Exam : SAA-C03

Title : Amazon AWS Certified Solutions Architect - Associate (SAA-C03) Exam

Vendor : Amazon

Version : Examtopics(Q623) + V17.95(Q566) = 총 Q667

Q1

A company collects data for temperature, humidity, and atmospheric pressure in cities across multiple continents. The average volume of data that the company collects from each site daily is 500 GB. Each site has a high-speed Internet connection.

The company wants to aggregate the data from all these global sites as quickly as possible in a single Amazon S3 bucket. The solution must minimize operational complexity.

Which solution meets these requirements?

A. Turn on S3 Transfer Acceleration on the destination S3 bucket. Use multipart uploads to directly upload site data to the destination S3 bucket.

B. Upload the data from each site to an S3 bucket in the closest Region. Use S3 Cross-Region Replication to copy objects to the destination S3 bucket. Then remove the data from the origin S3 bucket.

C. Schedule AWS Snowball Edge Storage Optimized device jobs daily to transfer data from each site to the closest Region. Use S3 Cross-Region Replication to copy objects to the destination S3 bucket.

D. Upload the data from each site to an Amazon EC2 instance in the closest Region. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. At regular intervals, take an EBS snapshot and copy it to the Region that contains the destination S3 bucket. Restore the EBS volume in that Region.

Answer: A

https://www.examtopics.com/discussions/amazon/view/84973-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

여러 글로벌 사이트의 데이터를 단일 Amazon S3 버킷에 최대한 빨리 집계하는 동시에

운영 복잡성을 최소화하려면 가장 적합한 솔루션은 옵션 A: 대상 S3 버킷에서 S3 전송 가속화를 설정하고 멀티파트 업로드를 사용하여 사이트 데이터를 대상 S3 버킷에 직접 업로드하는 것입니다.

요약하면 옵션 A 는 여러 글로벌 사이트의 데이터를 단일 Amazon S3 버킷으로 신속하게 집계하는 가장 효율적이고 운영상 간단한 솔루션을 제공합니다. S3 Transfer Acceleration 및 멀티파트 업로드를 활용하여 회사는 복잡성을 최소화하면서 빠른 데이터 수집을 달성할 수 있습니다.

Q2

A company needs the ability to analyze the log files of its proprietary application. The logs are stored in JSON format in an Amazon S3 bucket. Queries will be simple and will run on-demand. A solutions architect needs to perform the analysis with minimal changes to the existing architecture.

What should the solutions architect do to meet these requirements with the LEAST amount of operational overhead?

A. Use Amazon Redshift to load all the content into one place and run the SQL queries as needed.

B. Use Amazon CloudWatch Logs to store the logs. Run SQL queries as needed from the Amazon CloudWatch console.

C. Use Amazon Athena directly with Amazon S3 to run the queries as needed.

D. Use AWS Glue to catalog the logs. Use a transient Apache Spark cluster on Amazon EMR to run the SQL queries as needed.

Answer: C

https://www.examtopics.com/discussions/amazon/view/84848-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

S3 에 쿼리하는 건 Athena.

Athena 가 사용 가능한 모든 리전에서 Amazon Athena 를 사용하여 표준 SQL 로 Amazon S3 인벤토리를 쿼리할 수 있습니다.

https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/storage-inventory-athena-query.html

Athena 로 JSON 쿼리 가능.

Amazon Athena 를 사용하면 JSON 인코딩 값을 구문 분석하고, JSON 에서 데이터를

추출하고, 값을 검색하고, JSON 배열의 길이와 크기를 찾을 수 있습니다.
https://docs.aws.amazon.com/athena/latest/ug/querying-JSON.html

Q3
A company uses AWS Organizations to manage multiple AWS accounts for different departments. The management account has an Amazon S3 bucket that contains project reports. The company wants to limit access to this S3 bucket to only users of accounts within the organization in AWS Organizations.
Which solution meets these requirements with the LEAST amount of operational overhead?
A. Add the aws PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy.
B. Create an organizational unit (OU) for each department. Add the aws:PrincipalOrgPaths global condition key to the S3 bucket policy.
C. Use AWS CloudTrail to monitor the CreateAccount, InviteAccountToOrganization, LeaveOrganization, and RemoveAccountFromOrganization events. Update the S3 bucket policy accordingly.
D. Tag each user that needs access to the S3 bucket. Add the aws:PrincipalTag global condition key to the S3 bucket policy.
Answer: A
https://www.examtopics.com/discussions/amazon/view/84838-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(O) : aws:PrincipalOrgID 라는 새로운 조건 키를 권한 정책에 사용하여 조직 내의 계정에 해당하는 IAM 보안 주체(사용자 및 역할)만 리소스에 액세스할 수 있도록 합니다.
https://aws.amazon.com/ko/about-aws/whats-new/2018/05/principal-org-id/
B(X) : aws:PrincipalOrgPaths 는 다중 값 조건 키입니다. 다중 값 키에는 하나 이상의 값이 목록 형식으로 포함됩니다. 결과는 논리적 OR 입니다.
https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/reference_policies_condition-keys.html
C(X) : CloudTrail 은 리소스 내역을 기록/전송하는 서비스로 지문에서 요구하는 사항에 불필요.
D(X) : 각 사용자마다 태그를 달아야 하므로 최소 운영 오버헤드라는 조건 불충족.
aws:PrincipalTag/tag-key : 문자열 연산자를 사용합니다. 이 키를 사용하여 요청한 보안 주체에 연결된 태그를 정책에서 지정한 태그와 비교합니다.

https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/reference_policies_condition-keys.html

설명 2:
aws:PrincipalOrgID 전역 키는 조직의 모든 AWS 계정에 대한 모든 계정 ID 를 나열하는 대신 사용할 수 있습니다. 예를 들어 다음 Amazon S3 버킷 정책은 XXX 조직의 모든 계정 구성원이 시험 주제 버킷에 객체를 추가하도록 허용합니다.

```
{"Version": "2020-09-10",
"Statement": {
"Sid": "AllowPutObject",
"Effect": "Allow",
"Principal": "*",
"Action": "s3:PutObject",
"Resource": "arn:aws:s3:::examtopics/*",
"Condition": {"StringEquals":
{"aws:PrincipalOrgID":["XXX"]}}}}
```

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition-keys.html

Q4
An application runs on an Amazon EC2 instance in a VPC. The application processes logs that are stored in an Amazon S3 bucket. The EC2 instance needs to access the S3 bucket without connectivity to the internet.
Which solution will provide private network connectivity to Amazon S3?
A. Create a gateway VPC endpoint to the S3 bucket.
B. Stream the logs to Amazon CloudWatch Logs. Export the logs to the S3 bucket.
C. Create an instance profile on Amazon EC2 to allow S3 access.
D. Create an Amazon API Gateway API with a private link to access the S3 endpoint.
Answer: A
https://www.examtopics.com/discussions/amazon/view/84980-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
VPC-S3 간 인터넷을 통하지 않는 연결 = S3 VPC Gateway Endpoint. 정답은 A.

설명 2:
VPC 종단점을 사용하면 공용 인터넷을 사용하는 대신 사설 네트워크를 사용하여 AWS 서비스에 연결할 수 있습니다.

Q5
A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user-uploaded documents in an Amazon EBS volume. For better scalability and availability, the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone, placing both behind an Application Load Balancer. After completing this change, users reported that, each time they refreshed the website, they could see one subset of their documents or the other, but never all of the documents at the same time.
What should a solutions architect propose to ensure users see all of their documents at once?
A. Copy the data so both EBS volumes contain all the documents.
B. Configure the Application Load Balancer to direct a user to the server with the documents.
C. Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS.
D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server.
Answer: C
https://www.examtopics.com/discussions/amazon/view/84981-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
EBS와 EFS의 가장 큰 차이점 중 하나는 EBS는 단일 AZ안에서만 접근이 가능한 저장소인 반면, EFS 는 다중 AZ 안에서도 접근이 가능한 저장소라는 점입니다. 위 문제에서는 초기 단일 AZ 에서 운영하던 EC2 및 EBS 를 복제한뒤 AZ 를 2 중화하여 멀티 EC2 및 EBS 시스템으로 구성하였지만, 각 AZ 내에서 공유되지 않는 EBS 저장소를 별도로 운영하였기때문에 고객들에게 일관성있는 데이터를 제공할 수 없었던 것으로 보입니다. 이는 각 AZ 의 EC2 인스턴스가 동일한 저장소를 공유하도록 함으로써 해결할 수 있을 것 같습니다. 초기 EBS 에 저장되어있던 데이터들을 일관성있게 보정하여 EFS 로 일회성 마이그레이션을 수행한뒤 EC2 어플리케이션 서버 인스턴스가 EBS가 아닌 EFS에 데이터를 저장하도록 변경하는 것이 바람직해보입니다.

설명 2:

Amazon EFS 는 AWS 클라우드에서 파일 스토리지를 제공합니다. Amazon EFS 를 사용하면 파일 시스템을 생성하고 파일 시스템을 Amazon EC2 인스턴스에 탑재한 다음 파일 시스템에서 데이터를 읽고 쓸 수 있습니다. Network File System 버전 4.0 및 4.1(NFSv4) 프로토콜을 통해 VPC 에 Amazon EFS 파일 시스템을 탑재할 수 있습니다. Amazon EFS Mount Helper 와 함께 최신 Amazon Linux, Redhat 및 Ubuntu AMI 에 있는 것과 같은 현재 세대 Linux NFSv4.1 클라이언트를 사용하는 것이 좋습니다. 지침은 amazon-efs-utils 도구 사용 단원을 참조하십시오.

이 프로토콜을 지원하는 Amazon EC2 Linux Amazon 머신 이미지(AMI) 목록은 NFS 지원을 참조하십시오. 일부 AMI 의 경우 파일 시스템을 Amazon EC2 인스턴스에 탑재하려면 NFS 클라이언트를 설치해야 합니다. 지침은 NFS 클라이언트 설치를 참조하십시오.

여러 NFS 클라이언트에서 동시에 Amazon EFS 파일 시스템에 액세스할 수 있으므로 단일 연결 이상으로 확장되는 애플리케이션이 파일 시스템에 액세스할 수 있습니다. 동일한 AWS 리전 내의 여러 가용 영역에서 실행되는 Amazon EC2 인스턴스는 파일 시스템에 액세스할 수 있으므로 많은 사용자가 공통 데이터 원본에 액세스하고 공유할 수 있습니다.

https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html#how-it-works-ec2

Q6

A company uses NFS to store large video files in on-premises network attached storage. Each video file ranges in size from 1 MB to 500 GB. The total storage is 70 TB and is no longer growing. The company decides to migrate the video files to Amazon S3. The company must migrate the video files as soon as possible while using the least possible network bandwidth.

Which solution will meet these requirements?

A. Create an S3 bucket. Create an IAM role that has permissions to write to the S3 bucket. Use the AWS CLI to copy all files locally to the S3 bucket.

B. Create an AWS Snowball Edge job. Receive a Snowball Edge device on premises. Use the Snowball Edge client to transfer data to the device. Return the device so that AWS can import the data into Amazon S3.

C. Deploy an S3 File Gateway on premises. Create a public service endpoint to connect to the S3 File Gateway. Create an S3 bucket. Create a new NFS file share on the S3 File Gateway. Point the new file share to the S3 bucket. Transfer the data from the existing NFS file share to the S3 File Gateway.

D. Set up an AWS Direct Connect connection between the on-premises network and AWS.

Deploy an S3 File Gateway on premises. Create a public virtual interface (VIF) to connect to the S3 File Gateway. Create an S3 bucket. Create a new NFS file share on the S3 File Gateway. Point the new file share to the S3 bucket. Transfer the data from the existing NFS file share to the S3 File Gateway.
Answer: B
https://www.examtopics.com/discussions/amazon/view/84875-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
가능한 한 최소한의 네트워크 대역폭을 사용하라 했으니 아예 오프라인에서 Snowball Edge 로 올리는 게 맞음.
AWS Snowball 및 AWS Snowball Edge 는 기존 저장소에서 네트워크 대역폭이 충분하지 않을 때, 대용량 데이터 세트를 클라우드로 이전하는데 도움이 됩니다.
Snowball 장치는 80TB, Snowball Edge 는 100TB 까지 한번에 이동 가능합니다.
https://aws.amazon.com/ko/blogs/korea/aws-snowball-and-aws-snowball-edge-available-in-asia-pacific-seoul-region/

설명 2:
Snowball 과 Snowball Edge 의 기본적인 차이점은 제공하는 용량입니다. Snowball 은 총 50TB 또는 80TB 를 제공하며 그 중 42TB 또는 72TB 를 사용할 수 있고 Amazon Snowball Edge 는 100TB 를 제공하며 그 중 83TB 를 사용할 수 있습니다.

Q7
A company has an application that ingests incoming messages. Dozens of other applications and microservices then quickly consume these messages. The number of messages varies drastically and sometimes increases suddenly to 100,000 each second. The company wants to decouple the solution and increase scalability.
Which solution meets these requirements?
A. Persist the messages to Amazon Kinesis Data Analytics. Configure the consumer applications to read and process the messages.
B. Deploy the ingestion application on Amazon EC2 instances in an Auto Scaling group to scale the number of EC2 instances based on CPU metrics.
C. Write the messages to Amazon Kinesis Data Streams with a single shard. Use an AWS Lambda function to preprocess messages and store them in Amazon DynamoDB. Configure the consumer applications to read from DynamoDB to process the messages.

D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with multiple Amazon Simple Queue Service (Amazon SOS) subscriptions. Configure the consumer applications to process the messages from the queues.
Answer: D
https://www.examtopics.com/discussions/amazon/view/84721-exam-aws-certified-solutions-architect-associate-saa-c03/

설명
https://aws.amazon.com/sqs/features/
들어오는 요청을 Amazon SQS 로 라우팅함으로써 회사는 처리 인스턴스에서 작업 요청을 분리할 수 있습니다. 이를 통해 대기열 크기에 따라 인스턴스 수를 확장하여 필요할 때 더 많은 리소스를 제공할 수 있습니다. 또한 대기열 크기를 기반으로 하는 Auto Scaling 그룹을 사용하면 워크로드에 따라 자동으로 인스턴스 수를 늘리거나 줄일 수 있습니다. 대기열에서 읽을 수 있도록 소프트웨어를 업데이트하면 보다 효율적인 방식으로 작업 요청을 처리할 수 있어 시스템 성능이 향상됩니다.

솔루션을 분리 = SQS.

Q8
A company is migrating a distributed application to AWS. The application serves variable workloads. The legacy platform consists of a primary server that coordinates jobs across multiple compute nodes. The company wants to modernize the application with a solution that maximizes resiliency and scalability.
How should a solutions architect design the architecture to meet these requirements?
A. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs. Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure EC2 Auto Scaling to use scheduled scaling.
B. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs. Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure EC2 Auto Scaling based on the size of the queue.
C. Implement the primary server and the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure AWS CloudTrail as a destination for the jobs. Configure EC2 Auto Scaling based on the load on the primary server.
D. Implement the primary server and the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure Amazon EventBridge (Amazon

CloudWatch Events) as a destination for the jobs. Configure EC2 Auto Scaling based on the load on the compute nodes.
Answer: B
https://www.examtopics.com/discussions/amazon/view/84679-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : Scheduled Scaling 은 실시간 현황에 맞춰 적용되는 탄력성이 부족.
B(O) : SQS Queue 로 갑작스레 작업이 몰려도 추후 처리하도록 보관 가능. Auto Scaling 그룹으로 여러 EC2 인스턴스의 확장/축소를 적절하게 지원.
C(X) : CloudTrail 은 리소스 내역을 기록/전송하는 서비스.
D(X) : CPU 사용률에 따라 EC2 Auto Scaling 하려면 Target Tracking Policy 를 사용하면 됨. 대상 추적 조정 정책을 사용하여 Application Load Balancer 의 RequestCountPerTarget 지표 또는 평균 CPU 사용률 같은 지표에 따라 확장하는 것이 좋습니다. 용량이 증가할 때 감소하고 용량이 감소할 때 증가하는 지표를 사용하여 비례적으로 확장하거나 대상 추적을 사용하여 인스턴스 수를 늘릴 수 있습니다.
https://docs.aws.amazon.com/ko_kr/autoscaling/ec2/userguide/as-scaling-simple-step.html

설명 2:
복원력과 확장성을 극대화하기 위한 최상의 솔루션은 Amazon SQS 대기열을 작업의 대상으로 사용하는 것입니다. 이렇게 하면 컴퓨팅 노드에서 기본 서버가 분리되어 독립적으로 확장할 수 있습니다. 이는 또한 실패 시 일자리 손실을 방지하는 데 도움이 됩니다. 컴퓨팅 노드에 대해 Amazon EC2 인스턴스의 Auto Scaling 그룹을 사용하면 워크로드에 따라 자동 조정이 가능합니다. 이 경우 Amazon SQS 대기열의 크기를 기반으로 Auto Scaling 그룹을 구성하는 것이 좋습니다. 이는 기본 서버 또는 컴퓨팅 노드의 로드보다 실제 워크로드를 더 잘 나타내는 지표입니다. 이 접근 방식은 애플리케이션이 가변 워크로드를 처리할 수 있도록 하는 동시에 필요에 따라 컴퓨팅 노드를 자동으로 확장 또는 축소하여 비용을 최소화합니다.

Q9
A company is running an SMB file server in its data center. The file server stores large files that are accessed frequently for the first few days after the files are created. After 7 days the files are rarely accessed.
The total data size is increasing and is close to the company's total storage capacity. A

solutions architect must increase the company's available storage space without losing low-latency access to the most recently accessed files. The solutions architect must also provide file lifecycle management to avoid future storage issues.
Which solution will meet these requirements?
A. Use AWS DataSync to copy data that is older than 7 days from the SMB file server to AWS.
B. Create an Amazon S3 File Gateway to extend the company's storage space. Create an S3 Lifecycle policy to transition the data to S3 Glacier Deep Archive after 7 days.
C. Create an Amazon FSx for Windows File Server file system to extend the company's storage space.
D. Install a utility on each user's computer to access Amazon S3. Create an S3 Lifecycle policy to transition the data to S3 Glacier Flexible Retrieval after 7 days.
Answer: B
https://www.examtopics.com/discussions/amazon/view/84680-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
사용 가능한 스토리지 공간을 늘림 = Storage Gateway. 답은 B.
A(X) : AWS 에서 무슨 스토리지를 사용할 건지에 대한 언급이 없음. 또한 하이브리드 스토리지인 Storage Gateway 가 더 적절한 방식임.
B(O) : 정답. 스토리지 게이트웨이는 온프레미스 스토리지와 AWS 스토리지를 합쳐 사실상 무제한의 스토리지를 향유하는 것을 목적으로 하는 서비스.
Amazon S3 File Gateway 의 사용 사례로는 (a) 최근에 액세스한 데이터에 대해 빠른 로컬 액세스를 유지하면서 온프레미스 파일 데이터를 Amazon S3 로 마이그레이션. SMB(서버 메시지 블록) 버전 2 및 3 을 사용하여 게이트웨이에 연결하는 Windows 클라이언트를 지원합니다.
https://aws.amazon.com/ko/storagegateway/faqs/?nc=sn&loc=6
C(X) : A 와 같은 이유로 오답.
D(X) : SMB 사용 여부 불투명.

설명 2:
Amazon S3 File Gateway 는 온프레미스 애플리케이션이 Amazon S3 클라우드 스토리지를 원활하게 사용할 수 있도록 하는 하이브리드 클라우드 스토리지 서비스입니다. Amazon S3 에 대한 파일 인터페이스를 제공하고 SMB 및 NFS 프로토콜을 지원합니다. 또한 지정된 기간이 지나면 데이터를 S3 Standard 에서 S3 Glacier Deep Archive 로 자동 전환할 수 있는 S3 수명 주기 정책을 지원합니다. 이 솔루션은 짧은 대기 시간 액세스를 유지하면서 회사의 사용 가능한 저장 공간을 늘리는 요구 사항을 충족합니다.

가장 최근에 액세스한 파일에 저장하고 파일 수명 주기 관리를 제공하여 향후 스토리지 문제를 방지합니다.

Q10

A company is building an ecommerce web application on AWS. The application sends information about new orders to an Amazon API Gateway REST API to process. The company wants to ensure that orders are processed in the order that they are received.

Which solution will meet these requirements?

A. Use an API Gateway integration to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic when the application receives an order. Subscribe an AWS Lambda function to the topic to perform processing.

B. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) FIFO queue when the application receives an order. Configure the SQS FIFO queue to invoke an AWS Lambda function for processing.

C. Use an API Gateway authorizer to block any requests while the application processes an order.

D. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) standard queue when the application receives an order. Configure the SQS standard queue to invoke an AWS Lambda function for processing.

Answer: B

https://www.examtopics.com/discussions/amazon/view/84681-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

주문이 접수된 순서대로 처리되도록 하기 위한 최상의 솔루션은 Amazon SQS FIFO(선입선출) 대기열을 사용하는 것입니다. 이 유형의 대기열은 메시지를 보내고 받는 정확한 순서를 유지합니다. 이 경우 애플리케이션은 새 주문에 대한 정보를 Amazon API Gateway REST API 로 보낼 수 있습니다. 그런 다음 API Gateway 통합을 사용하여 처리를 위해 메시지를 Amazon SQS FIFO 대기열로 보낼 수 있습니다. 그런 다음 AWS Lambda 함수를 호출하여 각 주문에 필요한 처리를 수행하도록 대기열을 구성할 수 있습니다. 이렇게 하면 주문이 접수된 정확한 순서대로 처리됩니다.

즉. 주문한 순서대로 = FIFO

Q11

A company has an application that runs on Amazon EC2 instances and uses an Amazon Aurora database. The EC2 instances connect to the database by using user names and passwords that are stored locally in a file. The company wants to minimize the operational overhead of credential management.

What should a solutions architect do to accomplish this goal?

A. Use AWS Secrets Manager. Turn on automatic rotation.

B. Use AWS Systems Manager Parameter Store. Turn on automatic rotation.

C. Create an Amazon S3 bucket to store objects that are encrypted with an AWS Key Management Service (AWS KMS) encryption key. Migrate the credential file to the S3 bucket. Point the application to the S3 bucket.

D. Create an encrypted Amazon Elastic Block Store (Amazon EBS) volume for each EC2 instance. Attach the new EBS volume to each EC2 instance. Migrate the credential file to the new EBS volume. Point the application to the new EBS volume.

Answer: A

https://www.examtopics.com/discussions/amazon/view/84682-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

A(O) : Secrets Manager 는 자격증명을 저장해두고 관리할 수 있는 서비스.

AWS Secrets Manager 는 애플리케이션, 서비스 및 IT 리소스에 대한 액세스를 보호하는 데 도움이 되는 보안 정보 관리 서비스입니다. 이 서비스를 사용하면 수명 주기 동안 데이터베이스 자격 증명, API 키 및 기타 보안 정보를 손쉽게 교체, 관리 및 검색할 수 있습니다. https://aws.amazon.com/ko/secrets-manager/faqs/

Secrets Manager 에서 보안 암호에 대한 자동 교체를 설정할 수 있습니다.

https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotating-secrets.html

B(X) : Systems Manager Parameter Store 는 구성 데이터 같은 걸 코드와 분리하여 원치 않는 노출을 막는 것.

Q:AWS Systems Manager parameter store 란 무엇입니까? AWS Systems Manager 는 데이터베이스 문자열과 같은 평문 데이터든 암호와 같은 비밀이든 관계없이 구성 데이터를 관리할 수 있는 중앙 스토어를 제공합니다. 따라서 비밀과 구성 데이터를 코드와 분리할 수 있습니다. https://aws.amazon.com/ko/systems-manager/faq/

C(X) : KMS 키는 S3 버킷에 저장하는 것이 아니라 Secrets Manager 등을 이용해 관리.

D(X) : C 와 비슷한 이유로 오답."

Q12

A global company hosts its web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The web application has static data and dynamic data. The company stores its static data in an Amazon S3 bucket. The company wants to improve performance and reduce latency for the static data and dynamic data. The company is using its own domain name registered with Amazon Route 53.

What should a solutions architect do to meet these requirements?

A. Create an Amazon CloudFront distribution that has the S3 bucket and the ALB as origins. Configure Route 53 to route traffic to the CloudFront distribution.

B. Create an Amazon CloudFront distribution that has the ALB as an origin. Create an AWS Global Accelerator standard accelerator that has the S3 bucket as an endpoint Configure Route 53 to route traffic to the CloudFront distribution.

C. Create an Amazon CloudFront distribution that has the S3 bucket as an origin. Create an AWS Global Accelerator standard accelerator that has the ALB and the CloudFront distribution as endpoints. Create a custom domain name that points to the accelerator DNS name. Use the custom domain name as an endpoint for the web application.

D. Create an Amazon CloudFront distribution that has the ALB as an origin. Create an AWS Global Accelerator standard accelerator that has the S3 bucket as an endpoint. Create two domain names. Point one domain name to the CloudFront DNS name for dynamic content. Point the other domain name to the accelerator DNS name for static content. Use the domain names as endpoints for the web application.

Answer: A

https://www.examtopics.com/discussions/amazon/view/85010-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

A(O) : 배포를 만들 때 CloudFront 가 파일에 대한 요청을 보내는 원본을 지정합니다. CloudFront 에서 여러 원본을 사용할 수 있습니다. 예를 들어 Amazon S3 버킷, MediaStore 컨테이너, MediaPackage 채널, Application Load Balancer 또는 AWS Lambda 함수 URL 을 사용할 수 있습니다.

https://docs.aws.amazon.com/ko_kr/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html

Amazon Route 53 을 구성하여 CloudFront 배포로 트래픽을 라우팅합니다. 이하 항목 참고

https://docs.aws.amazon.com/ko_kr/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html

B(X) : 지문의 상황은 애플리케이션 계층에서 벌어지는 일이므로 TCP/UDP 를 사용하는 AWS Global Accelerator 는 부적절.

C(X) : B 와 같은 이유로 오답.
D(X) : B 와 같은 이유로 오답.

설명 2:
정적 콘텐츠는 S3 의 클라우드 프런트 엣지 위치와 ALB 뒤의 동적 콘텐츠 EC2 에서 캐싱할 수 있습니다. 그 성능은 하나의 엔드포인트가 ALB 이고 다른 클라우드 프런트인 Global Accelerator 에 의해 개선될 수 있습니다.
따라서 사용자 지정 도메인 이름 끝점과 관련하여 웹 응용 프로그램은 웹 응용 프로그램에 대한 사용자 지정 도메인 지점에 대한 R53 별칭 레코드입니다.
https://aws.amazon.com/blogs/networking-and-content-delivery/improving-availability-andperformance-for-app

Q13
A company performs monthly maintenance on its AWS infrastructure. During these maintenance activities, the company needs to rotate the credentials for its Amazon RDS for MySQL databases across multiple AWS Regions.
Which solution will meet these requirements with the LEAST operational overhead?
A. Store the credentials as secrets in AWS Secrets Manager. Use multi-Region secret replication for the required Regions. Configure Secrets Manager to rotate the secrets on a schedule.
B. Store the credentials as secrets in AWS Systems Manager by creating a secure string parameter. Use multi-Region secret replication for the required Regions. Configure Systems Manager to rotate the secrets on a schedule.
C. Store the credentials in an Amazon S3 bucket that has server-side encryption (SSE) enabled. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke an AWS Lambda function to rotate the credentials.
D. Encrypt the credentials as secrets by using AWS Key Management Service (AWS KMS) multi-Region customer managed keys. Store the secrets in an Amazon DynamoDB global table. Use an AWS Lambda function to retrieve the secrets from DynamoDB. Use the RDS API to rotate the secrets.
Answer: A
https://www.examtopics.com/discussions/amazon/view/84728-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

다중 리전 애플리케이션에 필수 리전의 복제된 암호에 대한 액세스 권한을 부여하고 Secrets Manager 를 사용하여 복제본이 기본 암호와 동기화된 상태를 유지할 수 있습니다. Secrets Manager 를 사용하면 데이터베이스 자격 증명, API 키 및 기타 비밀을 포함한 비밀을 저장, 검색, 관리 및 교체할 수 있습니다.
https://aws.amazon.com/ko/blogs/security/how-to-replicate-secrets-aws-secrets-manager-multiple-regions/

Q14
A company runs an ecommerce application on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales based on CPU utilization metrics. The ecommerce application stores the transaction data in a MySQL 8.0 database that is hosted on a large EC2 instance.
The database's performance degrades quickly as application load increases. The application handles more read requests than write transactions. The company wants a solution that will automatically scale the database to meet the demand of unpredictable read workloads while maintaining high availability.
Which solution will meet these requirements?
A. Use Amazon Redshift with a single node for leader and compute functionality.
B. Use Amazon RDS with a Single-AZ deployment Configure Amazon RDS to add reader instances in a different Availability Zone.
C. Use Amazon Aurora with a Multi-AZ deployment. Configure Aurora Auto Scaling with Aurora Replicas.
D. Use Amazon ElastiCache for Memcached with EC2 Spot Instances.
Answer: C
https://www.examtopics.com/discussions/amazon/view/85019-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : 단일 노드에서 고가용성 불만족. RedShift 는 MySQL 과 같은 관계형 데이터베이스 서비스가 아니라 데이터 웨어하우스 서비스.
B(X) : 단일 AZ 이기 때문에 고가용성 불만족.
C(O) : Aurora 는 자동으로 3 개의 AZ 에 6 개의 복제본을 생성. 이러한 복제본은 읽기 부하 분산 효과가 있음.
D(X) : 스팟 인스턴스를 사용할 때는 언제든 중지될 위험에 대비해야 함이 기본임. 즉,

중지될 수 있는 위험이 높은 인스턴스라는 이야기. 그리고 다중 AZ 를 사용하지 않으므로 고가용성을 만족하지 못했음.

설명 2:
Aurora 는 RDS 에서 MySQL 보다 5 배 향상된 성능을 제공하며 쓰기보다 더 많은 읽기 요청을 처리합니다. 고가용성 유지 = 다중 AZ 배포.

Q15
A company recently migrated to AWS and wants to implement a solution to protect the traffic that flows in and out of the production VPC. The company had an inspection server in its on-premises data center. The inspection server performed specific operations such as traffic flow inspection and traffic filtering. The company wants to have the same functionalities in the AWS Cloud.
Which solution will meet these requirements?
A. Use Amazon GuardDuty for traffic inspection and traffic filtering in the production VPC.
B. Use Traffic Mirroring to mirror traffic from the production VPC for traffic inspection and filtering.
C. Use AWS Network Firewall to create the required rules for traffic inspection and traffic filtering for the production VPC.
D. Use AWS Firewall Manager to create the required rules for traffic inspection and traffic filtering for the production VPC.
Answer: C
https://www.examtopics.com/discussions/amazon/view/84731-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
AWS Network Firewall 은 필요에 따라 검사와 필터링을 모두 지원합니다.

설명 2:
A(X) : GuardDuty 는 계정 보호 서비스.
Amazon GuardDuty 는 AWS 계정 및 워크로드에서 악의적 활동을 모니터링하고 상세한 보안 결과를 제공하여 가시성 및 해결을 촉진하는 위협 탐지 서비스입니다.
https://aws.amazon.com/ko/guardduty/
B(X) : 트래픽 미러링은 네트워크 트래픽 복사 서비스.
트래픽 미러링은 유형의 탄력적 네트워크 인터페이스에서 네트워크 트래픽을 복사하는 데

사용할 수 있는 Amazon VPC 기능입니다.
https://docs.aws.amazon.com/vpc/latest/mirroring/what-is-traffic-mirroring.html
C(O) : AWS Network Firewall 을 사용하면 VPC 경계에서 네트워크 트래픽을 필터링할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/network-firewall.html
D(X) : Firewall Manager 는 중앙에서 방화벽 규칙 관리하는 서비스.
AWS Firewall Manager 는 AWS Organization 의 여러 계정과 애플리케이션에서 방화벽 규칙을 중앙에서 구성 및 관리할 수 있는 보안 관리 서비스입니다. AWS Firewall Manager 를 사용하면 조직의 여러 계정 및 리소스에 대한 AWS WAF 규칙, AWS Shield Advanced 보호, Amazon Virtual Private Cloud(VPC) 보안 그룹 및 AWS Network Firewall 및 Amazon Route 53 Resolver DNS Firewall 규칙을 중앙에서 구성할 수 있습니다.
https://aws.amazon.com/ko/firewall-manager/faqs/

Q16
A company hosts a data lake on AWS. The data lake consists of data in Amazon S3 and Amazon RDS for PostgreSQL. The company needs a reporting solution that provides data visualization and includes all the data sources within the data lake. Only the company's management team should have full access to all the visualizations. The rest of the company should have only limited access.
Which solution will meet these requirements?
A. Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate IAM roles.
B. Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate users and groups.
C. Create an AWS Glue table and crawler for the data in Amazon S3. Create an AWS Glue extract, transform, and load (ETL) job to produce reports. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.
D. Create an AWS Glue table and crawler for the data in Amazon S3. Use Amazon Athena Federated Query to access data within Amazon RDS for PostgreSQL. Generate reports by using Amazon Athena. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.
Answer: B
https://www.examtopics.com/discussions/amazon/view/84732-exam-aws-certified-solut

ions-architect-associate-saa-c03/

설명 1:
시각화 = QuickSight. A,B 둘 중 하나가 정답. 대시보드를 그룹과 사용자와 공유해야하므로 정답은 B.
기본적으로 Amazon QuickSight 의 대시보드는 누구와도 공유되지 않으며 소유자만 액세스할 수 있습니다. 그러나 대시보드를 게시한 후에는 QuickSight 계정의 다른 사용자 또는 그룹과 공유할 수 있습니다.
https://docs.aws.amazon.com/quicksight/latest/user/sharing-a-dashboard.html

설명 2:
Amazon QuickSight 는 PostgreSQL 용 Amazon S3 및 Amazon RDS 를 비롯한 다양한 데이터 소스에서 대화형 대시보드 및 보고서를 생성할 수 있는 데이터 시각화 서비스입니다. 모든 데이터 소스를 연결하고 QuickSight 에서 새 데이터 세트를 만든 다음 대시보드를 게시하여 데이터를 시각화할 수 있습니다. 또한 적절한 사용자 및 그룹과 대시보드를 공유하고 IAM 역할 및 권한을 사용하여 액세스 수준을 제어할 수 있습니다.

Q17
A company is implementing a new business application. The application runs on two Amazon EC2 instances and uses an Amazon S3 bucket for document storage. A solutions architect needs to ensure that the EC2 instances can access the S3 bucket.
What should the solutions architect do to meet this requirement?
A. Create an IAM role that grants access to the S3 bucket. Attach the role to the EC2 instances.
B. Create an IAM policy that grants access to the S3 bucket. Attach the policy to the EC2 instances.
C. Create an IAM group that grants access to the S3 bucket. Attach the group to the EC2 instances.
D. Create an IAM user that grants access to the S3 bucket. Attach the user account to the EC2 instances.
Answer: A
https://www.examtopics.com/discussions/amazon/view/85032-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

https://aws.amazon.com/premiumsupport/knowledge-center/ec2-instance-access-s3-bucket/

설명 2:
EC2 인스턴스가 S3 버킷에 액세스할 수 있는 권한이 있어야 하므로 IAM 역할을 부여해야 함.
EC2 인스턴스에서 S3 버킷에 연결하려면 다음을 실행해야 합니다.
1. Amazon S3 에 대한 액세스 권한을 부여하는 AWS Identity and Access Management(IAM) 프로파일 역할을 생성합니다.
2. 인스턴스에 IAM 인스턴스 프로파일을 연결합니다.
3. S3 버킷에 대한 권한을 확인합니다.
https://aws.amazon.com/ko/premiumsupport/knowledge-center/ec2-instance-access-s3-bucket/

Q18
An application development team is designing a microservice that will convert large images to smaller, compressed images. When a user uploads an image through the web interface, the microservice should store the image in an Amazon S3 bucket, process and compress the image with an AWS Lambda function, and store the image in its compressed form in a different S3 bucket.
A solutions architect needs to design a solution that uses durable, stateless components to process the images automatically.
Which combination of actions will meet these requirements? (Choose two.)
A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket.
B. Configure the Lambda function to use the Amazon Simple Queue Service (Amazon SQS) queue as the invocation source. When the SQS message is successfully processed, delete the message in the queue.
C. Configure the Lambda function to monitor the S3 bucket for new uploads. When an uploaded image is detected, write the file name to a text file in memory and use the text file to keep track of the images that were processed.
D. Launch an Amazon EC2 instance to monitor an Amazon Simple Queue Service (Amazon SQS) queue. When items are added to the queue, log the file name in a text file on the EC2 instance and invoke the Lambda function.
E. Configure an Amazon EventBridge (Amazon CloudWatch Events) event to monitor the S3

bucket. When an image is uploaded, send an alert to an Amazon ample Notification Service (Amazon SNS) topic with the application owner's email address for further processing.
Answer: A, B
https://www.examtopics.com/discussions/amazon/view/85033-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A,E 조합으로 S3 버킷->EventBridge->SNS Topic->SQS->Lambda 프로세스도 가능하긴 한데, A,B 조합으로 S3->SQS->Lambda 가 훨씬 운영 및 비용 효율적.
・S3 Events -> SQS Queue
Amazon S3 은 다음과 같은 대상으로 이벤트 알림 메시지를 보낼 수 있습니다....◎Amazon Simple Queue Service(Amazon SQS) 대기열
https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/NotificationHowTo.html
・SQS Queue -> Lambda
Lambda 함수를 사용하여 Amazon Simple Queue Service(Amazon SQS) 대기열의 메시지를 처리할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/lambda/latest/dg/with-sqs.html

설명 2:
Amazon Simple Queue Service(SQS) 대기열을 생성하고 이미지가 S3 버킷에 업로드될 때 SQS 대기열에 알림을 보내도록 S3 버킷을 구성하면 Lambda 함수가 상태 비저장 및 내구성 방식으로 트리거됩니다.
SQS 대기열을 호출 소스로 사용하도록 Lambda 함수를 구성하고 성공적으로 처리된 후 대기열에서 메시지를 삭제하면 Lambda 함수가 상태 비저장 및 내구성 방식으로 이미지를 처리합니다.
Amazon SQS는 마이크로서비스, 분산 시스템 및 서버리스 애플리케이션을 분리하고 확장할 수 있는 완전관리형 메시지 대기열 서비스입니다. SQS 는 메시지 지향 미들웨어 관리 및 운영과 관련된 복잡성과 오버헤드를 제거하고 개발자가 차별화 작업에 집중할 수 있도록 합니다. 새 이미지가 S3 버킷에 업로드되면 SQS 는 Lambda 함수를 트리거하여 이미지를 처리하고 압축합니다. 이미지가 처리되면 SQS 메시지가 삭제되어 Lambda 함수가 상태 비저장 및 내구성이 보장됩니다.

Q19
A company has a three-tier web application that is deployed on AWS. The web servers are deployed in a public subnet in a VPC. The application servers and database servers are

deployed in private subnets in the same VPC. The company has deployed a third-party virtual firewall appliance from AWS Marketplace in an inspection VPC. The appliance is configured with an IP interface that can accept IP packets.
A solutions architect needs to integrate the web application with the appliance to inspect all traffic to the application before the traffic reaches the web server.
Which solution will meet these requirements with the LEAST operational overhead?
A. Create a Network Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.
B. Create an Application Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.
C. Deploy a transit gateway in the inspection VPConfigure route tables to route the incoming packets through the transit gateway.
D. Deploy a Gateway Load Balancer in the inspection VPC. Create a Gateway Load Balancer endpoint to receive the incoming packets and forward the packets to the appliance.
Answer: D
https://www.examtopics.com/discussions/amazon/view/84727-exam-aws-certified-solutions-architect-associate-saa-c03/

해설:
Gateway Load Balancer 를 사용하면 방화벽, 침입 탐지 및 방지 시스템, 심층 패킷 검사 시스템과 같은 가상 어플라이언스를 배포, 확장 및 관리할 수 있습니다. Gateway Load Balancer 는 Gateway Load Balancer 엔드포인트를 사용하여 VPC 경계 전체에서 트래픽을 안전하게 교환합니다.
https://docs.aws.amazon.com/ko_kr/elasticloadbalancing/latest/gateway/introduction.html
오늘 AWS Gateway Load Balancer(GWLB)가 정식 출시되었다는 소식을 알려드리고자 합니다. 이를 통해 타사 가상 어플라이언스의 가용성을 쉽고 비용 효율적으로 배포, 확장 및 관리 할 수있는 서비스 방화벽 , 침입 감지 및 방지 시스템과 클라우드의 심층 패킷 검사 시스템. AWS 파트너 네트워크 및 AWS Marketplace 파트너는 규모, 가용성 및 서비스 제공이라는 복잡한 문제를 해결하지 않고도 AWS 고객에게 가상 어플라이언스를 서비스로 제공 할 수도 있습니다.
https://aws.amazon.com/ko/blogs/korea/introducing-aws-gateway-load-balancer-easy-deployment-scalability-and-high-availability-for-partner-appliances/

Q20

A company wants to improve its ability to clone large amounts of production data into a test environment in the same AWS Region. The data is stored in Amazon EC2 instances on Amazon Elastic Block Store (Amazon EBS) volumes. Modifications to the cloned data must not affect the production environment. The software that accesses this data requires consistently high I/O performance.
A solutions architect needs to minimize the time that is required to clone the production data into the test environment.
Which solution will meet these requirements?
A. Take EBS snapshots of the production EBS volumes. Restore the snapshots onto EC2 instance store volumes in the test environment.
B. Configure the production EBS volumes to use the EBS Multi-Attach feature. Take EBS snapshots of the production EBS volumes. Attach the production EBS volumes to the EC2 instances in the test environment.
C. Take EBS snapshots of the production EBS volumes. Create and initialize new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment before restoring the volumes from the production EBS snapshots.
D. Take EBS snapshots of the production EBS volumes. Turn on the EBS fast snapshot restore feature on the EBS snapshots. Restore the snapshots into new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment.
Answer: D
https://www.examtopics.com/discussions/amazon/view/85226-exam-aws-certified-solutions-architect-associate-saa-c03/

해설:
A(X) : 인스턴스 스토어 볼륨은 휘발성이라 꺼지면 데이터 날라감.
B(X) : EBS 다중 연결을 사용하게 되면 복제된 데이터를 수정할 때 프로덕션 환경에 영향을 주게 됨. 이는 지문에서 요구한 사항과 위배됨.
C(X) : 스냅샷으로 새로운 볼륨을 만드는 것이지 만들어진 볼륨에 스냅샷을 복원하는 게 아님.
D(O) : 정답.

Q21
An ecommerce company wants to launch a one-deal-a-day website on AWS. Each day will feature exactly one product on sale for a period of 24 hours. The company wants to be able to handle millions of requests each hour with millisecond latency during peak hours.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use Amazon S3 to host the full website in different S3 buckets. Add Amazon CloudFront distributions. Set the S3 buckets as origins for the distributions. Store the order data in Amazon S3.

B. Deploy the full website on Amazon EC2 instances that run in Auto Scaling groups across multiple Availability Zones. Add an Application Load Balancer (ALB) to distribute the website traffic. Add another ALB for the backend APIs. Store the data in Amazon RDS for MySQL.

C. Migrate the full application to run in containers. Host the containers on Amazon Elastic Kubernetes Service (Amazon EKS). Use the Kubernetes Cluster Autoscaler to increase and decrease the number of pods to process bursts in traffic. Store the data in Amazon RDS for MySQL.

D. Use an Amazon S3 bucket to host the website's static content. Deploy an Amazon CloudFront distribution. Set the S3 bucket as the origin. Use Amazon API Gateway and AWS Lambda functions for the backend APIs. Store the data in Amazon DynamoDB.

Answer: D

https://www.examtopics.com/discussions/amazon/view/85195-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

A(X) : 전체 웹사이트를 호스팅하기에는 동적인 요소들이 들어가 있을 수 있는데 S3+CloudFront 조합은 정적 웹사이트 호스팅을 위한 것임.

B(X) : RDS 는 기본적으로 Auto Scaling 을 사용하지 않음. 따로 켜야하는데 해당 선택지엔 Auto Scaling 을 사용한단 언급이 없음.

워크로드를 예측할 수 없는 경우 Amazon RDS DB 인스턴스에 대해 스토리지 Autoscaling 을 활성화할 수 있습니다.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIOPS.StorageTypes.html#USER_PIOPS.Autoscaling

C(X) : B 와 동일한 이유로 오답.

D(O) : 정적인 웹사이트 요소들은 S3 + CloudFront 로 빠르게 제공하고, API Gateway 에서 Lambda 함수를 호출해 DynamoDB 에 데이터 저장 가능. DynamoDB 는 확장성이 뛰어나고 밀리초 단위 액세스를 지원하는 데이터베이스 유형.

・S3 + CloudFront 조합의 정적 웹사이트 호스팅 :

https://aws.amazon.com/ko/premiumsupport/knowledge-center/cloudfront-serve-static-website/

・즉, HTTPS 엔드포인트를 통해 API 를 호출하면 API Gateway 가 Lambda 함수를 호출합니다.

https://docs.aws.amazon.com/ko_kr/lambda/latest/dg/services-apigateway-tutorial.html
・개발자는 DynamoDB 를 사용해 최신 서버리스 애플리케이션을 구축하여 우선 작은 규모에서 시작했다가 전역적으로 확장하여 초당 페타바이트 단위의 데이터와 수천만 건의 읽기 및 쓰기 요청을 지원하도록 할 수 있습니다.....DynamoDB 는 용량에 맞게 테이블을 자동으로 조정하므로 별도로 관리하지 않아도 성능을 유지합니다.
https://aws.amazon.com/ko/dynamodb/features/#Enterprise_ready

설명 2:
사용량이 많은 시간 동안 지연 시간이 밀리초이고 운영 오버헤드가 최소인 AWS 에서 하루 1 회 거래 웹 사이트를 시작하려면 가장 좋은 옵션은 Amazon S3 버킷을 사용하여 웹 사이트의 정적 콘텐츠를 호스팅하고 Amazon CloudFront 배포를 배포하는 것입니다.
S3 버킷을 오리진으로 설정하고 백엔드 API 에 Amazon API Gateway 및 AWS Lambda 함수를 사용하고 데이터를 Amazon DynamoDB 에 저장합니다.
이 옵션은 최소한의 운영 오버헤드가 필요하며 사용량이 많은 시간 동안 밀리초 대기 시간으로 시간당 수백만 건의 요청을 처리할 수 있습니다. 따라서 보기 D 가 정답입니다.

Q22
A solutions architect is using Amazon S3 to design the storage architecture of a new digital media application. The media files must be resilient to the loss of an Availability Zone. Some files are accessed frequently while other files are rarely accessed in an unpredictable pattern. The solutions architect must minimize the costs of storing and retrieving the media files.
Which storage option meets these requirements?
A. S3 Standard
B. S3 Intelligent-Tiering
C. S3 Standard-Infrequent Access (S3 Standard-IA)
D. S3 One Zone-Infrequent Access (S3 One Zone-IA)
Answer: B
https://www.examtopics.com/discussions/amazon/view/84943-exam-aws-certified-solutions-architect-associate-saa-c03/

설명
S3 Intelligent-Tiering - 액세스 빈도 또는 불규칙한 사용 패턴을 모를 때 완벽한 사용 사례입니다.
Amazon S3 는 다양한 사용 사례를 위해 설계된 다양한 스토리지 클래스를 제공합니다. 여기에는 자주 액세스하는 데이터의 범용 스토리지를 위한 S3 Standard 가 포함됩니다.

액세스 패턴을 알 수 없거나 변경하는 데이터를 위한 S3 Intelligent-Tiering; S3 Standard-Infrequent Access(S3 Standard-IA) 및 S3 One Zone-Infrequent Access(S3 One Zone-IA)는 수명이 길지만 액세스 빈도가 낮은 데이터를 위한 것입니다. 장기 아카이브 및 디지털 보존을 위한 Amazon S3 Glacier(S3 Glacier) 및 Amazon S3 Glacier Deep Archive(S3 Glacier Deep Archive). 기존 AWS 리전에서 충족할 수 없는 데이터 레지던시 요구 사항이 있는 경우 S3 Outposts 스토리지 클래스를 사용하여 S3 데이터를 온프레미스에 저장할 수 있습니다.
Amazon S3 는 수명 주기 동안 데이터를 관리하는 기능도 제공합니다. S3 수명 주기 정책이 설정되면 애플리케이션을 변경하지 않고도 데이터가 자동으로 다른 스토리지 클래스로 전송됩니다.
https://aws.amazon.com/getting-started/hands-on/getting-started-using-amazon-s3-intelligent-tiering/?nc1=h_ls

예측할 수 없는 패턴 = S3 Intelligent Tiering.

Q23
A company is storing backup files by using Amazon S3 Standard storage. The files are accessed frequently for 1 month. However, the files are not accessed after 1 month. The company must keep the files indefinitely.
Which storage solution will meet these requirements MOST cost-effectively?
A. Configure S3 Intelligent-Tiering to automatically migrate objects.
B. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 month.
C. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) after 1 month.
D. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 month.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85092-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이러한 요구 사항을 가장 비용 효율적으로 충족하는 스토리지 솔루션은 B 입니다.
1 개월 후에 객체를 S3 Standard 에서 S3 Glacier Deep Archive 로 전환하는 S3 수명 주기 구성을 생성합니다. Amazon S3 Glacier Deep Archive 는 거의 액세스하지 않고 몇 시간의

검색 시간이 허용되는 데이터의 장기 보존을 위한 안전하고 내구성이 있으며 매우 저렴한 Amazon S3 스토리지 클래스입니다. Amazon S3 에서 가장 저렴한 스토리지 옵션이므로 1 개월 후에 액세스하지 않는 백업 파일을 저장하는 데 비용 효율적인 선택입니다. S3 수명 주기 구성을 사용하여 1 개월 후에 객체를 S3 Standard 에서 S3 Glacier Deep Archive 로 자동 전환할 수 있습니다. 이렇게 하면 자주 액세스하지 않는 백업 파일의 저장 비용이 최소화됩니다.

1 개월 이후 파일에 접근하지 않음 = S3 Glacier Deep Archive. 답은 B.

Q24

A company observes an increase in Amazon EC2 costs in its most recent bill. The billing team notices unwanted vertical scaling of instance types for a couple of EC2 instances. A solutions architect needs to create a graph comparing the last 2 months of EC2 costs and perform an in-depth analysis to identify the root cause of the vertical scaling.

