs? (Choose two.)

- A. Purchase Reserved instances for baseline capacity requirements and use On-Demand instances for the demand spikes.
- B. Configure a lifecycle policy to move the .jpg images on Amazon S3 to S3 IA after 30 days.
- C. Use On-Demand instances for baseline capacity requirements and use Spot Fleet instances for the demand spikes.
- D. Configure a lifecycle policy to move the .jpg images on Amazon S3 to Amazon Glacier after 30 days.
- E. Create a script that checks the load on all web servers and terminates unnecessary On-Demand instances.

**Answer: AB**

#### NEW QUESTION 151

A company has an application that generates a weather forecast that is updated every 15 minutes with an output resolution of 1 billion unique positions, each approximately 20 bytes in size (20 Gigabytes per forecast). Every hour, the forecast data is globally accessed approximately 5 million times (1,400 requests per second), and up to 10 times more during weather events. The forecast data is overwritten every update. Users of the current weather forecast application expect responses to queries to be returned in less than two seconds for each request.

Which design meets the required request rate and response time?

- A. Store forecast locations in an Amazon ES cluster
- B. Use an Amazon CloudFront distribution targeting an Amazon API Gateway endpoint with AWS Lambda functions responding to queries as the origin
- C. Enable API caching on the API Gateway stage with a cache-control timeout set for 15 minutes.
- D. Store forecast locations in an Amazon EFS volume
- E. Create an Amazon CloudFront distribution that targets an Elastic Load Balancing group of an Auto Scaling fleet of Amazon EC2 instances that have mounted the Amazon EFS volume
- F. Set the cache-control timeout for 15 minutes in the CloudFront distribution.
- G. Store forecast locations in an Amazon ES cluster
- H. Use an Amazon CloudFront distribution targeting an API Gateway endpoint with AWS Lambda functions responding to queries as the origin
- I. Create an Amazon Lambda@Edge function that caches the data locally at edge locations for 15 minutes.
- J. Store forecast locations in an Amazon S3 as individual object
- K. Create an Amazon CloudFront distribution targeting an Elastic Load Balancing group of an Auto Scaling fleet of EC2 instances, querying the origin of the S3 object
- L. Set the cache-control timeout for 15 minutes in the CloudFront distribution.

**Answer: C**

#### Explanation:

<https://aws.amazon.com/blogs/networking-and-content-delivery/lambdaedge-design-best-practices/>

#### NEW QUESTION 156

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 catalog page. Auto Scaling is configured to maintain the web fleet size based on the ALB health check.

Recently, the application experienced an outage. Auto Scaling continuously replaced the instances during the outage. A subsequent investigation determined that the web server metrics were within the normal range, but the database tier was experiencing high load, resulting in severely elevated query response times.

Which of the following changes together would remediate these issues while improving monitoring capabilities for the availability and functionality of the entire application stack for future growth? (Select TWO.)

- A. Configure read replicas for Amazon RDS MySQL and use the single reader endpoint in the web application to reduce the load on the backend database tier.
- B. Configure the target group health check to point at a simple HTML page instead of a product catalog page and the Amazon Route 53 health check against the product page to evaluate full application functionality
- C. Configure Amazon CloudWatch alarms to notify administrators when the site fails.
- D. Configure the target group health check to use a TCP check of the Amazon EC2 web server and the Amazon Route 53 health check against the product page to evaluate full application functionality
- E. Configure Amazon CloudWatch alarms to notify administrators when the site fails.
- F. Configure an Amazon CloudWatch alarm for Amazon RDS with an action to recover a high-load, impaired RDS instance in the database tier.
- G. Configure an Amazon ElastiCache cluster and place it between the web application and RDS MySQL instances to reduce the load on the backend database tier.

**Answer: BE**

#### NEW QUESTION 157

A company with multiple accounts is currently using a configuration that does not meet the following security governance policies

- Prevent ingress from port 22 to any Amazon EC2 instance
- Require billing and application tags for resources
- Encrypt all Amazon EBS volumes

A Solutions Architect wants to provide preventive and detective controls including notifications about a specific resource, if there are policy deviations.

Which solution should the Solutions Architect implement?

- A. Create an AWS CodeCommit repository containing policy-compliant AWS CloudFormation templates. Create an AWS Service Catalog portfolio. Import the CloudFormation templates by attaching the CodeCommit repository to the portfolio. Restrict users across all accounts to items from the AWS Service Catalog portfolio. Use AWS Config managed rules to detect deviations from the policies.
- B. Configure an Amazon CloudWatch Events rule for deviations, and associate a CloudWatch alarm to send notifications when the TriggeredRules metric is greater than zero.
- C. Use AWS Service Catalog to build a portfolio with products that are in compliance with the governance policies in a central account. Restrict users across all accounts to AWS Service Catalog products. Share a compliant portfolio to other accounts. Use AWS Config managed rules to detect deviations from the policies. Configure an Amazon CloudWatch Events rule to send a notification when a deviation occurs.
- D. Implement policy-compliant AWS CloudFormation templates for each account and ensure that all provisioning is completed by CloudFormation. Configure Amazon Inspector to perform regular checks against resources. Perform policy validation and write the assessment output to Amazon CloudWatch Log.