How should the solutions architect generate the information with the LEAST operational overhead?

A. Use AWS Budgets to create a budget report and compare EC2 costs based on instance types.

B. Use Cost Explorer's granular filtering feature to perform an in-depth analysis of EC2 costs based on instance types.

C. Use graphs from the AWS Billing and Cost Management dashboard to compare EC2 costs based on instance types for the last 2 months.

D. Use AWS Cost and Usage Reports to create a report and send it to an Amazon S3 bucket. Use Amazon QuickSight with Amazon S3 as a source to generate an interactive graph based on instance types.

Answer: B

https://www.examtopics.com/discussions/amazon/view/85038-exam-aws-certified-solutions-architect-associate-saa-c03/

설명

AWS Cost Explorer 는 비용과 사용량을 보고 분석할 수 있는 도구입니다. 기본 그래프, Cost Explorer 비용 및 사용량 보고서 또는 Cost Explorer RI 보고서를 사용하여 사용량 및 비용을 탐색할 수 있습니다. 최대 지난 12 개월 동안의 데이터를 보고 향후 12 개월 동안 지출할 가능성이 있는 금액을 예측하고 구매할 예약 인스턴스에 대한 추천을 받을 수 있습니다. 비용 탐색기를 사용하여 추가 조사가 필요한 영역을 식별하고 비용을 이해하는

데 사용할 수 있는 추세를 볼 수 있습니다.
https://docs.aws.amazon.com/cost-management/latest/userguide/ce-what-is.html

Q25

A company is designing an application. The application uses an AWS Lambda function to receive information through Amazon API Gateway and to store the information in an Amazon Aurora PostgreSQL database.

During the proof-of-concept stage, the company has to increase the Lambda quotas significantly to handle the high volumes of data that the company needs to load into the database. A solutions architect must recommend a new design to improve scalability and minimize the configuration effort.

Which solution will meet these requirements?

A. Refactor the Lambda function code to Apache Tomcat code that runs on Amazon EC2 instances. Connect the database by using native Java Database Connectivity (JDBC) drivers.

B. Change the platform from Aurora to Amazon DynamoDProvision a DynamoDB Accelerator (DAX) cluster. Use the DAX client SDK to point the existing DynamoDB API calls at the DAX cluster.

C. Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using Amazon Simple Notification Service (Amazon SNS).

D. Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using an Amazon Simple Queue Service (Amazon SQS) queue.

Answer: D

https://www.examtopics.com/discussions/amazon/view/85197-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

대기열(SQS)로 병목 현상을 방지할 수 있습니다.

대량의 데이터 처리 + 확장성 개선 = SQS queue + Lambda 조합.

Q26

A company needs to review its AWS Cloud deployment to ensure that its Amazon S3 buckets

do not have unauthorized configuration changes.
What should a solutions architect do to accomplish this goal?
A. Turn on AWS Config with the appropriate rules.
B. Turn on AWS Trusted Advisor with the appropriate checks.
C. Turn on Amazon Inspector with the appropriate assessment template.
D. Turn on Amazon S3 server access logging. Configure Amazon EventBridge (Amazon Cloud Watch Events).
Answer: A
https://www.examtopics.com/discussions/amazon/view/84940-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
AWS Config 는 AWS 리소스 구성을 측정, 감사 및 평가할 수 있는 서비스입니다. Config 는 AWS 리소스 구성을 지속적으로 모니터링 및 기록하고, 원하는 구성을 기준으로 기록된 구성을 자동으로 평가해 줍니다.
https://aws.amazon.com/ko/config/

설명 2:
Amazon S3 버킷에 무단 구성 변경이 없도록 하려면 솔루션 설계자가 적절한 규칙으로 AWS Config 를 켜야 합니다. AWS Config 는 사용자가 업계 표준 및 내부 정책을 준수하는지 AWS 리소스 구성을 감사하고 평가할 수 있는 서비스입니다. 리소스가 서로 어떻게 관련되어 있는지에 대한 정보를 포함하여 리소스 및 해당 구성에 대한 자세한 보기를 제공합니다. 적절한 규칙으로 AWS Config 를 켜면 사용자는 Amazon S3 버킷에 대한 무단 구성 변경을 식별하고 수정할 수 있습니다.

Q27
A company is launching a new application and will display application metrics on an Amazon CloudWatch dashboard. The company's product manager needs to access this dashboard periodically. The product manager does not have an AWS account. A solutions architect must provide access to the product manager by following the principle of least privilege.
Which solution will meet these requirements?
A. Share the dashboard from the CloudWatch console. Enter the product manager's email address, and complete the sharing steps. Provide a shareable link for the dashboard to the product manager.
B. Create an IAM user specifically for the product manager. Attach the

CloudWatchReadOnlyAccess AWS managed policy to the user. Share the new login credentials with the product manager. Share the browser URL of the correct dashboard with the product manager.
C. Create an IAM user for the company's employees. Attach the ViewOnlyAccess AWS managed policy to the IAM user. Share the new login credentials with the product manager. Ask the product manager to navigate to the CloudWatch console and locate the dashboard by name in the Dashboards section.
D. Deploy a bastion server in a public subnet. When the product manager requires access to the dashboard, start the server and share the RDP credentials. On the bastion server, ensure that the browser is configured to open the dashboard URL with cached AWS credentials that have appropriate permissions to view the dashboard.
Answer: A
https://www.examtopics.com/discussions/amazon/view/85227-exam-aws-certified-solutions-architect-associate-saa-c03/

해설:
AWS 계정에 직접 액세스할 수 없는 사람들과 CloudWatch 대시보드를 공유할 수 있습니다. 대시보드를 공유할 때 다음 세 가지 방법으로 대시보드를 볼 수 있는 사람을 지정할 수 있습니다.
◎하나의 대시보드를 공유하고 대시보드를 볼 수 있는 사람들의 특정 이메일 주소를 지정합니다. 이러한 각 사용자는 대시보드를 보기 위해 입력해야 하는 고유한 암호를 만듭니다.
◎링크가 있는 모든 사용자가 대시보드를 볼 수 있도록 단일 대시보드를 공개적으로 공유합니다.
◎계정의 모든 CloudWatch 대시보드를 공유하고 대시보드 액세스를 위한 타사 SSO(Single Sign-On) 공급자를 지정합니다. 이 SSO 공급자 목록의 구성원인 모든 사용자는 계정의 모든 대시보드에 액세스할 수 있습니다. 이를 활성화하려면 SSO 공급자를 Amazon Cognito 와 통합합니다. SSO 공급자는 SAML(Security Assertion Markup Language)을 지원해야 합니다.
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-dashboard-sharing.html

Q28
A company is migrating applications to AWS. The applications are deployed in different accounts. The company manages the accounts centrally by using AWS Organizations. The

company's security team needs a single sign-on (SSO) solution across all the company's accounts. The company must continue managing the users and groups in its on-premises self-managed Microsoft Active Directory.
Which solution will meet these requirements?
A. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a one-way forest trust or a one-way domain trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.
B. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a two-way forest trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.
C. Use AWS Directory Service. Create a two-way trust relationship with the company's self-managed Microsoft Active Directory.
D. Deploy an identity provider (IdP) on premises. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85231-exam-aws-certified-solutions-architect-associate-saa-c03/

해설:
・AWS Organizations 로 SSO 설정하여 Active Directory 사용 가능.
AWS IAM Identity Center(AWS SSO 의 후속 서비스)를 설정하여 Active Directory 를 통해 AWS 계정 및 리소스에 대한 액세스를 제공하며, 별도의 작업 역할에 따라 권한을 사용자 지정합니다. https://aws.amazon.com/ko/organizations/features/
・AWS Directory Service 를 사용하여 AWS Managed Microsoft AD 디렉터리에 연결 가능.
IAM Identity Center 는 AWS Identity and Access Management(IAM)를 기반으로 구축된 서비스로, 여러 AWS 계정, AWS 애플리케이션 및 다른 SAML 사용 클라우드 애플리케이션에 대한 액세스 관리를 간소화합니다. AWS Directory Service 를 사용하여 IAM Identity Center 를 온프레미스 Active Directory(AD) 또는 AWS Managed Microsoft AD 디렉터리에 연결할 수 있습니다. https://aws.amazon.com/ko/iam/identity-center/faqs/
A(X) : SSO, AWS 관리 콘솔에는 양방향 트러스트가 필요.
AWS Managed Microsoft AD 는 수신, 발신 및 양방향(양방향)의 세 가지 신뢰 관계 방향을 모두 지원합니다. AWS Managed Microsoft AD 는 외부 및 포리스트 트러스트를 모두 지원합니다. Amazon Chime, Amazon Connect, Amazon QuickSight, AWS IAM Identity Center(AWS Single Sign-On 의 후속 제품), Amazon WorkDocs, Amazon WorkMail, Amazon WorkSpaces 및 AWS Management Console 과 같은 AWS 엔터프라이즈 앱에는 양방향

신뢰가 필요합니다. Amazon EC2, Amazon RDS 및 Amazon FSx 는 단방향 또는 양방향 신뢰로 작동합니다.
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_setup_trust.html
B(O) : A 와 같은 이유로 정답.
C(X) : SSO 는 온프레미스 Active Directory 나 AWS 관리형 Microsoft AD Directory 에 연결할 수 있지, 온프레미스 Microsoft AD Direcotry 에 연결할 수는 없음. ▲위의 설명 참고
D(X) : IdP 는 외부 자격 증명 서비스.
자격 증명 공급자(IdP)를 사용하면 AWS 외부의 사용자 자격 증명을 관리할 수 있고 이 외부 사용자 자격 증명에 계정의 AWS 리소스에 대한 사용 권한을 부여할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/id_roles_providers.html

Q29
A company provides a Voice over Internet Protocol (VoIP) service that uses UDP connections. The service consists of Amazon EC2 instances that run in an Auto Scaling group. The company has deployments across multiple AWS Regions.
The company needs to route users to the Region with the lowest latency. The company also needs automated failover between Regions.
Which solution will meet these requirements?
A. Deploy a Network Load Balancer (NLB) and an associated target group. Associate the target group with the Auto Scaling group. Use the NLB as an AWS Global Accelerator endpoint in each Region.
B. Deploy an Application Load Balancer (ALB) and an associated target group. Associate the target group with the Auto Scaling group. Use the ALB as an AWS Global Accelerator endpoint in each Region.
C. Deploy a Network Load Balancer (NLB) and an associated target group. Associate the target group with the Auto Scaling group. Create an Amazon Route 53 latency record that points to aliases for each NLB. Create an Amazon CloudFront distribution that uses the latency record as an origin.
D. Deploy an Application Load Balancer (ALB) and an associated target group. Associate the target group with the Auto Scaling group. Create an Amazon Route 53 weighted record that points to aliases for each ALB. Deploy an Amazon CloudFront distribution that uses the weighted record as an origin.
Answer: A
https://www.examtopics.com/discussions/amazon/view/85029-exam-aws-certified-solut

ions-architect-associate-saa-c03/

해설:
UDP 연결을 사용한다고 했으므로 NLB. 대기 시간이 가장 짧은 리전으로 라우팅 + UDP 사용 = AWS Global Accelerator.
AWS Global Accelerator 에서 제공하는 고정 IP 주소와 AWS 엣지 로케이션의 애니캐스트를 리전별 AWS 리소스 또는 엔드포인트(예: Network Load Balancer, Application Load Balancer EC2 인스턴스 및 탄력적 IP 주소)에 연결할 수 있습니다. IP 주소는 AWS 엣지 로케이션에서 애니캐스트 되므로 사용자와 가까운 AWS 글로벌 네트워크에 온보딩 기능을 제공합니다.
https://aws.amazon.com/ko/global-accelerator/faqs/

https://aws.amazon.com/global-accelerator/faqs/
HTTP /HTTPS - ALB ; TCP and UDP - NLB; Lowest latency routing and more throughput. Also supports failover, uses Anycast Ip addressing - Global Accelerator Caching at Egde Locations - CloudFront WS Global Accelerator automatically checks the health of your applications and routes user traffic only to healthy application endpoints. If the health status changes or you make configuration updates, AWS Global Accelerator reacts instantaneously to route your users to the next available endpoint.

Q30
A development team runs monthly resource-intensive tests on its general purpose Amazon RDS for MySQL DB instance with Performance Insights enabled. The testing lasts for 48 hours once a month and is the only process that uses the database. The team wants to reduce the cost of running the tests without reducing the compute and memory attributes of the DB instance.
Which solution meets these requirements MOST cost-effectively?
A. Stop the DB instance when tests are completed. Restart the DB instance when required.
B. Use an Auto Scaling policy with the DB instance to automatically scale when tests are completed.
C. Create a snapshot when tests are completed. Terminate the DB instance and restore the snapshot when required.
D. Modify the DB instance to a low-capacity instance when tests are completed. Modify the DB instance again when required.
Answer: C

https://www.examtopics.com/discussions/amazon/view/85030-exam-aws-certified-solutions-architect-associate-saa-c03/

해설:
한 달에 한 번 48 시간 동안만 사용하고, 가장 비용 효율적인 방법을 사용해야하므로 스냅샷이 제일 저렴.
A(X) : DB 인스턴스를 중지해도 DB 인스턴스가 돌아가는 EBS 볼륨이나 이런 건 사용하지 않아도 보유 중인 용량에 따라 요금이 부과됨.
B(X) : Auto Scaling 을 사용하게 되면 사용하지 않을 때에도 인스턴스가 실행 상태가 되므로 스냅샷 보관보다 비용이 더 부과됨
C(O) : 스냅샷으로 보관해서 저장하면 스냅샷 용량만큼만 비용이 부과됨.
D(X) : 사용 중이 아닐 때도 인스턴스가 실행 상태이므로 스냅샷 보관보다 비용이 더 부과됨

Q31
A company that hosts its web application on AWS wants to ensure all Amazon EC2 instances. Amazon RDS DB instances. and Amazon Redshift clusters are configured with tags. The company wants to minimize the effort of configuring and operating this check.
What should a solutions architect do to accomplish this?
A. Use AWS Config rules to define and detect resources that are not properly tagged.
B. Use Cost Explorer to display resources that are not properly tagged. Tag those resources manually.
C. Write API calls to check all resources for proper tag allocation. Periodically run the code on an EC2 instance.
D. Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.
Answer: A
https://www.examtopics.com/discussions/amazon/view/85198-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
사후 대응적 거버넌스는 Resource Groups Tagging API, AWS Config Rules, 사용자 지정 스크립트 등의 도구를 사용하여 제대로 태그가 지정되지 않은 리소스를 찾습니다.
https://docs.aws.amazon.com/ko_kr/general/latest/gr/aws_tagging.html

설명 2:
모든 Amazon EC2 인스턴스, Amazon RDS DB 인스턴스 및 Amazon Redshift 클러스터가 태그로 구성되도록 하려면 솔루션 설계자가 AWS Config 규칙을 사용하여 적절하게 태그가 지정되지 않은 리소스를 정의하고 감지해야 합니다. AWS Config 규칙은 AWS Config 가 모범 사례 및 회사 정책을 준수하는지 AWS 리소스 구성을 평가하는 데 사용하는 사용자 지정 가능한 규칙 세트입니다. AWS Config 규칙을 사용하면 비준수 리소스를 식별하고 담당 팀에 알리는 프로세스를 자동화하므로 이 검사를 구성하고 운영하는 노력을 최소화할 수 있습니다.
참조: AWS Config 규칙:
(https://docs.aws.amazon.com/ko_kr/config/latest/developerguide/evaluate-config_use-managed-rules.html)

Q32
A development team needs to host a website that will be accessed by other teams. The website contents consist of HTML, CSS, client-side JavaScript, and images.
Which method is the MOST cost-effective for hosting the website?
A. Containerize the website and host it in AWS Fargate.
B. Create an Amazon S3 bucket and host the website there.
C. Deploy a web server on an Amazon EC2 instance to host the website.
D. Configure an Application Load Balancer with an AWS Lambda target that uses the Express.js framework.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85199-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
정적 웹 사이트에서 웹 페이지는 사전 구축된 서버에 의해 반환됩니다. HTML, CSS 또는 JavaScript 와 같은 간단한 언어를 사용합니다. 정적 웹 사이트에서는 서버에서(사용자에 따라) 콘텐츠를 처리하지 않습니다. 웹 페이지는 변경 없이 서버에 의해 반환되므로 정적 웹 사이트는 빠릅니다. 데이터베이스와의 상호 작용이 없습니다.
또한 호스트가 다른 언어로 서버 측 처리를 지원할 필요가 없기 때문에 비용이 적게 듭니다.
동적 웹 사이트에서 웹 페이지는 런타임 중에 처리되는 서버에 의해 반환됩니다. 즉, 사전 구축된 웹 페이지가 아니라 사용자의 요구에 따라 런타임 중에 구축됩니다. 이들은 PHP, Node.js, ASP.NET 및 서버에서 지원하는 더 많은 것과 같은 서버 측 스크립팅 언어를 사용합니다. 따라서 정적 웹 사이트보다 느리지만 업데이트 및 데이터베이스와의 상호

작용이 가능합니다.

설명 2:
모두 정적 웹사이트 콘텐츠 유형에 해당.
Amazon S3 를 사용하여 웹 서버를 구성하거나 관리할 필요 없이 정적 웹 사이트를 호스팅할 수 있습니다. 다음 단계를 완료하여 웹사이트에 모든 고정 자산을 호스팅할 새 Amazon S3 버킷을 생성합니다. 이 자산에는 HTML, CSS, JavaScript, 이미지 파일이 포함됩니다.
https://aws.amazon.com/ko/getting-started/hands-on/app-onboarding/module-5/

Q33
A company runs an online marketplace web application on AWS. The application serves hundreds of thousands of users during peak hours. The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications. Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval.
What should a solutions architect recommend to meet these requirements?
A. Store the transactions data into Amazon DynamoDB. Set up a rule in DynamoDB to remove sensitive data from every transaction upon write. Use DynamoDB Streams to share the transactions data with other applications.
B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3. Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3.
C. Stream the transactions data into Amazon Kinesis Data Streams. Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB. Other applications can consume the transactions data off the Kinesis data stream.
D. Store the batched transactions data in Amazon S3 as files. Use AWS Lambda to process every file and remove sensitive data before updating the files in Amazon S3. The Lambda function then stores the data in Amazon DynamoDB. Other applications can consume transaction files stored in Amazon S3.
Answer: C
https://www.examtopics.com/discussions/amazon/view/85201-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
피크 시간에 수십만 명의 사용자에게 서비스 제공 = Kinesis 사용. B,C 둘 중 하나가 답.
B(X) : Kinesis Data Firehose 는 데이터 변환 및 전송 서비스. 데이터 수집을 하려면 Kinesis Data Streams 가 필요.
Kinesis Data Firehose 로 데이터를 보내도록 데이터 생산자를 구성하면 지정한 대상으로 데이터가 자동으로 전달됩니다. 데이터를 전송하기 전에 변환하도록 Kinesis Data Firehose 를 구성할 수도 있습니다.
https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html
C(O) : Amazon Kinesis Data Streams 를 사용하면 특수 요구에 맞춰 스트리밍 데이터를 처리 또는 분석하는 사용자 지정 애플리케이션을 구축할 수 있습니다. 수십 만개의 소스에서 클릭 스트림, 애플리케이션 로그, 소셜 미디어와 같은 다양한 유형의 데이터를 Kinesis 데이터 스트림에 추가할 수 있습니다. 그러면 몇 초 안에 애플리케이션에서 스트림의 해당 데이터를 읽고 처리할 수 있습니다.
https://aws.amazon.com/ko/kinesis/data-streams/faqs/?nc=sn&loc=6

설명 2:
Kinesis Data Firehose 전송 스트림의 대상입니다. Kinesis Data Firehose 는 Amazon Simple Storage Service(Amazon S3), Amazon 을 비롯한 다양한 대상으로 데이터 레코드를 보낼 수 있습니다.
Redshift, Amazon OpenSearch Service 및 귀하 또는 귀하의 제 3 자 서비스 공급자가 소유한 모든 HTTP 엔드포인트.
다음은 지원되는 대상입니다.
* Amazon 오픈서치 서비스(Amazon OpenSearch Service)
* Amazon S3
* 데이터독(Datadog)
* 다이나트레이스(Dynatrace)
* 벌집(Honeycomb)
* HTTP 끝점(Endpoint)
* 로직 모니터(Logic Monitor)
* 몽고디비 클라우드(MongoDB Cloud)
* 새로운 유물(New Relic)
* 스플렁크(Splunk)
* 스모 로직(Sumo Logic)
https://docs.aws.amazon.com/firehose/latest/dev/create-name.html
https://aws.amazon.com/kinesis/data-streams/
Amazon Kinesis Data Streams(KDS)는 확장성과 내구성이 뛰어난 실시간 데이터 스트리밍

서비스입니다.
KDS 는 웹사이트 클릭 스트림, 데이터베이스 이벤트 스트림, 금융 거래, 소셜 미디어 피드, IT 로그 및 위치 추적 이벤트와 같은 수십만 개의 소스에서 초당 기가바이트의 데이터를 지속적으로 캡처할 수 있습니다.

Q34
A company hosts its multi-tier applications on AWS. For compliance, governance, auditing, and security, the company must track configuration changes on its AWS resources and record a history of API calls made to these resources.
What should a solutions architect do to meet these requirements?
A. Use AWS CloudTrail to track configuration changes and AWS Config to record API calls.
B. Use AWS Config to track configuration changes and AWS CloudTrail to record API calls.
C. Use AWS Config to track configuration changes and Amazon CloudWatch to record API calls.
D. Use AWS CloudTrail to track configuration changes and Amazon CloudWatch to record API calls.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85202-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
리소스 구성 사항 변경 추적 = AWS Config / 리소스 내역 기록 = CloudTrail
AWS Config 는 AWS 리소스 인벤토리, 구성 기록, 구성 변경 알림을 제공하여 보안 및 거버넌스를 실현하는 완벽한 관리형 서비스입니다.
https://aws.amazon.com/ko/config/faq/
AWS Cloudtrail 은 사용자 활동 및 API 사용을 추적하여 감사, 보안 모니터링 및 운영 문제 해결을 지원합니다. CloudTrail 은 AWS 인프라 전체에서 작업과 관련된 계정 활동을 로그하고 지속적으로 모니터링하고 보존하여 스토리지, 분석 및 해결 작업을 제어할 수 있도록 합니다.
https://aws.amazon.com/ko/cloudtrail/faqs/

설명 2:
AWS Config 는 회사가 AWS 리소스의 구성을 평가, 감사 및 평가할 수 있는 완전관리형 서비스입니다. 사용 중인 리소스에 대한 자세한 인벤토리를 제공하고 리소스 구성에 대한 변경 사항을 추적합니다. AWS Config 는 구성 변경을 감지하고 변경이 발생하면 회사에

알릴 수 있습니다. 또한 규정 준수 및 거버넌스 목적에 필수적인 변경 기록 보기를 제공합니다. AWS CloudTrail 은 회사의 AWS 리소스에 대한 자세한 API 호출 기록을 제공하는 완전 관리형 서비스입니다. API 호출을 한 사람, 호출한 시간, 호출의 영향을 받은 리소스를 포함하여 AWS 계정의 모든 API 활동을 기록합니다. 이 정보를 통해 회사는 AWS 리소스에서 발생할 수 있는 의심스러운 활동을 조사할 수 있으므로 보안 및 감사 목적에 매우 중요합니다.

Q35

A company is preparing to launch a public-facing web application in the AWS Cloud. The architecture consists of Amazon EC2 instances within a VPC behind an Elastic Load Balancer (ELB). A third-party service is used for the DNS. The company's solutions architect must recommend a solution to detect and protect against large-scale DDoS attacks.

Which solution meets these requirements?

A. Enable Amazon GuardDuty on the account.

B. Enable Amazon Inspector on the EC2 instances.

C. Enable AWS Shield and assign Amazon Route 53 to it.

D. Enable AWS Shield Advanced and assign the ELB to it.

Answer: D

https://www.examtopics.com/discussions/amazon/view/85203-exam-aws-certified-solutions-architect-associate-saa-c03/

해설:

A(X) : GuardDuty 는 계정 보호 서비스.

Amazon GuardDuty 는 AWS 계정 및 워크로드에서 악의적 활동을 모니터링하고 상세한 보안 결과를 제공하여 가시성 및 해결을 촉진하는 위협 탐지 서비스입니다.

https://aws.amazon.com/ko/guardduty/

B(X) : Amazon Inspector 는 취약점 스캔 서비스.

Amazon Inspector 는 지속적으로 스캔하는 취약성 관리 서비스입니다.

https://docs.aws.amazon.com/ko_kr/inspector/latest/user/what-is-inspector.html

C(X) : 대규모 DDoS 방어는 AWS Shield Advanced 가 더 적합.

D(O) : AWS Shield Advanced 는 정교한 대규모 DDoS 공격에 대한 추가 보호 및 완화, 실시간에 가까운 공격에 대한 가시성, 웹 애플리케이션 방화벽 AWS WAF 와의 통합을 제공합니다. DDoS 관련 급증 시 Amazon Elastic Compute Cloud(EC2), Elastic Load Balancing(ELB), Amazon CloudFront, AWS Global Accelerator 및 Amazon Route 53 요금 보호를 제공합니다.

https://aws.amazon.com/ko/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc

Q36

A company is building an application in the AWS Cloud. The application will store data in Amazon S3 buckets in two AWS Regions. The company must use an AWS Key Management Service (AWS KMS) customer managed key to encrypt all data that is stored in the S3 buckets. The data in both S3 buckets must be encrypted and decrypted with the same KMS key. The data and the key must be stored in each of the two Regions.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create an S3 bucket in each Region. Configure the S3 buckets to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Configure replication between the S3 buckets.

B. Create a customer managed multi-Region KMS key. Create an S3 bucket in each Region. Configure replication between the S3 buckets. Configure the application to use the KMS key with client-side encryption.

C. Create a customer managed KMS key and an S3 bucket in each Region. Configure the S3 buckets to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Configure replication between the S3 buckets.

D. Create a customer managed KMS key and an S3 bucket in each Region. Configure the S3 buckets to use server-side encryption with AWS KMS keys (SSE-KMS). Configure replication between the S3 buckets.

Answer: B

https://www.examtopics.com/discussions/amazon/view/84747-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.html

대부분의 사용자는 FIPS 140-2 인증 암호화 모듈로 보호되는 기본 AWS KMS 키 스토어가 보안 요구 사항을 충족합니다. 추가 유지 관리 책임 계층이나 추가 서비스에 대한 종속성을 추가할 필요가 없습니다. 그러나 조직에 다음과 같은 요구 사항이 있는 경우 사용자 지정 키 스토어 생성을 고려할 수 있습니다. 키 자료는 공유 환경에 저장할 수 없습니다. 키 자료는 독립적인 보조 감사 경로를 따라야 합니다. 키 자료를 생성하고 저장하는 HSM 은 FIPS 140-2 레벨 3 에서 인증을 받아야 합니다.

https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.html
https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-overview.html

설명 2:
A(X) : SSE-S3은 AWS에서 데이터 키와 마스터 키 모두 관리하기 때문에 고객 관리형 키가 사용되지 않음.
참고: AWS KMS 키로 암호화된 개체를 업로드하려면 키와 S3 버킷이 동일한 AWS 리전에 있어야 합니다.
Note: To upload an object encrypted by an AWS KMS key, the key and the S3 bucket must be in the same AWS Region.
https://aws.amazon.com/ko/premiumsupport/knowledge-center/s3-bucket-store-kms-encrypted-objects/
B(O) : 고객 관리형 다중 리전 KMS 키 생성. 각 리전에 S3 버킷 생성. S3 버킷 간 복제 설정. 클라이언트 측 암호화로 KMS 키 사용하도록 애플리케이션 설정
C(X) : A 와 같은 이유로 오답.
D(X) : 각 리전에 고객 관리형 KMS 키 및 S3 버킷 생성. AWS KMS keys(SSE-KMS)로 KMS 키(SSE-KMS)로 서버 측 암호화 사용하도록 S3 버킷 설정. S3 버킷 간 복제 설정.

Q37
A company recently launched a variety of new workloads on Amazon EC2 instances in its AWS account. The company needs to create a strategy to access and administer the instances remotely and securely. The company needs to implement a repeatable process that works with native AWS services and follows the AWS Well-Architected Framework.
Which solution will meet these requirements with the LEAST operational overhead?
A. Use the EC2 serial console to directly access the terminal interface of each instance for administration.
B. Attach the appropriate IAM role to each existing instance and new instance. Use AWS Systems Manager Session Manager to establish a remote SSH session.
C. Create an administrative SSH key pair. Load the public key into each EC2 instance. Deploy a bastion host in a public subnet to provide a tunnel for administration of each instance.
D. Establish an AWS Site-to-Site VPN connection. Instruct administrators to use their local on-premises machines to connect directly to the instances by using SSH keys across the

VPN tunnel.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85037-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A(X) : 물리적으로 케이블 갖다 꽂는 것이기 때문에 원격 접속이 아님.
B(O) : 세션 관리자는 사용자 인스턴스에 SSH 키 또는 인증서를 유지하거나 인바운드 포트를 열도록 요구하지 않고 보안 태세를 강화합니다. 또한, AWS IAM 을 사용하여 인스턴스 액세스를 중앙에서 관리합니다. 세션 관리자를 사용하면 Linux 또는 Windows EC2 인스턴스와 연결하여 각 인스턴스에서 세션을 시작한 각 사용자를 추적할 수 있습니다. 인스턴스에 액세스한 사용자와 AWS CloudTrail 을 사용한 시점을 감사할 수 있으며, 인스턴스에서 실행된 각 명령을 Amazon S3 또는 Amazon CloudWatch Logs 에 기록할 수 있습니다. 끝으로 Session Manager 를 사용하면 배스쳔 호스트를 운영하고 관리하기 위한 초기 투자 비용이 들지 않습니다. https://aws.amazon.com/ko/systems-manager/faq/
C(X) : SSH 키 쌍이 필요하므로 B 보다 운영 오버헤드가 많이 발생함.
D(X) : C 와 동일한 이유로 오답.

참고
https://docs.aws.amazon.com/ko_kr/systems-manager/latest/userguide/setup-instance-permissions.html

Q38
A company is hosting a static website on Amazon S3 and is using Amazon Route 53 for DNS. The website is experiencing increased demand from around the world. The company must decrease latency for users who access the website.
Which solution meets these requirements MOST cost-effectively?
A. Replicate the S3 bucket that contains the website to all AWS Regions. Add Route 53 geolocation routing entries.
B. Provision accelerators in AWS Global Accelerator. Associate the supplied IP addresses with the S3 bucket. Edit the Route 53 entries to point to the IP addresses of the accelerators.
C. Add an Amazon CloudFront distribution in front of the S3 bucket. Edit the Route 53 entries to point to the CloudFront distribution.
D. Enable S3 Transfer Acceleration on the bucket. Edit the Route 53 entries to point to the new endpoint.

Answer: C
https://www.examtopics.com/discussions/amazon/view/85238-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : S3 버킷을 각 리전마다 복제하면 콘텐츠가 업로드될 때마다 각 리전의 버킷에 복제해야하므로 낭비임. CloudFront 를 사용하는 것이 훨씬 더 효율적이고 경제적.
B(X) : AWS Global Accelerator 는 TCP/UDP 를 사용하는 네트워크 계층에서 동작하는데, 지문에서 사용된 Route 53 은 DNS 서비스로서, 애플리케이션 계층에서 동작.
C(O) : Route 53 으로 CloudFront 배포를 가리킬 수 있음.
S3 를 사용해 정적 콘텐츠를 저장하면 다양한 이점이 있습니다. 하지만 비용을 효과적으로 관리하는 동시에 애플리케이션의 성능과 보안까지 최적화하려면 Amazon CloudFront 를 설정해 S3 버킷과 함께 사용하면서 콘텐츠를 제공하고 보호하는 것이 좋습니다. CloudFront 는 전 세계의 정적/동적 웹 콘텐츠, 비디오 스트림 및 API 를 안전하게 대규모로 전송할 수 있는 콘텐츠 전송 네트워크(CDN) 서비스입니다. CloudFront 에서 데이터를 전송하면 설계상 S3 에서 직접 사용자에게 전송하는 것보다 더욱 비용 효율적입니다.
https://aws.amazon.com/ko/blogs/korea/amazon-s3-amazon-cloudfront-a-match-made-in-the-cloud/
자체 도메인 이름을 사용하려는 경우 Amazon Route 53 을 사용하여 CloudFront 배포를 가리키는 별칭 레코드(alias record)를 생성합니다
https://docs.aws.amazon.com/ko_kr/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html
D(X) : S3 Transfer Acceleration 은 각지에서 중앙 S3 버킷으로 업로드하는 서비스.
S3 Transfer Acceleration 은 전 세계에서 S3 버킷으로 전송되는 속도를 최적화하도록 설계되었습니다. 지리적으로 분산된 위치에서 중앙 집중식 버킷으로 데이터를 업로드하거나, 대륙 간에 GB 또는 TB 규모의 데이터를 정기적으로 전송하는 경우, S3 Transfer Acceleration 을 사용하면 몇 시간 또는 며칠의 데이터 전송 시간을 절약할 수 있습니다.
https://aws.amazon.com/ko/s3/faqs/#s3ta

설명 2:
Amazon CloudFront 는 전 세계 엣지 로케이션에서 콘텐츠를 캐싱하여 콘텐츠에 액세스하는 사용자에게 짧은 지연 시간과 빠른 전송 속도를 제공하는 콘텐츠 전송 네트워크(CDN)입니다. S3 버킷 앞에 CloudFront 배포를 추가하면 전 세계 엣지 위치에서 정적 웹 사이트의 콘텐츠를 캐싱하여 웹 사이트에 액세스하는 사용자의 지연 시간을 줄입니다. 또한 이 솔루션은 CloudFront 엣지 로케이션에서 콘텐츠에 액세스하는 사용자의 데이터 전송 및 요청에 대해서만 비용을 청구하므로 비용 효율적입니다. 또한 이 솔루션은

CloudFront 가 자동으로 확장하여 수요 증가를 처리하고 웹 사이트에 고가용성을 제공할 수 있으므로 확장성과 안정성 이점을 제공합니다.

Q39

A company maintains a searchable repository of items on its website. The data is stored in an Amazon RDS for MySQL database table that contains more than 10 million rows. The database has 2 TB of General Purpose SSD storage. There are millions of updates against this data every day through the company's website.

The company has noticed that some insert operations are taking 10 seconds or longer. The company has determined that the database storage performance is the problem.

Which solution addresses this performance issue?

A. Change the storage type to Provisioned IOPS SSD.

B. Change the DB instance to a memory optimized instance class.

C. Change the DB instance to a burstable performance instance class.

D. Enable Multi-AZ RDS read replicas with MySQL native asynchronous replication.

Answer: A

https://www.examtopics.com/discussions/amazon/view/84748-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

https://aws.amazon.com/ebs/features/

프로비저닝된 IOPS 볼륨은 솔리드 스테이트 드라이브(SSD)로 지원되며 중요한 I/O 집약적인 데이터베이스 애플리케이션을 위해 설계된 최고 성능의 EBS 볼륨입니다.

이러한 볼륨은 극히 짧은 대기 시간이 필요한 IOPS 집약적 워크로드와 처리량 집약적 워크로드 모두에 이상적입니다.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

설명 2:

'삽입' 작업이라고 했으므로 I/O 성능과 관련되어있음을 유추할 수 있음. 그리고 '저장소 성능'이 문제라고 판단했고, 범용 'SSD' 스토리지가 있다고 했으므로 A 가 정답.

D(X) : 버스트 가능한 성능 인스턴스는 잠시 I/O 성능을 끌어올리는 것일 뿐 근본적인 I/O 성능 개선은 하지 못함.

획득한 크레딧이 남아 있지 않으면 인스턴스가 기준 CPU 사용률로 점진적으로 저하되고 크레딧이 더 많이 적립될 때까지 기준 이상으로 버스트할 수 없습니다.

https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/burstable-credits-baselin

e-concepts.html

Q40

A company has thousands of edge devices that collectively generate 1 TB of status alerts each day. Each alert is approximately 2 KB in size. A solutions architect needs to implement a solution to ingest and store the alerts for future analysis.

The company wants a highly available solution. However, the company needs to minimize costs and does not want to manage additional infrastructure. Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days.

What is the MOST operationally efficient solution that meets these requirements?

A. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.

B. Launch Amazon EC2 instances across two Availability Zones and place them behind an Elastic Load Balancer to ingest the alerts. Create a script on the EC2 instances that will store the alerts in an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.

C. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster. Set up the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster to take manual snapshots every day and delete data from the cluster that is older than 14 days.

D. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to ingest the alerts, and set the message retention period to 14 days. Configure consumers to poll the SQS queue, check the age of the message, and analyze the message data as needed. If the message is 14 days old, the consumer should copy the message to an Amazon S3 bucket and delete the message from the SQS queue.

Answer: A

https://www.examtopics.com/discussions/amazon/view/85204-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

수 천 개의 Edge 장치로부터 경고 수집 및 저장 = Kinesis. A,C 둘 중 하나가 답.

A(O) : 정답.

・Kinesis Firehose Delivery Stream 에서 데이터 수집
다양한 유형의 소스를 사용하여 Kinesis Data Firehose 전송 스트림으로 데이터를 보낼 수 있습니다. https://docs.aws.amazon.com/firehose/latest/dev/basic-write.html
・Kinesis Firehose 에서 S3 로 데이터 전송
Kinesis Data Firehose 전송 스트림을 설정할 때 데이터의 최종 대상을 선택합니다. 대상 옵션은 Amazon Simple Storage Service(Amazon S3), Amazon OpenSearch Service 및 Amazon Redshift 입니다.
https://docs.aws.amazon.com/ko_kr/ses/latest/dg/event-publishing-kinesis-analytics-firehose-stream.html
・S3 에서 Life Cycle Policy 를 사용해 S3 Glacier 로 객체 이전
수명 주기 규칙을 사용하여 객체 수명 주기 동안 Amazon S3 에서 수행하려는 작업을 정의할 수 있습니다(예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/how-to-set-lifecycle-configuration-intro.html)
C(X) : 14 일이 지난 데이터를 보관하길 원한다고 했는데 삭제해버리므로 오답.

설명 2:
https://aws.amazon.com/ko/kinesis/data-firehose/features/?nc=sn&loc=2#:~:text=into%20Amazon%20S3%2C%20

Q41
A company's application integrates with multiple software-as-a-service (SaaS) sources for data collection. The company runs Amazon EC2 instances to receive the data and to upload the data to an Amazon S3 bucket for analysis. The same EC2 instance that receives and uploads the data also sends a notification to the user when an upload is complete. The company has noticed slow application performance and wants to improve the performance as much as possible.
Which solution will meet these requirements with the LEAST operational overhead?
A. Create an Auto Scaling group so that EC2 instances can scale out. Configure an S3 event notification to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.
B. Create an Amazon AppFlow flow to transfer data between each SaaS source and the S3 bucket. Configure an S3 event notification to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.

C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for each SaaS source to send output data. Configure the S3 bucket as the rule's target. Create a second EventBridge (Cloud Watch Events) rule to send events when the upload to the S3 bucket is complete. Configure an Amazon Simple Notification Service (Amazon SNS) topic as the second rule's target.
D. Create a Docker container to use instead of an EC2 instance. Host the containerized application on Amazon Elastic Container Service (Amazon ECS). Configure Amazon CloudWatch Container Insights to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85446-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
Amazon AppFlow 는 Salesforce, SAP, Zendesk, Slack 및 ServiceNow 와 같은 SaaS(Software-as-a-Service) 애플리케이션과 Amazon S3 및 Amazon Redshift 와 같은 AWS 서비스 간에 데이터를 안전하게 전송할 수 있는 완전 관리형 통합 서비스입니다. 클릭 몇 번이면 됩니다.
https://aws.amazon.com/appflow/

설명 2:
SaaS = Appflow. Appflow 는 완전 관리형 통합 서비스이기 때문에 운영 오버헤드가 적음.
Amazon AppFlow 는 클릭 몇 번으로 Salesforce, Marketo, Slack 및 ServiceNow 와 같은 SaaS(Software-as-a-Service) 애플리케이션과 Amazon S3 및 Amazon Redshift 와 같은 AWS 서비스 간에 데이터를 안전하게 전송할 수 있게 해 주는 완전관리형 통합 서비스.
https://aws.amazon.com/ko/appflow/faqs/

Q42
A company runs a highly available image-processing application on Amazon EC2 instances in a single VPC. The EC2 instances run inside several subnets across multiple Availability Zones. The EC2 instances do not communicate with each other. However, the EC2 instances download images from Amazon S3 and upload images to Amazon S3 through a single NAT gateway. The company is concerned about data transfer charges.
What is the MOST cost-effective way for the company to avoid Regional data transfer charges?

A. Launch the NAT gateway in each Availability Zone.
B. Replace the NAT gateway with a NAT instance.
C. Deploy a gateway VPC endpoint for Amazon S3.
D. Provision an EC2 Dedicated Host to run the EC2 instances.
Answer: C
https://www.examtopics.com/discussions/amazon/view/85205-exam-aws-certified-solutions-architect-associate-saa-c03/

해설 1: ▪
데이터 전송 요금이 걱정되니 전용 전송 통로를 뚫으면 됨. VPC-S3 간 전용 통로는 S3 VPC Gateway Endpoint. 답은 C.

해설 2:
S3 용 게이트웨이 VPC 엔드포인트를 배포함으로써 회사는 인터넷 게이트웨이나 NAT 게이트웨이를 거치지 않고 VPC 와 S3 사이에 직접 연결을 설정할 수 있습니다. 이렇게 하면 EC2 와 S3 사이의 트래픽이 Amazon 네트워크 내에 머물면서 지역 데이터 전송 요금을 피할 수 있습니다.

A 는 각 AZ 에서 NAT 게이트웨이를 시작할 것을 제안합니다. 이는 가용성과 중복성에 도움이 될 수 있지만 트래픽이 여전히 NAT 게이트웨이를 통과하고 데이터 전송 요금이 발생하므로 데이터 전송 요금 문제를 해결하지 못합니다.

B 는 NAT 게이트웨이를 NAT 인스턴스로 교체할 것을 제안합니다. 그러나 이 솔루션은 여전히 NAT 인스턴스를 통해 인스턴스와 S3 간에 데이터를 전송하므로 데이터 전송 요금이 발생합니다.

D 는 EC2 를 실행하기 위해 EC2 전용 호스트를 프로비저닝할 것을 제안합니다. 이는 인스턴스 전용 하드웨어를 제공할 수 있지만 데이터 전송 요금 문제를 직접적으로 해결하지는 않습니다.

Q43
A company has an on-premises application that generates a large amount of time-sensitive data that is backed up to Amazon S3. The application has grown and there are user complaints about internet bandwidth limitations. A solutions architect needs to design a long-term solution that allows for both timely backups to Amazon S3 and with minimal

impact on internet connectivity for internal users.
Which solution meets these requirements?
A. Establish AWS VPN connections and proxy all traffic through a VPC gateway endpoint.
B. Establish a new AWS Direct Connect connection and direct backup traffic through this new connection.
C. Order daily AWS Snowball devices. Load the data onto the Snowball devices and return the devices to AWS each day.
D. Submit a support ticket through the AWS Management Console. Request the removal of S3 service limits from the account.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85206-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : VPN 은 인터넷을 통과하는데다가, VPC Gateway Endpoint 는 VPC-S3,Dynamo 간 전송을 담당.
B(O) : Direct Connect 는 전용선을 통과하기 때문에 인터넷에 전송중인 데이터가 노출되지 않음
C(X) : Snowball Device 는 배송기간까지 합하면 보통 7 일 정도 걸리는데 이를 매일 주문한다는 것은 무리수.
D(X) : 한도 증가만 가능. 한도 제거 옵션은 없음.
https://docs.aws.amazon.com/ko_kr/general/latest/gr/aws_service_limits.html

설명 2:
회사의 온프레미스 애플리케이션에 대한 대역폭 제한 문제를 해결하고 내부 사용자 연결에 대한 영향을 최소화하려면 이 새로운 연결을 통해 백업 트래픽을 전달하도록 새로운 AWS Direct Connect 연결을 설정해야 합니다. 이 솔루션은 회사의 데이터 센터와 AWS 간에 안전한 고속 연결을 제공하여 회사가 인터넷 대역폭을 사용하지 않고 데이터를 빠르게 전송할 수 있도록 합니다.
참조:
AWS Direct Connect 설명서: https://aws.amazon.com/directconnect/

Q44
A company has an Amazon S3 bucket that contains critical data. The company must protect the data from accidental deletion.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two)

A. Enable versioning on the S3 bucket.

B. Enable MFA Delete on the S3 bucket.

C. Create a bucket policy on the S3 bucket.

D. Enable default encryption on the S3 bucket.

E. Create a lifecycle policy for the objects in the S3 bucket.

Answer: A, B

https://www.examtopics.com/discussions/amazon/view/84750-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

A(O) : 버전 관리는 실수로 삭제했을 때 이전 버전의 파일을 불러올 수 있도록 해줌.

Amazon S3 의 버전 관리는 동일 버킷 내에 여러 개의 객체 변형을 보유하는 수단입니다. S3 버전 관리를 사용하면 버킷에 저장된 모든 버전의 객체를 모두 보존, 검색 및 복원할 수 있습니다.

https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/Versioning.html

B(O) : MFA Delete 는 함부로 삭제하지 못하도록 막음.

MFA Delete 는 다음 작업에 대해 추가 인증을 요구합니다. ◎버킷의 버전 관리 상태 변경 ◎객체 버전 영구 삭제

https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/MultiFactorAuthenticationDelete.html

C(X) : 버킷 정책은 액세스 권한에 관련된 것. 버킷 정책은 버킷과 해당 버킷의 객체에 대한 액세스 권한을 부여할 수 있는 리소스 기반 정책입니다.

https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/bucket-policies.html

D(X) : 암호화는 파일 내용을 함부로 볼 수 없게하는 등의 기능은 있지만 기본적으로 삭제는 막지 못함. 우리가 직장에서 DRM 걸린 문서는 열람 못해도 액세스 권한이 있다면 삭제할 수 있는 거랑 비슷함.

E(X) : 객체 수명 주기 정책은 객체를 언제 이동하고 삭제할 거냐의 문제.

설명 2:

S3 버킷의 데이터를 실수로 삭제하지 않도록 보호하려면 S3 버킷에 있는 모든 객체의 모든 버전을 보존, 검색 및 복원할 수 있는 버전 관리를 활성화해야 합니다.

또한 S3 버킷에서 MFA(다단계 인증) 삭제를 활성화하면 버킷의 객체를 삭제하기 위해 사용자의 액세스 키 외에 인증 토큰을 요구함으로써 추가 보호 계층이 추가됩니다.

참조:

AWS S3 버전 관리 설명서:
https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html
AWS S3 MFA 문서 삭제:
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html

Q45
A company has a data ingestion workflow that consists of the following:
• An Amazon Simple Notification Service (Amazon SNS) topic for notifications about new data deliveries
• An AWS Lambda function to process the data and record metadata
The company observes that the ingestion workflow fails occasionally because of network connectivity issues. When such a failure occurs, the Lambda function does not ingest the corresponding data unless the company manually reruns the job.
Which combination of actions should a solutions architect take to ensure that the Lambda function ingests all data in the future? (Choose two.)
A. Deploy the Lambda function in multiple Availability Zones.
B. Create an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe it to the SNS topic.
C. Increase the CPU and memory that are allocated to the Lambda function.
D. Increase provisioned throughput for the Lambda function.
E. Modify the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue.
Answer: B, E
https://www.examtopics.com/discussions/amazon/view/85408-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
네트워크 연결 문제로 데이터 수집이 잠시 실패하는 현상이 일어남. 이런 경우 데이터 손실이 일어날 위험성이 크므로 데이터를 보관해둘 곳이 필요하고, 대책으로는 SQS Queue 가 적절. 또한 SQS Queue 에 머물러 있는 작업들은 Lambda 로 처리 가능. 답은 BE. SQS 를 사용하면 메시지 손실 위험을 감수하거나 다른 서비스를 가동할 필요 없이 소프트웨어 구성 요소 간에 모든 볼륨의 메시지를 전송, 저장 및 수신할 수 있습니다.
https://aws.amazon.com/ko/sqs/
Lambda 함수를 사용하여 Amazon Simple Queue Service(Amazon SQS) 대기열의 메시지를 처리할 수 있습니다.

https://docs.aws.amazon.com/ko_kr/lambda/latest/dg/with-sqs.html

설명 2:
간헐적인 네트워크 연결 문제에도 불구하고 Lambda 함수가 향후 모든 데이터를 수집하도록 하려면 다음 조치를 취해야 합니다.
Amazon Simple Queue Service(SQS) 대기열을 생성하고 SNS 주제를 구독합니다. 이를 통해 알림과 처리를 분리할 수 있으므로 처리 Lambda 함수가 실패하더라도 나중에 추가 처리를 위해 메시지가 대기열에 남아 있습니다.
SNS 에서 직접 읽지 않고 SQS 대기열에서 읽도록 Lambda 함수를 수정합니다. 이 분리는 재시도 및 내결함성을 허용하고 모든 메시지가 Lambda 함수에 의해 처리되도록 합니다.
참조:
AWS SNS 설명서: https://aws.amazon.com/sns/
AWS SQS 설명서: https://aws.amazon.com/sqs/
AWS Lambda 설명서: https://aws.amazon.com/lambda/

Q46
A company has an application that provides marketing services to stores. The services are based on previous purchases by store customers. The stores upload transaction data to the company through SFTP, and the data is processed and analyzed to generate new marketing offers. Some of the files can exceed 200 GB in size.
Recently, the company discovered that some of the stores have uploaded files that contain personally identifiable information (PII) that should not have been included. The company wants administrators to be alerted if PII is shared again. The company also wants to automate remediation.
What should a solutions architect do to meet these requirements with the LEAST development effort?
A. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Inspector to scan the objects in the bucket. If objects contain PII, trigger an S3 Lifecycle policy to remove the objects that contain PII.
B. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Macie to scan the objects in the bucket. If objects contain PII, use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain PII.
C. Implement custom scanning algorithms in an AWS Lambda function. Trigger the function when objects are loaded into the bucket. If objects contain PII, use Amazon Simple

Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain PII.
D. Implement custom scanning algorithms in an AWS Lambda function. Trigger the function when objects are loaded into the bucket. If objects contain PII, use Amazon Simple Email Service (Amazon SES) to trigger a notification to the administrators and trigger an S3 Lifecycle policy to remove the meats that contain PII.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85264-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
Amazon Macie 는 AWS 에서 PII 와 같은 민감한 데이터를 자동으로 검색, 분류 및 보호하는 관리형 서비스입니다. S3 에서 Macie 를 활성화하면 업로드된 객체에서 PII 를 검색할 수 있습니다.

A. Amazon Inspector 를 사용하여 S3 의 객체를 스캔하는 것은 PII 데이터 스캔을 위한 최적의 선택이 아닙니다. Amazon Inspector 는 콘텐츠 스캔이 아닌 호스트 수준 취약성 평가를 위해 설계되었습니다.

C. AWS Lambda 함수에서 사용자 지정 검색 알고리즘을 구현하려면 대용량 파일 검색을 처리하기 위해 상당한 개발 노력이 필요합니다.

D. 알림에 SES 를 사용하고 S3 수명 주기 정책을 트리거하면 솔루션에 불필요한 복잡성이 추가될 수 있습니다.

따라서 최소한의 개발 노력으로 요구 사항을 충족하는 최상의 옵션은 S3 를 안전한 전송 지점으로 사용하고 Amazon Macie 를 PII 스캔에 활용하고 관리자에게 SNS 알림을 트리거하는 것입니다(옵션 B).

설명 2:
최소한의 개발 노력으로 PII 가 공유될 때 관리자에게 탐지 및 경고하고 수정을 자동화하는 요구 사항을 충족하려면 Amazon S3 버킷을 안전한 전송 지점으로 사용하고 Amazon Macie 로 버킷의 객체를 스캔하는 것이 가장 좋습니다.
Amazon Macie 는 기계 학습 및 패턴 일치를 사용하여 Amazon S3 에 저장된 중요한 데이터를 검색하고 보호하는 완전 관리형 데이터 보안 및 데이터 개인 정보 보호 서비스입니다. 민감한 데이터를 분류하고, 민감한 데이터에 대한 액세스를 모니터링하고,

수정 작업을 자동화하는 데 사용할 수 있습니다.
이 시나리오에서는 파일을 Amazon S3 버킷에 업로드한 후 Amazon Macie 에서 객체를 스캔하여 PII 를 찾을 수 있으며, PII 가 감지되면 Amazon Simple Notification Service(SNS) 알림을 트리거하여 관리자에게 제거하도록 알릴 수 있습니다. PII 를 포함하는 객체. Amazon Macie 에는 이미 다양한 형식의 PII 를 탐지할 수 있는 사전 구축된 데이터 분류 규칙이 있으므로 이 접근 방식은 최소한의 개발 노력이 필요합니다.
개인정보 = Macie. 정답은 B.
참조:
html AWS Well-Architected 프레임워크 - 보안 기반:
https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html

Q47
A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week.
What should the company do to guarantee the EC2 capacity?
A. Purchase Reserved Instances that specify the Region needed.
B. Create an On-Demand Capacity Reservation that specifies the Region needed.
C. Purchase Reserved Instances that specify the Region and three Availability Zones needed.
D. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed.
Answer: D
https://www.examtopics.com/discussions/amazon/view/85529-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : 예약 인스턴스는 1 년 또는 3 년 단위 약정 방식.
예약 인스턴스(RI)는 1 년 또는 3 년 기간으로 약정하는 경우 EC2 사용 요금을 상당히 할인해 주는 EC2 상품입니다. https://aws.amazon.com/ko/ec2/faqs/
B(X) : 용량 예약을 생성할 때 다음을 지정합니다. ◎용량을 예약할 가용 영역
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html
C(X) : 예약 인스턴스는 1 년 또는 3 년 단위 약정 방식.
D(O) : B 번 참조.

설명 2:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html
예비 인스턴스: 비용 효율적이지 않은 전체 기간(1 년 또는 3 년)에 대해 비용을 지불해야 합니다.

Q48

A company's website uses an Amazon EC2 instance store for its catalog of items. The company wants to make sure that the catalog is highly available and that the catalog is stored in a durable location.

What should a solutions architect do to meet these requirements?

A. Move the catalog to Amazon ElastiCache for Redis.

B. Deploy a larger EC2 instance with a larger instance store.

C. Move the catalog from the instance store to Amazon S3 Glacier Deep Archive.

D. Move the catalog to an Amazon Elastic File System (Amazon EFS) file system.

Answer: D

https://www.examtopics.com/discussions/amazon/view/85119-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

A(X) : ElastiCache 는 캐시 서비스.

B(X) : 인스턴스 스토어는 휘발성 스토리지. 내구성 불충족.

C(X) : Amazon S3 Glacier Deep Archive 는 콜드 스토리지. 가용성 불충족.

D(O) : 정답.

설명 2:

카탈로그를 Amazon Elastic File System(Amazon EFS) 파일 시스템으로 이동하면 고가용성과 내구성이 모두 제공됩니다. Amazon EFS 는 필요에 따라 확장할 수 있도록 구축된 완전 관리형, 가용성 및 내구성이 뛰어난 파일 시스템입니다. Amazon EFS 를 사용하면 다양한 가용 영역에 있는 여러 EC2 인스턴스에서 카탈로그 데이터를 저장하고 액세스할 수 있으므로 고가용성이 보장됩니다. 또한 Amazon EFS 는 여러 가용 영역 내에서 파일을 자동으로 중복 저장하므로 내구성 있는 스토리지 옵션이 됩니다.

Q49

A company stores call transcript files on a monthly basis. Users access the files randomly within 1 year of the call, but users access the files infrequently after 1 year. The company

wants to optimize its solution by giving users the ability to query and retrieve files that are less than 1-year-old as quickly as possible. A delay in retrieving older files is acceptable. Which solution will meet these requirements MOST cost-effectively?

A. Store individual files with tags in Amazon S3 Glacier Instant Retrieval. Query the tags to retrieve the files from S3 Glacier Instant Retrieval.

B. Store individual files in Amazon S3 Intelligent-Tiering. Use S3 Lifecycle policies to move the files to S3 Glacier Flexible Retrieval after 1 year. Query and retrieve the files that are in Amazon S3 by using Amazon Athena. Query and retrieve the files that are in S3 Glacier by using S3 Glacier Select.

C. Store individual files with tags in Amazon S3 Standard storage. Store search metadata for each archive in Amazon S3 Standard storage. Use S3 Lifecycle policies to move the files to S3 Glacier Instant Retrieval after 1 year. Query and retrieve the files by searching for metadata from Amazon S3.

D. Store individual files in Amazon S3 Standard storage. Use S3 Lifecycle policies to move the files to S3 Glacier Deep Archive after 1 year. Store search metadata in Amazon RDS. Query the files from Amazon RDS. Retrieve the files from S3 Glacier Deep Archive.

Answer: B

https://www.examtopics.com/discussions/amazon/view/85211-exam-aws-certified-solutions-architect-associate-saa-c03/

해설:

의료 이미지, 뉴스 미디어 자산 또는 유전체학 데이터와 같이 즉각적인 액세스가 필요한 아카이브 데이터의 경우 S3 Glacier Instant Retrieve 스토리지 클래스를 선택하십시오. S3 Glacier Instant Retrieve 스토리지 클래스는 밀리초 검색으로 최저 비용의 스토리지를 제공합니다.

즉각적인 액세스가 필요하지는 않지만 백업 또는 재해 복구 사용 사례와 같이 비용 없이 대용량 데이터 세트를 검색할 수 있는 유연성이 필요한 아카이브 데이터의 경우 S3 Glacier Flexible Retrieve(이전의 S3 Glacier)를 선택하고, 몇 분 내에 검색하거나 5-12 시간 내에 대량 검색을 무료로 제공합니다.

Q50

A company has a production workload that runs on 1,000 Amazon EC2 Linux instances. The workload is powered by third-party software. The company needs to patch the third-party software on all EC2 instances as quickly as possible to remediate a critical security vulnerability.

What should a solutions architect do to meet these requirements?

A. Create an AWS Lambda function to apply the patch to all EC2 instances.

B. Configure AWS Systems Manager Patch Manager to apply the patch to all EC2 instances.

C. Schedule an AWS Systems Manager maintenance window to apply the patch to all EC2 instances.

D. Use AWS Systems Manager Run Command to run a custom command that applies the patch to all EC2 instances.

Answer: D

https://www.examtopics.com/discussions/amazon/view/85026-exam-aws-certified-solutions-architect-associate-saa-c03/

해설:

A(X) : 1000 개의 인스턴스에 일일이 다 Lambda 로 패치 적용한다는 것은 비효율적이고 번거로움

B(X) : 자동 업데이트에는 시간이 좀 걸림. ""패치 관리자는 승인 및 거부된 패치 목록과 함께 릴리스 후 며칠 이내에 패치를 자동 승인하기 위한 규칙을 포함 하는 패치 기준선 을 사용합니다.

https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html

C(X) : 가능한 빨리 패치해야한다고 했는데 예약을 하고 있어서 안 됨.

D(O) : 리소스 그룹을 통해 한 번에 여러 인스턴스를 업데이트 가능. 리소스 그룹이 명령 대상으로 지원됨에 따라 해당 리소스 그룹에 속한 모든 관리형 인스턴스에서 관리 및 임시 작업을 자동화할 수 있습니다.

https://aws.amazon.com/ko/about-aws/whats-new/2019/08/now-select-resource-groups-as-targets-for-aws-systems-manager-run-command/

참고:

https://docs.aws.amazon.com/ko_kr/systems-manager/latest/userguide/about-windows-app-patching.html

Q51

A company is developing an application that provides order shipping statistics for retrieval by a REST API. The company wants to extract the shipping statistics, organize the data into an easy-to-read HTML format, and send the report to several email addresses at the same time every morning.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two)

A. Configure the application to send the data to Amazon Kinesis Data Firehose.

B. Use Amazon Simple Email Service (Amazon SES) to format the data and to send the report by email.

C. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Glue job to query the application's API for the data.

D. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Lambda function to query the application's API for the data.

E. Store the application data in Amazon S3. Create an Amazon Simple Notification Service (Amazon SNS) topic as an S3 event destination to send the report by email.

Answer: B, D

https://www.examtopics.com/discussions/amazon/view/85557-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

https://docs.aws.amazon.com/ses/latest/dg/send-email-formatted.html

1. 데이터에 대한 애플리케이션의 API 를 쿼리하기 위해 AWS Lambda 함수를 호출하는 Amazon EventBridge(Amazon CloudWatch Events) 예약 이벤트를 생성합니다. 이 단계는 AWS Lambda 를 사용하여 배송 통계를 추출하고 데이터를 HTML 형식으로 구성할 수 있습니다.

2. Amazon Simple Email Service(Amazon SES)를 사용하여 데이터 형식을 지정하고 이메일로 보고서를 보냅니다.

이 단계는 Amazon SES 를 사용하여 매일 아침 동시에 여러 이메일 주소로 보고서를 전송함으로써 수행할 수 있습니다.

따라서 옵션 D 와 B 는 이 질문에 대한 올바른 선택입니다. Kinesis Data Firehose 가 이 사용 사례에 필요하지 않기 때문에 옵션 A 는 올바르지 않습니다. 애플리케이션의 API 를 쿼리하는 데 AWS Glue 가 필요하지 않기 때문에 옵션 C 는 올바르지 않습니다. S3 이벤트 알림을 사용하여 이메일로 보고서를 보낼 수 없기 때문에 옵션 E 는 올바르지 않습니다.

설명 2:

B(O) : HTML 형식의 이메일 요구사항을 충족

D(O) : 매일 아침 일정 이벤트 요구사항 충족

Q52

A company wants to migrate its on-premises application to AWS. The application produces output files that vary in size from tens of gigabytes to hundreds of terabytes. The application data must be stored in a standard file system structure. The company wants a solution that scales automatically. is highly available, and requires minimum operational overhead.
Which solution will meet these requirements?
A. Migrate the application to run as containers on Amazon Elastic Container Service (Amazon ECS). Use Amazon S3 for storage.
B. Migrate the application to run as containers on Amazon Elastic Kubernetes Service (Amazon EKS). Use Amazon Elastic Block Store (Amazon EBS) for storage.
C. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic File System (Amazon EFS) for storage.
D. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic Block Store (Amazon EBS) for storage.
Answer: C
https://www.examtopics.com/discussions/amazon/view/85265-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
EFS 는 표준 파일 시스템으로 자동 확장되며 가용성이 높습니다.

설명 2:
고가용성이므로 Auto Scaling 이 들어간 C,D 둘 중 하나가 정답. EFS vs EBS 를 비교해보면 보통은 EFS 가 정답인 경우가 많음. 일단 EBS 는 여러 EC2 인스턴스에서 동시 접속할 수 없다는 단점이 치명적이기 때문.
Amazon Elastic File System 은 전체 파일 시스템 액세스 의미 체계를 지원하는 표준 파일 시스템 인터페이스를 제공합니다.
https://docs.aws.amazon.com/efs/latest/ug/using-fs.html
EBS 다중 연결 볼륨에서 표준 파일 시스템 작업은 지원되는 구성이 아닙니다.
https://aws.amazon.com/ko/premiumsupport/knowledge-center/ebs-access-volumes-using-multi-attach/

Q53
A company needs to store its accounting records in Amazon S3. The records must be immediately accessible for 1 year and then must be archived for an additional 9 years. No one at the company, including administrative users and root users, can be able to delete the

records during the entire 10-year period. The records must be stored with maximum resiliency.
Which solution will meet these requirements?
A. Store the records in S3 Glacier for the entire 10-year period. Use an access control policy to deny deletion of the records for a period of 10 years.
B. Store the records by using S3 Intelligent-Tiering. Use an IAM policy to deny deletion of the records. After 10 years, change the IAM policy to allow deletion.
C. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year. Use S3 Object Lock in compliance mode for a period of 10 years.
D. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 year. Use S3 Object Lock in governance mode for a period of 10 years.
Answer: C
https://www.examtopics.com/discussions/amazon/view/85532-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : 1 년 동안 즉시 액세스할 수 있어야 한다고 했으므로 액세스 시간이 1 분 이상 걸리는 S3 Glacier 는 오답.
B(X) : 특정 기간동안 즉시 액세스할 수 있어야 하므로 Intelligent Tiering 이 아니라 Life Cycle Policy 가 적합.
C(O) : S3 Standard = 즉시 액세스 가능 / S3 Glacier Deep Archive = 콜드 스토리지. 보관용으로 사용됨. Object Lock 으로 객체 삭제 방지.
S3 객체 잠금을 사용하면 write-once-read-many(WORM) 모델을 사용하여 객체를 저장할 수 있습니다. 객체 잠금은 고정된 시간 동안 또는 무기한으로 객체의 삭제 또는 덮어쓰기를 방지하는 데 도움이 될 수 있습니다.
https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/object-lock.html
D(X) : 기록은 최대한의 복원력으로 저장해야한다고 했으므로 One Zone-IA 는 적합하지 않음.

설명 2:
1 년 동안 즉시 액세스 가능한 레코드의 요구 사항을 충족한 다음 최대 복원력으로 추가 9 년 동안 보관하기 위해 S3 수명 주기 정책을 사용하여 1 년 후 S3 Standard 에서 S3 Glacier Deep Archive 로 레코드를 전환할 수 있습니다. 또한 관리자 및 루트 사용자를 포함하여 누구도 레코드를 삭제할 수 없도록 10 년 동안 규정 준수 모드에서 S3 객체 잠금을 사용할 수 있습니다. 따라서 정답은 옵션 C 입니다.

Q54

A company runs multiple Windows workloads on AWS. The company's employees use Windows file shares that are hosted on two Amazon EC2 instances. The file shares synchronize data between themselves and maintain duplicate copies. The company wants a highly available and durable storage solution that preserves how users currently access the files.

What should a solutions architect do to meet these requirements?

A. Migrate all the data to Amazon S3. Set up IAM authentication for users to access files.

B. Set up an Amazon S3 File Gateway. Mount the S3 File Gateway on the existing EC2 instances.

C. Extend the file share environment to Amazon FSx for Windows File Server with a Multi-AZ configuration. Migrate all the data to FSx for Windows File Server.

D. Extend the file share environment to Amazon Elastic File System (Amazon EFS) with a Multi-AZ configuration. Migrate all the data to Amazon EFS.

Answer: C

https://www.examtopics.com/discussions/amazon/view/85574-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

Windows File 공유가 핵심 키워드. 답은 C.

설명 2:

https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/AmazonEFS.html

Amazon FSx for Windows File Server 는 완전히 네이티브로 지원되는 완전히 관리되는 Microsoft Windows 파일 서버를 제공합니다.

윈도우 파일 시스템.

https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html

Q55

A solutions architect is developing a VPC architecture that includes multiple subnets. The architecture will host applications that use Amazon EC2 instances and Amazon RDS DB instances. The architecture consists of six subnets in two Availability Zones. Each Availability Zone includes a public subnet, a private subnet, and a dedicated subnet for

databases. Only EC2 instances that run in the private subnets can have access to the RDS databases.
Which solution will meet these requirements?
A. Create a new route table that excludes the route to the public subnets' CIDR blocks. Associate the route table with the database subnets.
B. Create a security group that denies inbound traffic from the security group that is assigned to instances in the public subnets. Attach the security group to the DB instances.
C. Create a security group that allows inbound traffic from the security group that is assigned to instances in the private subnets. Attach the security group to the DB instances.
D. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.
Answer: C
https://www.examtopics.com/discussions/amazon/view/85409-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
프라이빗 서브넷의 인스턴스에 할당된 보안 그룹의 인바운드 트래픽을 허용하는 보안 그룹을 생성하면 프라이빗 서브넷에서 실행되는 EC2 만 RDS 데이터베이스에 액세스할 수 있습니다. 보안 그룹을 DB 와 연결하여 지정된 보안 그룹에 속한 인스턴스로만 접근을 제한합니다.

질문에 설명된 요구 사항을 충족하는 솔루션은 옵션 C 입니다. 프라이빗 서브넷의 인스턴스에 할당된 보안 그룹에서 인바운드 트래픽을 허용하는 보안 그룹을 생성합니다. 보안 그룹을 DB 인스턴스에 연결합니다.

이 솔루션에서 DB 인스턴스에 적용된 보안 그룹은 프라이빗 서브넷의 인스턴스에 할당된 보안 그룹의 인바운드 트래픽을 허용합니다. 이렇게 하면 프라이빗 서브넷에서 실행되는 EC2 인스턴스만 RDS 데이터베이스에 액세스할 수 있습니다.

Q56
A company has registered its domain name with Amazon Route 53. The company uses Amazon API Gateway in the ca-central-1 Region as a public interface for its backend microservice APIs. Third-party services consume the APIs securely. The company wants to design its API Gateway URL with the company's domain name and corresponding certificate

so that the third-party services can use HTTPS.
Which solution will meet these requirements?
A. Create stage variables in API Gateway with Name="Endpoint-URL" and Value="Company Domain Name" to overwrite the default URL. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM).
B. Create Route 53 DNS records with the company's domain name. Point the alias record to the Regional API Gateway stage endpoint. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region.
C. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Region. Attach the certificate to the API Gateway endpoint. Configure Route 53 to route traffic to the API Gateway endpoint.
D. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region. Attach the certificate to the API Gateway APIs. Create Route 53 DNS records with the company's domain name. Point an A record to the company's domain name.
Answer: C
https://www.examtopics.com/discussions/amazon/view/85266-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
사용자 정의 도메인 이름 은 API 사용자에게 제공할 수 있는 더 간단하고 직관적인 URL 입니다. API 를 배포한 후 귀하(및 귀하의 고객)는 다음 형식의 기본 기본 URL 을 사용하여 API 를 호출할 수 있습니다.
https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-custom-domains.html

리전 사용자 지정 도메인 이름은 API 와 동일한 AWS 리전에 있는 SSL/TLS 인증서를 사용해야 합니다.
https://aws.amazon.com/ko/premiumsupport/knowledge-center/custom-domain-name-amazon-api-gateway/

・여기서 API Gateway URL 이란, Route 53 에 등록된 도메인 이름으로, 이를 통해 API 를 호출할 수 있음.

• 인증서는 HTTPS 에 사용됨. HTTPS=HTTL + SSL 인데, SSL 에 인증서가 필요하기 때문. 인증서는 ACM 으로 가져올 수 있음.

1. 리전 API 게이트웨이 엔드포인트 생성 및 회사 도메인 이름과 연결
또한 API Gateway REST API, Amazon CLI 또는 Amazon SDK 중 하나를 호출하여 사용자 지정 도메인 이름을 호스트 이름으로 사용하여 API 의 기본 경로 매핑을 설정할 수 있습니다.
https://docs.amazonaws.cn/en_us/apigateway/latest/developerguide/how-to-edge-optimized-custom-domain-name.html#how-to-custom-domains-mapping-console
2. 회사 도메인 이름과 연결된 공인 인증서를 동일 리전의 ACM 으로 가져옴
API Gateway 리전 사용자 지정 도메인 이름의 경우 API 와 동일한 리전에서 인증서를 요청하거나 가져와야 합니다.....도메인 이름에 대한 인증서를 ACM 으로 가져오려면....
https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-custom-domains-prerequisites.html
3. API 게이트웨이 엔드포인트에 인증서 연결
ACM 인증서로 리전 사용자 지정 도메인 이름을 생성(또는 마이그레이션)하면 API Gateway 는 해당 계정에 서비스 연결 역할을 생성합니다(이 역할이 아직 없는 경우). 서비스 연결 역할은 ACM 인증서를 해당 리전 엔드포인트에 연결하는 데 필요합니다.
https://docs.aws.amazon.com/ko_kr/apigateway/latest/developerguide/apigateway-regional-api-custom-domain-create.html
4. API 게이트웨이 엔드포인트로 트래픽 라우팅 하도록 Route 53 설정

API Gateway 리전 사용자 지정 도메인 이름의 경우 API 와 동일한 리전에서 인증서를 요청하거나 가져와야 합니다. 그리하여 회사의 도메인 이름과 연결된 공인 인증서는 동일 리전의 ACM 으로 가져와야됩니다. 따라서 정답은 C 에 한표 입니다.
도메인 이름을 사용하여 Amazon API Gateway API 로 트래픽 라우팅
• 리전 API 엔드포인트(Regional API endpoint): 리전 API 엔드포인트로 트래픽을 라우팅하는 Route 53 별칭 레코드를 생성합니다.
https://docs.aws.amazon.com/ko_kr/Route53/latest/DeveloperGuide/routing-to-api-gateway.html

설명 2
회사의 도메인 이름과 해당 인증서로 API Gateway URL 을 설계하려면 회사에서 다음을 수행해야 합니다.
1. 지역 API 게이트웨이 엔드포인트 생성: 이를 통해 회사는 지역에 특정한 엔드포인트를 생성할 수 있습니다.

2. API 게이트웨이 엔드포인트를 회사의 도메인 이름과 연결: 이렇게 하면 회사에서 API 게이트웨이 URL 에 자체 도메인 이름을 사용할 수 있습니다.
3. 회사의 도메인 이름과 연결된 공인 인증서를 동일한 리전의 AWS Certificate Manager(ACM)로 가져옵니다. 이렇게 하면 회사에서 API 와의 보안 통신을 위해 HTTPS 를 사용할 수 있습니다.
4. API Gateway 엔드포인트에 인증서 첨부: 회사에서 API Gateway URL 보안을 위해 인증서를 사용할 수 있습니다.
5. 트래픽을 API 게이트웨이 엔드포인트로 라우팅하도록 Route 53 구성: 이를 통해 회사는 Route 53 을 사용하여 회사의 도메인 이름을 사용하는 API 게이트웨이 URL 로 트래픽을 라우팅할 수 있습니다.

Q57
A company is running a popular social media website. The website gives users the ability to upload images to share with other users. The company wants to make sure that the images do not contain inappropriate content. The company needs a solution that minimizes development effort.
What should a solutions architect do to meet these requirements?
A. Use Amazon Comprehend to detect inappropriate content. Use human review for low-confidence predictions.
B. Use Amazon Rekognition to detect inappropriate content. Use human review for low-confidence predictions.
C. Use Amazon SageMaker to detect inappropriate content. Use ground truth to label low-confidence predictions.
D. Use AWS Fargate to deploy a custom machine learning model to detect inappropriate content. Use ground truth to label low-confidence predictions.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85452-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Amazon Rekognition 을 사용하여 부적절하거나 원치 않거나 불쾌감을 주는 콘텐츠를 감지할 수 있습니다.
https://docs.aws.amazon.com/rekognition/latest/dg/moderation.html

참조

https://docs.aws.amazon.com/rekognition/latest/dg/moderation.html?pg=ln&sec=ft
https://docs.aws.amazon.com/rekognition/latest/dg/a2i-rekognition.html

Q58

A company wants to run its critical applications in containers to meet requirements for scalability and availability. The company prefers to focus on maintenance of the critical applications. The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload.

What should a solutions architect do to meet these requirements?

A. Use Amazon EC2 instances, and install Docker on the instances.

B. Use Amazon Elastic Container Service (Amazon ECS) on Amazon EC2 worker nodes.

C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.

D. Use Amazon EC2 instances from an Amazon Elastic Container Service (Amazon ECS)-optimized Amazon Machine Image (AMI).

Answer: C

https://www.examtopics.com/discussions/amazon/view/85453-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

AWS 에서 컨테이너라고 하면 ECS, ECS 라고 하면 일단 Fargate 부터 떠올리면 됨. AWS Fargate Fargate 는 Amazon EC2 인스턴스의 서버나 클러스터를 관리할 필요 없이 컨테이너를 실행하기 위해 Amazon ECS 에 사용할 수 있는 기술입니다.

https://docs.aws.amazon.com/ko_kr/AmazonECS/latest/developerguide/AWS_Fargate.html

설명 2:

요구 사항은 컨테이너화된 워크로드를 실행하기 위해 기본 인프라를 프로비저닝하고 관리할 필요 없이 확장성과 가용성을 위한 것이므로 AWS Fargate 에서 AWS ECS 를 사용합니다.

https://docs.aws.amazon.com/AmazonECS/latest/userguide/what-is-fargate.html

Q59

A company hosts more than 300 global websites and applications. The company requires a platform to analyze more than 30 TB of clickstream data each day.

What should a solutions architect do to transmit and process the clickstream data?

A. Design an AWS Data Pipeline to archive the data to an Amazon S3 bucket and run an Amazon EMR cluster with the data to generate analytics.
B. Create an Auto Scaling group of Amazon EC2 instances to process the data and send it to an Amazon S3 data lake for Amazon Redshift to use for analysis.
C. Cache the data to Amazon CloudFront. Store the data in an Amazon S3 bucket. When an object is added to the S3 bucket. run an AWS Lambda function to process the data for analysis.
D. Collect the data from Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to transmit the data to an Amazon S3 data lake. Load the data in Amazon Redshift for analysis.
Answer: D
https://www.examtopics.com/discussions/amazon/view/85793-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
대량의 스트림 데이터 수집 = Kinesis Data Streams. 정답은 D.
※실제 사례가 있음.
◎전 세계 300 개 이상의 Hearst 웹사이트에서 스트리밍되는 하루 30 테라바이트 이상의 클릭스트림 데이터를 전송하고 처리하는 클릭스트림 분석 플랫폼을 구축했습니다.
◎Amazon Kinesis Firehose 는 버퍼링된 데이터를 Amazon Kinesis Data Streams 에서 Amazon Simple Storage Service (Amazon S3) 의 영구 스토리지로 자동 이동합니다. 이는 팀이 이전에 관리해야 했던 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 대체합니다.
◎변환된 클릭스트림 데이터는 Hearst 데이터 레이크에서 가져와 분석 쿼리 및 복잡한 데이터 과학 작업을 위해 Amazon Redshift 로 전송됩니다.
◎Amazon Redshift 에서 데이터는 API 를 통해 회사의 콘텐츠 관리 시스템으로 최종 사용자에게 푸시됩니다.
https://aws.amazon.com/ko/solutions/case-studies/hearst-data-analytics/

Q60
A company has a website hosted on AWS. The website is behind an Application Load Balancer (ALB) that is configured to handle HTTP and HTTPS separately. The company wants to forward all requests to the website so that the requests will use HTTPS.
What should a solutions architect do to meet this requirement?
A. Update the ALB's network ACL to accept only HTTPS traffic.

B. Create a rule that replaces the HTTP in the URL with HTTPS.
C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.
D. Replace the ALB with a Network Load Balancer configured to use Server Name Indication (SNI).
Answer: C
https://www.examtopics.com/discussions/amazon/view/85121-exam-aws-certified-solutions-architect-associate-saa-c03/

해설:
Application Load Balancer 를 위한 리스너…..쿼리 문자열 조건을 사용하여 쿼리 문자열의 키/값 페어 또는 값을 기반으로 요청을 라우팅하는 규칙을 구성할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/elasticloadbalancing/latest/application/load-balancer-listeners.html
Application Load Balancer 리스너 규칙을 사용하여 HTTP 요청을 HTTPS 로 리디렉션하려고 합니다. 어떻게 해야 하나요?
①HTTP 요청을 HTTPS 로 리디렉션하는 HTTP 리스너 규칙 생성.
②HTTPS 리스너 생성.
③Application Load Balancer 의 보안 그룹이 443 의 트래픽을 허용하는지 확인
https://aws.amazon.com/ko/premiumsupport/knowledge-center/elb-redirect-http-to-https-using-alb/

참조
https://aws.amazon.com/premiumsupport/knowledge-center/elb-redirect-http-to-https-using-alb/
https://repost.aws/ko/knowledge-center/elb-redirect-http-to-https-using-alb

Q61
A company is developing a two-tier web application on AWS. The company's developers have deployed the application on an Amazon EC2 instance that connects directly to a backend Amazon RDS database. The company must not hardcode database credentials in the application. The company must also implement a solution to automatically rotate the database credentials on a regular basis.
Which solution will meet these requirements with the LEAST operational overhead?
A. Store the database credentials in the instance metadata. Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates

the RDS credentials and instance metadata at the same time.
B. Store the database credentials in a configuration file in an encrypted Amazon S3 bucket. Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and the credentials in the configuration file at the same time. Use S3 Versioning to ensure the ability to fall back to previous values.
C. Store the database credentials as a secret in AWS Secrets Manager. Turn on automatic rotation for the secret. Attach the required permission to the EC2 role to grant access to the secret.
D. Store the database credentials as encrypted parameters in AWS Systems Manager Parameter Store. Turn on automatic rotation for the encrypted parameters. Attach the required permission to the EC2 role to grant access to the encrypted parameters.
Answer: C
https://www.examtopics.com/discussions/amazon/view/85580-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
애플리케이션에 자격증명 하드코딩 안 됨 = Secrets Manager.
Secrets Manager 를 사용하면 애플리케이션 소스 코드에서 하드 코딩된 자격 증명을 제거하고 애플리케이션 자체에 자격 증명을 저장하지 않음으로써 보안 태세를 개선할 수 있습니다. 사용자의 개입 없이 지정한 일정에 따라 자동으로 보안 암호를 교체하도록 Secrets Manager 를 구성할 수 있습니다. 교체는 AWS Lambda 함수를 사용하여 정하고 실행합니다.
https://docs.aws.amazon.com/ko_kr/secretsmanager/latest/userguide/intro.html

참고:
https://docs.aws.amazon.com/secretsmanager/latest/userguide/create_database_secret.html

Q62
A company is deploying a new public web application to AWS. The application will run behind an Application Load Balancer (ALB). The application needs to be encrypted at the edge with an SSL/TLS certificate that is issued by an external certificate authority (CA). The certificate must be rotated each year before the certificate expires.
What should a solutions architect do to meet these requirements?
A. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate. Apply the certificate

to the ALB. Use the managed renewal feature to automatically rotate the certificate.
B. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate. Import the key material from the certificate. Apply the certificate to the ALUse the managed renewal feature to automatically rotate the certificate.
C. Use AWS Certificate Manager (ACM) Private Certificate Authority to issue an SSL/TLS certificate from the root CA. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.
D. Use AWS Certificate Manager (ACM) to import an SSL/TLS certificate. Apply the certificate to the ALB. Use Amazon EventBridge (Amazon CloudWatch Events) to send a notification when the certificate is nearing expiration. Rotate the certificate manually.
Answer: D
https://www.examtopics.com/discussions/amazon/view/85524-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
외부 인증기관에서 발급한 SSL/TLS 인증서가 이미 있고 이를 사용해야하므로 ACM 쪽에서 SSL/TLS 인증서를 발급하는 A,B 는 모두 오답.
C(X) : 인증서가 있는데 또 발급받을 필요가 없음.
https://www.amazonaws.cn/en/certificate-manager/faqs/#Managed_renewal_and_deployment

Q63
A company runs its infrastructure on AWS and has a registered base of 700,000 users for its document management application. The company intends to create a product that converts large .pdf files to .jpg image files. The .pdf files average 5 MB in size. The company needs to store the original files and the converted files. A solutions architect must design a scalable solution to accommodate demand that will grow rapidly over time.
Which solution meets these requirements MOST cost-effectively?
A. Save the .pdf files to Amazon S3. Configure an S3 PUT event to invoke an AWS Lambda function to convert the files to .jpg format and store them back in Amazon S3.
B. Save the .pdf files to Amazon DynamoDUse the DynamoDB Streams feature to invoke an AWS Lambda function to convert the files to .jpg format and store them back in DynamoDB.
C. Upload the .pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic Block Store (Amazon EBS) storage, and an Auto Scaling group. Use a program in the EC2 instances to convert the files to .jpg format. Save the .pdf files and

the .jpg files in the EBS store.
D. Upload the .pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic File System (Amazon EFS) storage, and an Auto Scaling group. Use a program in the EC2 instances to convert the file to .jpg format. Save the .pdf files and the .jpg files in the EBS store.
Answer: A
https://www.examtopics.com/discussions/amazon/view/85795-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(O) : S3 에 넣으면 Lambda 를 통해 자동으로 처리가 되도록 하는 거라 OK. S3 는 저렴함.
B(X) : dynamodb 는 이미지 저장용으론…
C(X) : 저렴한 S3 가 있는데 굳이... 인스턴스 비용도 나감.
D(x) : C 와 마찬가지.

설명 2:
Elastic BeanStalk 는 비싸고 DocumentDB 는 최대 400KB 의 파일을 업로드할 수 있습니다. 따라서 Lambda 와 S3 가 하나여야 합니다.

Q64
A company has more than 5 TB of file data on Windows file servers that run on premises. Users and applications interact with the data each day.
The company is moving its Windows workloads to AWS. As the company continues this process, the company requires access to AWS and on-premises file storage with minimum latency. The company needs a solution that minimizes operational overhead and requires no significant changes to the existing file access patterns. The company uses an AWS Site-to-Site VPN connection for connectivity to AWS.
What should a solutions architect do to meet these requirements?
A. Deploy and configure Amazon FSx for Windows File Server on AWS. Move the on-premises file data to FSx for Windows File Server. Reconfigure the workloads to use FSx for Windows File Server on AWS.
B. Deploy and configure an Amazon S3 File Gateway on premises. Move the on-premises file data to the S3 File Gateway. Reconfigure the on-premises workloads and the cloud workloads to use the S3 File Gateway.
C. Deploy and configure an Amazon S3 File Gateway on premises. Move the on-premises

file data to Amazon S3. Reconfigure the workloads to use either Amazon S3 directly or the S3 File Gateway. depending on each workload's location.
D. Deploy and configure Amazon FSx for Windows File Server on AWS. Deploy and configure an Amazon FSx File Gateway on premises. Move the on-premises file data to the FSx File Gateway. Configure the cloud workloads to use FSx for Windows File Server on AWS. Configure the on-premises workloads to use the FSx File Gateway.
Answer: D
https://www.examtopics.com/discussions/amazon/view/85173-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
Windows File Server + AWS 로 이동 = Amazon FSx File Gateway.
Amazon FSx 파일 게이트웨이는 Amazon FSx 의 Windows 파일 공유에 대한 온프레미스 액세스를 최적화하여 사용자가 짧은 지연 시간과 공유 대역폭을 유지하면서 Windows 파일 서버용 FSx 데이터에 쉽게 액세스할 수 있도록 합니다. 사용자는 액세스할 수 있는 자주 사용하는 데이터의 로컬 캐시를 활용하여 성능을 높이고 데이터 전송 트래픽을 줄일 수 있습니다. 파일 읽기 및 쓰기와 같은 파일 시스템 작업은 모두 로컬 캐시에 대해 수행되는 반면 Amazon FSx 파일 게이트웨이는 변경된 데이터를 백그라운드에서 Windows 파일 서버용 FSx 와 동기화합니다. 이러한 기능을 사용하면 Windows 파일 서버용 FSx 에서 AWS 의 모든 온프레미스 파일 공유 데이터를 통합하고 보호되고 탄력적인 완전 관리형 파일 시스템의 이점을 누릴 수 있습니다.
https://aws.amazon.com/storagegateway/faqs/?nc1=h_ls

설명 2:
https://docs.aws.amazon.com/filegateway/latest/filefsxw/what-is-file-fsxw.html
대기 시간을 최소화하면서 AWS 와 온프레미스 파일 스토리지 모두에 액세스해야 하는 회사의 요구 사항을 충족하기 위해 하이브리드 클라우드 아키텍처를 사용할 수 있습니다. 한 가지 솔루션은 완벽하게 관리되는 Windows 파일 서버를 제공하는 AWS 에서 Windows 파일 서버용 Amazon FSx 를 배포 및 구성하는 것입니다.
온프레미스 파일 데이터는 온프레미스와 AWS 파일 스토리지 간의 브리지 역할을 할 수 있는 FSx 파일 게이트웨이로 이동할 수 있습니다. 클라우드 워크로드는 AWS 에서 Windows File Server 용 FSx 를 사용하도록 구성할 수 있으며 온프레미스 워크로드는 FSx 파일 게이트웨이를 사용하도록 구성할 수 있습니다.
이 솔루션은 운영 오버헤드를 최소화하고 기존 파일 액세스 패턴을 크게 변경할 필요가 없습니다. 온프레미스와 AWS 간의 연결은 AWS Site-to-Site VPN 연결을 사용하여 설정할 수 있습니다.

참조:
Windows 파일 서버용 AWS FSx: https://aws.amazon.com/fsx/windows/
AWS FSx 파일 게이트웨이: https://aws.amazon.com/fsx/file-gateway/
AWS 사이트 간 VPN: https://aws.amazon.com/vpn/site-to-site-vpn/

Q65
A hospital recently deployed a RESTful API with Amazon API Gateway and AWS Lambda. The hospital uses API Gateway and Lambda to upload reports that are in PDF format and JPEG format. The hospital needs to modify the Lambda code to identify protected health information (PHI) in the reports.
Which solution will meet these requirements with the LEAST operational overhead?
A. Use existing Python libraries to extract the text from the reports and to identify the PHI from the extracted text.
B. Use Amazon Textract to extract the text from the reports. Use Amazon SageMaker to identify the PHI from the extracted text.
C. Use Amazon Textract to extract the text from the reports. Use Amazon Comprehend Medical to identify the PHI from the extracted text.
D. Use Amazon Rekognition to extract the text from the reports. Use Amazon Comprehend Medical to identify the PHI from the extracted text.
Answer: C
https://www.examtopics.com/discussions/amazon/view/85367-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
・Textract 로 텍스트 추출, Comprehend Medical 을 통해 식별
A(X) : Textract 와 Comprehend Medical 을 사용하는 것이 파이썬 코드를 별도로 관리할 필요가 없어서 운영하기 편함.
B(X) : SageMaker 는 기계 학습 모델 서비스.
Amazon SageMaker 는 완전관리형 인프라, 도구 및 워크플로를 사용하여 모든 사용 사례에 대해 기계 학습(ML) 모델을 구축, 훈련 및 배포하는 완전관리형 서비스입니다.
https://aws.amazon.com/ko/sagemaker/faqs/
C(O) : Textract 는 OCR 같은 서비스. Comprehend 는 의료용 텍스트 식별 서비스.
Amazon Textract 는 스캔한 문서에서 텍스트, 필기 및 데이터를 자동으로 추출하는 기계 학습(ML) 서비스입니다. 단순한 광학 문자 인식(OCR) 이상으로 양식 및 표의 데이터를 식별하고 이해하며 추출합니다.

https://aws.amazon.com/ko/textract/
Amazon Comprehend Medical 은 HIPAA 적격 자연어 처리(NLP) 서비스로, 미리 학습된 기계 학습을 사용하여 처방전, 처치, 진단과 같은 의료 텍스트에서 의료 데이터를 파악하고 추출합니다.
https://aws.amazon.com/ko/comprehend/medical/
D(X) : Rekognition 은 이미지나 비디오 분석 서비스지 텍스트 추출 서비스가 아님.
Amazon Rekognition 은 애플리케이션에 강력한 시각 분석 기능을 쉽게 추가할 수 있게 해주는 서비스입니다. Rekognition Image 를 통해 수백만 개의 이미지를 검색, 확인 및 구성할 수 있는 강력한 애플리케이션을 쉽게 구축할 수 있습니다. Rekognition Video 를 통해 저장된 동영상 또는 실시간 스트림 동영상에서 동작 기반 컨텍스트를 추출하고 이를 분석할 수 있습니다.
https://aws.amazon.com/ko/rekognition/faqs/?nc=sn&loc=7

설명 2:
대기 시간을 최소화하면서 AWS 와 온프레미스 파일 스토리지 모두에 액세스해야 하는 회사의 요구 사항을 충족하기 위해 하이브리드 클라우드 아키텍처를 사용할 수 있습니다. 한 가지 솔루션은 완벽하게 관리되는 Windows 파일 서버를 제공하는 AWS 에서 Windows 파일 서버용 Amazon FSx 를 배포 및 구성하는 것입니다. 온프레미스 파일 데이터는 온프레미스와 AWS 파일 스토리지 간의 브리지 역할을 할 수 있는 FSx 파일 게이트웨이로 이동할 수 있습니다. 클라우드 워크로드는 AWS 에서 Windows File Server 용 FSx 를 사용하도록 구성할 수 있으며 온프레미스 워크로드는 FSx 파일 게이트웨이를 사용하도록 구성할 수 있습니다. 이 솔루션은 운영 오버헤드를 최소화하고 기존 파일 액세스 패턴을 크게 변경할 필요가 없습니다. 온프레미스와 AWS 간의 연결은 AWS Site-to-Site VPN 연결을 사용하여 설정할 수 있습니다.
참조:
AWS FSx for Windows File Server: https://aws.amazon.com/fsx/windows/
AWS FSx File Gateway: https://aws.amazon.com/fsx/file-gateway/
AWS Site-to-Site VPN: https://aws.amazon.com/vpn/site-to-site-vpn/

Q66
A company has an application that generates a large number of files, each approximately 5 MB in size. The files are stored in Amazon S3. Company policy requires the files to be stored for 4 years before they can be deleted. Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce. The files are frequently accessed in the first 30 days of the object creation but are rarely accessed after the first 30

days.
Which storage solution is MOST cost-effective?
A. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Glacier 30 days from object creation. Delete the files 4 years after object creation.
B. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) 30 days from object creation. Delete the files 4 years after object creation.
C. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation. Delete the files 4 years after object creation.
D. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation. Move the files to S3 Glacier 4 years after object creation.
Answer: C
https://www.examtopics.com/discussions/amazon/view/85310-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A(X) : 즉각적인 액세스가 항상 필요하다고 했기 때문에 S3 Glacier 사용은 적합하지 않음.
B(X) : 재생산하기 쉽지 않은 중요한 비즈니스 데이터라고 했기 때문에 One Zone-IA 보다는 S3 Standard-IA 가 더 적합
C(O) : 30 일 동안은 자주 액세스하므로 S3 Standard, 30 일 이후에는 자주 액세스하진 않지만 즉각적인 액세스가 필요하므로 S3 Standard-IA, 4 년이 지나면 중요한 비즈니스 데이터므로 함부로 보관해서는 안됨. 따라서 삭제.
D(X) : 중요한 비즈니스 데이터라고 했으므로 보관기간인 4 년이 지나고 나서는 함부로 보관해서는 안되며 삭제해야 함.

참고:
https://aws.amazon.com/ko/s3/storage-classes/?trk=66264cd8-3b73-416c-9693-ea7cf4fe846a&sc_channel=ps&s_kw

Q67
A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue, writes to an Amazon RDS table, and deletes the message from the queue. Occasional duplicate records are found in the RDS

table. The SQS queue does not contain any duplicate messages.
What should a solutions architect do to ensure messages are being processed once only?
A. Use the CreateQueue API call to create a new queue.
B. Use the AddPermission API call to add appropriate permissions.
C. Use the ReceiveMessage API call to set an appropriate wait time.
D. Use the ChangeMessageVisibility API call to increase the visibility timeout.
Answer: D
https://www.examtopics.com/discussions/amazon/view/85583-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
가시성 제한 시간은 Amazon SQS 가 메시지를 반환할 때 시작됩니다. 이 시간 동안 소비자는 메시지를 처리하고 삭제합니다. 그러나 메시지를 삭제하기 전에 소비자가 실패하고 가시성 제한 시간이 만료되기 전에 시스템에서 해당 메시지에 대한 DeleteMessage 작업을 호출하지 않으면 메시지가 다른 소비자에게 표시되고 메시지가 다시 수신됩니다. 메시지를 한 번만 수신해야 하는 경우 소비자는 가시성 제한 시간 내에 메시지를 삭제해야 합니다.
https://docs.aws.amazon.com/ko_kr/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html
키워드: Amazon RDS 에 대한 SQS 대기열 쓰기 여기에서 옵션 D 최상의 기타 옵션 제외[옵션 A - 기존 대기열에 하나 이상의 대기열을 도입할 수 없습니다. 옵션 B - 권한만 허용; 옵션 C - 메시지만 검색] FIFO 대기열은 중복 메시지를 도입하지 않도록 설계되었습니다. 그러나 메시지 생성자는 특정 시나리오에서 중복을 생성할 수 있습니다. 예를 들어 생성자가 메시지를 보내고 응답을 받지 못한 다음 동일한 메시지를 다시 보내는 경우입니다. Amazon SQS API 는 메시지 생성자가 중복 전송을 방지하는 중복 제거 기능을 제공합니다. 메시지 생성자에 의해 도입된 모든 중복 항목은 5 분 중복 제거 간격 내에 제거됩니다. 표준 대기열의 경우 때때로 메시지의 복제본을 받을 수 있습니다(최소 1 회 전달). 표준 대기열을 사용하는 경우 애플리케이션을 멱등적으로 설계해야 합니다(즉, 동일한 메시지를 두 번 이상 처리할 때 부정적인 영향을 받지 않아야 함).

설명 2:
메시지를 수신한 직후에는 메시지가 대기열에 그대로 있습니다. 다른 소비자가 메시지를 다시 처리하지 못하게 Amazon SQS 에서는 다른 소비자가 메시지를 수신하고 처리할 수 없도록 막는 기간인 Visibility timeout 을 설정합니다.
https://docs.aws.amazon.com/ko_kr/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html

Q68

A solutions architect is designing a new hybrid architecture to extend a company's on-premises infrastructure to AWS. The company requires a highly available connection with consistent low latency to an AWS Region. The company needs to minimize costs and is willing to accept slower traffic if the primary connection fails.

What should the solutions architect do to meet these requirements?

A. Provision an AWS Direct Connect connection to a Region. Provision a VPN connection as a backup if the primary Direct Connect connection fails.

B. Provision a VPN tunnel connection to a Region for private connectivity. Provision a second VPN tunnel for private connectivity and as a backup if the primary VPN connection fails.

C. Provision an AWS Direct Connect connection to a Region. Provision a second Direct Connect connection to the same Region as a backup if the primary Direct Connect connection fails.

D. Provision an AWS Direct Connect connection to a Region. Use the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails.

Answer: A

https://www.examtopics.com/discussions/amazon/view/85593-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

어떤 경우에는 이 연결만으로는 충분하지 않습니다. 항상 DX 의 백업으로 폴백 연결을 보장하는 것이 좋습니다. 여러 옵션이 있지만 AWS Site-To-Site VPN 으로 구현하는 것이 비용 효율적입니다. 비용을 줄이기 위해 활용하거나 그 동안 두 번째 DX 설정을 기다릴 수 있는 솔루션입니다.

https://blog.besharp.it/hybrid-cloud-networking-backup-aws-direct-connect-network-connection-with-aws-site-to-site-vpn/

설명 2:

VPN 과 Direct Connect 는 같이 사용할 수 있음.

https://docs.aws.amazon.com/ko_kr/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-vpn.html

Q69

A company is running a business-critical web application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances are in an Auto Scaling group. The application uses an Amazon Aurora PostgreSQL database that is deployed in a single Availability Zone. The company wants the application to be highly available with minimum downtime and minimum loss of data.

Which solution will meet these requirements with the LEAST operational effort?

A. Place the EC2 instances in different AWS Regions. Use Amazon Route 53 health checks to redirect traffic. Use Aurora PostgreSQL Cross-Region Replication.

B. Configure the Auto Scaling group to use multiple Availability Zones. Configure the database as Multi-AZ. Configure an Amazon RDS Proxy instance for the database.

C. Configure the Auto Scaling group to use one Availability Zone. Generate hourly snapshots of the database. Recover the database from the snapshots in the event of a failure.

D. Configure the Auto Scaling group to use multiple AWS Regions. Write the data from the application to Amazon S3. Use S3 Event Notifications to launch an AWS Lambda function to write the data to the database.

Answer: B

https://www.examtopics.com/discussions/amazon/view/85594-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

A(X) : 다중 AZ 사용이 더 바람직. 게다가 뜬금없이 잘 쓰고 있던 EC2 인스턴스를 다른 AZ 도 아니고 다른 리전에 배치하는 건 무리수.

B(O) : 다중 AZ + Auto Scaling 으로 고가용성 확보.

C(X) : 하나의 가용영역을 사용하므로 고가용성 불충족.

D(X) : 다중 AZ 가 더 바람직할 뿐더러 굳이 불필요하게 S3 를 거쳐가고 있음.