- E. Create a CloudWatch Logs metric filter to increment a metric when a deviation occurs. Configure a CloudWatch alarm to send notifications when the configured metric is greater than zero.
- F. Restrict users and enforce least privilege access using AWS IAM.
- G. Consolidate all AWS CloudTrail logs into a single account. Send the CloudTrail logs to Amazon Elasticsearch Service (Amazon ES). Implement monitoring, alerting, and reporting using the Kibana dashboard in Amazon ES and with Amazon SNS.

**Answer: C**

#### NEW QUESTION 162

A company has an application written using an in-house software framework. The framework installation takes 30 minutes and is performed with a user data script. Company Developers deploy changes to the application frequently. The framework installation is becoming a bottleneck in this process. Which of the following would speed up this process?

- A. Create a pipeline to build a custom AMI with the framework installed and use this AMI as a baseline for application deployments.
- B. Employ a user data script to install the framework but compress the installation files to make them smaller.
- C. Create a pipeline to parallelize the installation tasks and call this pipeline from a user data script.
- D. Configure an AWS OpsWorks cookbook that installs the framework instead of employing user data.
- E. Use this cookbook as a base for all deployments.

**Answer: A**

#### Explanation:

<https://aws.amazon.com/codepipeline/features/?nc=sn&loc=2>

#### NEW QUESTION 167

A company that is new to AWS reports it has exhausted its service limits across several accounts that are on the Basic Support plan. The company would like to prevent this from happening in the future.

What is the MOST efficient way of monitoring and managing all service limits in the company's accounts?

- A. Use Amazon CloudWatch and AWS Lambda to periodically calculate the limits across all linked accounts using AWS Trusted Advisor, provide notifications using Amazon SNS if the limits are close to exceeding the threshold.
- B. Reach out to AWS Support to proactively increase the limits across all accounts.
- C. That way, the customer avoids creating and managing infrastructure just to raise the service limits.
- D. Use Amazon CloudWatch and AWS Lambda to periodically calculate the limits across all linked accounts using AWS Trusted Advisor, programmatically increase the limits that are close to exceeding the threshold.
- E. Use Amazon CloudWatch and AWS Lambda to periodically calculate the limits across all linked accounts using AWS Trusted Advisor, and use Amazon SNS for notifications if a limit is close to exceeding the threshold.
- F. Ensure that the accounts are using the AWS Business Support plan at a minimum.

**Answer: D**

#### Explanation:

<https://github.com/awslabs/aws-limit-monitor> <https://aws.amazon.com/solutions/limit-monitor/>

#### NEW QUESTION 170

A company has developed a web application that runs on Amazon EC2 instances in one AWS Region. The company has taken on new business in other countries and must deploy its application into other regions to meet low-latency requirements for its users. The regions can be segregated, and an application running in one region does not need to communicate with instances in other regions.

How should the company's Solutions Architect automate the deployment of the application so that it can be MOST efficiently deployed into multiple regions?

- A. Write a bash script that uses the AWS CLI to query the current state in one region and output a JSON representation.
- B. Pass the JSON representation to the AWS CLI, specifying the --region parameter to deploy the application to other regions.
- C. Write a bash script that uses the AWS CLI to query the current state in one region and output an AWS CloudFormation template.
- D. Create a CloudFormation stack from the template by using the AWS CLI, specifying the --region parameter to deploy the application to other regions.
- E. Write a CloudFormation template describing the application's infrastructure in the Resources section. Create a CloudFormation stack from the template by using the AWS CLI, specify multiple regions using the --regions parameter to deploy the application.
- F. Write a CloudFormation template describing the application's infrastructure in the Resources section. Use a CloudFormation stack set from an administrator account to launch stack instances that deploy the application to other regions.

**Answer: D**

#### Explanation:

A stack set lets you create stacks in AWS accounts across regions by using a single AWS CloudFormation template. All the resources included in each stack are defined by the stack set's AWS CloudFormation template. As you create the stack set, you specify the template to use, as well as any parameters and capabilities that the template requires. <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-concepts.html>  
<https://sanderknape.com/2017/07/cloudformation-stacksets-automated-cross-account-region-deployments/>

#### NEW QUESTION 175

A company has a security event whereby an Amazon S3 bucket with sensitive information was made public. Company policy is to never have public S3 objects, and the Compliance team must be informed immediately when any public objects are identified.

How can the presence of a public S3 object be detected, set to trigger alarm notifications, and automatically remediated in the future? (Choose two.)

- A. Turn on object-level logging for Amazon S3. Turn on Amazon S3 event notifications to notify by using an Amazon SNS topic when a PutObject API call is made with a public-read permission.
- B. Configure an Amazon CloudWatch Events rule that invokes an AWS Lambda function to secure the S3 bucket.
- C. Use the S3 bucket permissions for AWS Trusted Advisor and configure a CloudWatch event to notify by using Amazon SNS.
- D. Turn on object-level logging for Amazon S3. Configure a CloudWatch event to notify by using an SNS topic when a PutObject API call with public-read permission is detected in the AWS CloudTrail logs.
- E. Schedule a recursive Lambda function to regularly change all object permissions inside the S3 bucket.

**Answer:** BD

**Explanation:**

<https://aws.amazon.com/blogs/security/how-to-detect-and-automatically-remediate-unintended-permissions-in-a>

**NEW QUESTION 178**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your SAP-C01 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/SAP-C01-dumps.html>