설명 2:

최소한의 가동 중지 시간과 최소한의 데이터 손실로 고가용성을 달성하려면 단일 장애 지점이 없도록 여러 가용 영역을 사용하도록 Auto Scaling 그룹을 구성해야 합니다. 기본 가용 영역에서 정전이 발생한 경우 자동 장애 조치를 활성화하려면 데이터베이스를 다중 AZ 로 구성해야 합니다. 또한 Amazon RDS Proxy 인스턴스를 사용하여 연결 실패를 줄이고 장애 조치 시간을 개선하여 데이터베이스의 확장성과 가용성을 개선할 수 있습니다.

Q70

A company's HTTP application is behind a Network Load Balancer (NLB). The NLB's target group is configured to use an Amazon EC2 Auto Scaling group with multiple EC2 instances that run the web service.

The company notices that the NLB is not detecting HTTP errors for the application. These errors require a manual restart of the EC2 instances that run the web service. The company needs to improve the application's availability without writing custom scripts or code.

What should a solutions architect do to meet these requirements?

A. Enable HTTP health checks on the NLB, supplying the URL of the company's application.

B. Add a cron job to the EC2 instances to check the local application's logs once each minute. If HTTP errors are detected. the application will restart.

C. Replace the NLB with an Application Load Balancer. Enable HTTP health checks by supplying the URL of the company's application. Configure an Auto Scaling action to replace unhealthy instances.

D. Create an Amazon Cloud Watch alarm that monitors the UnhealthyHostCount metric for the NLB. Configure an Auto Scaling action to replace unhealthy instances when the alarm is in the ALARM state.

Answer: C

https://www.examtopics.com/discussions/amazon/view/85734-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

이 회사는 NLB 가 응용 프로그램에 대한 HTTP 오류를 감지하지 못한다고 알고 있습니다'라는 대목에서 응용프로그램에 대한 HTTP 오류를 감지하려면 ALB(Applicaton Load Balancer)가 필요함을 유추할 수 있음.

A(X) : 응용프로그램에 대한 HTTP 오류를 감지해야하므로 NLB 는 부적절.

B(X) : 자동이 아니라 정기적으로 로그를 확인하는 것이므로 오답.

C(O) : Application Load Balancer 는 등록된 대상으로 요청을 주기적으로 전송하여 상태를 확인합니다. 이러한 테스트를 바로 상태 확인이라고 합니다....◎HealthCheckProtocol : 대상에 대한 상태 확인을 수행할 때 로드 밸런서가 사용하는 프로토콜입니다. HTTP, HTTPS 등의 프로토콜이 여기에 해당됩니다. HTTP 프로토콜이 기본 설정값입니다. ◎HealthCheckPath : 대상에 대한 상태 확인을 위한 대상입니다. 프로토콜 버전이 HTTP/1.1 또는 HTTP/2 인 경우 유효한 URI(/path?query)를 참조하세요. 기본값은 /입니다. 프로토콜 버전이 gRPC 인 경우, 사용자 지정 상태 확인 방법의 경로를 /package.service/method 형식으로 지정합니다. 기본값은 /AWS.ALB/healthcheck 입니다.

https://docs.aws.amazon.com/ko_kr/elasticloadbalancing/latest/application/target-group

-health-checks.html
D(X) : A 와 같은 이유로 오답.

설명 2:
애플리케이션 가용성: NLB 는 애플리케이션의 가용성을 보장할 수 없습니다. 이는 네트워크 및 TCP 계층 변수에만 의존하여 결정을 내리며 애플리케이션을 전혀 인식하지 못하기 때문입니다.
일반적으로 NLB 는 ICMP ping 에 응답하거나 3 방향 TCP 핸드셰이크를 올바르게 완료하는 서버의 기능을 기반으로 가용성을 결정합니다. ALB 는 훨씬 더 깊이 들어가 특정 페이지의 성공적인 HTTP GET 뿐만 아니라 콘텐츠가 입력 매개변수를 기반으로 예상한 대로라는 확인을 기반으로 가용성을 결정할 수 있습니다.

Q71
A company runs a shopping application that uses Amazon DynamoDB to store customer information. In case of data corruption, a solutions architect needs to design a solution that meets a recovery point objective (RPO) of 15 minutes and a recovery time objective (RTO) of 1 hour.
What should the solutions architect recommend to meet these requirements?
A. Configure DynamoDB global tables. For RPO recovery, point the application to a different AWS Region.
B. Configure DynamoDB point-in-time recovery. For RPO recovery, restore to the desired point in time.
C. Export the DynamoDB data to Amazon S3 Glacier on a daily basis. For RPO recovery, import the data from S3 Glacier to DynamoDB.
D. Schedule Amazon Elastic Block Store (Amazon EBS) snapshots for the DynamoDB table every 15 minutes. For RPO recovery, restore the DynamoDB table by using the EBS snapshot.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85603-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A(X) : 리전 장애 발생 시 리디렉션에는 탁월하나 데이터 손상에는 취약함. 글로벌 테이블에서 새로 작성된 항목은 1 초 이내에 모든 복제본 테이블에 전파되는데, 이는 데이터를 잘못 건드리면 1 초 이내에 모든 복제본 테이블에 해당 변경 사항이 적용되기

때문.
전역 테이블에서 새로 작성된 항목은 일반적으로 1 초 이내에 모든 복제본 테이블에 전파됩니다.
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/V2globaltables_HowItWorks.html
B(O) : DynamoDB 는 주문형 백업 기능을 제공합니다. 이를 통해 규정 준수 요구 사항에 대한 장기 보존 및 보관을 위해 테이블의 전체 백업을 생성할 수 있습니다. 주문형 백업을 생성하고 Amazon DynamoDB 테이블에 대한 특정 시점 복구를 활성화할 수 있습니다. 지정 시간 복구는 우발적인 쓰기 또는 삭제 작업으로부터 테이블을 보호하는 데 도움이 됩니다. 특정 시점 복구를 사용하면 지난 35 일 동안의 특정 시점으로 테이블을 복원할 수 있습니다.
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html
C(X) : S3 Glacier 는 콜드 스토리지로 액세스 시간이 더 김. 괜히 RTO 만 늘어남.
D(X) : DynamoDB 는 서버리스라 EBS 스냅샷을 찍을 수 있는지도 의문이고 애초에 PITR(특정 시점으로 복구)이 더 좋은 옵션임.

참조
https://docs.aws.amazon.com/ko_kr/amazondynamodb/latest/developerguide/PointInTimeRecovery.html

Q72
A company runs a photo processing application that needs to frequently upload and download pictures from Amazon S3 buckets that are located in the same AWS Region. A solutions architect has noticed an increased cost in data transfer fees and needs to implement a solution to reduce these costs.
How can the solutions architect meet this requirement?
A. Deploy Amazon API Gateway into a public subnet and adjust the route table to route S3 calls through it.
B. Deploy a NAT gateway into a public subnet and attach an endpoint policy that allows access to the S3 buckets.
C. Deploy the application into a public subnet and allow it to route through an internet gateway to access the S3 buckets.
D. Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets.
Answer: D

https://www.examtopics.com/discussions/amazon/view/85604-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : VPC-온프레미스 간 통신은 이루어지나 VPC 간 통신은 이루어지지 않고 있음.
B(X) : A 와 같은 이유로 오답.
C(X) : A 와 같은 이유로 오답.
D(O) : Transit Gateway 는 동일한 리전 내에 있는 여러 VPC 들을 연결하는 전송 '허브'이므로 Transit Gateway 를 거쳐 VPC 끼리 통신이 가능
AWS Transit Gateway 는 동일한 리전의 VPC 를 상호 연결하여 Amazon VPC 라우팅 구성을 한 곳에 통합하는 네트워크 전송 허브입니다.
https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway.html

설명 2:
정답은 옵션 D 입니다. S3 VPC 게이트웨이 엔드포인트를 VPC 에 배포하고 S3 버킷에 대한 액세스를 허용하는 엔드포인트 정책을 연결합니다. S3 VPC 게이트웨이 엔드포인트를 배포하면 애플리케이션이 VPC 내의 프라이빗 네트워크 연결을 통해 S3 버킷에 액세스할 수 있으므로 인터넷을 통한 데이터 전송이 필요하지 않습니다. 이를 통해 데이터 전송 비용을 줄이고 애플리케이션의 성능을 향상시킬 수 있습니다. 엔드포인트 정책을 사용하여 애플리케이션이 액세스할 수 있는 S3 버킷을 지정할 수 있습니다.

Q73
A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon EC2 instance in a public subnet of a VPC. A solutions architect needs to connect from the on-premises network, through the company's internet connection, to the bastion host, and to the application servers. The solutions architect must make sure that the security groups of all the EC2 instances will allow that access.
Which combination of steps should the solutions architect take to meet these requirements? (Choose two)
A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances.
B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company.

C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company.
D. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host.
E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host.
Answer: C, D
https://www.examtopics.com/discussions/amazon/view/85613-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
전체적인 프로세스는 사내네트워크 -> 외부 인터넷 -> Bastion Host(퍼블릭서브넷 내에 NAT 게이트웨이와 함께 위치) -> Application(프라이빗서브넷 내에 위치)으로 이루어짐.
Bastion Host 는 내부네트워크(여기서는 Application 이 있는 곳)에 접속할 수 있는 유일한 창구로, SSH 접속도 여길 통과해야만 가능함.
일단 Bastion Host 에 오는 트래픽(인바운드 트래픽)은 외부 인터넷을 통해서 온 회사의 IP(즉, 외부 IP)이므로 C 가 정답.
그 다음으로는 Bastion Host 로부터 Application 으로 오는 트래픽(인바운드 트래픽)을 허용해야하는데 이미 Bastion Host 에서 안쪽의 내부 네트워크와 통신하려고 프라이빗 IP 를 들고 온 상태임. 따라서 D 가 정답이며 최종적으로는 C,D 가 정답.

내부 아이피는 온프레미스 환경 사내 안에서 쓰는 아이피를 보통 뜻하고 인터넷으로 나오는 IP 는 외부 IP 개념이라 사내 네트워크에서 외부인터넷으로 나온 external ip 범위의 대역에서 인바운드 액세스만 허용하는 C 가 B 보다 더 적절한 답으로 보임.

Q74
A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company.
How should security groups be configured in this situation? (Choose two.)
A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.
B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.

C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.
D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.
E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.
Answer: A, C
https://www.examtopics.com/discussions/amazon/view/85346-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
전체적인 구조는 EC2 인스턴스에서 실행되는 웹 애플리케이션(퍼블릭 서브넷 내에 위치)---->EC2 인스턴스에서 실행되는 데이터베이스(프라이빗 서브넷 내에 위치)으로 되어있고, 인스턴스 단위의 보안은 보안 그룹이 담당.
보안 그룹은 기본적으로 인바운드 트래픽에 관해서는 허용만 지정할 수 있고, 허용하지 않은 건 기본적으로 모두 차단하기 때문에 외부 인터넷->웹 애플리케이션으로의 액세스를 허용하려면 0.0.0.0/0 으로부터 온 포트 443(HTTPS)를 허용해야 함.
그 다음으로 웹 애플리케이션->데이터베이스로의 액세스를 허용하려면 웹 애플리케이션이 있는 웹 계층에서 오는 포트 1433(MySQL) 인바운드 트래픽을 허용하도록 보안 그룹 설정을 해야 함. 따라서 정답은 A,C.

설명 2:
"보안 그룹은 모든 인바운드 규칙에 대한 아웃바운드 규칙을 생성합니다." 완전히 옳지 않습니다. Statefull 은 인바운드(또는 아웃바운드) 규칙을 생성하는 경우 아웃바운드(또는 인바운드) 규칙을 생성한다는 의미가 아닙니다. 이것이 의미하는 바는 다음과 같습니다. X IP 에 대한 포트 443 에서 인바운드 규칙을 생성한다고 가정합니다. 요청이 X ip 에서 포트 443 으로 들어오면 포트 443 에서 해당 요청에 대한 트래픽 아웃을 허용합니다.
그러나 아웃바운드 규칙을 보면 명시적으로 생성하지 않는 한 포트 443 에 대한 아웃바운드 규칙이 없을 것입니다. 상태 비저장 ACL 에서는 들어오는 요청을 허용하는 인바운드 규칙과 애플리케이션이 이러한 들어오는 요청에 응답할 수 있도록 하는 아웃바운드 규칙을 만들어야 합니다.
https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/VPC_SecurityGroups.html#SecurityGroupRules

Q75

A company wants to move a multi-tiered application from on premises to the AWS Cloud to improve the application's performance. The application consists of application tiers that communicate with each other by way of RESTful services. Transactions are dropped when one tier becomes overloaded. A solutions architect must design a solution that resolves these issues and modernizes the application.

Which solution meets these requirements and is the MOST operationally efficient?

A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services.

B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the servers' peak utilization during the performance failures. Increase the size of the application server's Amazon EC2 instances to meet the peak requirements.

C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.

D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

Answer: A

https://www.examtopics.com/discussions/amazon/view/86120-exam-aws-certified-solutions-architect-associate-saa-c03/

설명

AWS Lambda, Amazon API Gateway, AWS Amplify, Amazon DynamoDB 및 Amazon Cognito 를 사용하여 서버리스 웹 애플리케이션을 구축하십시오. 이 예에서는 AWS Lambda, Amazon API Gateway, AWS Amplify, Amazon DynamoDB 및 Amazon Cognito 를 사용하여 서버리스 웹 애플리케이션 구축 질문과 유사한 설정을 보여줍니다.

RESTful API = API Gateway 사용.

트랜잭션 삭제되는 문제 = SQS.

Q76

A company receives 10 TB of instrumentation data each day from several machines located at a single factory. The data consists of JSON files stored on a storage area network (SAN)

in an on-premises data center located within the factory. The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-time analytics. A secure transfer is important because the data is considered sensitive.
Which solution offers the MOST reliable data transfer?
A. AWS DataSync over public internet
B. AWS DataSync over AWS Direct Connect
C. AWS Database Migration Service (AWS DMS) over public internet
D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect
Answer: B
https://www.examtopics.com/discussions/amazon/view/85801-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : 퍼블릭 인터넷으로 전송하면 노출 위험이 큼. 심지어는 VPN 도 안 했음.
B(O) : Direct Connect 는 전용선 연결로 온프레미스-AWS 간 통신하는 것이고, DataSync 는 데이터 전송/마이그레이션에 사용되는 서비스.
AWS DataSync 는 온프레미스와 AWS 스토리지 서비스 사이에서 데이터 이동을 자동화 및 가속화하는 안전한 온라인 서비스입니다. Amazon Simple Storage Service(S3) 버킷 간에 데이터를 복사할 수 있습니다. https://aws.amazon.com/ko/datasync/
C(X) : A 와 마찬가지 이유로 오답.
D(X) : DMS 는 데이터베이스 마이그레이션 서비스로 S3 로 데이터를 전송해야하는 지문 상황과는 맞지 않음.

설명 2:
다음은 AWS DataSync 의 주요 사용 사례 중 일부입니다. * 데이터 마이그레이션 - 활성 데이터 세트를 네트워크를 통해 Amazon S3, Amazon EFS 또는 FSx for Windows File Server 로 빠르게 이동합니다. DataSync 에는 자동 암호화 및 데이터 무결성 검증이 포함되어 데이터가 안전하고 온전하며 사용할 준비가 되었는지 확인하는 데 도움이 됩니다. "DataSync 에는 암호화 및 무결성 검증이 포함되어 있어 데이터가 안전하고 온전하며 사용할 준비가 되었는지 확인하는 데 도움이 됩니다."
https://aws.amazon.com/datasync/faqs/

Q77
A company needs to configure a real-time data ingestion architecture for its application.

The company needs an API, a process that transforms data as the data is streamed, and a storage solution for the data.
Which solution will meet these requirements with the LEAST operational overhead?
A. Deploy an Amazon EC2 instance to host an API that sends data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
B. Deploy an Amazon EC2 instance to host an API that sends data to AWS Glue. Stop source/destination checking on the EC2 instance. Use AWS Glue to transform the data and to send the data to Amazon S3.
C. Configure an Amazon API Gateway API to send data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
D. Configure an Amazon API Gateway API to send data to AWS Glue. Use AWS Lambda functions to transform the data. Use AWS Glue to send the data to Amazon S3.
Answer: C
https://www.examtopics.com/discussions/amazon/view/85740-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
실시간 데이터 수집 = Kinesis Data Streams. A,C 둘 중 하나가 답.
A(X) : API 는 API Gateway 를 사용하여 전송.
Amazon API Gateway 는 어떤 규모에서든 개발자가 API 를 손쉽게 생성, 게시, 유지 관리, 모니터링 및 보안 유지할 수 있도록 하는 완전관리형 서비스입니다. API 는 애플리케이션이 백엔드 서비스의 데이터, 비즈니스 로직 또는 기능에 액세스할 수 있는 "정문" 역할을 합니다. https://aws.amazon.com/ko/api-gateway/
C(O) :
・API Gateway API 를 Kinesis Data Streams 와 같이 사용 가능
API Gateway API 를 Kinesis 와 통합하려면 API Gateway 와 Kinesis 서비스를 모두 사용할 수 있는 리전을 선택해야 합니다.
https://docs.aws.amazon.com/apigateway/latest/developerguide/integrating-api-with-aws-services-kinesis.html
・Kinesis Data Streams 로 데이터 수집.
Amazon Kinesis Data Streams 를 사용하면 특수 요구에 맞춰 스트리밍 데이터를 처리 또는 분석하는 사용자 지정 애플리케이션을 구축할 수 있습니다. 수십 만개의 소스에서 클릭

스트림, 애플리케이션 로그, 소셜 미디어와 같은 다양한 유형의 데이터를 Kinesis 데이터 스트림에 추가할 수 있습니다.
https://aws.amazon.com/ko/kinesis/data-streams/faqs/
・Kinesis Data Streams -> Kinesis Data Firehose
Amazon Kinesis Data Firehose 전송 스트림에 정보를 전송하도록 Amazon Kinesis Data Streams 를 구성할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/firehose/latest/dev/writing-with-kinesis-streams.html
・Lambda 로 데이터 변환
Kinesis Data Firehose Firehose 는 Lambda 함수를 호출하여 수신되는 소스 데이터를 변환하고 변환된 데이터를 대상으로 전송할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/firehose/latest/dev/data-transformation.html
・S3 로 전송
Amazon Kinesis Data Firehose 는 실시간 스트리밍 데이터를 Amazon S3, Amazon RedShift, Amazon OpenSearch Service, Splunk 및 사용자 지정 HTTP 엔드포인트 또는 Datadog, Dynatrace, LogicMonitor, MongoDB, New Relic, Sumo Logic 을 포함한 지원되는 서드파티 소유의 HTTP 엔드포인트 대상에 전달하기 위한 완전관리형 서비스입니다.
https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html

Q78
A company needs to keep user transaction data in an Amazon DynamoDB table. The company must retain the data for 7 years.
What is the MOST operationally efficient solution that meets these requirements?
A. Use DynamoDB point-in-time recovery to back up the table continuously.
B. Use AWS Backup to create backup schedules and retention policies for the table.
C. Create an on-demand backup of the table by using the DynamoDB console. Store the backup in an Amazon S3 bucket. Set an S3 Lifecycle configuration for the S3 bucket.
D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function. Configure the Lambda function to back up the table and to store the backup in an Amazon S3 bucket. Set an S3 Lifecycle configuration for the S3 bucket.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85742-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

A(X) : 35 일 제한이 있습니다. ""특정 시점으로 복구가 설정되어 있으면 최근 35 일 중 원하는 시점으로 테이블을 복원할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/amazondynamodb/latest/developerguide/PointInTimeRecovery.html
B(O) : 한 곳에서 백업 현황 모니터링 및 콜드 스토리지에 저장, 예약 저장 가능합니다. AWS Backup 을 사용하면 백업 정책을 구성하고 AWS 리소스 및 온프레미스 워크로드에 대한 활동을 한 곳에서 모니터링할 수 있습니다. AWS Backup 과 함께 DynamoDB 를 사용하면 AWS 계정 및 리전에서 온디맨드 백업을 복사하고, 온디맨드 백업에 비용 할당 태그를 추가하고, 온디맨드 백업을 콜드 스토리지로 전환하여 비용을 절감할 수 있습니다.
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/BackupRestore.html
AWS Backup 을 사용하여 DynamoDB 온디맨드 백업을 자동으로 예약, 복사, 태그 지정 및 수명 주기를 수행할 수 있습니다. DynamoDB 콘솔에서 이러한 백업을 계속 보고 복원할 수 있습니다.
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/backuprestore_HowItWorksAWS.html
C(X) : 불가능한 건 아닌데, B 가 더 유리합니다. 운영 측면에서는 한 곳에서 모니터링하는 게 편하고, S3 버킷에 저장한다고 했는데 7 년 동안 보관할 거면 S3 콜드 스토리지에 보관하는 게 비용이 더 저렴합니다.
D(X) : 너무 단계가 많습니다. 아마존에서는 DynamoDB 테이블 백업에 AWS Backup 또는 DynamoDB 콘솔을 사용할 것을 언급하고 있습니다. ""DynamoDB 온디맨드 백업을 생성하고 관리하는 데 사용할 수 있는 두 가지 옵션이 있습니다. AWS 백업 서비스 다이나모 DB
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/BackupRestore.html

Q79
A company is planning to use an Amazon DynamoDB table for data storage. The company is concerned about cost optimization. The table will not be used on most mornings. In the evenings, the read and write traffic will often be unpredictable. When traffic spikes occur, they will happen very quickly.
What should a solutions architect recommend?
A. Create a DynamoDB table in on-demand capacity mode.
B. Create a DynamoDB table with a global secondary index.
C. Create a DynamoDB table with provisioned capacity and auto scaling.

D. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table.

Answer: A

https://www.examtopics.com/discussions/amazon/view/85743-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

사용량 예측이 안 되므로 프로비저닝은 무의미. 따라서 C,D 는 제외되고 A,B 둘 중 하나가 정답.

A(O) : 온디맨드 모드를 사용하는 테이블의 경우 DynamoDB 는 이전에 관찰된 트래픽 수준까지 상승하거나 하락할 때 고객의 워크로드를 즉시 수용할 수 있습니다. 트래픽 수준이 새로운 고점에 도달하면 DynamoDB 는 신속하게 대응하여 워크로드를 수용합니다.

https://aws.amazon.com/ko/blogs/korea/amazon-dynamodb-on-demand-no-capacity-planning-and-pay-per-request-pricing/

B(X) : 고가용성 언급이 없고 비용 최적화를 언급하고 있으므로 B 보다는 A 가 적합.

Q80

A company recently signed a contract with an AWS Managed Service Provider (MSP) Partner for help with an application migration initiative. A solutions architect needs ta share an Amazon Machine Image (AMI) from an existing AWS account with the MSP Partner's AWS account. The AMI is backed by Amazon Elastic Block Store (Amazon EBS) and uses an AWS Key Management Service (AWS KMS) customer managed key to encrypt EBS volume snapshots.

What is the MOST secure way for the solutions architect to share the AMI with the MSP Partner's AWS account?

A. Make the encrypted AMI and snapshots publicly available. Modify the key policy to allow the MSP Partner's AWS account to use the key.

B. Modify the launchPermission property of the AMI. Share the AMI with the MSP Partner's AWS account only. Modify the key policy to allow the MSP Partner's AWS account to use the key.

C. Modify the launchPermission property of the AMI. Share the AMI with the MSP Partner's AWS account only. Modify the key policy to trust a new KMS key that is owned by the MSP Partner for encryption.

D. Export the AMI from the source account to an Amazon S3 bucket in the MSP Partner's AWS account, Encrypt the S3 bucket with a new KMS key that is owned by the MSP Partner.

Copy and launch the AMI in the MSP Partner's AWS account.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85606-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : '공개적'이라는 키워드가 애초에 보안과는 거리가 멈.
B(O) : 기존 KMS 키는 스냅샷을 암호화하는 데 사용되었기 때문에 MSP 파트너와 공유해도 괜찮음.
C(X) : 파트너의 KMS 키를 신뢰하면 파트너가 해당 키를 가지고 악의적인 용도로 사용할 때 문제가 됨.
D(X) : 파트너와 공유해야 하는데 파트너가 S3 버킷을 암호화하도록 냅둬버리면 파트너가 공유받는 입장이 아니라 내가 공유받는 입장이 되어버리는 역전현상이 벌어짐.

설명 2:
AMI 스냅샷을 암호화하는 데 이미 사용되었기 때문에 기존 KMS 키를 MSP 외부 계정과 공유합니다.
https://docs.aws.amazon.com/ko_kr/kms/latest/developerguide/key-policy-modifying-external-accounts.html

Q81
A solutions architect is designing the cloud architecture for a new application being deployed on AWS. The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed. The processor application is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored.
Which design should the solutions architect use?
A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.
B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch

configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage.
C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.
D. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.
Answer: C
https://www.examtopics.com/discussions/amazon/view/86621-exam-aws-certified-solutions-architect-associate-saa-c03/

설명
"처리해야 하는 작업을 보관할 Amazon SQS 대기열을 생성합니다.
컴퓨팅 애플리케이션에 대한 Amazon EC2 Auto Scaling 그룹을 생성합니다. SQS 대기열의 항목 수에 따라 노드를 추가 및 제거하도록 Auto Scaling 그룹에 대한 조정 정책을 설정합니다.
Amazon SQS 는 이 사용 사례에 이상적이며 대기열에서 대기 중인 작업 수에 따라 동적 조정을 사용하도록 구성할 수 있습니다. 이 조정을 구성하려면 유지 관리할 인스턴스당 허용되는 백로그인 대상 값과 함께 인스턴스당 백로그 메트릭을 사용할 수 있습니다.
이러한 수치는 다음과 같이 계산할 수 있습니다.
인스턴스당 백로그:
인스턴스당 백로그를 계산하려면 ApproximateNumberOfMessages 대기열 속성으로 시작하여 SQS 대기열의 길이를 결정합니다.

Q82
A company hosts its web applications in the AWS Cloud. The company configures Elastic Load Balancers to use certificates that are imported into AWS Certificate Manager (ACM). The company's security team must be notified 30 days before the expiration of each certificate.
What should a solutions architect recommend to meet this requirement?

A. Add a rule in ACM to publish a custom message to an Amazon Simple Notification Service (Amazon SNS) topic every day, beginning 30 days before any certificate will expire.
B. Create an AWS Config rule that checks for certificates that will expire within 30 days. Configure Amazon EventBridge (Amazon CloudWatch Events) to invoke a custom alert by way of Amazon Simple Notification Service (Amazon SNS) when AWS Config reports a noncompliant resource.
C. Use AWS Trusted Advisor to check for certificates that will expire within 30 days. Create an Amazon CloudWatch alarm that is based on Trusted Advisor metrics for check status changes. Configure the alarm to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS).
D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to detect any certificates that will expire within 30 days. Configure the rule to invoke an AWS Lambda function. Configure the Lambda function to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS).
Answer: B
https://www.examtopics.com/discussions/amazon/view/85615-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A(X) : 30 일 전에 통보하랬지 맨날 통보하란 이야기는 없었음.
B(O) : AWS Config 를 사용하여 만료 날짜가 가까워지는 인증서를 확인할 수 있습니다. 인증서 만료 날짜가 가까워지면 Amazon EventBridge 를 사용하여 이메일 알림을 받을 수도 있습니다.
https://aws.amazon.com/ko/premiumsupport/knowledge-center/acm-certificate-expiration/
C(X) : Trusted Advisor 는 ""AWS 환경을 검사한 후 비용 절감, 시스템 가용성 및 성능 향상 또는 보안 격차를 해결할 기회가 있을 때 권장 사항을 제시
https://docs.aws.amazon.com/ko_kr/awssupport/latest/user/trusted-advisor.html
하는 서비스로 이 경우엔 해당 사항이 없음.
D(X) : EventBridge 는 이벤트 발생을 감지해서 뭔가를 하는 서비스이지 이벤트 발생 전에 뭔가 감지해서 하는 게 아님

참고
https://repost.aws/ko/knowledge-center/acm-certificate-expiration
https://aws.amazon.com/ko/premiumsupport/knowledge-center/acm-certificate-expiration/

Q83

A company's dynamic website is hosted using on-premises servers in the United States. The company is launching its product in Europe, and it wants to optimize site loading times for new European users. The site's backend must remain in the United States. The product is being launched in a few days, and an immediate solution is needed.

What should the solutions architect recommend?

A. Launch an Amazon EC2 instance in us-east-1 and migrate the site to it.

B. Move the website to Amazon S3. Use Cross-Region Replication between Regions.

C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.

D. Use an Amazon Route 53 geoproximity routing policy pointing to on-premises servers.

Answer: C

https://www.examtopics.com/discussions/amazon/view/85902-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

https://aws.amazon.com/pt/blogs/aws/amazon-cloudfront-support-for-custom-origins/

이제 사용자 지정 오리진을 사용하여 CloudFront 배포를 생성할 수 있습니다. 각 배포는 S3 또는 사용자 지정 오리진을 가리킬 수 있습니다. 이것은 다른 스토리지 서비스일 수도 있고 EC2 인스턴스 또는 Elastic Load Balancer 와 같이 더 흥미롭고 동적인 것일 수도 있습니다.

설명 2:

A(X) : 유럽과 가까워야 하므로 us-east-1 은 오답.

B(X) : 동적 웹 사이트라고 했으므로 S3 가 들어가지 않음.

C(O) : CloudFront 는 사용자 지정 오리진으로 온프레미스 서버를 가리킬 수 있음.

사용자 지정 출처는 웹 서버와 같은 HTTP 서버입니다. HTTP 서버는 Amazon EC2 인스턴스이거나 다른 곳에서 호스팅하는 HTTP 서버일 수 있습니다. 웹 사이트 엔드포인트로 구성된 Amazon S3 오리진도 사용자 지정 오리진으로 간주됩니다.자체 HTTP 서버를 사용자 지정 오리진으로 사용하는 경우 오리진에서 객체를 가져올 때 CloudFront 에서 사용할 HTTP 및 HTTPS 포트 및 프로토콜과 함께 서버의 DNS 이름을 지정합니다.

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html#concept_CustomOrigin

D(X) : 웹 사이트엔 CDN 서비스인 CloudFront 가 필요.

Q84

A company wants to reduce the cost of its existing three-tier web architecture. The web, application, and database servers are running on Amazon EC2 instances for the development, test, and production environments. The EC2 instances average 30% CPU utilization during peak hours and 10% CPU utilization during non-peak hours.

The production EC2 instances run 24 hours a day. The development and test EC2 instances run for at least 8 hours each day. The company plans to implement automation to stop the development and test EC2 instances when they are not in use.

Which EC2 instance purchasing solution will meet the company's requirements MOST cost-effectively?

A. Use Spot Instances for the production EC2 instances. Use Reserved Instances for the development and test EC2 instances.

B. Use Reserved Instances for the production EC2 instances. Use On-Demand Instances for the development and test EC2 instances.

C. Use Spot blocks for the production EC2 instances. Use Reserved Instances for the development and test EC2 instances.

D. Use On-Demand Instances for the production EC2 instances. Use Spot blocks for the development and test EC2 instances.

Answer: B

https://www.examtopics.com/discussions/amazon/view/85665-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

A(X) : 하루 24 시간 실행하는 프로덕션 EC2 인스턴스에 스팟 인스턴스는 적절치 않음. 스팟 인스턴스는 도중에 중지될 가능성이 높은 인스턴스에 더 적합.

B(O) : 1 년 또는 3 년 단위로 예약 인스턴스를 계약해서 사용하면 비용이 절감됨. 개발 및 테스트용 EC2 인스턴스는 매일 최소 8 시간 이상 실행된다고 했으므로 그 이상 사용될 수 있어 Scheduled Reserved 인스턴스보다는 온디맨드 인스턴스를 사용하는 것이 더 적절함

C(X) : 스팟 블록은 기간이 정의된 스팟 인스턴스로 A 와 같은 이유로 오답.

""기간이 정의된 스팟 인스턴스(스팟 블록이라고도 함)는 2021 년 7 월 1 일부로 신규 고객이 더 이상 사용할 수 없습니다.

https://aws.amazon.com/ko/blogs/aws/new-ec2-spot-blocks-for-defined-duration-workloads/

D(X) : 24 시간 동안 사용할 EC2 인스턴스에는 예약 인스턴스 방식을 사용해 비용을 더

절감할 수 있음.

Q85

A company has a production web application in which users upload documents through a web interface or a mobile app. According to a new regulatory requirement. new documents cannot be modified or deleted after they are stored.

What should a solutions architect do to meet this requirement?

A. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled.

B. Store the uploaded documents in an Amazon S3 bucket. Configure an S3 Lifecycle policy to archive the documents periodically.

C. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning enabled. Configure an ACL to restrict all access to read-only.

D. Store the uploaded documents on an Amazon Elastic File System (Amazon EFS) volume. Access the data by mounting the volume in read-only mode.

Answer: A

https://www.examtopics.com/discussions/amazon/view/85751-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

수정하거나 삭제할 수 없음 = S3 Object Lock.

S3 객체 잠금을 사용하면 write-once-read-many(WORM) 모델을 사용하여 객체를 저장할 수 있습니다. 객체 잠금은 고정된 시간 동안 또는 무기한으로 객체의 삭제 또는 덮어쓰기를 방지하는 데 도움이 될 수 있습니다.

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

Q86

A company has several web servers that need to frequently access a common Amazon RDS MySQL Multi-AZ DB instance. The company wants a secure method for the web servers to connect to the database while meeting a security requirement to rotate user credentials frequently.

Which solution meets these requirements?

A. Store the database user credentials in AWS Secrets Manager. Grant the necessary IAM permissions to allow the web servers to access AWS Secrets Manager.

B. Store the database user credentials in AWS Systems Manager OpsCenter. Grant the necessary IAM permissions to allow the web servers to access OpsCenter.
C. Store the database user credentials in a secure Amazon S3 bucket. Grant the necessary IAM permissions to allow the web servers to retrieve credentials and access the database.
D. Store the database user credentials in files encrypted with AWS Key Management Service (AWS KMS) on the web server file system. The web server should be able to decrypt the files and access the database.
Answer: A
https://www.examtopics.com/discussions/amazon/view/85753-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
AWS Secrets Manager 는 애플리케이션, 서비스 및 IT 리소스에 액세스하는 데 필요한 암호를 보호하는 데 도움이 됩니다. 이 서비스를 사용하면 수명 주기 동안 데이터베이스 자격 증명, API 키 및 기타 암호를 쉽게 교체, 관리 및 검색할 수 있습니다.
https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html
Secrets Manager 를 사용하면 암호를 포함하여 코드의 하드코딩된 자격 증명을 Secrets Manager 에 대한 API 호출로 대체하여 프로그래밍 방식으로 암호를 검색할 수 있습니다. 이렇게 하면 비밀이 코드에 더 이상 존재하지 않기 때문에 코드를 검사하는 누군가가 비밀을 손상시킬 수 없습니다. 또한 지정된 일정에 따라 암호를 자동으로 교체하도록 Secrets Manager 를 구성할 수 있습니다. 이를 통해 장기 비밀을 단기 비밀로 대체하여 손상 위험을 크게 줄일 수 있습니다.

설명 2:
사용자 자격 증명을 자주 바꿈 + 안전한 방법 = Secrets Manager.
Secrets Manager 를 사용하면 애플리케이션 소스 코드에서 하드 코딩된 자격 증명을 제거하고 애플리케이션 자체에 자격 증명을 저장하지 않음으로써 보안 태세를 개선할 수 있습니다. 사용자의 개입 없이 지정한 일정에 따라 자동으로 보안 암호를 교체하도록 Secrets Manager 를 구성할 수 있습니다. 교체는 AWS Lambda 함수를 사용하여 정하고 실행합니다.
https://docs.aws.amazon.com/ko_kr/secretsmanager/latest/userguide/intro.html
또한 여러 리전과 여러 AZ 에 걸쳐 작동.
https://docs.aws.amazon.com/ko_kr/secretsmanager/latest/userguide/disaster-recovery-resiliency.html

Q87

A company hosts an application on AWS Lambda functions that are invoked by an Amazon API Gateway API. The Lambda functions save customer data to an Amazon Aurora MySQL database. Whenever the company upgrades the database, the Lambda functions fail to establish database connections until the upgrade is complete. The result is that customer data is not recorded for some of the event.

A solutions architect needs to design a solution that stores customer data that is created during database upgrades.

Which solution will meet these requirements?

A. Provision an Amazon RDS proxy to sit between the Lambda functions and the database. Configure the Lambda functions to connect to the RDS proxy.

B. Increase the run time of the Lambda functions to the maximum. Create a retry mechanism in the code that stores the customer data in the database.

C. Persist the customer data to Lambda local storage. Configure new Lambda functions to scan the local storage to save the customer data to the database.

D. Store the customer data in an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Create a new Lambda function that polls the queue and stores the customer data in the database.

Answer: D

https://www.examtopics.com/discussions/amazon/view/85319-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

잠시 고객 데이터를 저장하는 솔루션 = SQS. 손실될 위험이 있는 처리 대상 데이터를 잠시 보관하는 용도로는 SQS 가 주로 쓰인다고 보면 됨. 답은 D.

설명 2:

https://www.learnaws.org/2020/12/13/aws-rds-proxy-deep-dive/

RDS 프록시는 새 데이터베이스 인스턴스가 작동할 때까지 대기하고 이 시간 동안 애플리케이션에서 받은 모든 요청을 유지함으로써 이러한 상황에서 애플리케이션 가용성을 향상시킬 수 있습니다. 최종 결과는 응용 프로그램이 기본 데이터베이스의 문제에 대해 더 탄력적이라는 것입니다. 이렇게 하면 DB 가 정상으로 돌아올 때까지 솔루션이 데이터를 보유할 수 있습니다. RDS 프록시는 Lambda 와 DB 간의 연결을 최적으로 활용하기 위한 것입니다. Lambda 는 DB 컴퓨팅 리소스에 부담을 줄 수 있는 여러 연결을 동시에 열 수 있습니다.

Q88

A survey company has gathered data for several years from areas in the United States. The company hosts the data in an Amazon S3 bucket that is 3 TB in size and growing. The company has started to share the data with a European marketing firm that has S3 buckets. The company wants to ensure that its data transfer costs remain as low as possible.

Which solution will meet these requirements?

A. Configure the Requester Pays feature on the company's S3 bucket.

B. Configure S3 Cross-Region Replication from the company's S3 bucket to one of the marketing firm's S3 buckets.

C. Configure cross-account access for the marketing firm so that the marketing firm has access to the company's S3 bucket.

D. Configure the company's S3 bucket to use S3 Intelligent-Tiering. Sync the S3 bucket to one of the marketing firm's S3 buckets.

Answer: A

https://www.examtopics.com/discussions/amazon/view/85738-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

요청자 지불 버킷을 사용하면 버킷 소유자 대신 요청자가 버킷에서 데이터 다운로드 및 요청 비용을 지불합니다. 버킷 소유자는 항상 데이터 저장 비용을 지불합니다.

https://docs.aws.amazon.com/AmazonS3/latest/userguide/RequesterPaysBuckets.html

설명 2:

"일반적으로 데이터를 공유하고 싶지만 데이터에 액세스하는 다른 사람과 관련된 요금을 부과하지 않으려면 버킷을 요청자 지불 버킷으로 구성합니다.

예를 들어 우편 번호 디렉터리, 참조 데이터 지리 공간 정보 또는 웹 크롤링 데이터와 같은 대용량 데이터 세트를 만들 때 요청자 지불 버킷을 사용할 수 있습니다."

https://docs.aws.amazon.com/AmazonS3/latest/userguide/RequesterPaysBuckets.html

Q89

A company uses Amazon S3 to store its confidential audit documents. The S3 bucket uses bucket policies to restrict access to audit team IAM user credentials according to the principle of least privilege. Company managers are worried about accidental deletion of documents in the S3 bucket and want a more secure solution.

What should a solutions architect do to secure the audit documents?

A. Enable the versioning and MFA Delete features on the S3 bucket.

B. Enable multi-factor authentication (MFA) on the IAM user credentials for each audit team IAM user account.

C. Add an S3 Lifecycle policy to the audit team's IAM user accounts to deny the s3:DeleteObject action during audit dates.

D. Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key.

Answer: A

https://www.examtopics.com/discussions/amazon/view/85808-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

・버전 관리는 실수로 삭제했을 때 이전 버전의 파일을 불러올 수 있도록 해줌.

Amazon S3 의 버전 관리는 동일 버킷 내에 여러 개의 객체 변형을 보유하는 수단입니다. S3 버전 관리를 사용하면 버킷에 저장된 모든 버전의 객체를 모두 보존, 검색 및 복원할 수 있습니다.

https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/Versioning.html

・MFA Delete 는 함부로 삭제하지 못하도록 막음.

MFA Delete 는 다음 작업에 대해 추가 인증을 요구합니다. ◎버킷의 버전 관리 상태 변경 ◎객체 버전 영구 삭제

https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/MultiFactorAuthenticationDelete.html

Q90

A company is using a SQL database to store movie data that is publicly accessible. The database runs on an Amazon RDS Single-AZ DB instance. A script runs queries at random intervals each day to record the number of new movies that have been added to the database. The script must report a final total during business hours.

The company's development team notices that the database performance is inadequate for development tasks when the script is running. A solutions architect must recommend a solution to resolve this issue.

Which solution will meet this requirement with the LEAST operational overhead?

A. Modify the DB instance to be a Multi-AZ deployment.

B. Create a read replica of the database. Configure the script to query only the read replica.

C. Instruct the development team to manually export the entries in the database at the end of each day.
D. Use Amazon ElastiCache to cache the common queries that the script runs against the database.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85339-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
• 스크립트는 데이터베이스에 추가된 새로운 영화의 수를 기록하기 위해 매일 임의의 간격으로 쿼리를 실행합니다. = 스크립트는 쿼리를 수행하고 있음
• '회사의 개발 팀은 스크립트가 실행 중일 때 데이터베이스 성능이 개발 작업에 부적절하다는 것을 알아차렸습니다.' = 스크립트 때문에 데이터베이스 성능이 떨어지고 있음.
따라서 쿼리가 너무 많이 수행되어서 데이터베이스 성능에 영향이 가는 상황입니다. 이런 경우 read replica 를 통해 쿼리 부하를 분산할 수 있습니다.
B(O) : 애플리케이션에서 읽기 전용 복제본으로 읽기 쿼리를 라우팅하여 기본 DB 인스턴스의 로드를 줄일 수 있습니다.
https://docs.aws.amazon.com/ko_kr/AmazonRDS/latest/UserGuide/USER_ReadRepl.html
D(X) : ElastiCache 는 웹 애플리케이션 성능 향상 용도로 주로 사용됨.
Amazon ElastiCache 는 더 느린 디스크 기반 데이터베이스에 전적으로 의존하기보다는 신속한 관리형 인 메모리 시스템에서 정보를 검색할 수 있는 기능을 지원함으로써 웹 애플리케이션의 성능을 향상합니다. https://aws.amazon.com/ko/elasticache/faqs/

Q91
A company has applications that run on Amazon EC2 instances in a VPC. One of the applications needs to call the Amazon S3 API to store and read objects. According to the company's security regulations, no traffic from the applications is allowed to travel across the internet.
Which solution will meet these requirements?
A. Configure an S3 gateway endpoint.
B. Create an S3 bucket in a private subnet.
C. Create an S3 bucket in the same AWS Region as the EC2 instances.
D. Configure a NAT gateway in the same subnet as the EC2 instances.
Answer: A

https://www.examtopics.com/discussions/amazon/view/85667-exam-aws-certified-solutions-architect-associate-saa-c03/

해설: ▪
B. 프라이빗 서브넷에서 S3 를 생성하면 버킷에 대한 직접적인 인터넷 액세스가 제한되지만 EC2 와 S3 간의 직접적이고 안전한 연결은 제공되지 않습니다. 애플리케이션은 여전히 S3 API 에 액세스하기 위해 인터넷을 통과해야 합니다.

C. EC2 와 동일한 지역에 S3 를 생성한다고 해서 본질적으로 트래픽이 인터넷을 통과하는 것을 막지는 않습니다.

D. NAT 게이트웨이를 구성하면 프라이빗 서브넷의 리소스에 대한 아웃바운드 인터넷 연결이 허용되지만 S3 서비스에 대한 직접적이고 안전한 연결은 제공되지 않습니다. EC2 에서 S3 API 로의 트래픽은 여전히 인터넷을 통과합니다.

가장 적합한 솔루션은 S3 게이트웨이 엔드포인트를 구성하는 것입니다(옵션 A). 트래픽이 인터넷을 통과할 필요 없이 VPC 와 S3 서비스 간에 안전한 비공개 연결을 제공합니다. S3 게이트웨이 엔드포인트를 통해 EC2 는 VPC 내에서 직접 S3 API 에 액세스할 수 있으므로 트래픽이 인터넷을 통해 이동하지 못하도록 하는 보안 요구 사항을 충족합니다.

참고:
https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/privatelink-interface-endpoints.html#types-of-vpc-endpoints-for-s3
https://docs.aws.amazon.com/ko_kr/vpc/latest/privatelink/vpc-endpoints-s3.html

Q92
A company is storing sensitive user information in an Amazon S3 bucket. The company wants to provide secure access to this bucket from the application tier running on Amazon EC2 instances inside a VPC.
Which combination of steps should a solutions architect take to accomplish this? (Choose two.)
A. Configure a VPC gateway endpoint for Amazon S3 within the VPC.
B. Create a bucket policy to make the objects in the S3 bucket public.
C. Create a bucket policy that limits access to only the application tier running in the VPC.
D. Create an IAM user with an S3 access policy and copy the IAM credentials to the EC2

instance.
E. Create a NAT instance and have the EC2 instances use the NAT instance to access the S3 bucket.
Answer: A, C
https://www.examtopics.com/discussions/amazon/view/85903-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A(O) : Gateway Endpoint 는 퍼블릭 인터넷망을 통과하지 않는 전용 연결.
게이트웨이 엔드포인트는 VPC 용 인터넷 게이트웨이 또는 NAT 디바이스가 없어도 Amazon S3 및 DynamoDB 에 대한 안정적인 연결을 제공합니다. 게이트웨이 엔드포인트는 AWS PrivateLink 를 활성화하지 않습니다.
https://docs.aws.amazon.com/ko_kr/vpc/latest/privatelink/vpce-gateway.html
B(X) : 객체를 퍼블릭으로 만드는 것은 보안과는 거리가 멈.
C(O) : 버킷 정책으로 버킷에 대한 액세스 제어.
버킷 정책은 버킷과 해당 버킷의 객체에 대한 액세스 권한을 부여할 수 있는 리소스 기반 정책입니다.
https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/example-bucket-policies.html
D(X) : 차라리 IAM 사용자 정책을 사용하는 것이 더 나음.
Amazon S3 에 대한 사용자 액세스를 제어하는 IAM 사용자 정책을 생성하고 구성할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/user-policies.html
E(X) : Gateway Endpoint 가 더 좋은 선택임.

Q93
A company runs an on-premises application that is powered by a MySQL database. The company is migrating the application to AWS to increase the application's elasticity and availability.
The current architecture shows heavy read activity on the database during times of normal operation. Every 4 hours, the company's development team pulls a full export of the production database to populate a database in the staging environment. During this period, users experience unacceptable application latency. The development team is unable to use the staging environment until the procedure completes.
A solutions architect must recommend replacement architecture that alleviates the

application latency issue. The replacement architecture also must give the development team the ability to continue using the staging environment without delay.
Which solution meets these requirements?
A. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.
B. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Use database cloning to create the staging database on-demand.
C. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Use the standby instance for the staging database.
D. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85729-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
RDS 에 비해 Aurora 는 항상 3 개의 AZ 에 6 개의 복제본(Replica)를 보유하고 있으므로 애플리케이션 가용성에 더 유리. A,B 둘 중 하나가 답.여기서 mysqldump 가 문젠데,
Q: MySQL 에서 Amazon Aurora 로 또는 그 반대로 마이그레이션하려면 어떻게 해야 하나요?
여러 가지 옵션이 있습니다. 표준 mysqldump 유틸리티를 사용하여 MySQL 에서 데이터를 내보내고 mysqlimport 유틸리티를 사용하여 Amazon Aurora 로 데이터를 가져올 수 있습니다. 그 반대도 마찬가지입니다. 또한, AWS 관리 콘솔에서 Amazon RDS 의 DB 스냅샷 마이그레이션 기능을 이용하여 Amazon RDS for MySQL DB 스냅샷을 Amazon Aurora 로 마이그레이션할 수 있습니다. 대부분 고객은 [1 시간 이내]에 마이그레이션을 완료하지만
https://aws.amazon.com/ko/rds/aurora/faqs/
최대 1GB 정도의 소규모 데이터베이스라면 mysqldump 를 실행
https://aws.amazon.com/ko/rds/mysql/features/
이걸로 봤을 때 mysqldump 는 데이터백업에 많은 시간이 소요되는 방법으로 보이므로 A 제외. 답은 B.

참고
https://aws.amazon.com/blogs/aws/amazon-aurora-fast-database-cloning/

Q94

A company is designing an application where users upload small files into Amazon S3. After a user uploads a file, the file requires one-time simple processing to transform the data and save the data in JSON format for later analysis.

Each file must be processed as quickly as possible after it is uploaded. Demand will vary. On some days, users will upload a high number of files. On other days, users will upload a few files or no files.

Which solution meets these requirements with the LEAST operational overhead?

A. Configure Amazon EMR to read text files from Amazon S3. Run processing scripts to transform the data. Store the resulting JSON file in an Amazon Aurora DB cluster.

B. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue. Use Amazon EC2 instances to read from the queue and process the data. Store the resulting JSON file in Amazon DynamoDB.

C. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function to read from the queue and process the data. Store the resulting JSON file in Amazon DynamoDB.

D. Configure Amazon EventBridge (Amazon CloudWatch Events) to send an event to Amazon Kinesis Data Streams when a new file is uploaded. Use an AWS Lambda function to consume the event from the stream and process the data. Store the resulting JSON file in an Amazon Aurora DB cluster.

Answer: C

https://www.examtopics.com/discussions/amazon/view/86676-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

A(X) : EMR 은 빅데이터 플랫폼 서비스라 사용 분야가 좀 다르고, 파일을 업로드하지 않는 날이나 업로드가 거의 없는 날에는 과도한 지출이 발생할 우려가 있음.

B(X) : 파일에 일회성 단순 처리가 필요하다고 했으므로 EC2 인스턴스로 처리하는 것보다는 Lambda 가 더 지문 요구사항에 부합.

C(O) : 유일하게 마음에 걸리는 게 '업로드 후 최대한 빨리 처리'해야한다는 건데 가장 정답에 가까운 선택지로 보임. 업로드하는 파일 숫자도 변동이 심한데 이를 SQS 대기열에 집어넣음으로서 대처할 수 있고, Lambda 함수로 파일에 일회성 단순 처리가 가능하며 추가적인 SQS->Lambda->DynamoDB 에 저장이라는 단순한 프로세스로 인해 운영 오버헤드도 매우 적음. DynamoDB 는 JSON 파일을 지원

DynamoDB 는 JSON 을 사용하여 문서에 대한 기본 지원을 제공합니다. 따라서 DynamoDB 는 Tags 같은 반정형 데이터를 저장하는 데 적합합니다. JSON 문서 안에서

데이터를 가져오고 조작할 수도 있습니다.
https://docs.aws.amazon.com/ko_kr/amazondynamodb/latest/developerguide/SQLtoNoSQL.WriteData.html
D(X) : 파일에 일회성 단순 처리가 필요하다고 했으므로 Kinesis Data Streams 로 처리하는 것보다는 Lambda 가 더 지문 요구사항에 부합. 또한 파일 업로드가 없거나 거의 없는 날에는 Kinesis 사용은 과도한 지출을 야기할 우려가 있음.

설명 2:
Amazon S3 는 S3 버킷(예: 객체 생성, 객체 제거 또는 객체 복원)에 대한 이벤트 알림을 동일한 리전의 SNS 주제로 보냅니다.
SNS 주제는 중앙 리전의 SQS 대기열에 이벤트를 게시합니다.
SQS 대기열은 Lambda 함수의 이벤트 소스로 구성되며 Lambda 함수의 이벤트 메시지를 버퍼링합니다.
Lambda 함수는 메시지에 대한 SQS 대기열을 폴링하고 애플리케이션의 요구 사항에 따라 Amazon S3 이벤트 알림을 처리합니다.
https://docs.aws.amazon.com/ko_kr/prescriptive-guidance/latest/patterns/subscribe-a-lambda-function-to-event-notifications-from-s3-buckets-in-different-aws-regions.html

Q95
An application allows users at a company's headquarters to access product data. The product data is stored in an Amazon RDS MySQL DB instance. The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic. A solutions architect needs to optimize the application's performance quickly.
What should the solutions architect recommend?
A. Change the existing database to a Multi-AZ deployment. Serve the read requests from the primary Availability Zone.
B. Change the existing database to a Multi-AZ deployment. Serve the read requests from the secondary Availability Zone.
C. Create read replicas for the database. Configure the read replicas with half of the compute and storage resources as the source database.
D. Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.
Answer: D
https://www.examtopics.com/discussions/amazon/view/85906-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
복제가 효과적으로 작동하려면 각 읽기 전용 복제본에 원본 DB 인스턴스와 동일한 양의 컴퓨팅 및 스토리지 리소스가 있어야 합니다. 원본 DB 인스턴스를 확장하는 경우 읽기 전용 복제본도 확장합니다.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_MySQL.Replication.ReadReplicas.html

참조
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_MySQL.Replication.ReadReplicas.html

Q96
An Amazon EC2 administrator created the following policy associated with an IAM group containing several users:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:TerminateInstances",
            "Resource": "*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "10.100.100.0/24"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "ec2:Region": "us-east-1"
                }
            }
        }
    ]
}
```

What is the effect of this policy?

A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
B. Users can terminate an EC2 instance with the IP address 10.100.100.1 in the us-east-1 Region.
C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.
D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.
Answer: C
https://www.examtopics.com/discussions/amazon/view/86460-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
Allow 문 해석 : 소스 IP 가 10.100.100.0/24 인 모든 리소스(*)에 대해 ec2 인스턴스 종료를 허용.
Deny 문 해석 : ec2 리전이 us-east-1 이 아닌 모든 리소스(*)에 대해 ec2 의 모든 작업을 불허. 따라서 정답은 C.

설명 2:
정책은 us-east-1 을 제외한 모든 지역에서 EC2 작업을 수행하는 것을 금지하고 소스 IP 가 10.100.100.0/24 인 사용자만 인스턴스를 종료하도록 허용하기 때문입니다. 따라서 소스 IP 가 10.100.100.254 인 사용자는 us-east-1 지역의 인스턴스를 종료할 수 있습니다.

Q97
A company has a large Microsoft SharePoint deployment running on-premises that requires Microsoft Windows shared file storage. The company wants to migrate this workload to the AWS Cloud and is considering various storage options. The storage solution must be highly available and integrated with Active Directory for access control.
Which solution will satisfy these requirements?
A. Configure Amazon EFS storage and set the Active Directory domain for authentication.
B. Create an SMB file share on an AWS Storage Gateway file gateway in two Availability Zones.
C. Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume.
D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

Answer: D
https://www.examtopics.com/discussions/amazon/view/86626-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Mcrosoft Active Directory 용 AWS Directory Service :
AWS Managed Microsoft AD 에 대한 패치 및 유지 관리. 기본적으로 각 디렉터리는 서로 다른 가용 영역에 설치된 두 개의 DC 로 구성됩니다.
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_key_concepts_maintenance.html
Windows 파일 서버용 FSx 를 AWS Managed Microsoft AD 와 통합하면 Windows 기반 애플리케이션 및 클라이언트(공유 파일 스토리지 활용)를 AWS 로 쉽게 이동할 수 있는 완전 관리형 기본 Microsoft Windows 기반 서버 메시지 블록(SMB) 프로토콜 파일 시스템을 제공합니다.
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/usecase1.html

Q98
An image-processing company has a web application that users use to upload images. The application uploads the images into an Amazon S3 bucket. The company has set up S3 event notifications to publish the object creation events to an Amazon Simple Queue Service (Amazon SQS) standard queue. The SQS queue serves as the event source for an AWS Lambda function that processes the images and sends the results to users through email.
Users report that they are receiving multiple email messages for every uploaded image. A solutions architect determines that SQS messages are invoking the Lambda function more than once, resulting in multiple email messages.
What should the solutions architect do to resolve this issue with the LEAST operational overhead?
A. Set up long polling in the SQS queue by increasing the ReceiveMessage wait time to 30 seconds.
B. Change the SQS standard queue to an SQS FIFO queue. Use the message deduplication ID to discard duplicate messages.
C. Increase the visibility timeout in the SQS queue to a value that is greater than the total of the function timeout and the batch window timeout.
D. Modify the Lambda function to delete each message from the SQS queue immediately after the message is read before processing.

Answer: C
https://www.examtopics.com/discussions/amazon/view/85185-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A(X) : 긴 폴링 대기 시간의 최대값은 20 초입니다.
https://docs.aws.amazon.com/ko_kr/AWSSimpleQueueService/latest/SQSDeveloperGuide/working-with-messages.html
B(X) : 솔루션 설계자는 SQS 메시지가 Lambda 함수를 두 번 이상 호출하여 여러 이메일 메시지를 생성하는 것이 문제의 원인이라고 보고 있음. 즉, SQS 쪽 문제이지 이미지 생성 및 업로드까지는 문제가 없다는 것. 중복 ID 제거는 생산자가 중복 메시지를 발생시키는 문제를 SQS FIFO Queue 에서 해결하는 서비스 유형이므로 지문의 상황에는 적합하지 않음. 더군다나 모든 이미지 업로드 시마다 같은 문제가 계속 발생한다는 건 가끔 중복 메시지가 유입되는 정도가 아니라 SQS 대기열 쪽에서 처리가 이루어질 때 문제가 발생했을 가능성이 더 높음.
FIFO 대기열은 중복 메시지가 절대 유입되지 않도록 설계되었습니다. 다만 일부 시나리오에서는 메시지 생산자가 중복 메시지를 유입할 수도 있습니다.
https://aws.amazon.com/ko/sqs/faqs/
C(O) : 하지만 소비자가 메시지를 삭제하기 전에 실패할 경우 제한 시간 초과가 만료되기 전에 시스템에서 해당 메시지에 대한 DeleteMessage 작업을 호출하지 않으면 다른 소비자가 메시지를 볼 수 있게 되고 메시지가 다시 수신됩니다. 일반적으로 애플리케이션에서 대기열의 메시지를 처리하고 삭제하는 데 소요되는 최대 시간으로 제한 시간 초과를 설정해야 합니다. 메시지의 제한 시간을 단축하거나 늘리기 위해 ChangeMessageVisibility 작업을 사용하여 새 제한 시간 값을 지정할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html#configuring-visibility-timeout
D(X) : Lambda 함수가 메시지 처리 및 삭제까지 담당하게 되므로 Lambda 비용이 추가로 발생하여 다른 방법보다 더 비용이 발생. 굳이 이 방법을 사용할 이유가 없음.

Q99
A company is implementing a shared storage solution for a gaming application that is hosted in an on-premises data center. The company needs the ability to use Lustre clients to access data. The solution must be fully managed.
Which solution meets these requirements?
A. Create an AWS Storage Gateway file gateway. Create a file share that uses the required

client protocol. Connect the application server to the file share.
B. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
C. Create an Amazon Elastic File System (Amazon EFS) file system, and configure it to support Lustre. Attach the file system to the origin server. Connect the application server to the file system.
D. Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.
Answer: D
https://www.examtopics.com/discussions/amazon/view/85811-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A. AWS Storage Gateway 파일 게이트웨이는 Lustre 클라이언트 액세스를 지원하지 않습니다.
B. EC2 Windows 인스턴스에서 Windows 파일 공유를 생성하는 것은 Windows 기반 파일 공유에 적합하지만 필요한 Lustre 클라이언트 액세스를 제공하지 않습니다. Lustre 는 고성능 컴퓨팅(HPC) 환경에서 주로 사용되는 고성능 병렬 파일 시스템입니다.
C. EFS 는 기본적으로 Lustre 클라이언트 액세스를 지원하지 않습니다. EFS 는 관리형 파일 스토리지 서비스이지만 범용 파일 스토리지용으로 설계되었으며 Lustre 워크로드에 최적화되어 있지 않습니다.
D. Amazon FSx for Lustre 는 Lustre 클라이언트를 포함하여 고성능 컴퓨팅 워크로드에 최적화된 완전관리형 파일 시스템입니다. Lustre 클라이언트를 사용하여 관리되고 확장 가능한 방식으로 데이터에 액세스할 수 있는 기능을 제공합니다. 이 옵션을 선택함으로써 회사는 Lustre 클라이언트 액세스 요구 사항을 충족하면서 Amazon FSx for Lustre 의 성능 및 관리 용이성으로부터 이점을 얻을 수 있습니다.

Q100
A company's containerized application runs on an Amazon EC2 instance. The application needs to download security certificates before it can communicate with other business applications. The company wants a highly secure solution to encrypt and decrypt the certificates in near real time. The solution also needs to store data in highly available storage after the data is encrypted.
Which solution will meet these requirements with the LEAST operational overhead?
A. Create AWS Secrets Manager secrets for encrypted certificates. Manually update the

certificates as needed. Control access to the data by using fine-grained IAM access.
B. Create an AWS Lambda function that uses the Python cryptography library to receive and perform encryption operations. Store the function in an Amazon S3 bucket.
C. Create an AWS Key Management Service (AWS KMS) customer managed key. Allow the EC2 role to use the KMS key for encryption operations. Store the encrypted data on Amazon S3.
D. Create an AWS Key Management Service (AWS KMS) customer managed key. Allow the EC2 role to use the KMS key for encryption operations. Store the encrypted data on Amazon Elastic Block Store (Amazon EBS) volumes.
Answer: C
https://www.examtopics.com/discussions/amazon/view/85186-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
고가용성 저장소 = S3. B,C 둘 중 하나가 답.
Lambda 보다 KMS 가 암호화 및 해독에 적합. 정답은 C.

Q101
A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.
What should the solutions architect do to enable Internet access for the private subnets?
A. Create three NAT gateways, one for each public subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.
B. Create three NAT instances, one for each private subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.
C. Create a second internet gateway on one of the private subnets. Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.
D. Create an egress-only internet gateway on one of the public subnets. Update the route table for the private subnets that forward non-VPC traffic to the egress-only Internet gateway.
Answer: A
https://www.examtopics.com/discussions/amazon/view/86019-exam-aws-certified-solut

ions-architect-associate-saa-c03/

설명:
프라이빗 서브넷에 있는 인스턴스가 외부 인터넷과 통신하기 위해선 NAT 게이트웨이가 필요.
A(O) : 각 가용 영역의 퍼블릭 서브넷마다 NAT 게이트웨이를 두어야 함. 프라이빗 서브넷의 인스턴스는 퍼블릭 NAT 게이트웨이를 통해 인터넷에 연결. 퍼블릭 서브넷에서 퍼블릭 NAT 게이트웨이를 생성하고 생성 시 탄력적 IP 주소를 NAT 게이트웨이와 연결해야 합니다. 여러 가용 영역에 리소스가 있고 NAT 게이트웨이 하나를 공유하는 경우, NAT 게이트웨이의 가용 영역이 다운되면 다른 가용 영역의 리소스도 인터넷에 액세스할 수 없게 됩니다. 가용 영역과 독립적인 아키텍처를 만들려면 각 가용 영역에 NAT 게이트웨이를 만들고 리소스가 동일한 가용 영역의 NAT 게이트웨이를 사용하도록 라우팅을 구성합니다.
https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/vpc-nat-gateway.html
B(X) : NAT 인스턴스는 더 이상 권장되지 않음
C(X) : 인터넷 게이트웨이는 프라이빗 서브넷과 외부 인터넷을 연결할 수 없음.
D(X) : NAT 게이트웨이가 필요한 상황임.

참고:
https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/vpc-nat-comparison.html

Q102
A company wants to migrate an on-premises data center to AWS. The data center hosts an SFTP server that stores its data on an NFS-based file system. The server holds 200 GB of data that needs to be transferred. The server must be hosted on an Amazon EC2 instance that uses an Amazon Elastic File System (Amazon EFS) file system.
Which combination of steps should a solutions architect take to automate this task? (Choose two)
A. Launch the EC2 instance into the same Availability Zone as the EFS file system.
B. Install an AWS DataSync agent in the on-premises data center.
C. Create a secondary Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instance for the data.
D. Manually use an operating system copy command to push the data to the EC2 instance.
E. Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server.
Answer: A, B

https://www.examtopics.com/discussions/amazon/view/85814-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A(O)
EFS 파일 시스템과 동일한 가용 영역으로 EC2 인스턴스 시작하는건 문제 없어보입니다.
B(O) : DataSync Agent 는 AWS 로 전송할 때 필요
에이전트 는 AWS DataSync 가 스토리지 시스템에서 읽거나 쓰는 데 사용하는 가상 머신(VM) 또는 Amazon EC2 인스턴스입니다 . 에이전트는 온프레미스 스토리지에서 AWS 로 데이터를 복사할 때 일반적으로 사용됩니다.
https://docs.aws.amazon.com/datasync/latest/userguide/working-with-agents.html
DataSync 는 DataSync 위치와 같이 사용됨
대부분의 워크로드의 경우 각 자체 관리 위치에 대해 하나의 AWS DataSync 에이전트를 사용하는 것이 좋습니다.
https://docs.aws.amazon.com/datasync/latest/userguide/multiple-agents.html
C(X) : EBS 가 아니라 EFS 가 NFS 지원.
D(X) : 수동으로 할 필요가 없이 DataSync 같은 대안을 사용하면 됨.
E(X) : 온프레미스 SFTP 에 좀 더 적합한 건 DataSync 보다 Transfer Family 가 더 적합해보입니다.

Q103
A company has an AWS Glue extract, transform, and load (ETL) job that runs every day at the same time. The job processes XML data that is in an Amazon S3 bucket. New data is added to the S3 bucket every day. A solutions architect notices that AWS Glue is processing all the data during each run.
What should the solutions architect do to prevent AWS Glue from reprocessing old data?
A. Edit the job to use job bookmarks.
B. Edit the job to delete data after the data is processed.
C. Edit the job by setting the NumberOfWorkers field to 1.
D. Use a FindMatches machine learning (ML) transform.
Answer: A
https://www.examtopics.com/discussions/amazon/view/85781-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

이것이 북마크의 목적입니다. "AWS Glue 는 작업 실행의 상태 정보를 유지하여 ETL 작업의 이전 실행 중에 이미 처리된 데이터를 추적합니다. 이 지속된 상태 정보를 작업 북마크라고 합니다. 작업 북마크는 AWS Glue 가 유지 관리하는 데 도움이 됩니다. 상태 정보를 제공하고 오래된 데이터의 재처리를 방지합니다."
https://docs.aws.amazon.com/glue/latest/dg/monitorcontinuations.html

설명 2:
A(O) : AWS Glue 는 작업 실행의 상태 정보를 유지하여 이전에 ETL 작업을 실행할 때 이미 처리된 데이터를 추적합니다. 이와 같은 지속 상태 정보를 작업 북마크라고 합니다.
https://docs.aws.amazon.com/ko_kr/glue/latest/dg/monitor-continuations.html
B(X) : 처리한 데이터를 어디에 쓸 줄 알고 삭제하는지...?
C(X) : ""NumberOfWorkers - 숫자(정수) : 작업이 실행될 때 할당되는 정의된 workerType 의 작업자 수입니다.
https://docs.aws.amazon.com/glue/latest/dg/aws-glue-api-jobs-job.html
D(X) : 기계 변환 학습은 전혀 관계 없음.

Q104
A solutions architect must design a highly available infrastructure for a website. The website is powered by Windows web servers that run on Amazon EC2 instances. The solutions architect must implement a solution that can mitigate a large-scale DDoS attack that originates from thousands of IP addresses. Downtime is not acceptable for the website.
Which actions should the solutions architect take to protect the website from such an attack? (Choose two)
A. Use AWS Shield Advanced to stop the DDoS attack.
B. Configure Amazon GuardDuty to automatically block the attackers.
C. Configure the website to use Amazon CloudFront for both static and dynamic content.
D. Use an AWS Lambda function to automatically add attacker IP addresses to VPC network ACLs.
E. Use EC2 Spot Instances in an Auto Scaling group with a target tracking scaling policy that is set to 80% CPU utilization.
Answer: A, C
https://www.examtopics.com/discussions/amazon/view/85342-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

A(O) : AWS Shield Advanced 보호는 네트워크 트래픽에 대한 상시 작동, 흐름 기반 모니터링과 적극적인 애플리케이션 모니터링을 통해 의심되는 DDoS 공격에 대한 거의 실시간 알림을 제공합니다. 또한 AWS Shield Advanced 는 공격을 자동으로 완화하기 위해 첨단 공격 완화 및 라우팅 기법을 적용합니다. https://aws.amazon.com/ko/shield/faqs/
B(X) : GuardDuty 는 AWS 계정 보호 서비스.
Amazon GuardDuty 는 AWS 계정 및 워크로드에서 악의적 활동을 모니터링하고 상세한 보안 결과를 제공하여 가시성 및 해결을 촉진하는 위협 탐지 서비스입니다.
https://aws.amazon.com/ko/guardduty/
C(O) : CloudFront 로도 DDoS 에 대처 가능. CloudFront 는 정적 및 동적 콘텐츠 모두에 작동. 또한 Amazon CloudFront, AWS Global Accelerator 및 Amazon Route 53 과 같은 엣지 로케이션에서 작동하는 AWS 서비스를 활용하여 알려진 모든 인프라 계층 공격에 대한 포괄적인 가용성 보호를 구축할 수 있습니다. 이러한 서비스는 AWS 글로벌 엣지 네트워크의 일부이며 전 세계에 분산된 엣지 로케이션에서 모든 유형의 애플리케이션 트래픽을 처리할 때 애플리케이션의 DDoS 복원력을 향상할 수 있습니다.
https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf
일반적으로 이미지나 동영상 파일 같은 정적 콘텐츠 전송을 위해서 Amazon CloudFront 를 많이 활용하고 있지만...TTL 을 0 으로 설정하여 매번 원본 저장소에 접속하여 동적 콘텐츠를 제공하더라도, CloudFront 를 프록시로 사용함으로써 전송 성능을 향상 시킬 수 있습니다.
https://aws.amazon.com/ko/blogs/korea/how-to-improve-dynamic-contents-delievery-using-amazon-cloudfront/
D(X) : DDoS 는 수많은 좀비 PC 를 동원하는데, 그런 PC 들의 IP 를 일일히 차단하여 막기는 비효율적.
E(X) : DDoS 로 발생하는 대규모 트래픽은 Auto Scaling 으로 막을 수 있는 스케일이 아님.

Q105
A company is preparing to deploy a new serverless workload. A solutions architect must use the principle of least privilege to configure permissions that will be used to run an AWS Lambda function. An Amazon EventBridge (Amazon CloudWatch Events) rule will invoke the function.
Which solution meets these requirements?
A. Add an execution role to the function with lambda:InvokeFunction as the action and * as the principal.
B. Add an execution role to the function with lambda:InvokeFunction as the action and Service: lambda.amazonaws.com as the principal.

C. Add a resource-based policy to the function with lambda:* as the action and Service: events.amazonaws.com as the principal.
D. Add a resource-based policy to the function with lambda:InvokeFunction as the action and Service: events.amazonaws.com as the principal.
Answer: D
https://www.examtopics.com/discussions/amazon/view/85816-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
• Lambda 의 전체 기능이 아닌 lambda 함수 호출 기능(lambda:InvokeFunction)만 사용하도록 하고, 전체 보안 주체(*)가 아닌 아마존 이벤트 서비스만 보안 주체로 설정하여야 하므로 B,D 둘 중 하나가 답.
• 서버리스 워크로드를 '배포'한다고 했으므로 다른 계정에서도 쓸 수 있는 D 가 유리함.
리소스 기반 정책은 해당 리소스에 액세스할 수 있는 사용자(보안 주체)를 지정합니다. 리소스 기반 정책을 사용한 교차 계정 액세스는 역할을 사용한 교차 계정 액세스에 비해 몇 가지 이점이 있습니다. 리소스 기반 정책을 통해 액세스한 리소스로 인해 보안 주체는 여전히 신뢰할 수 있는 계정에서 작업을 할 수 있고, 역할 권한을 수신하기 위해 자신의 권한을 포기할 필요가 없습니다. 즉, 보안 주체는 신뢰하는 계정의 리소스에 액세스하는 동시에 신뢰할 수 있는 계정의 리소스에 계속 액세스할 수 있습니다. 다른 계정의 공유 리소스로 정보를 복사하거나 공유 리소스의 정보를 복사하는 등의 작업에서 이는 특히 유용합니다.
https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/id_roles_compare-resource-policies.html
https://docs.aws.amazon.com/ko_kr/eventbridge/latest/userguide/eb-use-resource-based.html#lambda-per

Q106
A company is preparing to store confidential data in Amazon S3. For compliance reasons, the data must be encrypted at rest. Encryption key usage must be logged for auditing purposes. Keys must be rotated every year.
Which solution meets these requirements and is the MOST operationally efficient?
A. Server-side encryption with customer-provided keys (SSE-C)
B. Server-side encryption with Amazon S3 managed keys (SSE-S3)
C. Server-side encryption with AWS KMS keys (SSE-KMS) with manual rotation
D. Server-side encryption with AWS KMS keys (SSE-KMS) with automatic rotation

Answer: D
https://www.examtopics.com/discussions/amazon/view/85817-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
감사 목적으로 기록되어야 함 = AWS KMS. 따라서 C,D 둘 중 하나가 정답.
매년 키를 교체(rotate)해야하므로 운영 상 효율적인 방식은 수동이 아닌 자동 방식. 정답은 D.

설명 2:
https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html
고객 관리형 키에 대해 자동 키 교체를 활성화하면 AWS KMS 는 매년 KMS 키에 대한 새로운 암호화 자료를 생성합니다. 또한 AWS KMS 는 KMS 키가 암호화한 데이터를 해독하는 데 사용할 수 있도록 KMS 키의 이전 암호화 자료를 영구적으로 저장합니다. AWS KMS 의 키 순환은 투명하고 사용하기 쉽게 설계된 암호화 모범 사례입니다. AWS KMS 는 고객 관리형 CMK 에 대해서만 선택적 자동 키 교체를 지원합니다. 키 순환을 활성화 및 비활성화합니다. 자동 키 교체는 고객 관리형 CMK 에서 기본적으로 비활성화됩니다. 키 교체를 활성화(또는 재활성화)하면 AWS KMS 는 활성화 날짜로부터 365 일 후 그리고 이후 365 일마다 CMK 를 자동으로 교체합니다.

Q107
A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API. Which action meets these requirements for storing and retrieving location data?
A. Use Amazon Athena with Amazon S3.
B. Use Amazon API Gateway with AWS Lambda.
C. Use Amazon QuickSight with Amazon Redshift.
D. Use Amazon API Gateway with Amazon Kinesis Data Analytics.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85212-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

A(X) : 기존 분석 플랫폼을 사용하려고 한다고 했으므로 분석 기능이 있는 Athena 제외.
Amazon Athena 는 표준 SQL 을 사용해 Amazon S3 에 저장된 데이터를 간편하게 분석할 수 있는 대화식 쿼리 서비스입니다.
https://aws.amazon.com/ko/athena/faqs/
B(O) : Lambda 는 512MB 의 임시 스토리지를 가지고 있기도 하고, S3 에 데이터를 저장할 수도 있으며, 지문에서는 [이러한 데이터 포인트를 사용하려고 합니다.] 라고 언급함과 동시에 [다중 계층 옵션]이라고 했으므로 Lambda + API Gateway 조합인 B 가 정답에 가깝다고 봄.
• 512MB 에서 10,240MB 사이에서 1MB 단위로 자체 임시 스토리지로 각 Lambda 함수를 구성할 수 있습니다. 임시 스토리지는 각 함수의 /tmp 디렉터리에서 사용할 수 있습니다. 각 함수는 추가 비용 없이 512MB 의 스토리지에 액세스할 수 있습니다.
https://aws.amazon.com/ko/lambda/faqs/
• Lambda 는 웹 애플리케이션 개발자의 요구 사항을 충족하는 포괄적인 스토리지 옵션을 제공합니다. 여기에는 Amazon S3 및 Amazon EFS 와 같은 다른 AWS 서비스가 포함됩니다 . 임시 저장소 또는 Lambda 계층과 같은 기본 저장소 옵션도 사용할 수 있습니다.
https://aws.amazon.com/ko/blogs/compute/choosing-between-aws-lambda-data-storage-options-in-web-apps/
• Lambda 계층은 Lambda 함수와 함께 사용할 수 있는 라이브러리 및 기타 종속성을 패키징하는 편리한 방법을 제공합니다.
https://docs.aws.amazon.com/ko_kr/lambda/latest/dg/configuration-layers.html
C(X) : RedShift 는 Athena 에 비해 가격보다 성능이 더 우선시 될 때 사용. 위치 정보 서비스는 Athena 대신에 RedShift 를 사용해야할 정도의 서비스가 아님.
Amazon Athena 와 Amazon Redshift 는 모두 서버리스 서비스이지만 그 필요와 사용 사례가 서로 다릅니다. 어떤 규모에서든 높은 성능을 요하는 복잡한 BI 및 분석 워크로드를 위해 최고의 가격 대비 성능이 필요하다면 Amazon Redshift 와 같은 데이터 웨어하우스가 최선의 선택입니다.""(https://aws.amazon.com/ko/redshift/faqs/)
D(X) : 기존 분석 플랫폼을 사용하려고 한다고 했으므로 분석 서비스인 Amazon Kinesis Data Analytics 는 제외.

설명 2:
https://aws.amazon.com/solutions/implementations/aws-streaming-data-solution-for-amazonkinesis/

Q108

A company has an automobile sales website that stores its listings in a database on Amazon RDS. When an automobile is sold, the listing needs to be removed from the website and the data must be sent to multiple target systems.

Which design should a solutions architect recommend?

A. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) queue for the targets to consume.

B. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) FIFO queue for the targets to consume.

C. Subscribe to an RDS event notification and send an Amazon Simple Queue Service (Amazon SQS) queue fanned out to multiple Amazon Simple Notification Service (Amazon SNS) topics. Use AWS Lambda functions to update the targets.

D. Subscribe to an RDS event notification and send an Amazon Simple Notification Service (Amazon SNS) topic fanned out to multiple Amazon Simple Queue Service (Amazon SQS) queues. Use AWS Lambda functions to update the targets.

Answer: A

https://www.examtopics.com/discussions/amazon/view/85427-exam-aws-certified-solutions-architect-associate-saa-c03/

Q109

A company needs to store data in Amazon S3 and must prevent the data from being changed. The company wants new objects that are uploaded to Amazon S3 to remain unchangeable for a nonspecific amount of time until the company decides to modify the objects. Only specific users in the company's AWS account can have the ability 10 delete the objects.

What should a solutions architect do to meet these requirements?

A. Create an S3 Glacier vault. Apply a write-once, read-many (WORM) vault lock policy to the objects.

B. Create an S3 bucket with S3 Object Lock enabled. Enable versioning. Set a retention period of 100 years. Use governance mode as the S3 bucket's default retention mode for new objects.

C. Create an S3 bucket. Use AWS CloudTrail to track any S3 API events that modify the objects. Upon notification, restore the modified objects from any backup versions that the company has.

D. Create an S3 bucket with S3 Object Lock enabled. Enable versioning. Add a legal hold to the objects. Add the s3:PutObjectLegalHold permission to the IAM policies of users who need to delete the objects.

Answer: D

https://www.examtopics.com/discussions/amazon/view/85634-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

A(X) : S3 에 저장한다고 했지 S3 Glacier 같은 콜드 스토리지에 저장한다고 한 적 없음.

B(X) : 일정하지 않은 시간 동안이라고 지문에서 언급했는데, 보존 기간을 설정해뒀으므로 오답.

C(X) : 일단 일이 벌어지고 나서 수습하는 방식인데다가, 변경된 객체마다 일일히 CloudTrail 이 작동하므로 운영 오버헤드와 비용이 증가할 우려가 있음.

D(O) : 객체 잠금 법적 보존 작업을 사용하면 객체 버전에 법적 보전을 적용할 수 있습니다. 보관 기간 설정과 마찬가지로 법적 보존을 사용하면 객체 버전을 덮어쓰거나 삭제할 수 없습니다. 그러나 법적 보존에는 연결된 보관 기간이 없고, 제거될 때까지 유효합니다. S3 배치 작업은 매니페스트의 키를 처리하기 전에 S3 버킷에서 객체 잠금이 활성화되어 있는지 확인합니다. 객체 작업 및 버킷 수준 유효성 검사를 수행하려면 S3 배치 작업이 사용자를 대신하여 S3 객체 잠금을 호출할 수 있도록 IAM 역할의 s3:PutObjectLegalHold 및 s3:GetBucketObjectLockConfiguration 가 필요합니다.

https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/batch-ops-legal-hold.html

설명 2:

ALB 를 오리진으로 사용할 수 있음

원본이 하나 이상의 Amazon EC2 인스턴스에서 호스트되는 하나 이상의 HTTP 서버(웹 서버)인 경우 Application Load Balancer 를 사용하여 인스턴스에 트래픽을 분산할 수 있습니다. Application Load Balancer 를 CloudFront 의 원본으로 사용하는 방법에 대한 자세한 내용은

https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/batch-ops-legal-hold.html

Q110

A social media company allows users to upload images to its website. The website runs on Amazon EC2 instances. During upload requests, the website resizes the images to a

standard size and stores the resized images in Amazon S3. Users are experiencing slow upload requests to the website.

The company needs to reduce coupling within the application and improve website performance. A solutions architect must design the most operationally efficient process for image uploads.

Which combination of actions should the solutions architect take to meet these requirements? (Choose two)

A. Configure the application to upload images to S3 Glacier.

B. Configure the web server to upload the original images to Amazon S3.

C. Configure the application to upload images directly from each user's browser to Amazon S3 through the use of a presigned URL.

D. Configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded. Use the function to resize the image.

E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function on a schedule to resize uploaded images.

Answer: B, D

https://www.examtopics.com/discussions/amazon/view/86471-exam-aws-certified-solutions-architect-associate-saa-c03/

C, D??

Q111

A company recently migrated a message processing system to AWS. The system receives messages into an ActiveMQ queue running on an Amazon EC2 instance. Messages are processed by a consumer application running on Amazon EC2. The consumer application processes the messages and writes results to a MySQL database running on Amazon EC2. The company wants this application to be highly available with low operational complexity.

Which architecture offers the HIGHEST availability?

A. Add a second ActiveMQ server to another Availability Zone. Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.

B. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.

C. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for

MySQL with Multi-AZ enabled.
D. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use Amazon RDS for MySQL with Multi-AZ enabled.
Answer: D
https://www.examtopics.com/discussions/amazon/view/85910-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : 데이터베이스를 복제하는 것은 시간이 매우 걸리는 일임. 고가용성을 위해서라면 다중 AZ 를 사용하는 것이 좋음.
B(X) : A 와 마찬가지 이유로 오답.
C(X) : D 가 더 좋음.
D(O) : 평소에는 Standby 브로커 인스턴스에 낮은 트래픽 기준으로 AWS 리소스를 사용하여 비용을 절감하다가 Active 브로커 인스턴스가 다운되어 Standby 브로커 인스턴스 쪽으로 트래픽이 몰려오면 Auto Scaling 을 통해 대처.
일반적으로 한 번에 하나의 브로커 인스턴스만 활성 상태이고, 다른 브로커 인스턴스는 대기 상태입니다. 브로커 인스턴스 중 하나가 제대로 작동하지 않거나 유지 관리 중이면 Amazon MQ 가 비활성 인스턴스를 서비스 중지하는 데 잠깐 시간이 걸립니다. 그런 다음 정상 대기 인스턴스가 활성화되고 들어오는 통신을 수신하기 시작할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/amazon-mq/latest/developer-guide/active-standby-broker-deployment.html

설명 2:
Amazon S3 는 확장성이 뛰어나고 내구성이 뛰어난 객체 스토리지 서비스로, 웹 어디에서나 원하는 양의 데이터를 저장하고 검색할 수 있습니다. 사용자는 미리 서명된 URL 을 사용하여 각 사용자의 브라우저에서 Amazon S3 로 직접 이미지를 업로드하도록 애플리케이션을 구성할 수 있습니다. 미리 서명된 URL 은 제한된 시간 동안 특정 작업(예: 객체 업로드)으로 S3 버킷의 객체에 대한 액세스 권한을 부여하는 URL 입니다. 사용자는 AWS SDK 또는 AWS CLI 를 사용하여 프로그래밍 방식으로 미리 서명된 URL 을 생성할 수 있습니다. 미리 서명된 URL 을 사용하면 이미지를 웹 서버에 먼저 보낼 필요가 없으므로 사용자는 애플리케이션 내에서 결합을 줄이고 웹 사이트 성능을 향상시킬 수 있습니다.
AWS Lambda 는 이벤트에 대한 응답으로 코드를 실행하고 기본 컴퓨팅 리소스를 자동으로 관리하는 서버리스 컴퓨팅 서비스입니다. 사용자는 이미지가 업로드될 때 AWS Lambda 함수를 호출하도록 S3 이벤트 알림을 구성할 수 있습니다. S3 이벤트 알림은 객체 생성 또는 삭제와 같은 S3 버킷에서 특정 이벤트가 발생할 때 사용자가 알림을 받을 수 있도록

하는 기능입니다. 사용자는 이미지 크기를 조정하고 동일한 S3 버킷 또는 다른 S3 버킷에 다시 저장하는 Lambda 함수를 호출하도록 S3 이벤트 알림을 구성할 수 있습니다. 이러한 방식으로 사용자는 웹 서버에서 Lambda 로 이미지 크기 조정 작업을 오프로드할 수 있습니다.

Q112

A company hosts a containerized web application on a fleet of on-premises servers that process incoming requests. The number of requests is growing quickly. The on-premises servers cannot handle the increased number of requests. The company wants to move the application to AWS with minimum code changes and minimum development effort.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS Fargate on Amazon Elastic Container Service (Amazon ECS) to run the containerized web application with Service Auto Scaling. Use an Application Load Balancer to distribute the incoming requests.

B. Use two Amazon EC2 instances to host the containerized web application. Use an Application Load Balancer to distribute the incoming requests.

C. Use AWS Lambda with a new code that uses one of the supported languages. Create multiple Lambda functions to support the load. Use Amazon API Gateway as an entry point to the Lambda functions.

D. Use a high performance computing (HPC) solution such as AWS ParallelCluster to establish an HPC cluster that can process the incoming requests at the appropriate scale.

Answer: A

https://www.examtopics.com/discussions/amazon/view/85913-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

AWS Fargate 는 사용자가 Amazon EC2 인스턴스의 서버 또는 클러스터를 관리할 필요 없이 컨테이너를 실행할 수 있게 해주는 서버리스 컴퓨팅 엔진입니다. 사용자는 Amazon Elastic Container Service(Amazon ECS)에서 AWS Fargate 를 사용하여 Service Auto Scaling 으로 컨테이너화된 웹 애플리케이션을 실행할 수 있습니다.

Amazon ECS 는 Docker 와 Kubernetes 를 모두 지원하는 완전관리형 컨테이너 오케스트레이션 서비스입니다. Service Auto Scaling 은 사용자가 CPU 사용률 또는 요청 수와 같은 CloudWatch 지표를 기반으로 ECS 서비스에서 원하는 작업 수를 조정할 수 있는 기능입니다. 사용자는 Amazon ECS 에서 AWS Fargate 를 사용하여 애플리케이션을 컨테이너에 패키징하고 CPU 및 메모리 요구 사항을 지정하기만 하면 되므로 최소한의

코드 변경과 최소한의 개발 노력으로 애플리케이션을 AWS 로 마이그레이션할 수 있습니다. 사용자는 Application Load Balancer 를 사용하여 수신 요청을 분산할 수도 있습니다. Application Load Balancer 는 애플리케이션 계층에서 작동하고 요청 내용에 따라 대상으로 트래픽을 라우팅하는 로드 밸런서입니다. 사용자는 ECS 작업을 Application Load Balancer 의 대상으로 등록하고 경로 또는 호스트 헤더를 기반으로 요청을 다른 대상 그룹으로 라우팅하도록 리스너 규칙을 구성할 수 있습니다. 사용자는 Application Load Balancer 를 사용하여 웹 애플리케이션의 가용성과 성능을 개선할 수 있습니다.
컨테이너화된 웹 응용 프로그램이 핵심. Fargate + ECS 조합인 A 가 정답.

Q113
A company uses 50 TB of data for reporting. The company wants to move this data from on premises to AWS. A custom application in the company's data center runs a weekly data transformation job. The company plans to pause the application until the data transfer is complete and needs to begin the transfer process as soon as possible.
The data center does not have any available network bandwidth for additional workloads. A solutions architect must transfer the data and must configure the transformation job to continue to run in the AWS Cloud.
Which solution will meet these requirements with the LEAST operational overhead?
A. Use AWS DataSync to move the data. Create a custom transformation job by using AWS Glue.
B. Order an AWS Snowcone device to move the data. Deploy the transformation application to the device.
C. Order an AWS Snowball Edge Storage Optimized device. Copy the data to the device. Create a custom transformation job by using AWS Glue.
D. Order an AWS Snowball Edge Storage Optimized device that includes Amazon EC2 compute. Copy the data to the device. Create a new EC2 instance on AWS to run the transformation application.
Answer: C
https://www.examtopics.com/discussions/amazon/view/85912-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
추가 워크로드에 사용할 네트워크 대역폭이 없다는 게 핵심. 따라서 Snowball 디바이스가 필요.
A(X) : 추가 워크로드에 사용할 네트워크 대역폭이 없다고 했으므로 DataSync 는 사용 불가.

B(X) : Snowcone 으로 50TB 는 어림도 없음. 그리고 Snowcone 을 사용해서 업로드하는 방법은 DataSync 를 사용하거나 AWS 로 다시 반송(?)하는 방법 뿐인데 DataSync 는 추가 워크로드에 사용할 네트워크 대역폭이 없어서 불가능하다고 A 에서 이미 설명했고, AWS 로 다시 보내는 건 시간이 너무 걸리고 번거로움.
Snowcone 디바이스를 사용하여 디바이스를 AWS 로 배송하여 오프라인으로 또는 AWS DataSync 를 사용하여 온라인으로 데이터를 수집, 처리 및 AWS 클라우드로 이동할 수 있습니다. Snowcone 은 디바이스를 AWS 로 다시 배송하여 최대 8TB 또는 14TB 의 데이터를 AWS 클라우드로 전송할 수 있는 빠르고 저렴한 방법을 제공합니다.
https://docs.aws.amazon.com/snowball/latest/snowcone-guide/snowcone-what-is-snowcone.html
C(O) : Snowball Edge Storage Optimized 는 수십 테라바이트(TB)~페타바이트(PB)의 고용량 데이터를 안전하고 신속하게 AWS 로 전송해야 할 때 선택할 수 있는 가장 적합한 옵션입니다. 이 옵션은 대규모 데이터 전송 및 사전 처리 사용 사례를 위해 최대 80TB 의 가용 HDD 스토리지, 40 개의 vCPU, 1TB 의 SATA SSD 스토리지 및 최대 40Gb 네트워크 연결을 제공합니다.
https://aws.amazon.com/ko/snowball/faqs/
AWS Glue 를 사용하면 70 개 이상의 다양한 데이터 소스를 검색하여 연결하고 중앙 집중식 데이터 카탈로그에서 데이터를 관리할 수 있습니다. 추출, 변환, 로드(ETL) 파이프라인을 시각적으로 생성, 실행, 모니터링하여 데이터 레이크에 데이터를 로드할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/glue/latest/dg/what-is-glue.html
D(X) : 따로 변환 애플리케이션을 EC2 인스턴스에서 실행하므로 운영 오버헤드가 만만치 않음.

Q114
A company has created an image analysis application in which users can upload photos and add photo frames to their images. The users upload images and metadata to indicate which photo frames they want to add to their images. The application uses a single Amazon EC2 instance and Amazon DynamoDB to store the metadata.
The application is becoming more popular, and the number of users is increasing. The company expects the number of concurrent users to vary significantly depending on the time of day and day of week. The company must ensure that the application can scale to meet the needs of the growing user base.
Which solution meats these requirements?
A. Use AWS Lambda to process the photos. Store the photos and metadata in DynamoDB.
B. Use Amazon Kinesis Data Firehose to process the photos and to store the photos and

metadata.
C. Use AWS Lambda to process the photos. Store the photos in Amazon S3. Retain DynamoDB to store the metadata.
D. Increase the number of EC2 instances to three. Use Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volumes to store the photos and metadata.
Answer: C
https://www.examtopics.com/discussions/amazon/view/85189-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : DynamoDB 는 데이터베이스 서비스이기 때문에 이미지를 저장하기에는 적절치 않음.
B(X) : Amazon Kinesis Data Firehose 는 저장 기능이 없고 전송 기능만 있음.
Kinesis Data Firehose 는 스트리밍 ETL 솔루션입니다. 스트리밍 데이터를 캡처하고 변환한 후 Amazon S3, Amazon Redshift, Amazon OpenSearch Service 및 Splunk 로 로드하여 이미 사용하고 있는 기존 비즈니스 인텔리전스 도구 및 대시보드를 통해 거의 실시간으로 분석할 수 있습니다.
https://aws.amazon.com/ko/kinesis/data-firehose/faqs/
C(O) : 정답.
D(X) : 사용자 수가 증가하고 있으므로 프로비저닝은 적절치 않음.

설명 2:
이 솔루션은 확장성, 성능 및 가용성 요구 사항을 충족합니다. AWS Lambda 는 사진을 병렬로 처리하고 수요에 따라 자동으로 확장 또는 축소할 수 있습니다.
Amazon S3 는 사진과 메타데이터를 안정적이고 내구성 있게 저장할 수 있으며 고가용성과 짧은 지연 시간을 제공합니다. DynamoDB 는 메타데이터를 효율적으로 저장하고 일관된 성능을 제공할 수 있습니다. 또한 이 솔루션은 EC2 인스턴스 및 EBS 볼륨 관리의 비용과 복잡성을 줄입니다.
DynamoDB 에 사진을 저장하는 것은 스토리지 비용을 증가시키고 처리량을 제한할 수 있으므로 A 옵션은 올바르지 않습니다.
옵션 B 는 Kinesis Data Firehose 가 사진 처리용이 아니라 S3 또는 Redshift 와 같은 대상으로 데이터 스트리밍용으로 설계되었기 때문에 올바르지 않습니다.
옵션 D 는 EC2 인스턴스 수를 늘리고 프로비저닝된 IOPS SSD 볼륨을 사용하는 것이 로드 밸런서 및 애플리케이션 코드에 따라 확장성을 보장하지 않기 때문에 올바르지 않습니다. 또한 인프라 관리 비용과 복잡성도 증가합니다.
https://www.quora.com/How-can-I-use-DynamoDB-for-storing-metadata-for-Amazon-S3-objects

Q115

A medical records company is hosting an application on Amazon EC2 instances. The application processes customer data files that are stored on Amazon S3. The EC2 instances are hosted in public subnets. The EC2 instances access Amazon S3 over the internet, but they do not require any other network access.

A new requirement mandates that the network traffic for file transfers take a private route and not be sent over the internet.

Which change to the network architecture should a solutions architect recommend to meet this requirement?

A. Create a NAT gateway. Configure the route table for the public subnets to send traffic to Amazon S3 through the NAT gateway.

B. Configure the security group for the EC2 instances to restrict outbound traffic so that only traffic to the S3 prefix list is permitted.

C. Move the EC2 instances to private subnets. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets.

D. Remove the internet gateway from the VPC. Set up an AWS Direct Connect connection, and route traffic to Amazon S3 over the Direct Connect connection.

Answer: C

https://www.examtopics.com/discussions/amazon/view/86031-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

S3 에 액세스하지만 다른 네트워크 액세스는 필요하지 않음 = S3 Gateway Endpoint.

게이트웨이 엔드포인트는 인터넷 게이트웨이나 VPC 용 NAT 디바이스 없이 Amazon S3 및 DynamoDB 에 안정적인 연결을 제공합니다. 게이트웨이 엔드포인트는 AWS PrivateLink 를 활성화하지 않습니다.

https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html

설명 2:

프라이빗 경로를 통한 파일 전송의 새로운 요구 사항을 충족하려면 EC2 인스턴스를 인터넷에 직접 액세스할 수 없는 프라이빗 서브넷으로 이동해야 합니다. 이렇게 하면 파일 전송을 위한 트래픽이 인터넷을 통해 이동하지 않습니다. EC2 인스턴스가 Amazon S3 에 액세스할 수 있도록 Amazon S3 용 VPC 엔드포인트를 생성할 수 있습니다. VPC 엔드포인트를 사용하면 인터넷을 통해 트래픽을 전송하지 않고도 VPC 내의 리소스가 다른

서비스의 리소스와 통신할 수 있습니다. VPC 엔드포인트를 프라이빗 서브넷의 라우팅 테이블에 연결하면 EC2 인스턴스가 VPC 내의 프라이빗 연결을 통해 Amazon S3 에 액세스할 수 있습니다.

Q116

A company uses a popular content management system (CMS) for its corporate website. However, the required patching and maintenance are burdensome. The company is redesigning its website and wants anew solution. The website will be updated four times a year and does not need to have any dynamic content available. The solution must provide high scalability and enhanced security.

Which combination of changes will meet these requirements with the LEAST operational overhead? (Choose two)

A. Configure Amazon CloudFront in front of the website to use HTTPS functionality.

B. Deploy an AWS WAF web ACL in front of the website to provide HTTPS functionality.

C. Create and deploy an AWS Lambda function to manage and serve the website content.

D. Create the new website and an Amazon S3 bucket. Deploy the website on the S3 bucket with static website hosting enabled.

E. Create the new website. Deploy the website by using an Auto Scaling group of Amazon EC2 instances behind an Application Load Balancer.

Answer: A, D

https://www.examtopics.com/discussions/amazon/view/85996-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

지문은 정적 웹 사이트 호스팅에 대해서 설명하고 있음. 정적 웹사이트 호스팅에 관한 건 아래의 링크를 참조할 것.

https://aws.amazon.com/ko/getting-started/projects/build-serverless-web-app-lambda-apigateway-s3-dynamodb-cognito/module-1/

참고로 지문에서 높은 확장성을 요구하고 있는데, 높은 확장성이란 별 거 없고 정적 웹 사이트 호스팅 환경을 구축하면 그게 높은 확장성을 갖춘 것.

정적 웹 사이트 호스팅은 비용과 유지 관리 필요성이 가장 적은 옵션이고(예: 유지 관리해야 할 서버가 없음), 높은 수준의 신뢰성과 [[[확장성]]]을 제공하기 때문입니다.

https://aws.amazon.com/ko/getting-started/hands-on/host-static-website/faq/

A(O) : 뷰어가 HTTPS 를 사용할 것을 요청하도록 CloudFront 를 구성할 수 있습니다. 이렇게 하면 CloudFront 가 뷰어와 통신할 때 연결이 암호화됩니다. 또한 CloudFront 가

오리진과 HTTPS 를 사용하도록 구성할 수 있습니다. 이렇게 하면 CloudFront 가 오리진과 통신할 때 연결이 암호화됩니다.
https://docs.aws.amazon.com/ko_kr/AmazonCloudFront/latest/DeveloperGuide/using-https.html
B(X) : AWS Web ACL 은 HTTP(S) 웹 요청을 세부적으로 제어할 수 있게 해주는 것.
웹 ACL (웹 ACL) 를 사용하면 보호된 리소스가 응답하는 모든 HTTP (S) 웹 요청을 세부적으로 제어할 수 있게 해줍니다.
https://docs.aws.amazon.com/ko_kr/waf/latest/developerguide/web-acl.html
C(X) : 1 년에 4 번만 업데이트할 건데 그냥 Lambda 안 쓰고 수동으로 올려도 됨.
D(O) : 동적 콘텐츠가 필요하지 않다고 했으므로 정적 웹사이트 호스팅. 따라서 S3 버킷 + CloudFront 조합. CloudFront 는 ▲위 선택지 A 번에서 이미 준비되었으므로 S3 버킷만 준비하면 됨.
E(X) : 정적 웹사이트 호스팅은 서버리스로서 EC2 를 사용할 필요가 없음.
정적 웹 사이트 호스팅은 비용과 유지 관리 필요성이 가장 적은 옵션이고(예: 유지 관리해야 할 서버가 없음)
https://aws.amazon.com/ko/getting-started/hands-on/host-static-website/faq/

설명 2:
A -> 클라이언트에서 HTTPS 를 요구하도록 CloudFront 를 구성할 수 있습니다(보안 강화).
https://docs.aws.amazon.com/ko_kr/AmazonCloudFront/latest/DeveloperGuide/using-https-viewers-to-cloudfront.html
D -> S3 에 정적 웹 사이트를 저장하면 확장성이 제공되고 운영 오버헤드가 줄어듭니다. 그런 다음 애플리케이션 LB 및 EC2 인스턴스를 구성합니다(따라서 E 는 제외됨).

Q117
A company stores its application logs in an Amazon CloudWatch Logs log group. A new policy requires the company to store all application logs in Amazon OpenSearch Service (Amazon Elasticsearch Service) in near-real time.
Which solution will meet this requirement with the LEAST operational overhead?
A. Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).
B. Create an AWS Lambda function. Use the log group to invoke the function to write the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).
C. Create an Amazon Kinesis Data Firehose delivery stream. Configure the log group as the delivery streams sources. Configure Amazon OpenSearch Service (Amazon Elasticsearch

Service) as the delivery stream's destination.
D. Install and configure Amazon Kinesis Agent on each application server to deliver the logs to Amazon Kinesis Data Streams. Configure Kinesis Data Streams to deliver the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).
Answer: A
https://www.examtopics.com/discussions/amazon/view/85802-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
CloudWatch Logs 구독을 통해 실시간에 가깝게 Amazon OpenSearch Service 클러스터로 수신한 데이터를 스트리밍하도록 CloudWatch Logs 로그 그룹을 구성할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/AmazonCloudWatch/latest/logs/CWL_OpenSearch_Stream.html
정답은 A.
최소한의 운영헤드, 기본으로 cloudwatch log - opensearch 간 연동을 제공함

참고:
https://computingforgeeks.com/stream-logs-in-aws-from-cloudwatch-to-elasticsearch/

Q118
A company is building a web-based application running on Amazon EC2 instances in multiple Availability Zones. The web application will provide access to a repository of text documents totaling about 900 TB in size. The company anticipates that the web application will experience periods of high demand. A solutions architect must ensure that the storage component for the text documents can scale to meet the demand of the application at all times. The company is concerned about the overall cost of the solution.
Which storage solution meets these requirements MOST cost-effectively?
A. Amazon Elastic Block Store (Amazon EBS)
B. Amazon Elastic File System (Amazon EFS)
C. Amazon OpenSearch Service (Amazon Elasticsearch Service)
D. Amazon S3
Answer: D
https://www.examtopics.com/discussions/amazon/view/86512-exam-aws-certified-solutions-architect-associate-saa-c03/

설명
Amazon S3 는 가장 저렴하고 어디서나 액세스할 수 있습니다.

Amazon S3 (Simple Storage Service)는 확장성이 뛰어나고 비용 효율적인 스토리지 서비스입니다. 시나리오에서 언급한 900TB 의 텍스트 문서와 같은 대용량 데이터를 저장하는 데 적합합니다. S3 는 높은 내구성, 가용성 및 성능을 제공합니다.

옵션 A (Amazon EBS)는 개별 EC2 인스턴스용으로 설계된 블록 스토리지이며 대용량 데이터의 경우 S3 만큼 원활하고 비용 효율적으로 확장되지 않을 수 있습니다.
옵션 B (Amazon EFS)는 확장 가능한 파일 스토리지 서비스이지만 특히 예상 스토리지 크기가 900TB 인 경우 S3 에 비해 가장 비용 효율적인 옵션이 아닐 수 있습니다.
옵션 C(Amazon OpenSearch 서비스)는 검색 및 분석 서비스이며 텍스트 문서의 기본 스토리지 솔루션으로 적합하지 않을 수 있습니다.

요약하면 Amazon S3 는 웹 애플리케이션에 필요한 대규모 텍스트 문서 리포지토리를 저장하기 위한 높은 확장성, 비용 효율성 및 내구성을 제공하므로 권장되는 선택입니다.

Q119
A global company is using Amazon API Gateway to design REST APIs for its loyalty club users in the us-east-1 Region and the ap-southeast-2 Region. A solutions architect must design a solution to protect these API Gateway managed REST APIs across multiple accounts from SQL injection and cross-site scripting attacks.
Which solution will meet these requirements with the LEAST amount of administrative effort?
A. Set up AWS WAF in both Regions. Associate Regional web ACLs with an API stage.
B. Set up AWS Firewall Manager in both Regions. Centrally configure AWS WAF rules.
C. Set up AWS Shield in bath Regions. Associate Regional web ACLs with an API stage.
D. Set up AWS Shield in one of the Regions. Associate Regional web ACLs with an API stage.
Answer: B
https://www.examtopics.com/discussions/amazon/view/86450-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
[여러 계정]에서 SQL 주입, XSS 공격, DDoS 등을 방어하려면 AWS Firewall Manager 가 적격.

AWS Firewall Manager 는 AWS WAF 용 관리형 규칙과 통합되므로, 사전에 구성된 WAF 규칙을 애플리케이션에 손쉽게 배포할 수 있습니다. 사용자는 콘솔에서 클릭 몇 번으로 AWS Marketplace 판매자가 제공 및 업데이트하는 관리형 규칙을 선택하고 Application Load Balancer, API Gateway 및 Amazon CloudFront 인프라에서 일관되게 해당 규칙을 배포할 수 있습니다. https://aws.amazon.com/ko/firewall-manager/

Q120

A company has implemented a self-managed DNS solution on three Amazon EC2 instances behind a Network Load Balancer (NLB) in the us-west-2 Region. Most of the company's users are located in the United States and Europe. The company wants to improve the performance and availability of the solution. The company launches and configures three EC2 instances in the eu-west-1 Region and adds the EC2 instances as targets for a new NLB.

Which solution can the company use to route traffic to all the EC2 instances?

A. Create an Amazon Route 53 geolocation routing policy to route requests to one of the two NLBs. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.

B. Create a standard accelerator in AWS Global Accelerator. Create endpoint groups in us-west-2 and eu-west-1. Add the two NLBs as endpoints for the endpoint groups.

C. Attach Elastic IP addresses to the six EC2 instances. Create an Amazon Route 53 geolocation routing policy to route requests to one of the six EC2 instances. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.

D. Replace the two NLBs with two Application Load Balancers (ALBs). Create an Amazon Route 53 latency routing policy to route requests to one of the two ALBs. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.

Answer: B

https://www.examtopics.com/discussions/amazon/view/85807-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

A(X) : 자체 관리형 DNS 솔루션을 사용하고 있다고 이미 지문에서 언급했음. 자체적으로 해결할 수 있는 걸 Route 53 을 사용해서 추가적인 지출을 할 이유가 없음. 게다가 CDN 서비스를 사용해야한다는 단서가 없는데 굳이 CDN 서비스를 끼워넣을 이유가 없음.

B(O) : AWS Global Accelerator 는 애플리케이션 상태, 사용자의 위치 및 고객이 구성하는 정책의 변경에 즉각적으로 대응하여 항상 성능에 기반한 최적의 엔드포인트로 사용자

트래픽을 라우팅합니다.....온프레미스 엔드포인트를 처리하도록 각 AWS 리전에 Network Load Balancer(NLB)를 구성할 수 있습니다. 그러면 이러한 NLB 가 AWS Global Accelerator 구성에서 엔드포인트가 될 수 있습니다.
https://aws.amazon.com/ko/global-accelerator/faqs/
C(X) : 탄력적 IP 주소를 AWS Global Accelerator 에 연결하는 게 더 효과적. 앞으로 인스턴스가 늘어날 때마다 EC2 인스턴스에 탄력적 IP 를 부여할 건지?
D(X) : 가능은 한데 A 와 같은 이유로 out. 그리고 굳이 귀찮게 ALB 로 교체할 이유가 없음.

설명 2:
표준 액셀러레이터의 경우 Global Accelerator 는 AWS 글로벌 네트워크를 사용하여 사용자가 구성한 상태, 클라이언트 위치 및 정책을 기반으로 트래픽을 최적의 지역 엔드포인트로 라우팅하여 애플리케이션의 가용성을 높입니다. 표준 액셀러레이터의 엔드포인트는 Network Load Balancer, Application Load Balancer, Amazon EC2 인스턴스 또는 하나의 AWS 리전 또는 여러 리전에 위치한 탄력적 IP 주소일 수 있습니다.
https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html

Q121
A company is running an online transaction processing (OLTP) workload on AWS. This workload uses an unencrypted Amazon RDS DB instance in a Multi-AZ deployment. Daily database snapshots are taken from this instance.
What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?
A. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted snapshot.
B. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it. Enable encryption on the DB instance.
C. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS) Restore encrypted snapshot to an existing DB instance.
D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS).
Answer: A
https://www.examtopics.com/discussions/amazon/view/85941-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
Amazon RDS 암호화된 DB 인스턴스의 경우 모든 로그, 백업 및 스냅샷이 암호화됩니다. Amazon RDS DB 인스턴스의 암호화는 인스턴스를 생성할 때에만 가능하며 DB 인스턴스가 생성된 후에는 불가능합니다. 다만 암호화되지 않은 스냅샷의 사본을 암호화할 수 있기 때문에 암호화되지 않은 DB 인스턴스에 실질적으로 암호화를 추가할 수 있습니다. 즉, DB 인스턴스의 스냅샷을 만든 다음 해당 스냅샷의 암호화된 사본을 만들 수 있습니다. 그런 다음 암호화된 스냅샷에서 DB 인스턴스를 복구할 수 있고, 원본 DB 인스턴스의 암호화된 사본이 생깁니다.
https://docs.aws.amazon.com/ko_kr/AmazonRDS/latest/UserGuide/Overview.Encryption.html#Overview.Encryption.Limitations

설명 2:
https://docs.aws.amazon.com/ko_kr/AmazonRDS/latest/UserGuide/USER_RestoreFromSnapshot.html#USE
https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/EBSEncryption.html

Q122
A company wants to build a scalable key management infrastructure to support developers who need to encrypt data in their applications.
What should a solutions architect do to reduce the operational burden?
A. Use multi-factor authentication (MFA) to protect the encryption keys.
B. Use AWS Key Management Service (AWS KMS) to protect the encryption keys.
C. Use AWS Certificate Manager (ACM) to create, store, and assign the encryption keys.
D. Use an IAM policy to limit the scope of users who have access permissions to protect the encryption keys.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85942-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A(X) : MFA 는 다중 인증으로, 운영 부담 감소와는 아무런 상관 없음.
B(O) : ""AWS KMS 는 암호화 작업에 사용되는 키를 쉽게 생성하고 제어할 수 있도록 지원하는 관리형 서비스입니다. https://aws.amazon.com/ko/kms/faqs/
C(X) : ACM 은 SSL/TLS 인증서 관련 서비스.
AWS Certificate Manager 는 AWS 서비스 및 연결된 내부 리소스에 사용할 공인 및 사설

SSL/TLS(Secure Sockets Layer/전송 계층 보안) 인증서를 손쉽게 프로비저닝, 관리 및 배포할 수 있도록 지원하는 서비스입니다.
https://aws.amazon.com/ko/certificate-manager/faqs/
D(X) : IAM 정책은 키 관리 서비스가 아니라 권한 관련 서비스.

참고:
https://aws.amazon.com/ko/kms/faqs/#:~:text=If%20you%20are%20a%20developer%20who%20needs

Q123
A company has a dynamic web application hosted on two Amazon EC2 instances. The company has its own SSL certificate, which is on each instance to perform SSL termination. There has been an increase in traffic recently, and the operations team determined that SSL encryption and decryption is causing the compute capacity of the web servers to reach their maximum limit.
What should a solutions architect do to increase the application's performance?
A. Create a new SSL certificate using AWS Certificate Manager (ACM). Install the ACM certificate on each instance.
B. Create an Amazon S3 bucket Migrate the SSL certificate to the S3 bucket. Configure the EC2 instances to reference the bucket for SSL termination.
C. Create another EC2 instance as a proxy server. Migrate the SSL certificate to the new instance and configure it to direct connections to the existing EC2 instances.
D. Import the SSL certificate into AWS Certificate Manager (ACM). Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.
Answer: D
https://www.examtopics.com/discussions/amazon/view/85943-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
AWS Certificate Manager 를 사용하면 인증서를 신속하게 요청하고 Elastic Load Balancer, Amazon CloudFront 배포, API Gateway 의 API 와 같은 ACM 통합 AWS 리소스에 배포하고 AWS Certificate Manager 가 인증서 갱신을 처리하도록 할 수 있습니다. 또한 내부 리소스에 대한 개인 인증서를 만들고 중앙에서 인증서 수명 주기를 관리할 수 있습니다.

설명 2:

ACM(AWS Certificate Manager)이 필요한 상황.
AWS Certificate Manager(ACM)는 AWS 서비스 및 연결된 내부 리소스에 사용할 공인 및 사설 SSL/TLS(Secure Sockets Layer/전송 계층 보안) 인증서를 손쉽게 프로비저닝, 관리 및 배포할 수 있도록 지원하는 서비스입니다.
https://aws.amazon.com/ko/certificate-manager/
따라서 A,D 둘 중 하나가 정답.
A(X) : 기존에 이미 사용하던 SSL 인증서가 있는데 하나 새로 만들 필요는 없음.
D(O) : A 와 같은 이유로 정답.
리스너는 연결 요청을 확인하는 프로세스입니다. 로드 밸런서를 생성할 때 리스너를 정의하면 언제라도 로드 밸런서에 리스너를 추가할 수 있습니다. 암호화된 연결(SSL 오프로드라고도 함)을 사용하는 HTTPS 리스너를 생성할 수 있습니다. 이 기능을 사용하면 로드 밸런서와 SSL 또는 TLS 세션을 시작하는 클라이언트 간에 트래픽 암호화가 가능합니다.
https://docs.aws.amazon.com/ko_kr/elasticloadbalancing/latest/application/create-https-listener.html

Q124
A company has a highly dynamic batch processing job that uses many Amazon EC2 instances to complete it. The job is stateless in nature, can be started and stopped at any given time with no negative impact, and typically takes upwards of 60 minutes total to complete. The company has asked a solutions architect to design a scalable and cost-effective solution that meets the requirements of the job.
What should the solutions architect recommend?
A. Implement EC2 Spot Instances.
B. Purchase EC2 Reserved Instances.
C. Implement EC2 On-Demand Instances.
D. Implement the processing on AWS Lambda.
Answer: A
https://www.examtopics.com/discussions/amazon/view/86038-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
EC2 스팟 인스턴스를 통해 사용자는 여분의 Amazon EC2 컴퓨팅 용량에 입찰할 수 있으며 언제든지 시작 및 중지할 수 있는 상태 비저장 및 중단 가능한 워크로드를 위한 비용 효율적인 솔루션이 될 수 있습니다.

배치 처리 작업은 상태 비저장이고 언제든지 시작 및 중지할 수 있으며 일반적으로 완료하는 데 60 분 이상 걸리므로 EC2 스팟 인스턴스는 이 워크로드에 적합합니다.

설명 2:
상태비저장, 시작 및 중지 가능이라는 단서를 볼 때 스팟 인스턴스가 적절함.

Q125
A company runs its two-tier ecommerce website on AWS. The web tier consists of a load balancer that sends traffic to Amazon EC2 instances. The database tier uses an Amazon RDS DB instance. The EC2 instances and the RDS DB instance should not be exposed to the public internet. The EC2 instances require internet access to complete payment processing of orders through a third-party web service. The application must be highly available.
Which combination of configuration options will meet these requirements? (Choose two.)
A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.
B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.
C. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones. Deploy an RDS Multi-AZ DB instance in private subnets.
D. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnet.
E. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnets.
Answer: A, E
https://www.examtopics.com/discussions/amazon/view/85221-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
시작하기 전에: EC2 인스턴스에 사용할 두 개의 가용 영역을 결정합니다. 이러한 각 가용 영역에서 하나 이상의 퍼블릭 서브넷으로 Virtual Private Cloud(VPC)를 구성합니다.
이러한 퍼블릭 서브넷은 로드 밸런서를 구성하는 데 사용됩니다. 대신 이러한 가용 영역의 다른 서브넷에서 EC2 인스턴스를 시작할 수 있습니다.

설명 2:
• EC2 인스턴스와 RDS DB 인스턴스는 퍼블릭 인터넷에 노출되지 않아야 하므로 프라이빗

서브넷에 위치해야 함.
・그러면서도 EC2 인스턴스는 인터넷에 접속해야하니 NAT 서비스가 필요. NAT 게이트웨이(기본적으로 퍼블릭 NAT 게이트웨이를 말함)는 퍼블릭 서브넷에 위치해야 함.
퍼블릭 서브넷에서 퍼블릭 NAT 게이트웨이를 생성하고 생성 시 탄력적 IP 주소를 NAT 게이트웨이와 연결해야 합니다. 트래픽을 NAT 게이트웨이에서 VPC 용 인터넷 게이트웨이로 라우팅합니다.
https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/vpc-nat-gateway.html
・가용성 = Auto Scaling, Multi AZ
A(O) : EC2 인스턴스와 RDS 인스턴스 모두 프라이빗 서브넷에 위치해야하며 고가용성을 충족시켜야 하므로 다중 AZ 를 사용.
B(X) : ALB 는 퍼블릭 서브넷에 위치해야 함.
프라이빗 서브넷에 있는 Amazon EC2 인스턴스를 연결하려면 백엔드 인스턴스에서 사용하는 프라이빗 서브넷과 동일한 가용 영역에 퍼블릭 서브넷을 생성합니다. 그런 다음 퍼블릭 서브넷을 로드 밸런서와 연결합니다.
https://aws.amazon.com/ko/premiumsupport/knowledge-center/public-load-balancer-private-ec2/
C(X) : 퍼블릭 서브넷에서 EC2 인스턴스를 시작하기 때문에 오답. EC2 인스턴스는 퍼블릭 인터넷에 노출되지 않아야 하므로 프라이빗 서브넷에 있어야 함.
D(X) : 하나의 서브넷으로 두 개의 가용영역에 걸쳐 사용하는 것은 불가.
각 서브넷은 완전히 하나의 가용 영역 내에 있어야 하며 여러 영역에 걸쳐 있을 수 없습니다.
https://docs.aws.amazon.com/vpc/latest/userguide/configure-subnets.html#subnet-basics
E(O) : 각 AZ 에 퍼블릭 서브넷은 1 개 있어야 하고(NAT 게이트웨이가 들어가야 하므로), 프라이빗 서브넷은 1 개 이상 있어야 함(EC2 인스턴스와 RDS 가 들어갈 곳). 각 AZ 에 있는 퍼블릭 서브넷에 NAT 게이트웨이가 하나씩 들어가야 각 가용영역에 있는 프라이빗 서브넷마다 인터넷에 액세스가 가능한 상태가 되므로 NAT 게이트웨이는 총 2 개가 됨.
따라서 2 개의 AZ 에 걸쳐 퍼블릭 서브넷 2, 프라이빗 서브넷 2, NAT 게이트웨이 2 개가 됨."

Q126
A solutions architect needs to implement a solution to reduce a company's storage costs. All the company's data is in the Amazon S3 Standard storage class. The company must keep all data for at least 25 years. Data from the most recent 2 years must be highly available and immediately retrievable.
Which solution will meet these requirements?

A. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive immediately.
B. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 2 years.
C. Use S3 Intelligent-Tiering. Activate the archiving option to ensure that data is archived in S3 Glacier Deep Archive.
D. Set up an S3 Lifecycle policy to transition objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately and to S3 Glacier Deep Archive after 2 years.
Answer: B
https://www.examtopics.com/discussions/amazon/view/86731-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A(X) : 가장 최근 2 년의 데이터는 즉시 검색할 수 있어야 하므로 콜드 스토리지는 부적절.
B(O) : 정답
C(X) : 가장 최근 2 년의 데이터는 모두 가용성이 높아야 하고 즉시 검색할 수 있어야하는 데이터이므로 Intelligent-Tiering 이 따로 필요하진 않음.
D(X) : One Zone-IA 는 고가용성 조건 불충족.
https://aws.amazon.com/ko/about-aws/whats-new/2018/04/announcing-s3-one-zone-infrequent-access-a-new-amazon-s3-storage-class/?nc1=h_ls

Q127
A media company is evaluating the possibility of moving its systems to the AWS Cloud. The company needs at least 10 TB of storage with the maximum possible I/O performance for video processing, 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore.
Which set of services should a solutions architect recommend to meet these requirements?
A. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage
B. Amazon EBS for maximum performance, Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage
C. Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage
D. Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage
Answer: D

https://www.examtopics.com/discussions/amazon/view/85432-exam-aws-certified-solutions-architect-associate-saa-c03/

설명
고가용성이므로 Auto Scaling 이 들어간 C,D 둘 중 하나가 정답. EFS vs EBS 를 비교해보면 보통은 EFS 가 정답인 경우가 많음. 일단 EBS 는 여러 EC2 인스턴스에서 동시 접속할 수 없다는 단점이 치명적이기 때문.
Amazon Elastic File System 은 전체 파일 시스템 액세스 의미 체계를 지원하는 표준 파일 시스템 인터페이스를 제공합니다.
https://docs.aws.amazon.com/efs/latest/ug/using-fs.html
EBS 다중 연결 볼륨에서 표준 파일 시스템 작업은 지원되는 구성이 아닙니다.
https://aws.amazon.com/ko/premiumsupport/knowledge-center/ebs-access-volumes-using-multi-attach/

참조
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html

Q128
A company wants to run applications in containers in the AWS Cloud. These applications are stateless and can tolerate disruptions within the underlying infrastructure. The company needs a solution that minimizes cost and operational overhead.
What should a solutions architect do to meet these requirements?
A. Use Spot Instances in an Amazon EC2 Auto Scaling group to run the application containers.
B. Use Spot Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.
C. Use On-Demand Instances in an Amazon EC2 Auto Scaling group to run the application containers.
D. Use On-Demand Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85404-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

중단을 허용할 수 있음 = 스팟 인스턴스. 컨테이너에서 애플리케이션 실행 = ECS, EKS 같은 서비스. 답은 B.

Q129

A company is running a multi-tier web application on premises. The web application is containerized and runs on a number of Linux hosts connected to a PostgreSQL database that contains user records. The operational overhead of maintaining the infrastructure and capacity planning is limiting the company's growth. A solutions architect must improve the application's infrastructure.

Which combination of actions should the solutions architect take to accomplish this? (Choose two)

A. Migrate the PostgreSQL database to Amazon Aurora.

B. Migrate the web application to be hosted on Amazon EC2 instances.

C. Set up an Amazon CloudFront distribution for the web application content.

D. Set up Amazon ElastiCache between the web application and the PostgreSQL database.

E. Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).

Answer: A, E

https://www.examtopics.com/discussions/amazon/view/86658-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

• 컨테이너화 되어있음 = ECS(또는 EKS) + Fargate.

A(O) : Amazon Aurora 는 PostgreSQL 과 호환되고 다중 리전 및 AZ 를 기본적으로 지원하므로 인프라 및 용량 계획을 유지 관리 가능.

Amazon Aurora 는 서버리스 및 기계 학습 기반 애플리케이션의 구축을 위한 규모에 따른 성능 및 고가용성, 완전한 오픈 소스 MySQL 및 PostgreSQL 호환 버전과 광범위한 개발자 도구를 제공….Amazon Aurora 는 데이터베이스 볼륨을 10GB 세그먼트로 자동으로 분리하여 여러 디스크에 분산합니다. 데이터베이스 볼륨에서 각 10GB 청크가 3 개의 AZ 에 6 가지 방법으로 복제됩니다. https://aws.amazon.com/ko/rds/aurora/faqs/

B(X) : 애플리케이션이 컨테이너화 되어있다고 했으므로 Fargate 사용이 더 적절.

C(X) : CloudFront 는 CDN 서비스로 지문의 상황엔 적합치 않음.

D(X) : ElastiCache 는 웹 애플리케이션과 DB 간 캐시 서비스로 지문의 상황엔 적합치 않음.

E(O) : ECS + Fargate 로 컨테이너화된 애플리케이션 사용 가능.

AWS Fargate Fargate 는 Amazon EC2 인스턴스의 서버나 클러스터를 관리할 필요 없이

컨테이너를 실행하기 위해 Amazon ECS 에 사용할 수 있는 기술입니다.
https://docs.aws.amazon.com/ko_kr/AmazonECS/latest/userguide/what-is-fargate.html

설명 2:
Amazon Aurora 는 PostgreSQL 과 호환되는 완전히 관리되고 확장 가능하며 가용성이 높은 관계형 데이터베이스 서비스입니다. 데이터베이스를 Amazon Aurora 로 마이그레이션하면 데이터베이스 인프라를 유지 관리하는 운영 오버헤드가 줄어들고 회사는 애플리케이션 구축 및 확장에 집중할 수 있습니다. AWS Fargate 는 사용자가 기본 EC2 인스턴스를 관리할 필요 없이 컨테이너를 실행할 수 있도록 하는 완전 관리형 컨테이너 오케스트레이션 서비스입니다. 솔루션 설계자는 Amazon Elastic Container Service(Amazon ECS)와 함께 AWS Fargate 를 사용하여 웹 애플리케이션의 확장성과 효율성을 개선하고 기본 인프라를 유지 관리하는 운영 오버헤드를 줄일 수 있습니다.

Q130
An application runs on Amazon EC2 instances across multiple Availability Zonas. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%.
What should a solutions architect do to maintain the desired performance across all instances in the group?
A. Use a simple scaling policy to dynamically scale the Auto Scaling group.
B. Use a target tracking policy to dynamically scale the Auto Scaling group.
C. Use an AWS Lambda function to update the desired Auto Scaling group capacity.
D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group.
Answer: B
https://www.examtopics.com/discussions/amazon/view/86659-exam-aws-certified-solutions-architect-associate-saa-c03/

설명
CPU 사용률에 따라 Auto Scaling = Target Tracking Policy. 정답은 B.
https://docs.aws.amazon.com/autoscaling/application/userguide/application-auto-scaling-targettracking.html

Q131

A company is developing a file-sharing application that will use an Amazon S3 bucket for storage. The company wants to serve all the files through an Amazon CloudFront distribution. The company does not want the files to be accessible through direct navigation to the S3 URL.

What should a solutions architect do to meet these requirements?

A. Write individual policies for each S3 bucket to grant read permission for only CloudFront access.

B. Create an IAM user. Grant the user read permission to objects in the S3 bucket. Assign the user to CloudFront.

C. Write an S3 bucket policy that assigns the CloudFront distribution ID as the Principal and assigns the target S3 bucket as the Amazon Resource Name (ARN).

D. Create an origin access identity (OAI). Assign the OAI to the CloudFront distribution. Configure the S3 bucket permissions so that only the OAI has read permission.

Answer: D

https://www.examtopics.com/discussions/amazon/view/85992-exam-aws-certified-solutions-architect-associate-saa-c03/

설명

https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-access-to-amazon-s3/

https://docs.aws.amazon.com/ko_kr/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html#private-content-restricting-access-to-s3-overview

S3 + CloudFront 를 사용하는 상황에서 S3 에 직접 액세스하는 것을 막으려면 OAC 또는 OAI 를 사용하면 됨.

Amazon S3 버킷을 오리진으로 설정하여 CloudFront 를 사용하는 경우 다음과 같은 이점을 제공하는 방식으로 CloudFront 및 Amazon S3 를 구성할 수 있습니다. ◎공개적으로 액세스할 수 없도록 Amazon S3 버킷에 대한 액세스를 제한합니다. ◎뷰어(사용자)가 지정된 CloudFront 배포를 통해서만 버킷의 콘텐츠에 액세스할 수 있도록 합니다. 즉, 뷰어가 버킷에서 직접 또는 의도하지 않은 CloudFront 배포를 통해 콘텐츠에 액세스하는 것을 방지합니다. 이렇게 하려면 인증된 요청을 Amazon S3 로 보내도록 CloudFront 를 구성하고 CloudFront 의 인증된 요청에 대한 액세스만 허용하도록 Amazon S3 를 구성합니다. CloudFront 는 Amazon S3 오리진에 인증된 요청을 전송하는 두 가지 방법으로 오리진 액세스 제어(OAC)와 오리진 액세스 ID(OAI)를 제공합니다. OAC 는 다음을 지원하므로 OAC 를 사용하는 것이 좋습니다.

https://docs.aws.amazon.com/ko_kr/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html

Q132

A company's website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company's website demands globally. The solution should be cost-effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.

Which combination should a solutions architect recommend to meet these requirements?

A. Amazon CloudFront and Amazon S3

B. AWS Lambda and Amazon DynamoDB

C. Application Load Balancer with Amazon EC2 Auto Scaling

D. Amazon Route 53 with internal Application Load Balancers

Answer: A

https://www.examtopics.com/discussions/amazon/view/86654-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

전 세계적으로 웹 사이트 요구 충족 = CloudFront.

빠른 응답을 위한 Cloudfront 와 인프라를 최소화하기 위한 s3.

Q133

A company runs an Oracle database on premises. As part of the company's migration to AWS, the company wants to upgrade the database to the most recent available version. The company also wants to set up disaster recovery (DR) for the database. The company needs to minimize the operational overhead for normal operations and DR setup. The company also needs to maintain access to the database's underlying operating system.

Which solution will meet these requirements?

A. Migrate the Oracle database to an Amazon EC2 instance. Set up database replication to a different AWS Region.

B. Migrate the Oracle database to Amazon RDS for Oracle. Activate Cross-Region automated backups to replicate the snapshots to another AWS Region.

C. Migrate the Oracle database to Amazon RDS Custom for Oracle. Create a read replica for the database in another AWS Region.

D. Migrate the Oracle database to Amazon RDS for Oracle. Create a standby database in another Availability Zone.
Answer: C
https://www.examtopics.com/discussions/amazon/view/85423-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
기본 운영 체제에 대한 액세스 유지 = Amazon RDS Custom.
Amazon Relational Database Service(Amazon RDS) Custom 은 기본 OS 및 DB 환경에 액세스할 필요가 있는 레거시, 사용자 지정, 패키지 애플리케이션을 위한 관리형 데이터베이스 서비스입니다.
https://aws.amazon.com/ko/about-aws/whats-new/2021/10/amazon-rds-custom-oracle/

참고:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-custom.html
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/working-with-custom-oracle.html

Q134
A company wants to move its application to a serverless solution. The serverless solution needs to analyze existing and new data by using SL. The company stores the data in an Amazon S3 bucket. The data requires encryption and must be replicated to a different AWS Region.
Which solution will meet these requirements with the LEAST operational overhead?
A. Create a new S3 bucket. Load the data into the new S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with AWS KMS multi-Region kays (SSE-KMS). Use Amazon Athena to query the data.
B. Create a new S3 bucket. Load the data into the new S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with AWS KMS multi-Region keys (SSE-KMS). Use Amazon RDS to query the data.
C. Load the data into the existing S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption

with Amazon S3 managed encryption keys (SSE-S3). Use Amazon Athena to query the data.
D. Load the data into the existing S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon RDS to query the data.
Answer: C
https://www.examtopics.com/discussions/amazon/view/85993-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A(X) : 최소한의 운영 오버헤드라고 했으므로 SSE-KMS 보다는 SSE-S3 가 AWS 에서 다 관리하기 때문에 더 적합. 또한 회사는 데이터를 S3 버킷에 저장한다고 했으므로 기존 버킷이 있는 것이고, 이는 현재 리전에서 새 S3 버킷을 생성할 필요가 없음을 의미. 그리고 지문에서 운영 오버헤드에 대한 언급은 있어도 비용에 대한 언급은 없음.
B(X) : S3 에 쿼리하는 건 RDS 가 아니라 Athena 가 더 적합.
C(O) : KMS 필요없이 S3 측에서 암호화할 수 있음. 기존 버킷에 데이터를 로드하고 다른 리전으로 복제하는 것이기 때문에 다른 리전에서도 기존 및 신규 데이터를 모두 사용할 수 있음.
D(X) : B 와 같은 이유로 오답.

Q135
A company runs workloads on AWS. The company needs to connect to a service from an external provider. The service is hosted in the provider's VPC. According to the company's security team, the connectivity must be private and must be restricted to the target service. The connection must be initiated only from the company's VPC.
Which solution will mast these requirements?
A. Create a VPC peering connection between the company's VPC and the provider's VPC. Update the route table to connect to the target service.
B. Ask the provider to create a virtual private gateway in its VPC. Use AWS PrivateLink to connect to the target service.
C. Create a NAT gateway in a public subnet of the company's VPUpdate the route table to connect to the target service.
D. Ask the provider to create a VPC endpoint for the target service. Use AWS PrivateLink to connect to the target service.
Answer: D
https://www.examtopics.com/discussions/amazon/view/85994-exam-aws-certified-solut

ions-architect-associate-saa-c03/

설명:
A(X) : 대상 서비스로 제한되어야 한다는 조건 불충족. VPC 내의 특정 애플리케이션이나 서비스에 연결하려면 PrivateLlnk 가 필요. 또한 연결은 회사의 VPC 에서만 시작되어야 한다는 점 불충족.
설명 1:
VPC 피어링을 사용하면 VPC 를 비공개로 연결할 수 있지만 AWS PrivateLink 를 사용하면 VPC 의 애플리케이션이나 서비스를 VPC 피어링 연결에서 연결할 수 있는 엔드포인트로 구성할 수 있습니다.
(https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/vpc-peering.html)
B(X) : Virtual Private Gateway 는 VPN 엔드포인트.
가상 프라이빗 게이트웨이는 단일 VPC 에 연결할 수 있는 사이트 간 VPN 연결의 Amazon 측 VPN 엔드포인트입니다.
https://docs.aws.amazon.com/ko_kr/vpn/latest/s2svpn/VPC_VPN.html
C(X) : 대상 서비스로 제한되어야 한다는 조건 불충족. 퍼블릭 서브넷의 NAT 게이트웨이는 퍼블릭 NAT 게이트웨이로서, IGW, VPC, 온프레미스 네트워크에 연결할 수 있지만 특정 서비스에만 접속하도록 할 수 있다는 건 없음.
""퍼블릭 서브넷에서 퍼블릭 NAT 게이트웨이를 생성하고 생성 시 탄력적 IP 주소를 NAT 게이트웨이와 연결해야 합니다. 트래픽을 NAT 게이트웨이에서 VPC 용 인터넷 게이트웨이로 라우팅합니다. 또는 퍼블릭 NAT 게이트웨이를 사용하여 다른 VPC 또는 온프레미스 네트워크에 연결할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/vpc-nat-gateway.html
D(O) : A 번 참고.

Q136
A company is migrating its on-premises PostgreSQL database to Amazon Aurora PostgreSQL. The on-premises database must remain online and accessible during the migration. The Aurora database must remain synchronized with the on-premises database. Which combination of actions must a solutions architect take to meet these requirements? (Choose two)
A. Create an ongoing replication task.
B. Create a database backup of the on-premises database.
C. Create an AWS Database Migration Service (AWS DMS) replication server.
D. Convert the database schema by using the AWS Schema Conversion Tool (AWS SCT).

E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to monitor the database synchronization.

Answer: A, C

https://www.examtopics.com/discussions/amazon/view/85438-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

A(O) : ongoing replication(진행중인 복제)은 CDC(변경 데이터 캡처)라고도 하며 소스 데이터 스토어에서 진행 중인 변경 사항을 복제할 때 이 프로세스를 사용. (https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Task.CDC.html)

이는 동기화된 상태를 만들어줌. "AWS DMS 를 사용하면 일회성 마이그레이션을 수행하고 지속적인 변경 사항을 복제하여 소스와 대상을 동기화 상태로 유지할 수 있습니다.

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

C(O) : DMS 는 대상이 소스와 동기화된 상태를 유지하도록 지속적 복제를 지원하지만, SCT 는 그렇지 않습니다. AWS Database Migration Service(DMS)는 다양한 동종 및 이기종 데이터 복제를 지원합니다.

https://aws.amazon.com/ko/dms/faqs/?refid=bef7080f-573e-4a75-b22b-85f316173744

설명 2:

AWS Database Migration Service 는 Oracle 에서 Oracle 로의 동종 마이그레이션은 물론 Oracle 또는 Microsoft SQL Server 에서 Amazon Aurora 로의 서로 다른 데이터베이스 플랫폼 간의 이기종 마이그레이션을 지원합니다. AWS Database Migration Service 를 사용하면 지원되는 소스에서 지원되는 대상으로 짧은 지연 시간으로 데이터를 지속적으로 복제할 수도 있습니다. 예를 들어 여러 소스에서 Amazon Simple Storage Service(Amazon S3)로 복제하여 가용성과 확장성이 뛰어난 데이터 레이크 솔루션을 구축할 수 있습니다. Amazon Redshift 로 데이터를 스트리밍하여 데이터베이스를 페타바이트 규모의 데이터 웨어하우스로 통합할 수도 있습니다. 지원되는 소스 및 대상 데이터베이스에 대해 자세히 알아보세요.

https://aws.amazon.com/dms/

Q137

A company uses AWS Organizations to create dedicated AWS accounts for each business unit to manage each business unit's account independently upon request. The root email recipient missed a notification that was sent to the root user email address of one account. The company wants to ensure that all future notifications are not missed. Future

notifications must be limited to account administrators.
Which solution will meet these requirements?
A. Configure the company's email server to forward notification email messages that are sent to the AWS account root user email address to all users in the organization.
B. Configure all AWS account root user email addresses as distribution lists that go to a few administrators who can respond to alerts. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.
C. Configure all AWS account root user email messages to be sent to one administrator who is responsible for monitoring alerts and forwarding those alerts to the appropriate groups.
D. Configure all existing AWS accounts and all newly created accounts to use the same root user email address. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85997-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A(X) : 향후 알림은 계정 관리자로 제한되어야 한다고 했으므로 오답.
B(O) : AWS Organizations 콘솔에서 또는 AWS CLI 또는 AWS SDK 를 사용하여 프로그래밍 방식으로 조직 내 계정의 대체 연락처를 업데이트할 수 있습니다. 조직의 관리 계정을 사용하여 조직의 모든 계정에 대한 계정 설정을 보고 편집할 수 있습니다. 기본 계정 소유자는 루트 계정의 이메일에 대한 모든 이메일 통신을 계속 수신합니다.
https://docs.aws.amazon.com/accounts/latest/reference/manage-acct-update-contact-alternate.html
C(X) : 루트 이메일 수신자가 한 계정의 루트 사용자 이메일 주소로 전송된 알림을 놓쳤다고 했는데, 선택지 C 의 방식은 기존의 방식과 동일함.
D(X) : 향후 알림은 계정 관리자로 제한되어야 한다고 했으므로 오답.

참고
https://docs.aws.amazon.com/ko_kr/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html#best-practices_mgmt-acct_email-address

Q138
A company runs its ecommerce application on AWS. Every new order is published as a massage in a RabbitMQ queue that runs on an Amazon EC2 instance in a single Availability

Zone. These messages are processed by a different application that runs on a separate EC2 instance. This application stores the details in a PostgreSQL database on another EC2 instance. All the EC2 instances are in the same Availability Zone.
The company needs to redesign its architecture to provide the highest availability with the least operational overhead.
What should a solutions architect do to meet these requirements?
A. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon MQ. Create a Multi-AZ Auto Scaling group for EC2 instances that host the application. Create another Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database.
B. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon MQ. Create a Multi-AZ Auto Scaling group for EC2 instances that host the application. Migrate the database to run on a Multi-AZ deployment of Amazon RDS for PostgreSQL.
C. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queue. Create another Multi-AZ Auto Scaling group for EC2 instances that host the application. Migrate the database to run on a Multi-AZ deployment of Amazon RDS for PostgreSQL.
D. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queue. Create another Multi-AZ Auto Scaling group for EC2 instances that host the application. Create a third Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database.
Answer: B
https://www.examtopics.com/discussions/amazon/view/85999-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
선택지는 활성/대기 인스턴스 쌍을 사용하는 A,B 와 대기열 호스팅 방식을 사용하는 C,D 로 나눠짐.
활성/대기 방식은 활성 인스턴스가 다운되어도 대기 인스턴스가 활성 인스턴스를 대체할 수 있으므로 가용성이 높은 방식. 따라서 A,B 둘 중 하나가 답.
PostgreSQL 데이터베이스를 사용하는 A 보다는 Amazon RDS for Postgre 를 사용하는 B 가 운영 오버헤드 절감 효과가 큼.
Amazon RDS 를 사용하면 클라우드에서 PostgreSQL 배포를 손쉽게 설정, 운영 및 확장할 수 있습니다. Amazon RDS 에서는 비용 효율적이고 크기 조정 가능한 하드웨어 용량을 갖춘 확장 가능한 PostgreSQL 을 몇 분 만에 배포할 수 있습니다. Amazon RDS 에서는 PostgreSQL 소프트웨어 설치 및 업그레이드, 스토리지 관리, 고가용성 및 읽기 처리량을

위한 복제, 재해 복구용 백업 등 복잡하고 시간 소모적인 관리 작업을 관리합니다.
https://aws.amazon.com/ko/rds/postgresql/

설명 2:
Amazon MQ 로 마이그레이션하면 대기열 관리의 오버헤드가 줄어듭니다. C 와 D 는 오답됩니다.
A 와 B 사이에서 결정한다는 것은 EC2 용 AutoScaling 그룹 또는 Postgress 용 RDS(모두 다중 AZ)로 이동하기로 결정하는 것을 의미합니다. RDS 옵션은 필요한 도구와 소프트웨어를 서비스로 제공하므로 운영에 미치는 영향이 적습니다. 예를 들어 읽기 복제본과 같은 추가 노드를 DB 에 추가하려는 노력을 고려하십시오.
https://docs.aws.amazon.com/amazon-mq/latest/developer-guide/activestandby-broker-deployment.html

Q139
A reporting team receives files each day in an Amazon S3 bucket. The reporting team manually reviews and copies the files from this initial S3 bucket to an analysis S3 bucket each day at the same time to use with Amazon QuickSight. Additional teams are starting to send more files in larger sizes to the initial S3 bucket.
The reporting team wants to move the files automatically analysis S3 bucket as the files enter the initial S3 bucket. The reporting team also wants to use AWS Lambda functions to run pattern-matching code on the copied data. In addition, the reporting team wants to send the data files to a pipeline in Amazon SageMaker Pipelines.
What should a solutions architect do to meet these requirements with the LEAST operational overhead?
A. Create a Lambda function to copy the files to the analysis S3 bucket. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s3:ObjectCreated:Put as the event type.
B. Create a Lambda function to copy the files to the analysis S3 bucket. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge (Amazon CloudWatch Events). Configure an ObjectCreated rule in EventBridge (CloudWatch Events). Configure Lambda and SageMaker Pipelines as targets for the rule.
C. Configure S3 replication between the S3 buckets. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s3:ObjectCreated:Put as the event type.
D. Configure S3 replication between the S3 buckets. Configure the analysis S3 bucket to

send event notifications to Amazon EventBridge (Amazon CloudWatch Events). Configure an ObjectCreated rule in EventBridge (CloudWatch Events). Configure Lambda and SageMaker Pipelines as targets for the rule.
Answer: D
https://www.examtopics.com/discussions/amazon/view/85872-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
S3 복제를 사용하면 S3 버킷 간에 자동으로 복제됩니다. S3 이벤트를 CloudWatch Events 에서 감지하여 특정 동작을 수행할 수 있습니다. Amazon S3 복제를 사용하면 S3 CRR(교차 리전 복제)을 사용하여 서로 다른 AWS 리전에서, 또는 S3 SRR(동일 리전 복제)을 사용하여 같은 AWS 리전 내의 버킷 간에 S3 객체를 자동으로 복제하도록 Amazon S3 를 구성할 수 있습니다. https://aws.amazon.com/ko/s3/features/replication/
Amazon S3 는 버킷에서 특정 이벤트가 발생할 때마다 Amazon EventBridge 에 이벤트를 보낼 수 있습니다. 이벤트 유형 : Object Created
https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/EventBridge.html)
Amazon EventBridge 는 Amazon SageMaker 의 상태 변경 이벤트를 모니터링합니다. EventBridge 를 사용하면 SageMaker 를 자동화하고 교육 작업 상태 변경 또는 끝점 상태 변경과 같은 이벤트에 자동으로 응답할 수 있습니다. 자동으로 트리거될 수 있는 작업의 몇 가지 예는 다음과 같습니다. AWS Lambda 함수 호출
https://docs.aws.amazon.com/sagemaker/latest/dg/automating-sagemaker-with-eventbridge.html

설명 2:
이 솔루션은 파일을 자동으로 이동하고, 복사된 데이터에서 Lambda 함수를 실행하고, 최소한의 운영 오버헤드로 데이터 파일을 SageMaker Pipelines 로 보내는 요구 사항을 충족합니다. S3 복제는 파일이 도착하면 초기 S3 버킷에서 분석 S3 버킷으로 파일을 복사할 수 있습니다. 분석 S3 버킷은 객체가 생성될 때 Amazon EventBridge(Amazon CloudWatch Events)에 이벤트 알림을 보낼 수 있습니다. EventBridge 는 Lambda 및 SageMaker 파이프라인을 ObjectCreated 규칙의 대상으로 트리거할 수 있습니다. Lambda 는 복사된 데이터에서 패턴 일치 코드를 실행할 수 있으며 SageMaker Pipelines 는 데이터 파일로 파이프라인을 실행할 수 있습니다.

S3 복제가 자동으로 수행할 수 있는 경우 분석 S3 버킷에 파일을 복사하는 Lambda 함수를 생성할 필요가 없기 때문에 옵션 A 는 올바르지 않습니다. 또한 Lambda 함수를 관리하기 위해 운영 오버헤드를 추가합니다.

S3 복제가 자동으로 수행할 수 있는 경우 분석 S3 버킷에 파일을 복사하는 Lambda 함수를 생성할 필요가 없기 때문에 옵션 B 는 올바르지 않습니다. 또한 Lambda 함수를 관리하기 위해 운영 오버헤드를 추가합니다.

여러 대상과 함께 S3 이벤트 알림을 사용하면 이벤트가 너무 많은 경우 제한 또는 전달 실패가 발생할 수 있으므로 옵션 C 는 올바르지 않습니다.

참조:
https://aws.amazon.com/ko/blogs/machine-learning/automate-feature-engineering-pipelines-with-amazon-sagemaker/
https://docs.aws.amazon.com/sagemaker/latest/dg/automating-sagemaker-with-eventbridge.html
https://aws.amazon.com/ko/about-aws/whats-new/2021/04/new-options-trigger-amazon-sagemaker-pipeline-executions/

Q140
A solutions architect needs to help a company optimize the cost of running an application on AWS. The application will use Amazon EC2 instances, AWS Fargate, and AWS Lambda for compute within the architecture.
The EC2 instances will run the data ingestion layer of the application. EC2 usage will be sporadic and unpredictable. Workloads that run on EC2 instances can be interrupted at any time. The application front end will run on Fargate, and Lambda will serve the API layer. The front-end utilization and API layer utilization will be predictable over the course of the next year.
Which combination of purchasing options will provide the MOST cost-effective solution for hosting this application? (Choose two)
A. Use Spot Instances for the data ingestion layer
B. Use On-Demand Instances for the data ingestion layer
C. Purchase a 1-year Compute Savings Plan for the front end and API layer.
D. Purchase 1-year All Upfront Reserved instances for the data ingestion layer.
E. Purchase a 1-year EC2 instance Savings Plan for the front end and API layer.
Answer: A, C
https://www.examtopics.com/discussions/amazon/view/86083-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
・EC2 인스턴스에서 실행되는 워크로드는 언제든지 중단될 수 있습니다 = 스팟 인스턴스
・프론트엔드 활용도와 API 계층 활용도는 내년에 예측할 수 있습니다 = Savings Plans
Savings Plans 는 1 년 또는 3 년 기간의 일정 사용량 약정(시간당 USD 요금으로 측정)을 조건으로 Amazon EC2, AWS Lambda 및 AWS Fargate 사용량에 대해 저렴한 요금을 제공하는 유연한 요금 모델입니다. Savings Plans 에 가입하면 약정 사용량까지 할인된 Savings Plans 요금을 적용받습니다.
https://aws.amazon.com/ko/savingsplans/compute-pricing/
・그 중에서도 Compute Savings Plans 가 정답.
Compute Savings Plans 는 최대 66%까지 비용을 절감할 수 있는 가장 유연한 요금 모델입니다. 이 플랜은 인스턴스 패밀리, 크기, AZ, 리전, OS 또는 테넌시와 관계없이 EC2 인스턴스 사용량에 적용되며, Fargate 또는 Lambda 사용량에도 적용됩니다.
https://aws.amazon.com/ko/savingsplans/compute-pricing/
정답은 A,C.

설명 2:
EC2 instance Savings Plan 은 72%, Compute Savings Plans 는 66%를 절약합니다. 그러나 링크에 따르면 "Compute Savings Plans 는 최고의 유연성을 제공하고 비용을 최대 66%까지 줄이는 데 도움이 됩니다.
이러한 요금제는 인스턴스 패밀리, 크기, AZ, 리전, OS 또는 테넌시에 관계없이 EC2 인스턴스 사용에 자동으로 적용되며 Fargate 및 Lambda 사용에도 적용됩니다." EC2 인스턴스 절약 계획은 Fargate 또는 Lambda 에 적용되지 않습니다.

Q141
A company runs a web-based portal that provides users with global breaking news, local alerts, and weather updates. The portal delivers each user a personalized view by using mixture of static and dynamic content. Content is served over HTTPS through an API server running on an Amazon EC2 instance behind an Application Load Balancer (ALB). The company wants the portal to provide this content to its users across the world as quickly as possible.
How should a solutions architect design the application to ensure the LEAST amount of latency for all users?
A. Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve all static and dynamic content by specifying the ALB as an origin.

B. Deploy the application stack in two AWS Regions. Use an Amazon Route 53 latency routing policy to serve all content from the ALB in the closest Region.
C. Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve the static content. Serve the dynamic content directly from the ALB.
D. Deploy the application stack in two AWS Regions. Use an Amazon Route 53 geolocation routing policy to serve all content from the ALB in the closest Region.
Answer: A
https://www.examtopics.com/discussions/amazon/view/85439-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
ALB 를 오리진으로 사용할 수 있음
원본이 하나 이상의 Amazon EC2 인스턴스에서 호스트되는 하나 이상의 HTTP 서버(웹 서버)인 경우 Application Load Balancer 를 사용하여 인스턴스에 트래픽을 분산할 수 있습니다. Application Load Balancer 를 CloudFront 의 원본으로 사용하는 방법에 대한 자세한 내용은
https://docs.aws.amazon.com/ko_kr/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html#concept_elb_origin

Q142
A gaming company is designing a highly available architecture. The application runs on a modified Linux kernel and supports only UDP-based traffic. The company needs the front-end tier to provide the best possible user experience. That tier must have low latency, route traffic to the nearest edge location, and provide static IP addresses for entry into the application endpoints.
What should a solutions architect do to meet these requirements?
A. Configure Amazon Route 53 to forward requests to an Application Load Balancer. Use AWS Lambda for the application in AWS Application Auto Scaling.
B. Configure Amazon CloudFront to forward requests to a Network Load Balancer. Use AWS Lambda for the application in an AWS Application Auto Scaling group.
C. Configure AWS Global Accelerator to forward requests to a Network Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.
D. Configure Amazon API Gateway to forward requests to an Application Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.
Answer: C

https://www.examtopics.com/discussions/amazon/view/86667-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
TCP/UDP+엔드포인트에 입력할 수 있는 고정 IP 주소를 가져야 한다는 대목에서 Global Accelerator 임을 유추할 수 있음.

설명 2:
AWS Global Accelerator 와 Amazon CloudFront 는 AWS 글로벌 네트워크와 전 세계 엣지 로케이션을 사용하는 별도의 서비스입니다. CloudFront 는 캐시 가능한 콘텐츠(예: 이미지 및 비디오)와 동적 콘텐츠(예: API 가속 및 동적 사이트 제공) 모두의 성능을 향상시킵니다. Global Accelerator 는 하나 이상의 AWS 리전에서 실행되는 애플리케이션에 대해 에지의 패킷을 프록시하여 TCP 또는 UDP 를 통해 광범위한 애플리케이션의 성능을 개선합니다. Global Accelerator 는 게임(UDP), IoT(MQTT) 또는 VoIP 와 같은 비 HTTP 사용 사례와 특히 고정 IP 주소 또는 결정론적이고 빠른 지역 장애 조치가 필요한 HTTP 사용 사례에 적합합니다. 두 서비스 모두 DDoS 보호를 위해 AWS Shield 와 통합됩니다.

Q143
A company wants to migrate its existing on-premises monolithic application to AWS. The company wants to keep as much of the front-end code and the backend code as possible. However, the company wants to break the application into smaller applications. A different team will manage each application. The company needs a highly scalable solution that minimizes operational overhead.
Which solution will meet these requirements?
A. Host the application on AWS Lambda. Integrate the application with Amazon API Gateway.
B. Host the application with AWS Amplify. Connect the application to an Amazon API Gateway API that is integrated with AWS Lambda.
C. Host the application on Amazon EC2 instances. Set up an Application Load Balancer with EC2 instances in an Auto Scaling group as targets.
D. Host the application on Amazon Elastic Container Service (Amazon ECS). Set up an Application Load Balancer with Amazon ECS as the target.
Answer: D
https://www.examtopics.com/discussions/amazon/view/86473-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
ECS 는 컨테이너화된 애플리케이션을 실행하기 위해 확장성이 뛰어난 관리형 환경을 제공하여 운영 오버헤드를 줄입니다. ECS 를 대상으로 ALB 를 설정하면 확장성과 가용성을 위해 애플리케이션의 여러 인스턴스에 트래픽을 분산할 수 있습니다. 이 솔루션을 사용하면 여러 팀이 각 애플리케이션을 독립적으로 관리하여 팀 자율성과 효율적인 개발을 촉진할 수 있습니다.
A 는 이벤트 기반 및 서버리스 워크로드에 더 적합합니다. 모놀리식 애플리케이션을 마이그레이션하고 기존 코드베이스를 유지 관리하는 데 이상적인 선택이 아닐 수 있습니다.
B 는 Lambda 및 API Gateway 와 통합되므로 애플리케이션을 더 작은 애플리케이션으로 분할하고 독립적으로 관리하는 데 필요한 유연성을 제공하지 못할 수 있습니다.
C 는 인프라 관리 및 수동 확장을 포함합니다. ECS 와 같은 컨테이너 서비스를 사용할 때보다 운영 오버헤드가 높아질 수 있습니다.

Q144
A company recently started using Amazon Aurora as the data store for its global ecommerce application. When large reports are run, developers report that the ecommerce application is performing poorly. After reviewing metrics in Amazon CloudWatch, a solutions architect finds that the ReadIOPS and CPUUtilizalion metrics are spiking when monthly reports run.
What is the MOST cost-effective solution?
A. Migrate the monthly reporting to Amazon Redshift.
B. Migrate the monthly reporting to an Aurora Replica.
C. Migrate the Aurora database to a larger instance class.
D. Increase the Provisioned IOPS on the Aurora instance.
Answer: B
https://www.examtopics.com/discussions/amazon/view/86781-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html
#Aurora.Replication.Replicas Aurora 복제본에는 두 가지 주요 목적이 있습니다. 애플리케이션에 대한 읽기 작업을 확장하기 위해 쿼리를 실행할 수 있습니다. 일반적으로 클러스터의 리더 엔드포인트에 연결하여 이를 수행합니다. 이렇게 하면 Aurora 는 클러스터에 있는 만큼 많은 Aurora 복제본에 읽기 전용 연결에 대한 로드를 분산시킬 수

있습니다. Aurora 복제본은 가용성을 높이는 데도 도움이 됩니다. 클러스터의 라이터 인스턴스를 사용할 수 없게 되면 Aurora 는 리더 인스턴스 중 하나를 자동으로 승격시켜 새 라이터로 대신합니다.
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.html

설명 2:
ReadIOPS 가 증가하고 있다고 했으므로 Aurora replica 를 통한 읽기 부하 분산 가능
"Aurora 는 클러스터에 있는 만큼의 Aurora 복제본에 읽기 전용 연결에 대한 로드를 분산할 수 있습니다.
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html#Aurora.Replication.Replicas

Q145
A company hosts a website analytics application on a single Amazon EC2 On-Demand Instance. The analytics software is written in PHP and uses a MySQL database. The analytics software, the web server that provides PHP, and the database server are all hosted on the EC2 instance. The application is showing signs of performance degradation during busy times and is presenting 5xx errors. The company needs to make the application scale seamlessly.
Which solution will meet these requirements MOST cost-effectively?
A. Migrate the database to an Amazon RDS for MySQL DB instance. Create an AMI of the web application. Use the AMI to launch a second EC2 On-Demand Instance. Use an Application Load Balancer to distribute the load to each EC2 instance.
B. Migrate the database to an Amazon RDS for MySQL DB instance. Create an AMI of the web application. Use the AMI to launch a second EC2 On-Demand Instance. Use Amazon Route 53 weighted routing to distribute the load across the two EC2 instances.
C. Migrate the database to an Amazon Aurora MySQL DB instance. Create an AWS Lambda function to stop the EC2 instance and change the instance type. Create an Amazon CloudWatch alarm to invoke the Lambda function when CPU utilization surpasses 75%.
D. Migrate the database to an Amazon Aurora MySQL DB instance. Create an AMI of the web application. Apply the AMI to a launch template. Create an Auto Scaling group with the launch template Configure the launch template to use a Spot Fleet. Attach an Application Load Balancer to the Auto Scaling group.
Answer: D
https://www.examtopics.com/discussions/amazon/view/86474-exam-aws-certified-solut

ions-architect-associate-saa-c03/

설명 1:
A(X) : 두 번째 온디맨드 인스턴스를 생성하기만 하고 Auto Scaling 설정을 안 하므로 확장성이 D 에 비해 떨어짐.
B(X) : Route 53 Weighted Routing 은 각 리소스로 라우팅되는 트래픽 양을 조절하는 기능 가중 라우팅을 사용하면 여러 리소스를 단일 도메인 이름(example.com) 또는 하위 도메인 이름(acme.example.com)과 연결하고 각 리소스로 라우팅되는 트래픽 양을 선택할 수 있습니다.
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy-weighted.html
C(X) : CloudWatch 경보는 임계값에 도달하면 자동으로 알림을 보내는 서비스.
""인스턴스 중 하나에 대한 CloudWatch 지표를 모니터링하는 CloudWatch 경보를 생성할 수 있습니다. 지표가 지정된 임계값에 도달하면 CloudWatch 에서 자동으로 알림을 보냅니다.
https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/using-cloudwatch-createalarm.html
D(O) : 스팟인스턴스라는 점이 걸리긴 하지만 어차피 인스턴스를 중지해서는 안 된다는 말이 나온 것도 아니고, Auto Scaling 이 명시되어있으므로 정답에 가장 가까움.

설명 2:
데이터베이스를 Amazon Aurora MySQL 로 마이그레이션합니다. 이렇게 하면 DB 가 자체적으로 확장됩니다. 조정할 필요 없이 자동으로 크기가 조정됩니다. 시작 템플릿을 사용하여 웹 앱의 AMI 를 생성합니다. 이렇게 하면 앱의 향후 인스턴스를 원활하게 생성할 수 있습니다. 그런 다음 Auto Scaling 그룹에 추가하면 수요에 따라 확장 및 축소되므로 비용을 절약할 수 있습니다.
스팟 집합을 사용하여 인스턴스를 시작합니다. 이것은 아마존이 적합하다고 판단하는 시점에 종료되는 비용으로 스팟 인스턴스가 크게 할인되기 때문에 질문의 "가장 비용 효율적인" 부분을 해결합니다. 이 부분에 대해서는 약간의 이견이 있기 때문이라고 생각합니다. 가장 비용 효율적이지만 아마존이 사용량이 많은 기간에 해당 스팟 인스턴스를 종료한다면 끔찍한 선택이 될 것입니다.

Q146
A company runs a stateless web application in production on a group of Amazon EC2 On-Demand Instances behind an Application Load Balancer. The application experiences

heavy usage during an 8-hour period each business day. Application usage is moderate and steady overnight. Application usage is low during weekends.
The company wants to minimize its EC2 costs without affecting the availability of the application.
Which solution will meet these requirements?
A. Use Spot Instances for the entire workload.
B. Use Reserved Instances for the baseline level of usage. Use Spot instances for any additional capacity that the application needs.
C. Use On-Demand Instances for the baseline level of usage. Use Spot Instances for any additional capacity that the application needs.
D. Use Dedicated Instances for the baseline level of usage. Use On-Demand Instances for any additional capacity that the application needs.
Answer: B
https://www.examtopics.com/discussions/amazon/view/86750-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A(X) : 계속 사용량이 있고, 사용량이 적은 주말에도 꾸준히 사용량은 나오고 있는데 계속 작동 중인 걸 스팟인스턴스로 둘 이유가 없음. 스팟 인스턴스는 중지해도 되는 인스턴스에 사용되는 인스턴스 유형. 사용량이 많은 시간을 예상할 수 있는 상황에선 예약 인스턴스가 적절.
B(O) : 상태 비저장 애플리케이션이라는 단서가 있으므로 추가 용량에 대해서는 스팟 인스턴스를 사용하여 비용 절감 가능.
C(X) : 기본 사용량 수준은 예상할 수 있으므로 예약 인스턴스가 적절.
D(X) : Dedicated Instance 는 온디맨드에 비해서도 비용이 많이 들어가는 인스턴스 유형임. 해당 부분에 대해서는 아래의 링크를 참고할 것.
https://aws.amazon.com/ko/ec2/pricing/on-demand/
https://aws.amazon.com/ko/ec2/pricing/dedicated-instances/

Q147
A company needs to retain application log files for a critical application for 10 years. The application team regularly accesses logs from the past month for troubleshooting, but logs older than 1 month are rarely accessed. The application generates more than 10 TB of logs per month.
Which storage option meets these requirements MOST cost-effectively?

A. Store the logs in Amazon S3. Use AWS Backup to move logs more than 1 month old to S3 Glacier Deep Archive.
B. Store the logs in Amazon S3. Use S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive.
C. Store the logs in Amazon CloudWatch Logs. Use AWS Backup to move logs more than 1 month old to S3 Glacier Deep Archive.
D. Store the logs in Amazon CloudWatch Logs. Use Amazon S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive.
Answer: B
https://www.examtopics.com/discussions/amazon/view/86864-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A(X) : Life Cycle Policy 를 사용하면 되는데 굳이 AWS Backup 까지 동원할 필요가 없음.
B(O) : 정답. 한 달 후에 로그를 보관하려면 S3 가 필요합니다. CloudWatch Logs 로는 그렇게 할 수 없습니다.
C(X) : CloudWatch Logs 는 스토리지 서비스가 아님.
D(X) : C 와 같은 이유로 오답.

Q148
A company has a data ingestion workflow that includes the following components:
* An Amazon Simple Notation Service (Amazon SNS) topic that receives notifications about new data deliveries.
* An AWS Lambda function that processes and stores the data.
The ingestion workflow occasionally fails because of network connectivity issues. When tenure occurs the corresponding data is not ingested unless the company manually reruns the job.
What should a solutions architect do to ensure that all notifications are eventually processed?
A. Configure the Lambda function for deployment across multiple Availability Zones.
B. Modify the Lambda function's configuration to increase the CPU and memory allocations for the function.
C. Configure the SNS topic's retry strategy to increase both the number of retries and the wait time between retries.
D. Configure an Amazon Simple Queue Service (Amazon SQS) queue as the on-failure

destination. Modify the Lambda function to process messages in the queue.
Answer: D
https://www.examtopics.com/discussions/amazon/view/85424-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
실패한 메시지를 보관할 SQS 대기열이 필요. 정답은 D.
https://docs.aws.amazon.com/ko_kr/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html
C 같은 경우엔 재시도 전략인데, 'When tenure occurs the corresponding data is not ingested unless company manually reruns the job' (Tenure 가 발생하면 회사에서 수동으로 작업을 다시 실행하지 않는 한 해당 데이터가 수집되지 않습니다.) 라는 대목이 있으므로 C 는 오답. Amazon SNS 가 메시지 전송을 재시도하는 방식이 전송 정책에 따라 결정됩니다. 전송 정책이 소진되면 Amazon SNS 는 전송 재시도를 중지하고 배달 못한 편지 대기열이 구독에 연결되어 있지 않는 한 메시지를 삭제합니다.
https://docs.aws.amazon.com/ko_kr/sns/latest/dg/sns-message-delivery-retries.html

참고:
https://docs.aws.amazon.com/ko_kr/sns/latest/dg/sns-dead-letter-queues.html

Q149
A company has a service that produces event data. The company wants to use AWS to process the event data as it is received. The data is written in a specific order that must be maintained throughout processing. The company wants to implement a solution that minimizes operational overhead.
How should a solutions architect accomplish this?
A. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue.
B. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an AWS Lambda function as a subscriber.
C. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to hold messages. Set up an AWS Lambda function to process messages from the queue independently.
D. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an Amazon Simple Queue Service (Amazon SQS)

queue as a subscriber.
Answer: A
https://www.examtopics.com/discussions/amazon/view/86784-exam-aws-certified-solutions-architect-associate-saa-c03/

설명
자세한 내용은 아래 URL.
https://docs.aws.amazon.com/ko_kr/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html
FIFO(First-In-First-Out) 대기열은 작업 및 이벤트 순서가 중요하거나 중복을 허용할 수 없는 경우 애플리케이션 간의 메시징을 향상하도록 설계되었습니다. FIFO 대기열을 사용할 수 있는 상황의 예는 다음과 같습니다. 사용자가 입력한 명령이 올바른 순서로 실행되도록 합니다. 올바른 순서로 가격 수정을 전송하여 올바른 제품 가격을 표시합니다. 학생이 계정을 등록하기 전에 코스에 등록하지 못하도록 합니다.

Q150
A company is migrating an application from on-premises servers to Amazon EC2 instances. As part of the migration design requirements, a solutions architect must implement infrastructure metric alarms. The company does not need to take action if CPU utilization increases to more than 50% for a short burst of time. However, if the CPU utilization increases to more than 50% and read IOPS on the disk are high at the same time, the company needs to act as soon as possible. The solutions architect also must reduce false alarms.
What should the solutions architect do to meet these requirements?
A. Create Amazon CloudWatch composite alarms where possible.
B. Create Amazon CloudWatch dashboards to visualize the metrics and react to issues quickly.
C. Create Amazon CloudWatch Synthetics canaries to monitor the application and raise an alarm.
D. Create single Amazon CloudWatch metric alarms with multiple metric thresholds where possible.
Answer: A
https://www.examtopics.com/discussions/amazon/view/86034-exam-aws-certified-solutions-architect-associate-saa-c03/

설명
자세한 내용은 아래 URL.
https://docs.aws.amazon.com/ko_kr/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html
FIFO(First-In-First-Out) 대기열은 작업 및 이벤트 순서가 중요하거나 중복을 허용할 수 없는 경우 애플리케이션 간의 메시징을 향상하도록 설계되었습니다. FIFO 대기열을 사용할 수 있는 상황의 예는 다음과 같습니다. 사용자가 입력한 명령이 올바른 순서로 실행되도록 합니다. 올바른 순서로 가격 수정을 전송하여 올바른 제품 가격을 표시합니다. 학생이 계정을 등록하기 전에 코스에 등록하지 못하도록 합니다.

Q151
A company wants to migrate its on-premises data center to AWS. According to the company's compliance requirements, the company can use only the ap-northeast-3 Region. Company administrators are not permitted to connect VPCs to the internet.
Which solutions will meet these requirements? (Choose two)
A. Use AWS Control Tower to implement data residency guardrails to deny internet access and deny access to all AWS Regions except ap-northeast-3.
B. Use rules in AWS WAF to prevent internet access. Deny access to all AWS Regions except ap-northeast-3 in the AWS account settings.
C. Use AWS Organizations to configure service control policies (SCPS) that prevent VPCs from gaining internet access. Deny access to all AWS Regions except ap-northeast-3.
D. Create an outbound rule for the network ACL in each VPC to deny all traffic from 0.0.0.0/0. Create an IAM policy for each user to prevent the use of any AWS Region other than ap-northeast-3.
E. Use AWS Config to activate managed rules to detect and alert for internet gateways and to detect and alert for new resources deployed outside of ap-northeast-3.
Answer: A, C
https://www.examtopics.com/discussions/amazon/view/86475-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A(O) : AWS Control Tower Guardrail 을 사용해 SCP 를 통한 AWS API 액세스를 제한하여 특정 AWS 리전에서의 특정 리소스 방지 가능.
오늘부터 AWS Control Tower 를 사용하여 가드레일 이라고 하는 데이터 상주 예방 및 탐지 제어를 배포할 수 있습니다 . 이러한 가드레일은 서비스 제어 정책(SCP) 을 통해 AWS

API 에 대한 액세스를 제한하여 원치 않는 AWS 리전에서 리소스 프로비저닝을 방지합니다. 예를 들어 독일의 AWS 고객은 AWS Identity and Access Management(IAM) 및 AWS Organizations 와 같은 글로벌 서비스를 제외하고 프랑크푸르트 이외의 지역에서 AWS 서비스에 대한 액세스를 거부할 수 있습니다. 또한 AWS Control Tower 는 Amazon Simple Storage Service(Amazon S3) 교차 리전 복제 차단 또는 인터넷 게이트웨이 생성 차단과 같은 기본 AWS 서비스 옵션의 데이터 상주를 추가로 제어하기 위한 가드레일을 제공합니다.
https://aws.amazon.com/blogs/aws/new-for-aws-control-tower-region-deny-and-guardrails-to-help-you-meet-data-residency-requirements/
B(X) : AWS WAF 는 Web ACL 을 통해 특정 국가나 지리적 위치, IP 의 요청을 차단할 수 있으나 리전을 차단하는 옵션은 없음.
https://aws.amazon.com/ko/premiumsupport/knowledge-center/waf-allow-block-country-geolocation/)(https://aws.amazon.com/ko/premiumsupport/knowledge-center/waf-allow-my-ip-block-other-ip/
C(O) : AWS Organizations 를 사용해 특정 리전에 대한 액세스 차단 가능.
이 SCP 는 지정된 리전 외부의 모든 작업에 대한 액세스를 거부합니다. 이 정책은 Deny 효과를 사용하여 승인된 두 리전(eu-central-1 및 eu-west-1) 중 하나를 대상으로 하지 않는 작업에 대한 모든 요청에 대한 액세스를 거부합니다.
https://docs.aws.amazon.com/ko_kr/organizations/latest/userguide/orgs_manage_policies_scps_examples_general.html
D(X) : NACL 0.0.0.0/0 의 아웃바운드 트래픽을 막아버리면 트래픽이 외부로 나갈 수 없어 아예 통신 자체가 안 됨. IAM 정책으로 다른 AWS 리전의 다른 리소스에 대한 액세스를 막는 것은 가능.
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_deny-requested-region.html
E(X) : AWS Config 는 리소스 구성 변경 사항을 감지하고 해당 구성 변경 기록 파일을 전송할 수 있는 서비스로 지문의 요구사항에는 부합하지 않음.

Q152
A company uses a three-tier web application to provide training to new employees. The application is accessed for only 12 hours every day. The company is using an Amazon RDS for MySQL DB instance to store information and wants to minimize costs.
What should a solutions architect do to meet these requirements?
A. Configure an IAM policy for AWS Systems Manager Session Manager. Create an IAM role for the policy. Update the trust relationship of the role. Set up automatic start and stop for

the DB instance.
B. Create an Amazon ElastiCache for Redis cache cluster that gives users the ability to access the data from the cache when the DB instance is stopped. Invalidate the cache after the DB instance is started.
C. Launch an Amazon EC2 instance. Create an IAM role that grants access to Amazon RDS. Attach the role to the EC2 instance. Configure a cron job to start and stop the EC2 instance on the desired schedule.
D. Create AWS Lambda functions to start and stop the DB instance. Create Amazon EventBridge (Amazon CloudWatch Events) scheduled rules to invoke the Lambda functions. Configure the Lambda functions as event targets for the rules.
Answer: D
https://www.examtopics.com/discussions/amazon/view/86046-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : 권한에 대한 언급이 없는데 굳이 IAM 을 사용할 이유가 없음.
B(X) : ElastiCache 는 웹 애플리케이션과 DB 간의 캐시 서비스.
C(X) : A 와 같은 이유로 오답.
D(O) : EC2 인스턴스를 자동으로 중지 및 시작하여 Amazon Elastic Compute Cloud(Amazon EC2) 사용량을 줄이려고 합니다. 이를 위해 AWS Lambda 및 Amazon EventBridge 를 사용하려면 어떻게 해야 하나요?
이하의 항목 참고
https://aws.amazon.com/ko/premiumsupport/knowledge-center/start-stop-lambda-eventbridge/

설명 2:
일반적인 개발 환경에서 개발 및 테스트 데이터베이스는 대부분 하루 8 시간 동안 사용되며 사용하지 않을 때는 유휴 상태입니다. 그러나 데이터베이스에는 이 유휴 시간 동안 컴퓨팅 및 스토리지 비용이 청구됩니다. 전체 비용을 줄이기 위해 Amazon RDS 에서는 인스턴스를 일시적으로 중지할 수 있습니다. 인스턴스가 중지된 동안에는 스토리지 및 백업에 대한 요금이 부과되지만 DB 인스턴스 시간에 대한 요금은 부과되지 않습니다. 중지된 인스턴스는 7 일 후에 자동으로 시작됩니다. 이 게시물은 컴퓨팅 비용을 절감하기 위해 특정 태그로 유휴 데이터베이스를 중지 및 시작하도록 Lambda 함수를 예약할 수 있는 AWS Lambda 및 Amazon EventBridge 를 사용하는 솔루션을 제시합니다. 두 번째 게시물은 AWS Systems Manager 를 사용하여 유휴 Amazon RDS 데이터베이스의 중지 및 시작을 수행하는 솔루션을 제시합니다.

Q153

A company sells ringtones created from clips of popular songs. The files containing the ringtones are stored in Amazon S3 Standard and are at least 128 KB in size. The company has millions of files, but downloads are infrequent for ringtones older than 90 days. The company needs to save money on storage while keeping the most accessed files readily available for its users.

Which action should the company take to meet these requirements MOST cost-effectively?

A. Configure S3 Standard-Infrequent Access (S3 Standard-IA) storage for the initial storage tier of the objects.

B. Move the files to S3 Intelligent-Tiering and configure it to move objects to a less expensive storage tier after 90 days.

C. Configure S3 inventory to manage objects and move them to S3 Standard-Infrequent Access (S3 Standard-1A) after 90 days.

D. Implement an S3 Lifecycle policy that moves the objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-1A) after 90 days.

Answer: D

https://www.examtopics.com/discussions/amazon/view/86933-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

A(X) : 초기에는 사용량이 많으므로 S3 Standard 가 적절.

B(X) : 90 일 이상된 벨소리는 다운로드가 드물다고 했으므로 부적절.

C(X) : Amazon S3 Inventory 는 Amazon S3 에서 스토리지 관리를 지원하기 위해 제공하는 도구 중 하나로, 이 인벤토리를 사용하여 비즈니스, 규정 준수 및 규제 요건에 대한 객체의 복제 및 암호화 상태를 감사하고 보고할 수 있습니다. 또한 Amazon S3 동기식 List API 작업의 대안으로 Amazon S3 인벤토리를 사용하면 비즈니스 워크플로 및 빅 데이터 업무를 단순화하고 속도를 높일 수 있습니다.

https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/storage-inventory.html

D(O) : 90 일 이전에는 S3 Standard 로 빈번한 액세스 처리, 90 일 이후에는 다운로드가 드물지만 가장 많이 액세스하는 일부 파일은 쉽게 사용, 즉 빠르게 액세스할 수 있어야 하므로 액세스 소요 시간이 적은 S3 Standard-IA 사용이 적절.

설명 2:

이 솔루션은 사용자가 가장 많이 액세스하는 파일을 쉽게 사용할 수 있도록 유지하면서

스토리지 비용을 절약해야 하는 요구 사항을 충족합니다. S3 수명 주기 정책은 사전 정의된 규칙에 따라 한 스토리지 클래스에서 다른 스토리지 클래스로 객체를 자동으로 이동할 수 있습니다. S3 Standard-IA 는 자주 액세스하지 않지만 필요할 때 신속하게 액세스해야 하는 데이터를 위한 저비용 스토리지 클래스입니다. 드물게 다운로드되는 90 일 이상의 벨소리에 적합합니다.

객체의 초기 스토리지 계층에 대해 S3 Standard-IA 를 구성하면 빈번한 액세스 및 검색 요금으로 더 많은 비용이 발생할 수 있으므로 옵션 A 는 올바르지 않습니다.

파일을 S3 Intelligent-Tiering 으로 이동하면 90 일보다 오래된 벨소리에는 필요하지 않을 수 있는 추가 모니터링 및 자동화 요금이 발생할 수 있으므로 옵션 B 는 올바르지 않습니다.

옵션 C 는 올바르지 않습니다. S3 인벤토리를 사용하여 객체를 관리하고 객체를 S3 Standard-IA 로 이동하는 것은 복잡하고 시간이 많이 소요될 수 있으며 자동 비용 절감을 제공하지 않기 때문입니다.
참조:
https://aws.amazon.com/s3/storage-classes/
https://aws.amazon.com/s3/cloud-storage-cost-optimization-ebook/

Q154
A company needs to save the results from a medical trial to an Amazon S3 repository. The repository must allow a few scientists to add new files and must restrict all other users to read-only access. No users can have the ability to modify or delete any files in the repository. The company must keep every file in the repository for a minimum of 1 year after its creation date.
Which solution will meet these requirements?
A. Use S3 Object Lock in governance mode with a legal hold of 1 year.
B. Use S3 Object Lock in compliance mode with a retention period of 365 days.
C. Use an IAM role to restrict all users from deleting or changing objects in the S3 bucket. Use an S3 bucket policy to only allow the IAM role.
D. Configure the S3 bucket to invoke an AWS Lambda function every time an object is added. Configure the function to track the hash of the saved object so that modified objects can be marked accordingly.
Answer: B
https://www.examtopics.com/discussions/amazon/view/86359-exam-aws-certified-solut

ions-architect-associate-saa-c03/

설명 1:
S3 객체 수정 및 삭제 방지 = S3 Object Lock.
S3 객체 잠금을 사용하면 write once, read many(WORM) 모델을 사용하여 객체를 저장할 수 있습니다. 객체 잠금은 고정된 시간 동안 또는 무기한으로 객체의 삭제 또는 덮어쓰기를 방지하는 데 도움이 될 수 있습니다. 보관 기간은 정해진 시간 동안 객체 버전을 보호합니다. 객체 버전에 보관 기간을 설정하면 Amazon S3 는 객체 버전의 메타데이터에 타임스탬프를 저장하여 보관 기간이 만료되는 시점을 표시합니다. 보관 기간이 만료된 후 객체 버전에 법적 보존을 설정하지 않는 한 객체 버전을 덮어쓰거나 삭제할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/object-lock-overview.html#object-lock-retention-periods

설명 2:
규정 준수 모드에서는 AWS 계정의 루트 사용자를 포함하여 어떤 사용자도 보호 객체 버전을 덮어쓰거나 삭제할 수 없습니다. 객체가 규정 준수 모드에서 잠겨 있으면 보관 모드를 변경할 수 없으며 보관 기간을 단축할 수 없습니다. 규정 준수 모드는 보존 기간 동안 개체 버전을 덮어쓰거나 삭제할 수 없도록 합니다. 거버넌스 모드에서 사용자는 특별한 권한이 없는 한 개체 버전을 덮어쓰거나 삭제할 수 없으며 잠금 설정을 변경할 수 없습니다. 거버넌스 모드를 사용하면 대부분의 사용자가 개체를 삭제하지 못하도록 보호하지만 필요한 경우 일부 사용자에게 보존 설정을 변경하거나 개체를 삭제할 수 있는 권한을 계속 부여할 수 있습니다. 거버넌스 모드에서는 특수 권한이 있는 일부 사용자가 개체를 삭제할 수 있으며 이는 요구 사항에 위배됩니다.
규정 준수:
- 객체 버전은 루트 사용자를 포함한 모든 사용자가 덮어쓰거나 삭제할 수 없습니다.
- 개체 보존 모드를 변경할 수 없으며 보존 기간을 단축할 수 없습니다. 거버넌스:
- 대부분의 사용자는 개체 버전을 덮어쓰거나 삭제할 수 없으며 잠금 설정을 변경할 수 없습니다.
- 일부 사용자는 보존을 변경하거나 개체를 삭제할 수 있는 특별한 권한이 있습니다.

Q155
A large media company hosts a web application on AWS. The company wants to start caching confidential media files so that users around the world will have reliable access to the files. The content is stored in Amazon S3 buckets. The company must deliver the content quickly, regardless of where the requests originate geographically.

Which solution will meet these requirements?
A. Use AWS DataSync to connect the S3 buckets to the web application.
B. Deploy AWS Global Accelerator to connect the S3 buckets to the web application.
C. Deploy Amazon CloudFront to connect the S3 buckets to CloudFront edge servers.
D. Use Amazon Simple Queue Service (Amazon SQS) to connect the S3 buckets to the web application.
Answer: C
https://www.examtopics.com/discussions/amazon/view/86795-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
S3 버킷에 저장 + 요청이 지리적으로 어디에서 발생했는지에 관계없이 콘텐츠를 신속하게 제공 = S3 + CloudFront. 답은 C.

설명 2:
CloudFront 는 로컬 캐시를 사용하여 응답을 제공하고, AWS Global Accelerator 는 요청을 프록시하고 응답을 위해 항상 애플리케이션에 연결합니다.

Q156
A company produces batch data that comes from different databases. The company also produces live stream data from network sensors and application APIs. The company needs to consolidate all the data into one place for business analytics. The company needs to process the incoming data and then stage the data in different Amazon S3 buckets. Teams will later run one-time queries and import the data into a business intelligence tool to show key performance indicators (KPIs).
Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two)
A. Use Amazon Athena for one-time queries. Use Amazon QuickSight to create dashboards for KPIs.
B. Use Amazon Kinesis Data Analytics for one-time queries. Use Amazon QuickSight to create dashboards for KPIs.
C. Create custom AWS Lambda functions to move the individual records from the databases to an Amazon Redshift cluster.
D. Use an AWS Glue extract, transform, and load (ETL) job to convert the data into JSON format. Load the data into multiple Amazon OpenSearch Service (Amazon Elasticsearch

Service) clusters.
E. Use blueprints in AWS Lake Formation to identify the data that can be ingested into a data lake. Use AWS Glue to crawl the source, extract the data, and load the data into Amazon S3 in Apache Parquet format.
Answer: A, E
https://www.examtopics.com/discussions/amazon/view/85770-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
KPI 로 표시하기 위해선 Athena 가 필요하고, Athena 는 S3 에 쿼리함. 따라서 KPI 만 기억해도 A,E 가 정답임을 쉽게 유추할 수 있음.
・데이터베이스에서 가져온 배치 데이터와 네트워크 센서 및 애플리케이션 API 에서 생성한 라이브 스트림 데이터를 한 곳에 모은다고 했으므로 형식이 다른 데이터를 한 곳에 모을 때 적절한 AWS LakeFormation 이 필요.
・그리고 AWS Glue 는 Amazon S3 데이터 레이크의 필수 구성 요소이며 최신 데이터 분석을 위한 데이터 카탈로그 및 변환 서비스 제공
https://aws.amazon.com/ko/blogs/korea/build-a-data-lake-foundation-with-aws-glue-and-amazon/
・AWS Glue 는 Athena 에서 쿼리 가능한 Parquet 파일을 쓸 수 있음.
AWS Glue 를 사용하여 Amazon S3 와 스트리밍 소스에서 Parquet 파일을 읽을 수 있을 뿐만 아니라 Amazon S3 에 Parquet 파일을 쓸 수 있습니다.
https://docs.aws.amazon.com/ko_kr/glue/latest/dg/aws-glue-programming-etl-format-parquet-home.html
Amazon Athena 에서 사용할 수 있는 Apache Parquet
https://aws.amazon.com/ko/blogs/korea/build-a-data-lake-foundation-with-aws-glue-and-amazon/
・S3 버킷에 있는 데이터를 Athena 로 쿼리 가능
Amazon Athena 는 표준 SQL 을 사용하여 Amazon S3(Amazon Simple Storage Service)에 있는 데이터를 직접 간편하게 분석할 수 있는 대화형 쿼리 서비스입니다.
https://docs.aws.amazon.com/ko_kr/athena/latest/ug/what-is.html
・QuickSight 로 KPI 표시 가능
https://docs.aws.amazon.com/ko_kr/quicksight/latest/user/kpi.html

설명 2:
Amazon Athena 는 스트리밍 데이터에 대한 일회성 쿼리를 실행하기 위한 최상의 선택입니다.

Amazon Kinesis Data Analytics 는 스트리밍 데이터를 실시간으로 분석할 수 있는 쉽고 친숙한 표준 SQL 언어를 제공하지만 일회성 쿼리가 아닌 지속적인 쿼리를 위해 설계되었습니다. 반면 Amazon Athena 는 SQL 을 사용하여 Amazon S3 의 데이터를 쿼리할 수 있는 서버리스 대화형 쿼리 서비스입니다. 임시 쿼리에 최적화되어 있으며 스트리밍 데이터에 대한 일회성 쿼리를 실행하는 데 이상적입니다.
AWS Lake Formation 은 분석 목적으로 모든 데이터를 보관하는 중앙 위치로 사용합니다. Athena 는 S3 와 완벽하게 통합되며 쿼리를 만들 수 있습니다.

Q157
A company stores data in an Amazon Aurora PostgreSQL DB cluster. The company must store all the data for 5 years and must delete all the data after 5 years. The company also must indefinitely keep audit logs of actions that are performed within the database. Currently, the company has automated backups configured for Aurora.
Which combination of steps should a solutions architect take to meet these requirements? (Choose two)
A. Take a manual snapshot of the DB cluster.
B. Create a lifecycle policy for the automated backups.
C. Configure automated backup retention for 5 years.
D. Configure an Amazon CloudWatch Logs export for the DB cluster.
E. Use AWS Backup to take the backups and to keep the backups for 5 years.
Answer: D, E
https://www.examtopics.com/discussions/amazon/view/87629-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이전에는 특히 AWS 서비스 전체에서 백업을 조정할 때 수동 Aurora 클러스터 스냅샷에 대한 백업 일정을 자동화하거나 보존 정책을 적용하거나 백업 활동을 통합하기 위해 사용자 지정 스크립트를 생성해야 했습니다. AWS Backup 을 사용하면 스냅샷 예약 및 스냅샷 보존 관리 기능이 있는 완전 관리형 정책 기반 백업 솔루션을 얻을 수 있습니다. 이제 PostgreSQL 호환 및 MySQL 호환 Aurora 버전 모두에 대해 AWS Backup 콘솔에서 직접 Aurora 백업을 생성, 관리 및 복원할 수 있습니다.
시작하려면 AWS Backup 콘솔에서 Amazon Aurora 클러스터를 선택하고 온디맨드 백업을 수행하거나 클러스터를 백업 계획에 할당하기만 하면 됩니다.

Q158

A solutions architect is optimizing a website for an upcoming musical event. Videos of the performances will be streamed in real time and then will be available on demand. The event is expected to attract a global online audience.

Which service will improve the performance of both the real-time and on-demand streaming?

A. Amazon CloudFront

B. AWS Global Accelerator

C. Amazon Route 53

D. Amazon S3 Transfer Acceleration

Answer: A

https://www.examtopics.com/discussions/amazon/view/87514-exam-aws-certified-solutions-architect-associate-saa-c03/

설명

CloudFront 를 사용하여 모든 HTTP 오리진을 사용하여 주문형 비디오(VOD) 또는 라이브 스트리밍 비디오를 제공할 수 있습니다.

클라우드에서 비디오 워크플로를 설정할 수 있는 한 가지 방법은 CloudFront 를 AWS Media Services 와 함께 사용하는 것입니다.

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streamingvideo.html

Q159

A company is running a publicly accessible serverless application that uses Amazon API Gateway and AWS Lambda. The application's traffic recently spiked due to fraudulent requests from botnets.

Which steps should a solutions architect take to block requests from unauthorized users? (Choose two)

A. Create a usage plan with an API key that is shared with genuine users only.

B. Integrate logic within the Lambda function to ignore the requests from fraudulent IP addresses.

C. Implement an AWS WAF rule to target malicious requests and trigger actions to filter them out.

D. Convert the existing public API to a private API. Update the DNS records to redirect users to the new API endpoint.

E. Create an IAM role for each user attempting to access the API. A user will assume the role when making the API call.
Answer: A, C
https://www.examtopics.com/discussions/amazon/view/87516-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
API 사용 계획을 WAF 로 보완 가능. ""비용을 제어하거나 API 에 대한 액세스를 차단하기 위해 사용량 계획 할당량 또는 조절에 의존하지 마십시오. AWS Budget 을 사용하여 비용을 모니터링하고 AWS WAF 를 사용하여 API 요청을 관리하는 것을 고려하십시오.
https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html
A(O) : 애플리케이션 요청, 즉 API 요청을 함부로 하지 못하도록 하는 것이므로 A 는 정답.
C(O) : 애플리케이션 계층 방어이고 봇넷 방어이므로 WAF 가 있는 C 는 정답
(https://aws.amazon.com/ko/waf/getting-started/)
E(X) : 공개적으로 사용가능한 서버리스 애플리케이션이라는 단서 때문에 제외됨.

Q160
An ecommerce company hosts its analytics application in the AWS Cloud. The application generates about 300 MB of data each month. The data is stored in JSON format. The company is evaluating a disaster recovery solution to back up the data. The data must be accessible in milliseconds if it is needed, and the data must be kept for 30 days.
Which solution meets these requirements MOST cost-effectively?
A. Amazon OpenSearch Service (Amazon Elasticsearch Service)
B. Amazon S3 Glacier
C. Amazon S3 Standard
D. Amazon RDS for PostgreSQL
Answer: C
https://www.examtopics.com/discussions/amazon/view/87632-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : Amazon OpenSerach Service 는 분석 및 모니터링 서비스인데 이미 회사에서 분석 애플리케이션을 따로 사용 중이므로 데이터를 저장하는 서비스만 필요한 상황이라 필요가 없음. Amazon OpenSearch Service 는 AWS 클라우드에서 OpenSearch 클러스터를 손쉽게

배포, 운영 및 확장할 수 있도록 해주는 관리형 서비스입니다. OpenSearch 는 로그 분석, 실시간 애플리케이션 모니터링, 클릭 스트림 분석 같은 사용 사례를 위한 완전한 오픈 소스 검색 및 분석 엔진입니다.
https://docs.aws.amazon.com/ko_kr/opensearch-service/latest/developerguide/what-is.html
B(X) : 아무리 빨라봤자 액세스 타임이 1 분 정도 걸림.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/restoring-objects-retrieval-options.html
C(O) : S3 + Life Cycle Policy 조합으로 밀리초 단위 액세스와 30 일간 보관 조건 충족 가능
https://aws.amazon.com/ko/s3/storage-classes/)(https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/object-lifecycle-mgmt.html
D(X) : 데이터베이스는 데이터를 수집하여 다른 서비스에 이용할 목적으로 사용하는 것이지, 특정 기간만 보관해두고자 하는 용도가 아님. 지문에서는 회사가 이미 분석 애플리케이션을 가지고 있는데다가 원하는 건 분석 애플리케이션으로 생성한 데이터를 보관할 곳을 찾는 것임. 따라서 C 가 더 적합.

설명 2:
이 솔루션은 분석 애플리케이션에서 생성되고 JSON 형식으로 저장되는 데이터를 백업하기 위한 재해 복구 솔루션의 요구 사항을 충족하며 필요한 경우 밀리초 내에 액세스할 수 있어야 합니다. Amazon S3 Standard 는 자주 액세스하는 데이터를 위한 내구성 있고 확장 가능한 스토리지 클래스입니다. 모든 양의 데이터를 저장할 수 있고 고가용성과 성능을 제공할 수 있습니다. 또한 데이터 검색을 위한 밀리초 액세스 시간을 지원할 수 있습니다.
Amazon OpenSearch Service(Amazon Elasticsearch Service)는 데이터를 인덱싱하고 쿼리할 수 있는 검색 및 분석 서비스이지만 JSON 형식으로 저장된 데이터에 대한 백업 솔루션이 아니기 때문에 옵션 A 는 올바르지 않습니다.
옵션 B 는 Amazon S3 Glacier 가 데이터 보관 및 장기 백업을 위한 저비용 스토리지 클래스이지만 데이터 검색을 위한 밀리초 액세스 시간을 지원하지 않기 때문에 정답이 아닙니다.
PostgreSQL 용 Amazon RDS 는 구조화된 데이터를 저장하고 쿼리할 수 있는 관계형 데이터베이스 서비스이지만 JSON 형식으로 저장된 데이터에 대한 백업 솔루션이 아니기 때문에 옵션 D 는 올바르지 않습니다.

참조:
https://aws.amazon.com/s3/storage-classes/
https://aws.amazon.com/s3/faqs/#Durability_and_data_protection

Q161

A company has a small Python application that processes JSON documents and outputs the results to an on-premises SQL database. The application runs thousands of times each day. The company wants to move the application to the AWS Cloud. The company needs a highly available solution that maximizes scalability and minimizes operational overhead.

Which solution will meet these requirements?

A. Place the JSON documents in an Amazon S3 bucket. Run the Python code on multiple Amazon EC2 instances to process the documents. Store the results in an Amazon Aurora DB cluster.

B. Place the JSON documents in an Amazon S3 bucket. Create an AWS Lambda function that runs the Python code to process the documents as they arrive in the S3 bucket. Store the results in an Amazon Aurora DB cluster.

C. Place the JSON documents in an Amazon Elastic Block Store (Amazon EBS) volume. Use the EBS Multi-Attach feature to attach the volume to multiple Amazon EC2 instances. Run the Python code on the EC2 instances to process the documents. Store the results on an Amazon RDS DB instance.

D. Place the JSON documents in an Amazon Simple Queue Service (Amazon SQS) queue as messages. Deploy the Python code as a container on an Amazon Elastic Container Service (Amazon ECS) cluster that is configured with the Amazon EC2 launch type. Use the container to process the SQS messages. Store the results on an Amazon RDS DB instance.

Answer: B

https://www.examtopics.com/discussions/amazon/view/87633-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

Lambda 를 사용하면 서버를 관리하고 프로비저닝할 필요가 없으므로 확장성이 보장되고 운영 오버헤드가 최소화됩니다. S3 는 JSON 문서를 위한 내구성 있고 가용성이 높은 스토리지를 제공합니다. Lambda 는 새 문서가 S3 버킷에 추가될 때마다 자동으로 트리거되어 실시간 처리가 가능합니다. 결과를 Aurora DB 클러스터에 저장하면 처리된 데이터의 고가용성과 확장성이 보장됩니다. 이 솔루션은 서버리스 아키텍처를 활용하여 인프라를 관리할 필요 없이 자동 확장 및 고가용성을 허용하므로 가장 적합한 선택입니다.

A. 이 옵션을 사용하려면 EC2 인스턴스를 수동으로 관리하고 확장해야 하므로 운영 오버헤드와 복잡성이 높아집니다.

C. 이 접근 방식에는 여전히 EC2 인스턴스의 수동 관리 및 확장이 포함되어 운영 복잡성과 오버헤드가 증가합니다.

D. 이 솔루션은 ECS 클러스터를 관리하고 확장해야 하므로 운영 오버헤드와 복잡성이 추가됩니다. SQS 를 활용하면 시스템에 복잡성이 추가되어 Python 코드에서 메시지 소비 및 처리를 사용자 지정 처리해야 합니다.

설명 2:
JSON 문서를 S3 버킷에 넣으면 문서가 내구성과 확장성이 뛰어난 객체 스토리지 서비스에 저장됩니다. AWS Lambda 를 사용하면 회사는 Python 코드를 실행하여 기본 인프라에 대해 걱정할 필요 없이 S3 버킷에 도착하는 문서를 처리할 수 있습니다. 또한 AWS Lambda 가 들어오는 요청 비율에 따라 함수의 인스턴스 수를 자동으로 조정하므로 수평적 확장성이 가능합니다. 결과는 MySQL 및 PostgreSQL 과 호환되는 완전 관리형 고성능 데이터베이스 서비스인 Amazon Aurora DB 클러스터에 저장할 수 있습니다. 이는 처리 결과에 필요한 내구성과 확장성을 제공합니다.
https://aws.amazon.com/rds/aurora/

Q162
A company wants to use high performance computing (HPC) infrastructure on AWS for financial risk modeling. The company's HPC workloads run on Linux. Each HPC workflow runs on hundreds of Amazon EC2 Spot Instances, is short-lived, and generates thousands of output files that are ultimately stored in persistent storage for analytics and long-term future use.
The company seeks a cloud storage solution that permits the copying of on-premises data to long-term persistent storage to make data available for processing by all EC2 instances. The solution should also be a high performance file system that is integrated with persistent storage to read and write datasets and output files.
Which combination of AWS services meets these requirements?
A. Amazon FSx for Lustre integrated with Amazon S3
B. Amazon FSx for Windows File Server integrated with Amazon S3
C. Amazon S3 Glacier integrated with Amazon Elastic Block Store (Amazon EBS)
D. Amazon S3 bucket with a VPC endpoint integrated with an Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume
Answer: A
https://www.examtopics.com/discussions/amazon/view/87634-exam-aws-certified-solutions-architect-associate-saa-c03/

설명

https://aws.amazon.com/fsx/lustre/
Amazon FSx for Lustre 는 컴퓨팅 워크로드를 위한 비용 효율적이고 확장 가능한 고성능 스토리지를 제공하는 완전관리형 서비스입니다. 기계 학습, 고성능 컴퓨팅(HPC), 비디오 렌더링, 재무 시뮬레이션과 같은 많은 워크로드는 고성능 공유 스토리지를 통해 동일한 데이터 세트에 액세스하는 컴퓨팅 인스턴스에 의존합니다.

HPC = Amazon FSx for Lustre. 정답은 A.

Q163
A company is building a containerized application on premises and decides to move the application to AWS. The application will have thousands of users soon after it is deployed. The company is unsure how to manage the deployment of containers at scale. The company needs to deploy the containerized application in a highly available architecture that minimizes operational overhead.
Which solution will meet these requirements?
A. Store container images in an Amazon Elastic Container Registry (Amazon ECR) repository. Use an Amazon Elastic Container Service (Amazon ECS) cluster with the AWS Fargate launch type to run the containers. Use target tracking to scale automatically based on demand.
B. Store container images in an Amazon Elastic Container Registry (Amazon ECR) repository. Use an Amazon Elastic Container Service (Amazon ECS) cluster with the Amazon EC2 launch type to run the containers. Use target tracking to scale automatically based on demand.
C. Store container images in a repository that runs on an Amazon EC2 instance. Run the containers on EC2 instances that are spread across multiple Availability Zones. Monitor the average CPU utilization in Amazon CloudWatch. Launch new EC2 instances as needed.
D. Create an Amazon EC2 Amazon Machine Image (AMI) that contains the container image. Launch EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon CloudWatch alarm to scale out EC2 instances when the average CPU utilization threshold is breached.
Answer: A
https://www.examtopics.com/discussions/amazon/view/87509-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

AWS Fargate 는 사용자 애플리케이션을 위한 서버리스 환경으로, 사용자는 서버 구성 및 관리 대신 애플리케이션 구축에 집중할 수 있습니다. 또한 Fargate 는 리소스 관리를 자동화하여 사용자가 수요에 따라 애플리케이션을 쉽게 확장할 수 있도록 합니다.

컨테이너화된 애플리케이션 배포 = Fargate + ECS. 정답은 A.

Q164

A company has two applications: a sender application that sends messages with payloads to be processed and a processing application intended to receive the messages with payloads. The company wants to implement an AWS service to handle messages between the two applications. The sender application can send about 1,000 messages each hour. The messages may take up to 2 days to be processed: If the messages fail to process, they must be retained so that they do not impact the processing of any remaining messages.

Which solution meets these requirements and is the MOST operationally efficient?

A. Set up an Amazon EC2 instance running a Redis database. Configure both applications to use the instance. Store, process, and delete the messages, respectively.

B. Use an Amazon Kinesis data stream to receive the messages from the sender application. Integrate the processing application with the Kinesis Client Library (KCL).

C. Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue. Configure a dead-letter queue to collect the messages that failed to process.

D. Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications to process. Integrate the sender application to write to the SNS topic.

Answer: C

https://www.examtopics.com/discussions/amazon/view/87523-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

메시지 처리에 실패하면 = SQS Dead Letter Queue. 정답은 C.

설명 2:

발신자 및 프로세서 애플리케이션을 모두 SQS 와 통합하면 처리를 위해 발신자에서 프로세서 애플리케이션으로 메시지를 안정적으로 보낼 수 있습니다. SQS 는 최소 1 회 전달을 제공하여 메시지가 전송 중에 손실되지 않도록 합니다. 메시지 처리에 실패하면

다른 메시지 처리에 영향을 주지 않고 대기열에 보관하고 다시 시도할 수 있습니다. DLQ 를 구성하면 반복적으로 처리에 실패하는 메시지를 수집할 수 있으므로 문제 해결 및 분석을 위해 실패한 메시지를 볼 수 있습니다.
A 는 운영 오버헤드 및 유지 관리 요구 사항을 추가하는 Redis 를 실행하는 EC2 인스턴스의 관리 및 구성과 관련되므로 최적의 선택이 아닙니다.
B 는 Amazon Kinesis 데이터 스트림을 사용하고 메시지 처리를 위해 Kinesis Client Library 와 통합함으로써 추가적인 복잡성을 도입하므로 운영상 가장 효율적인 솔루션은 아닙니다.
SNS 를 사용하는 D 는 두 애플리케이션 간의 메시지 처리라는 특정 요구 사항보다 Pub/Sub 메시징 및 방송 알림에 더 적합하므로 시나리오에 가장 적합하지 않습니다.

참고:
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letterqueues.html

Q165
A solutions architect must design a solution that uses Amazon CloudFront with an Amazon S3 origin to store a static website. The company's security policy requires that all website traffic be inspected by AWS WAF.
How should the solutions architect comply with these requirements?
A. Configure an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.
B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.
C. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only. Associate AWS WAF to CloudFront.
D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.
Answer: D
https://www.examtopics.com/discussions/amazon/view/87524-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
CloudFront 로만 접속할 수 있도록 한 뒤에 WAF 로 검사해야 함.
Amazon S3 버킷을 오리진으로 설정하여 CloudFront 를 사용하는 경우 다음과 같은 이점을

제공하는 방식으로 CloudFront 및 Amazon S3 를 구성할 수 있습니다.
◎공개적으로 액세스할 수 없도록 Amazon S3 버킷에 대한 액세스를 제한합니다.
◎뷰어(사용자)가 지정된 CloudFront 배포를 통해서만 버킷의 콘텐츠에 액세스할 수 있도록 합니다. 즉, 뷰어가 버킷에서 직접 또는 의도하지 않은 CloudFront 배포를 통해 콘텐츠에 액세스하는 것을 방지합니다. 이렇게 하려면 인증된 요청을 Amazon S3 로 보내도록 CloudFront 를 구성하고 CloudFront 의 인증된 요청에 대한 액세스만 허용하도록 Amazon S3 를 구성합니다. CloudFront 는 Amazon S3 오리진에 인증된 요청을 전송하는 두 가지 방법으로 오리진 액세스 제어(OAC)와 오리진 액세스 ID(OAI)를 제공합니다.
https://docs.aws.amazon.com/ko_kr/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html

AWS WAF 는 CloudFront 에 전달되는 HTTP 및 HTTPS 요청을 모니터링할 수 있게 해주고 콘텐츠에 대한 액세스를 제어할 수 있게 해주는 웹 애플리케이션 방화벽입니다.
https://docs.aws.amazon.com/ko_kr/AmazonCloudFront/latest/DeveloperGuide/distribution-web-awswaf.html

참조
https://docs.aws.amazon.com/ko_kr/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html
https://docs.aws.amazon.com/ko_kr/AmazonCloudFront/latest/DeveloperGuide/distribution-web-awswaf.html

Q166
Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users around the world. The files are stored in an Amazon S3 bucket. A solutions architect has been asked to design an efficient and effective solution.
Which action should the solutions architect take to accomplish this?
A. Generate presigned URLs for the files.
B. Use cross-Region replication to all Regions.
C. Use the geoproximity feature of Amazon Route 53.
D. Use Amazon CloudFront with the S3 bucket as its origin.
Answer: D
https://www.examtopics.com/discussions/amazon/view/87522-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
정적 HTML 페이지 + 전 세계 사용자의 조회 + S3 버킷에 저장된 데이터 = S3 + CloudFront 조합. 답은 D.

설명 2:
Amazon CloudFront 는 HTML 페이지, 이미지 및 비디오와 같은 정적 및 동적 웹 콘텐츠의 전송 속도를 높이는 콘텐츠 전송 네트워크(CDN)입니다. CloudFront 를 사용하면 HTML 페이지가 가장 가까운 엣지 로케이션에서 사용자에게 제공되므로 더 빠르게 전달되고 더 나은 사용자 경험을 얻을 수 있습니다. 또한 CloudFront 는 글로벌 이벤트에 예상되는 높은 트래픽과 많은 수의 요청을 처리하여 전 세계 사용자가 HTML 페이지를 사용할 수 있고 액세스할 수 있도록 합니다.

Q167
A company runs a production application on a fleet of Amazon EC2 instances. The application reads the data from an Amazon SQS queue and processes the messages in parallel. The message volume is unpredictable and often has intermittent traffic. This application should continually process messages without any downtime.
Which solution meets these requirements MOST cost-effectively?
A. Use Spot Instances exclusively to handle the maximum capacity required.
B. Use Reserved Instances exclusively to handle the maximum capacity required.
C. Use Reserved Instances for the baseline capacity and use Spot Instances to handle additional capacity.
D. Use Reserved Instances for the baseline capacity and use On-Demand Instances to handle additional capacity.
Answer: D
https://www.examtopics.com/discussions/amazon/view/87510-exam-aws-certified-solutions-architect-associate-saa-c03/
설명 1:
A(X) : 가동 중지 시간이 없어야 한다고 했으므로 중지될 위험이 잇는 스팟 인스턴스는 적절치 않음.
B(X) : 메시지 볼륨을 예측할 수 없고 간헐적인 트래픽이 발생하는 상황에서 예측할 수 있는 트래픽이 발생하는 데에 적합한 예약 인스턴스는 맞지 않음.
C(X) : A 와 같은 이유로 오답.
D(O) : 최소 사용량을 기준 용량으로 삼아 예약 인스턴스를 사용함으로서 비용을 절감하고,

추가적이고 유동적인 트래픽은 온디맨드 인스턴스로 유연하게 처리 가능.

설명 2:
중단할 수 없는 단기적이고 불규칙한 워크로드가 있는 애플리케이션에는 온디맨드 인스턴스를 사용하는 것이 좋습니다.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-on-demand-instances.html

Q168
A security team wants to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there must be a single point where permissions can be maintained. What should a solutions architect do to accomplish this?
A. Create an ACL to provide access to the services or actions.
B. Create a security group to allow accounts and attach it to user groups.
C. Create cross-account roles in each account to deny access to the services or actions.
D. Create a service control policy in the root organizational unit to deny access to the services or actions.
Answer: D
https://www.examtopics.com/discussions/amazon/view/87512-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
권한을 유지할 수 있는 단일 지점이 핵심 키워드. 답은 D.
서비스 제어 정책(SCP)은 조직에서 권한을 관리하는 데 사용할 수 있는 조직 정책 유형입니다. SCP 는 조직의 모든 계정에 대해 사용 가능한 최대 권한을 중앙에서 제어합니다.
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

설명 2:
서비스 제어 정책(SCP)은 조직을 관리하는 데 사용할 수 있는 정책 유형 중 하나입니다. SCP 는 조직의 모든 계정에 대해 사용 가능한 최대 권한에 대한 중앙 제어를 제공하므로 계정이 조직의 액세스 제어 지침을 준수하도록 할 수 있습니다.
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.

html

Q169

A company is concerned about the security of its public web application due to recent web attacks. The application uses an Application Load Balancer (ALB). A solutions architect must reduce the risk of DDoS attacks against the application.

What should the solutions architect do to meet this requirement?

A. Add an Amazon Inspector agent to the ALB.

B. Configure Amazon Macie to prevent attacks.

C. Enable AWS Shield Advanced to prevent attacks.

D. Configure Amazon GuardDuty to monitor the ALB.

Answer: C

https://www.examtopics.com/discussions/amazon/view/87526-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

AWS Shield Standard, AWS Shield Advanced 는 애플리케이션 계층에서 DDoS 공격을 방어. AWS Shield 는 AWS 에서 실행되는 애플리케이션을 보호하는 디도스(DDoS) 보호 서비스입니다. AWS Shield 에는 두 계층 – Standard 및 Advanced 가 있습니다.

https://aws.amazon.com/ko/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc

설명 2:

AWS Shield Advanced 는 Amazon EC2 인스턴스, Elastic Load Balancing 로드 밸런서, CloudFront 배포, Route 53 호스팅 영역 및 AWS Global Accelerator 표준 가속기에 대해 확장된 DDoS 공격 보호 기능을 제공합니다.

https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html

Q170

A company's web application is running on Amazon EC2 instances behind an Application Load Balancer. The company recently changed its policy, which now requires the application to be accessed from one specific country only.

Which configuration will meet this requirement?

A. Configure the security group for the EC2 instances.

B. Configure the security group on the Application Load Balancer.
C. Configure AWS WAF on the Application Load Balancer in a VPC.
D. Configure the network ACL for the subnet that contains the EC2 instances.
Answer: C
https://www.examtopics.com/discussions/amazon/view/87528-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
AWS WAF 를 사용하여 특정 국가 또는 지리적 위치로부터의 요청을 허용하거나 차단하려면 어떻게 해야 합니까?
특정 국가의 사이트 액세스를 차단하거나 특정 국가에서만 액세스하도록 허용하려면 지리적 일치 규칙 문을 사용합니다. 기원 국가를 기준으로 일부 웹 요청을 허용하려면 허용하려는 국가에 대한 지리적 일치 규칙 문을 추가합니다. 그런 다음 차단하려는 국가에 대한 두 번째 지리적 일치 규칙 문을 추가합니다.
https://aws.amazon.com/ko/premiumsupport/knowledge-center/waf-allow-block-country-geolocation/

Q171
A company provides an API to its users that automates inquiries for tax computations based on item prices. The company experiences a larger number of inquiries during the holiday season only that cause slower response times. A solutions architect needs to design a solution that is scalable and elastic.
What should the solutions architect do to accomplish this?
A. Provide an API hosted on an Amazon EC2 instance. The EC2 instance performs the required computations when the API request is made.
B. Design a REST API using Amazon API Gateway that accepts the item names. API Gateway passes item names to AWS Lambda for tax computations.
C. Create an Application Load Balancer that has two Amazon EC2 instances behind it. The EC2 instances will compute the tax on the received item names.
D. Design a REST API using Amazon API Gateway that connects with an API hosted on an Amazon EC2 instance. API Gateway accepts and passes the item names to the EC2 instance for tax computations.
Answer: B
https://www.examtopics.com/discussions/amazon/view/87529-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
API 제공 + 탄력적인 = API Gateway + Lambda. 답은 B.

설명 2:
Lambda 서버리스는 EC2 api 게이트웨이 솔루션보다 확장 가능하고 탄력적입니다.

Q172
A solutions architect is creating a new Amazon CloudFront distribution for an application. Some of the information submitted by users is sensitive. The application uses HTTPS but needs another layer of security. The sensitive information should.be protected throughout the entire application stack, and access to the information should be restricted to certain applications.
Which action should the solutions architect take?
A. Configure a CloudFront signed URL.
B. Configure a CloudFront signed cookie.
C. Configure a CloudFront field-level encryption profile.
D. Configure CloudFront and set the Origin Protocol Policy setting to HTTPS Only for the Viewer Protocol Policy.
Answer: C
https://www.examtopics.com/discussions/amazon/view/87517-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
Amazon CloudFront 를 사용하면 HTTPS 를 통해 오리진 서버에 대한 종단 간 보안 연결을 적용할 수 있습니다. 필드 레벨 암호화는 추가 보안 레이어를 추가하여 시스템 처리 전체에서 특정 데이터를 보호하고 특정 애플리케이션만 이를 볼 수 있도록 합니다.
https://docs.aws.amazon.com/ko_kr/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html

설명 2:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-levelencryption.html
"Amazon CloudFront 를 사용하면 HTTPS 를 사용하여 오리진 서버에 대한 엔드 투 엔드 보안 연결을 적용할 수 있습니다.

필드 수준 암호화는 특정 애플리케이션만 볼 수 있도록 시스템 처리 전반에 걸쳐 특정 데이터를 보호할 수 있는 추가 보안 계층을 추가합니다."

Q173

A gaming company hosts a browser-based application on AWS. The users of the application consume a large number of videos and images that are stored in Amazon S3. This content is the same for all users.

The application has increased in popularity, and millions of users worldwide accessing these media files. The company wants to provide the files to the users while reducing the load on the origin.

Which solution meets these requirements MOST cost-effectively?

A. Deploy an AWS Global Accelerator accelerator in front of the web servers.

B. Deploy an Amazon CloudFront web distribution in front of the S3 bucket.

C. Deploy an Amazon ElastiCache for Redis instance in front of the web servers.

D. Deploy an Amazon ElastiCache for Memcached instance in front of the web servers.

Answer: B

https://www.examtopics.com/discussions/amazon/view/87530-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

S3 + 많은 수의 비디오와 이미지 + 수백만명 액세스가 핵심. S3 + CloudFront 로 CDN 서비스 사용해야 부하를 줄일 수 있음.

설명 2:

ElastiCache 는 완전 관리형 인 메모리 데이터 저장소에서 정보를 신속하게 검색하여 웹 애플리케이션의 성능을 향상시킵니다. Memcached 및 Redis 를 활용하고 애플리케이션이 디스크 기반 데이터베이스에서 데이터를 읽는 데 걸리는 시간을 상당히 단축합니다. Amazon CloudFront 는 TCP(전송 제어 프로토콜) 프로토콜을 기반으로 하는 HTTP 및 WebSocket 프로토콜의 동적 콘텐츠를 지원합니다. 일반적인 사용 사례에는 동적 API 호출, 웹 페이지 및 웹 애플리케이션뿐만 아니라 오디오 및 이미지와 같은 애플리케이션의 정적 파일이 포함됩니다. 또한 HTTP 를 통한 주문형 미디어 스트리밍을 지원합니다. AWS Global Accelerator 는 UDP(사용자 데이터그램 프로토콜)와 TCP 기반 프로토콜을 모두 지원합니다. 일반적으로 게임, IoT 및 VoIP(Voice over IP)와 같은 비 HTTP 사용 사례에 사용됩니다. 고정 IP 주소 또는 빠른 지역 장애 조치가 필요한 HTTP 사용 사례에도 적합합니다.

Q174

A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer (ALB). A solutions architect needs to modify the infrastructure to be highly available without modifying the application.

Which architecture should the solutions architect choose that provides high availability?

A. Create an Auto Scaling group that uses three instances across each of two Regions.

B. Modify the Auto Scaling group to use three instances across each of two Availability Zones.

C. Create an Auto Scaling template that can be used to quickly create more instances in another Region.

D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier.

Answer: B

https://www.examtopics.com/discussions/amazon/view/87531-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

다중 AZ 를 사용해야 하는 상황.

A(X) : 리전 간 Auto Scaling 은 불가.

지리적 이중화의 안전성과 안정성을 활용하려면 Auto Scaling 그룹을 리전 내의 여러 가용 영역에 걸쳐 확장하고 로드 밸런서를 연결하여 해당 가용 영역에 들어오는 트래픽을 분산하십시오.

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-availability-zone.html

설명 2:

여러 가용 영역을 사용하도록 기존 Auto Scaling 그룹을 수정하여 이 아키텍처에 대해 매우 간단하게 고가용성을 활성화할 수 있습니다. ASG 는 부하를 자동으로 분산하므로 실제로 AZ 당 인스턴스를 지정할 필요가 없습니다.

참조:

https://aws.amazon.com/ec2/autoscaling/

Q175

An ecommerce company has an order-processing application that uses Amazon API

Gateway and an AWS Lambda function. The application stores data in an Amazon Aurora PostgreSQL database. During a recent sales event, a sudden surge in customer orders occurred. Some customers experienced timeouts, and the application did not process the orders of those customers.

A solutions architect determined that the CPU utilization and memory utilization were high on the database because of a large number of open connections. The solutions architect needs to prevent the timeout errors while making the least possible changes to the application.

Which solution will meet these requirements?

A. Configure provisioned concurrency for the Lambda function. Modify the database to be a global database in multiple AWS Regions.

B. Use Amazon RDS Proxy to create a proxy for the database. Modify the Lambda function to use the RDS Proxy endpoint instead of the database endpoint.

C. Create a read replica for the database in a different AWS Region. Use query string parameters in API Gateway to route traffic to the read replica.

D. Migrate the data from Aurora PostgreSQL to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS). Modify the Lambda function to use the DynamoDB table.

Answer: B

https://www.examtopics.com/discussions/amazon/view/87533-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

연결 수가 많음 = RDS Proxy. 정답은 B.

RDS 프록시를 사용하여 예기치 않은 데이터베이스 트래픽 급증을 처리할 수 있습니다. 급증을 처리하지 않으면 연결 초과 구독 또는 빠른 속도의 새 연결 생성으로 인한 문제가 발생할 수 있습니다. RDS 프록시는 데이터베이스 연결 풀을 설정하고 이 풀에서 연결을 재사용합니다. 이 접근 방식은 매번 새 데이터베이스 연결을 여는 데서 오는 메모리 및 CPU 오버헤드 를 방지합니다. 과다 구독으로부터 데이터베이스를 보호하기 위해 생성되는 데이터베이스 연결 수를 제어할 수 있습니다.

https://docs.aws.amazon.com/ko_kr/AmazonRDS/latest/UserGuide/rds-proxy.html

설명 2:

최신 서버리스 아키텍처에 구축된 애플리케이션을 포함하여 많은 애플리케이션은 데이터베이스 서버에 대해 많은 수의 열린 연결을 가질 수 있으며 빠른 속도로 데이터베이스 연결을 열고 닫을 수 있으므로 데이터베이스 메모리와 컴퓨팅 리소스가 고갈될 수 있습니다. Amazon RDS Proxy 를 사용하면 애플리케이션이 데이터베이스와 설정된 연결을 풀링하고 공유하여 데이터베이스 효율성과 애플리케이션 확장성을 개선할 수

있습니다.
https://aws.amazon.com/id/rds/proxy/

Q176
An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table.
What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?
A. Use a VPC endpoint for DynamoDB.
B. Use a NAT gateway in a public subnet.
C. Use a NAT instance in a private subnet.
D. Use the internet gateway attached to the VPC.
Answer: A
https://www.examtopics.com/discussions/amazon/view/87532-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
VPC 내에 있는 프라이빗 서브넷의 EC2 인스턴스와 DynamoDB 간 가장 안전한 AWS 네트워크 통신 = VPC Gateway Endpoint.
게이트웨이 엔드포인트는 VPC 용 인터넷 게이트웨이 또는 NAT 디바이스가 없어도 Amazon S3 및 DynamoDB 에 대한 안정적인 연결을 제공합니다.
https://docs.aws.amazon.com/ko_kr/vpc/latest/privatelink/vpce-gateway.html#vpc-endpoints-limitations

설명 2:
DynamoDB 용 VPC 엔드포인트를 사용하면 VPC 의 Amazon EC2 인스턴스가 프라이빗 IP 주소를 사용하여 퍼블릭 인터넷에 노출되지 않고 DynamoDB 에 액세스할 수 있습니다. EC2 인스턴스에는 퍼블릭 IP 주소가 필요하지 않으며 VPC 에 인터넷 게이트웨이, NAT 디바이스 또는 가상 프라이빗 게이트웨이가 필요하지 않습니다. 엔드포인트 정책을 사용하여 DynamoDB 에 대한 액세스를 제어합니다. VPC 와 AWS 서비스 간의 트래픽은 Amazon 네트워크를 벗어나지 않습니다.

Q177

An entertainment company is using Amazon DynamoDB to store media metadata. The application is read intensive and experiencing delays. The company does not have staff to handle additional operational overhead and needs to improve the performance efficiency of DynamoDB without reconfiguring the application.

What should a solutions architect recommend to meet this requirement?

A. Use Amazon ElastiCache for Redis.

B. Use Amazon DynamoDB Accelerator (DAX).

C. Replicate data by using DynamoDB global tables.

D. Use Amazon ElastiCache for Memcached with Auto Discovery enabled.

Answer: B

https://www.examtopics.com/discussions/amazon/view/87572-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

DynamoDB 와 DAX 가 결합되면 성능을 한 단계 업그레이드하여 읽기 중심의 워크로드에서 초당 수백만 개의 요청에도 마이크로초의 응답 시간을 지원합니다. DynamoDB 와 마찬가지로 DAX 는 완전관리형입니다. 따라서 하드웨어나 소프트웨어 프로비저닝, 설정 및 구성, 소프트웨어 패치, 분산 캐시 클러스터 운영 또는 확장 시 여러 인스턴스에 데이터 복제 등과 같은 관리 작업에 대해 더 이상 걱정할 필요가 없습니다. DAX 는 장애 탐지, 장애 복구, 소프트웨어 패치와 같은 일반적인 관리 작업 상당 부분을 자동화합니다. DAX 는 DynamoDB API 와 호환되므로 작동하는 애플리케이션 코드를 변경할 필요가 없습니다.

참고:

https://aws.amazon.com/dynamodb/dax/

Q178

A company's infrastructure consists of Amazon EC2 instances and an Amazon RDS DB instance in a single AWS Region. The company wants to back up its data in a separate Region.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS Backup to copy EC2 backups and RDS backups to the separate Region.

B. Use Amazon Data Lifecycle Manager (Amazon DLM) to copy EC2 backups and RDS backups to the separate Region.

C. Create Amazon Machine Images (AMIs) of the EC2 instances. Copy the AMIs to the separate Region. Create a read replica for the RDS DB instance in the separate Region.

D. Create Amazon Elastic Block Store (Amazon EBS) snapshots. Copy the EBS snapshots to the separate Region. Create RDS snapshots. Export the RDS snapshots to Amazon S3. Configure S3 Cross-Region Replication (CRR) to the separate Region.
Answer: A
https://www.examtopics.com/discussions/amazon/view/87639-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
AWS Backup을 사용하여 EC2 및 RDS 백업을 별도의 리전에 복사하는 것은 최소한의 운영 오버헤드로 요구 사항을 충족하는 솔루션입니다. AWS Backup 은 백업 프로세스를 간소화하고 백업을 다른 리전으로 자동 복사하여 EC2 인스턴스 및 RDS 데이터베이스에 대한 별도의 백업 프로세스 관리와 관련된 수동 작업 및 운영 복잡성을 줄입니다.

B: Amazon Data Lifecycle Manager(Amazon DLM)가 RDS 백업을 별도의 리전에 직접 복사하도록 설계되지 않았기 때문에 올바르지 않습니다.
C: Amazon 머신 이미지(AMI) 및 읽기 전용 복제본을 생성하면 전용 백업 솔루션에 비해 복잡성과 운영 오버헤드가 추가되기 때문에 올바르지 않습니다.
D: Amazon EBS 스냅샷, RDS 스냅샷 및 S3 CRR(Cross-Region Replication)을 사용하려면 여러 수동 단계와 추가 구성이 수반되어 복잡성이 증가하기 때문에 올바르지 않습니다.

Q179
A solutions architect needs to securely store a database user name and password that an application uses to access an Amazon RDS DB instance. The application that accesses the database runs on an Amazon EC2 instance. The solutions architect wants to create a secure parameter in AWS Systems Manager Parameter Store.
What should the solutions architect do to meet this requirement?
A. Create an IAM role that has read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM role to the EC2 instance.
B. Create an IAM policy that allows read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM policy to the EC2 instance.
C. Create an IAM trust relationship between the Parameter Store parameter and the EC2 instance. Specify Amazon RDS as a principal in the trust policy.
D. Create an IAM trust relationship between the DB instance and the EC2 instance. Specify

Systems Manager as a principal in the trust policy.
Answer: A
https://www.examtopics.com/discussions/amazon/view/87582-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
데이터베이스 사용자 이름과 암호를 AWS 시스템 관리자 파라미터 스토어에 안전하게 저장하고 EC2 인스턴스에서 실행 중인 애플리케이션이 액세스할 수 있도록 하려면 솔루션스 아키텍트는 파라미터 스토어 파라미터에 대한 읽기 액세스 권한이 있는 IAM 역할을 생성하고 파라미터를 암호화하는 데 사용되는 AWS KMS 키에 대한 암호 해독 액세스를 허용해야 합니다. 그런 다음 솔루션스 아키텍트는 이 IAM 역할을 EC2 인스턴스에 할당해야 합니다.
이 접근 방식을 사용하면 EC2 인스턴스가 파라미터 스토어의 파라미터에 액세스하고 지정된 KMS 키를 사용하여 해독하는 동시에 필요한 보안 제어를 적용하여 승인된 당사자만 파라미터에 액세스할 수 있도록 할 수 있습니다.

Q180
A company is designing a cloud communications platform that is driven by APIs. The application is hosted on Amazon EC2 instances behind a Network Load Balancer (NLB). The company uses Amazon API Gateway to provide external users with access to the application through APIs. The company wants to protect the platform against web exploits like SQL injection and also wants to detect and mitigate large, sophisticated DDoS attacks.
Which combination of solutions provides the MOST protection? (Choose two.)
A. Use AWS WAF to protect the NLB.
B. Use AWS Shield Advanced with the NLB.
C. Use AWS WAF to protect Amazon API Gateway.
D. Use Amazon GuardDuty with AWS Shield Standard
E. Use AWS Shield Standard with Amazon API Gateway.
Answer: B, C
https://www.examtopics.com/discussions/amazon/view/87640-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
AWS Shield Advanced 는 Amazon EC2 인스턴스, Elastic Load Balancing 로드 밸런서, CloudFront 배포, Route 53 호스팅 영역 및 AWS Global Accelerator 표준 가속기에 대해

확장된 DDoS 공격 보호 기능을 제공합니다. AWS WAF 는 보호된 웹 애플리케이션 리소스로 전달되는 HTTP 및 HTTPS 요청을 모니터링할 수 있는 웹 애플리케이션 방화벽입니다. 다음 리소스 유형을 보호할 수 있습니다.
Amazon CloudFront 배포
아마존 API 게이트웨이 REST API
애플리케이션 로드 밸런서
AWS AppSync GraphQL API
Amazon Cognito 사용자 풀
https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html

설명 2:
지문에서 등장한 수단은 AWS WAF, AWS Shield Standard, AWS Shield Advanced 로 3 개.
◈Shield Advanced = WAF + Shield Standard.
・Shield Advanced = Amazon Elastic Compute Cloud(EC2), Elastic Load Balancing(ELB), Amazon CloudFront, AWS Global Accelerator 및 Amazon Route 53 리소스에서 실행되는 애플리케이션을 목표로 하는 공격에 대해 더 높은 수준의 보호를 구현. 정교한 대규모 DDoS 공격에 대한 추가 보호 및 완화, 실시간에 가까운 공격에 대한 가시성, 웹 애플리케이션 방화벽 [AWS WAF 와의 통합]을 제공.
https://aws.amazon.com/ko/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc
AWS Shield Advanced 구독에는 다음 기능과 옵션이 포함됩니다. 이는 AWS 에서 이미 받은 DDoS 탐지 및 완화 기능을 보완합니다. ◎AWS WAF 통합. ◎보호 그룹. ◎AWS Firewall Manager 를 통한 Shield Advanced 보호의 중앙 집중식 관리.◎AWS Shield 대응 팀(SRT)
https://docs.aws.amazon.com/waf/latest/developerguide/ddos-advanced-summary-capabilities.html
・Shield Standard = ""네트워크 및 전송 계층 DDoS 공격으로부터 보호
https://aws.amazon.com/ko/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc
・WAF = 일반적인 웹 공격으로부터 웹 애플리케이션이나 API 를 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. SQL 주입 또는 사이트 간 스크립팅과 같은 일반적인 공격 패턴을 차단하는 보안 규칙 및 사용자가 정의한 특정 트래픽 패턴을 필터링하는 규칙을 생성하도록 지원 https://aws.amazon.com/ko/waf/
AWS WAF 로 보호할 수 있는 리소스. ◎Amazon CloudFront 배포. ◎Amazon API 게이트웨이 REST API ◎애플리케이션 로드 밸런서 ◎AWS AppSync GraphQL API ◎Amazon Cognito 사용자 풀
https://docs.aws.amazon.com/waf/latest/developerguide/how-aws-waf-works.html

A(X) : WAF 는 웹 애플리케이션 방화벽으로, 네트워크 계층이 아니라 애플리케이션 계층을 방어.
B(O) : AWS Shield Advanced 는 DDoS EC2, ELB, CloudFront, AGA, Route 53 리소스 방어하며 WAF 와 통합.
C(O) : AWS WAF 는 웹 애플리케이션 및 API 를 공격으로부터 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다.
https://docs.aws.amazon.com/ko_kr/apigateway/latest/developerguide/apigateway-control-access-aws-waf.html
D(X) : GuardDuty 는 AWS 계정 보호 시스템. https://aws.amazon.com/ko/guardduty/
E(X) : AWS Shield Standard 는 DDoS 보호만을 제공.

Q181
A company has a legacy data processing application that runs on Amazon EC2 instances. Data is processed sequentially, but the order of results does not matter. The application uses a monolithic architecture. The only way that the company can scale the application to meet increased demand is to increase the size of the instances.
The company's developers have decided to rewrite the application to use a microservices architecture on Amazon Elastic Container Service (Amazon ECS).
What should a solutions architect recommend for communication between the microservices?
A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Add code to the data producers, and send data to the queue. Add code to the data consumers to process data from the queue.
B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Add code to the data producers, and publish notifications to the topic. Add code to the data consumers to subscribe to the topic.
C. Create an AWS Lambda function to pass messages. Add code to the data producers to call the Lambda function with a data object. Add code to the data consumers to receive a data object that is passed from the Lambda function.
D. Create an Amazon DynamoDB table. Enable DynamoDB Streams. Add code to the data producers to insert data into the table. Add code to the data consumers to use the DynamoDB Streams API to detect new table entries and retrieve the data.
Answer: A
https://www.examtopics.com/discussions/amazon/view/87647-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
분리와 함께 처리할 응용 프로그램에 대한 메시지를 보관할 큐를 수용하도록 아키텍처를 변경하기만 하면 됨 A(O) - SQS

설명 2:
대기열의 처리량이 제한됨(일괄 처리 없이 300msg/s, 일괄 처리 시 3000msg/s, 일괄 작업당 최대 10msg, 대기열에서 메시지 복제가 허용되지 않음(정확히 한 번 전달), 메시지 순서가 보존됨(FIFO), 대기열 이름 .fifo 로 끝나야 합니다.

Q182
A company wants to migrate its MySQL database from on premises to AWS. The company recently experienced a database outage that significantly impacted the business. To ensure this does not happen again, the company wants a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes.
Which solution meets these requirements?
A. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.
B. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.
C. Create an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data.
D. Create an Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance.
Answer: B
https://www.examtopics.com/discussions/amazon/view/87641-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
데이터베이스의 고가용성이 필요한 상황이므로 Multi AZ 가 필수인 상황.
A(X) : AWS 로 MySQL 데이터베이스를 마이그레이션하려고 한다 했으므로 Amazon RDS for MySQL 이 맞음.
B(O) : Amazon RDS 다중 AZ 동기 복제 기술을 사용하여 대기 데이터베이스 인스턴스의 데이터를 프라이머리와 함께 최신 상태로 유지합니다. 장애를 감지하면 Amazon RDS 는

수동 개입 없이 자동으로 대기 인스턴스로 장애 조치합니다.
https://aws.amazon.com/ko/rds/features/multi-az/
C(X) : RDS read replica 는 동기식이 아닌 비동기식 방식임.
기본 DB 인스턴스에 적용된 업데이트는 읽기 전용 복제본에 비동기식으로 복사됩니다.
https://docs.aws.amazon.com/ko_kr/AmazonRDS/latest/UserGuide/USER_ReadRepl.html
D(X) : 다른 AZ 나 리전에 복제하는지에 대한 여부가 안 나와 있음. 그리고 굳이 Lambda 를 사용해야 하는지도 의문.

설명 2:
Q: Amazon RDS 는 나를 대신하여 무엇을 관리합니까?
Amazon RDS 는 요청한 인프라 용량 프로비저닝에서 데이터베이스 소프트웨어 설치에 이르기까지 관계형 데이터베이스 설정과 관련된 작업을 관리합니다. 데이터베이스가 가동되고 실행되면 Amazon RDS 는 백업 수행 및 데이터베이스를 강화하는 소프트웨어 패치와 같은 일반적인 관리 작업을 자동화합니다. 선택적 다중 AZ 배포를 통해 Amazon RDS 는 자동 장애 조치를 통해 가용 영역 전체에서 동기식 데이터 복제도 관리합니다.
https://aws.amazon.com/rds/faqs/

Q183
A company is building a new dynamic ordering website. The company wants to minimize server maintenance and patching. The website must be highly available and must scale read and write capacity as quickly as possible to meet changes in user demand.
Which solution will meet these requirements?
A. Host static content in Amazon S3. Host dynamic content by using Amazon API Gateway and AWS Lambda. Use Amazon DynamoDB with on-demand capacity for the database. Configure Amazon CloudFront to deliver the website content.
B. Host static content in Amazon S3. Host dynamic content by using Amazon API Gateway and AWS Lambda. Use Amazon Aurora with Aurora Auto Scaling for the database. Configure Amazon CloudFront to deliver the website content.
C. Host all the website content on Amazon EC2 instances. Create an Auto Scaling group to scale the EC2 instances. Use an Application Load Balancer to distribute traffic. Use Amazon DynamoDB with provisioned write capacity for the database.
D. Host all the website content on Amazon EC2 instances. Create an Auto Scaling group to scale the EC2 instances. Use an Application Load Balancer to distribute traffic. Use Amazon Aurora with Aurora Auto Scaling for the database.
Answer: A

https://www.examtopics.com/discussions/amazon/view/87570-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
질문의 핵심 문구는 읽기 및 쓰기 용량을 확장해야 한다는 것입니다. Aurora 는 읽기 전용입니다. Amazon DynamoDB 에는 테이블에 대한 읽기 및 쓰기를 처리하기 위한 두 가지 읽기/쓰기 용량 모드가 있습니다. 온디맨드 프로비저닝(기본, 프리 티어 가능)
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html

DynamoDB 는 주문 데이터(키값)을 저장하는데 적합하고 온디맨드 방식으로 쓰기 및 읽기 용량을 확장합니다.

Q184
A company has an AWS account used for software engineering. The AWS account has access to the company's on-premises data center through a pair of AWS Direct Connect connections. All non-VPC traffic routes to the virtual private gateway.
A development team recently created an AWS Lambda function through the console. The development team needs to allow the function to access a database that runs in a private subnet in the company's data center.
Which solution will meet these requirements?
A. Configure the Lambda function to run in the VPC with the appropriate security group.
B. Set up a VPN connection from AWS to the data center. Route the traffic from the Lambda function through the VPN.
C. Update the route tables in the VPC to allow the Lambda function to access the on-premises data center through Direct Connect.
D. Create an Elastic IP address. Configure the Lambda function to send traffic through the Elastic IP address without an elastic network interface.
Answer: A
https://www.examtopics.com/discussions/amazon/view/87534-exam-aws-certified-solutions-architect-associate-saa-c03/

해설:
A(O) : 보안 그룹을 정의하여 VPC 에 Lambda 연결 가능.
AWS 계정의 가상 사설 클라우드(VPC)에 있는 사설 서브넷에 연결하도록 Lambda 함수를

구성할 수 있습니다. Amazon Virtual Private Cloud(Amazon VPC)를 사용하여 데이터베이스, 캐시 인스턴스 또는 내부 서비스와 같은 리소스에 대한 사설 네트워크를 생성합니다. 함수가 실행되는 동안 프라이빗 리소스에 액세스하려면 함수를 VPC 에 연결합니다. 함수를 VPC 에 연결하면 Lambda 는 함수의 VPC 구성에 있는 각 서브넷의 Hyperplane ENI(탄력적 네트워크 인터페이스)에 함수를 할당합니다. Lambda 는 계정의 VPC 지원 기능에 대해 고유한 서브넷 및 보안 그룹 조합이 처음으로 정의될 때 Hyperplane ENI 를 생성합니다.
https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html#vpc-managing-eni
B(X) : ・선택지에서 말하는 VPN 연결이란 VPC-온프레미스 간 연결을 말함.
VPN 연결 이라는 용어 는 일반적인 용어이지만 이 설명서에서 VPN 연결은 VPC 와 자체 온프레미스 네트워크 간의 연결을 나타냅니다.
https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html
・먼저 Virtual Private Gateway 를 사용하여 VPC-온프레미스 간 Site to Site VPN 연결을 수립.
◎AWS Site-to-Site VPN : VPC 와 원격 네트워크 사이에 IPsec VPN 연결을 생성할 수 있습니다. AWS 측 Site-to-Site VPN 연결에서 가상 프라이빗 게이트웨이 또는 Transit Gateway 는 자동 장애 조치를 위한 2 개의 VPN 엔드포인트(터널)를 제공합니다. Site-to-Site VPN 원격 연결 측에서 고객 게이트웨이 디바이스를 구성합니다.
https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/vpn-connections.html
・Virtual Private Gateway + Direct Connect + VPN 조합을 사용하는 이유는 Virtual Private Gateway + VPN 조합은 IPv4 밖에 전송이 안 되는데, Virtual Private Gateway + Direct Connect 조합은 IPv6 를 지원하므로 3 가지를 조합하면 IPv4, IPv6 를 모두 사용할 수 있기 때문.
가상 프라이빗 게이트웨이로 라우팅 : AWS Site-to-Site VPN 연결을 사용하여 VPC 의 인스턴스를 사용자의 네트워크와 통신하도록 할 수 있습니다. 이렇게 하려면 가상 프라이빗 게이트웨이를 생성하여 VPC 에 연결합니다.그런 다음 네트워크 대상 및 가상 프라이빗 게이트웨이(vgw-xxxxxxxxxxxxxxxxx)의 대상이 있는 서브넷 라우팅 테이블에 라우팅을 추가합니다....가상 프라이빗 게이트웨이의 Site-to-Site VPN 연결은 IPv6 트래픽을 지원하지 않습니다. 그러나 가상 프라이빗 게이트웨이를 통해 AWS Direct Connect 연결로 라우팅되는 IPv6 트래픽은 지원합니다.
https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/route-table-options.html#route-tables-vgw
・VPC 과 Lambda 함수 연결
AWS 계정에서 VPC(Virtual Private Cloud)의 프라이빗 서브넷에 연결하도록 Lambda 함수를 구성할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/lambda/latest/dg/configuration-vpc.html

But, 여기까지는 가능하지만 정작 Lambda 함수가 VPN 을 통해 트래픽을 라우팅할 수 있는지는 불명확.
그리고 어차피 A 의 내용이 충족되어야만 가능하기 때문에 정답이 아닐 가능성이 큼.
C(X) : A 의 내용이 충족되지 않으면 수립 불가. 즉, VPC 에 Lambda 가 연결이 되어야 가능하던 말던 함.
Lambda 함수는 항상 Lambda 서비스가 소유한 VPC 내에서 실행됩니다. 기본적으로 Lambda 함수는 사용자 계정의 VPC 에 연결되지 않습니다.
https://docs.aws.amazon.com/ko_kr/lambda/latest/dg/foundation-networking.html
D(X) : 탄력적 IP 주소는 퍼블릭 IP 주소로, Direct Connect 가 있는 상황에서 굳이 사용할 필요가 없음. 게다가 온프레미스 데이터베이스가 있는 곳은 프라이빗 서브넷이라 퍼블릭 IP 주소로는 무리임.

참조
https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html#vpc-managing-eni

Q185
A company runs an application using Amazon ECS. The application creates resized versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3.
How can a solutions architect ensure that the application has permission to access Amazon S3?
A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.
B. Create an IAM role with S3 permissions, and then specify that role as the taskRoleArn in the task definition.
C. Create a security group that allows access from Amazon ECS to Amazon S3, and update the launch configuration used by the ECS cluster.
D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.
Answer: B
https://www.examtopics.com/discussions/amazon/view/87648-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

A(X) : S3 에 관한 권한을 물어본 거지 ECS 에 대한 권한을 물어본 게 아님.
B(O) : 태스크 정의를 등록할 때 태스크 권한의 컨테이너가 사용자 대신 연결된 정책에 지정된 AWS API 를 호출하도록 허용하는 IAM 역할에 태스크 역할을 제공할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/AmazonECS/latest/developerguide/task_definition_parameters.html
C(X) : 보안 그룹 아웃바운드는 별 설정 안 해놔도 모두 허용이 기본값임. 굳이 설정할 필요가 없음.
D(X) : 액세스 권한이 있는지 확인하겠다고 다른 걸로 로그인해서 굳이 EC2 인스턴스를 다시 시작하는 것은 비효율적.

Q186
A company has a Windows-based application that must be migrated to AWS. The application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances that are deployed across multiple Availability Zone:
What should a solutions architect do to meet this requirement?
A. Configure AWS Storage Gateway in volume gateway mode. Mount the volume to each Windows instance.
B. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx file system to each Windows instance.
C. Configure a file system by using Amazon Elastic File System (Amazon EFS). Mount the EFS file system to each Windows instance.
D. Configure an Amazon Elastic Block Store (Amazon EBS) volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.
Answer: B
https://www.examtopics.com/discussions/amazon/view/87650-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 솔루션은 여러 가용 영역에 배포된 여러 Amazon EC2 Windows 인스턴스에 연결된 공유 Windows 파일 시스템을 사용해야 하는 Windows 기반 애플리케이션 마이그레이션 요구사항을 충족합니다. Amazon FSx for Windows File Server 는 Windows Server 에 구축된 완전 관리형 공유 스토리지를 제공하며 광범위한 데이터 액세스, 데이터 관리 및 관리 기능을 제공합니다. SMB(서버 메시지 블록) 프로토콜을 지원하며 여러 가용 영역에서 EC2 Windows 인스턴스에 탑재할 수 있습니다.

Windows 기반 애플리케이션이 핵심 키워드. 답은 B.

옵션 A 의 볼륨 게이트웨이 모드의 AWS Storage Gateway 는 온프레미스 애플리케이션 서버에서 iSCSI 디바이스로 마운트할 수 있는 클라우드 지원 스토리지 볼륨을 제공하지만 SMB 프로토콜 또는 EC2 Windows 인스턴스를 지원하지 않기 때문에 올바르지 않습니다.
옵션 C 는 Amazon Elastic File System(Amazon EFS)이 Linux 기반 워크로드를 위한 확장 가능하고 탄력적인 NFS 파일 시스템을 제공하지만 SMB 프로토콜 또는 EC2 Windows 인스턴스를 지원하지 않기 때문에 올바르지 않습니다.
옵션 D 는 Amazon Elastic Block Store(Amazon EBS)가 EC2 인스턴스와 함께 사용할 영구 블록 스토리지 볼륨을 제공하지만 SMB 프로토콜을 지원하지 않거나 동일한 볼륨에 여러 인스턴스를 연결하기 때문에 올바르지 않습니다.

참조:
https://aws.amazon.com/fsx/windows/
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/using-file-shares.html

Q187
A company is developing an ecommerce application that will consist of a load-balanced front end, a container-based application, and a relational database. A solutions architect needs to create a highly available solution that operates with as little manual intervention as possible.
Which solutions meet these requirements? (Choose two)
A. Create an Amazon RDS DB instance in Multi-AZ mode.
B. Create an Amazon RDS DB instance and one or more replicas in another Availability Zone.
C. Create an Amazon EC2 instance-based Docker cluster to handle the dynamic application load.
D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with a Fargate launch type to handle the dynamic application load.
E. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type to handle the dynamic application load.
Answer: A, D
https://www.examtopics.com/discussions/amazon/view/87695-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

A(O) : 다중 AZ 모드로 고가용성 충족. 관계형 데이터베이스로 구성된 프로그램이어야 하므로 RDS 사용.
다중 AZ 배포로 실행되도록 DB 인스턴스를 생성 또는 수정하면 Amazon RDS 가 다른 가용 영역에 동기식 '예비' 복제본을 자동으로 프로비저닝하고 유지합니다. 특정 유형의 계획된 유지 관리를 수행하는 도중에, 또는 예기치 않은 DB 인스턴스 장애나 가용 영역 장애가 발생할 경우 Amazon RDS 가 자동으로 예비 복제본으로 장애 조치하므로 예비 복제본이 승격되자마자 데이터베이스 쓰기 및 읽기를 재개할 수 있습니다.
https://aws.amazon.com/ko/rds/faqs/
B(X) : 장애 발생 시 복구를 위한 것이면 Multi AZ 가 더 유리하므로 고가용성 면에선 Multi AZ 가 추천됨. 읽기 복제본을 사용해 데이터베이스 쓰기 가용성을 개선하거나 내 소스 DB 인스턴스의 데이터를 장애로부터 보호할 수 있습니까? 복제를 사용해 데이터베이스 쓰기 가용성을 높이고 최근 데이터베이스 업데이트를 다양한 장애 조건으로부터 보호하려면 DB 인스턴스를 다중 AZ 배포로 실행하는 것이 좋습니다. Amazon RDS 읽기 전용 복제본과 지원되는 엔진의 기본 비동기식 복제를 사용하면 데이터베이스 쓰기가 소스 DB 인스턴스에서 발생한 후, 읽기 전용 복제본에서 발생합니다. 이 복제 '지연 시간'은 상당히 다를 수 있습니다. https://aws.amazon.com/ko/rds/faqs/
C(X) : EC2 로 굳이 돌릴 거 없이 ECS 를 사용해서 서버리스로 돌릴 수 있음
D(O) : Fargate + ECS 조합으로 컨테이너 애플리케이션을 서버리스로 돌릴 수 있음.
AWS Fargate Fargate 는 Amazon EC2 인스턴스의 서버나 클러스터를 관리할 필요 없이 컨테이너를 실행하기 위해 Amazon ECS 에 사용할 수 있는 기술입니다.
https://docs.aws.amazon.com/ko_kr/AmazonECS/latest/developerguide/AWS_Fargate.html
E(X) : C 와 같은 이유로 오답.

설명 2:
https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html
1. 관계형 데이터베이스: RDS
2. 컨테이너 기반 애플리케이션: ECS
"Amazon ECS 를 사용하면 간단한 API 호출을 사용하여 컨테이너 기반 애플리케이션을 시작 및 중지할 수 있습니다. 또한 중앙 집중식 서비스에서 클러스터 상태를 검색하고 많은 익숙한 Amazon EC2 기능에 액세스할 수 있습니다."
3. 약간의 수동 개입: Fargate AWS Fargate 에서 관리하는 서버리스 인프라에서 작업과 서비스를 실행할 수 있습니다. 또는 인프라를 더 잘 제어하기 위해 관리하는 Amazon EC2 인스턴스의 클러스터에서 작업과 서비스를 실행할 수 있습니다.

Q188

A company uses Amazon S3 as its data lake. The company has a new partner that must use SFTP to upload data files. A solutions architect needs to implement a highly available SFTP solution that minimizes operational overhead.

Which solution will meet these requirements?

A. Use AWS Transfer Family to configure an SFTP-enabled server with a publicly accessible endpoint. Choose the S3 data lake as the destination.

B. Use Amazon S3 File Gateway as an SFTP server. Expose the S3 File Gateway endpoint URL to the new partner. Share the S3 File Gateway endpoint with the new partner.

C. Launch an Amazon EC2 instance in a private subnet in a VPInstruct the new partner to upload files to the EC2 instance by using a VPN. Run a cron job script, on the EC2 instance to upload files to the S3 data lake.

D. Launch Amazon EC2 instances in a private subnet in a VPC. Place a Network Load Balancer (NLB) in front of the EC2 instances. Create an SFTP listener port for the NLB. Share the NLB hostname with the new partner. Run a cron job script on the EC2 instances to upload files to the S3 data lake.

Answer: A

https://www.examtopics.com/discussions/amazon/view/87566-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

이 솔루션은 수동 관리 또는 운영 오버헤드 없이 고가용성 SFTP 솔루션을 제공합니다. AWS Transfer Family 를 사용하면 인증, 권한 부여 및 스토리지 백엔드로 S3 와의 통합을 통해 SFTP 서버를 쉽게 설정할 수 있습니다.

옵션 B 는 SFTP 액세스가 아닌 NFS 또는 SMB 프로토콜을 통한 S3 스토리지에 대한 파일 기반 액세스에 주로 사용되는 Amazon S3 파일 게이트웨이 사용을 제안하므로 최선의 선택이 아닙니다.

옵션 C 는 파일 업로드를 위한 EC2 인스턴스, VPN 설정 및 cron 작업 스크립트의 수동 관리가 필요하여 운영 오버헤드와 잠재적인 복잡성을 유발하므로 최선의 선택이 아닙니다.

옵션 D 는 파일 업로드를 위한 EC2 인스턴스, Network Load Balancer 및 cron 작업 스크립트의 수동 관리도 필요하므로 최선의 선택이 아닙니다. 옵션 A 에서 AWS Transfer Family 가 제공하는 더 단순하고 완벽하게 관리되는 솔루션에 비해 더 복잡하고 추가 구성 요소가 필요합니다.

Q189

A company needs to store contract documents. A contract lasts for 5 years. During the 5-year period, the company must ensure that the documents cannot be overwritten or deleted. The company needs to encrypt the documents at rest and rotate the encryption keys automatically every year.

Which combination of steps should a solutions architect take to meet these requirements with the LEAST operational overhead? (Choose two.)

A. Store the documents in Amazon S3. Use S3 Object Lock in governance mode.

B. Store the documents in Amazon S3. Use S3 Object Lock in compliance mode.

C. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Configure key rotation.

D. Use server-side encryption with AWS Key Management Service (AWS KMS) customer managed keys. Configure key rotation.

E. Use server-side encryption with AWS Key Management Service (AWS KMS) customer provided (imported) keys. Configure key rotation.

Answer: B, D

https://www.examtopics.com/discussions/amazon/view/87535-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

B. 규정 준수 모드에서 S3 객체 잠금을 사용하면 객체에 엄격한 보존 정책을 적용하여 수정이나 삭제를 방지합니다.

D. AWS KMS 고객 관리형 키와 함께 서버 측 암호화를 사용하면 문서가 고객 제어형 키로 암호화됩니다. 키 순환을 활성화하면 정의된 순환 간격으로 새 암호화 키가 자동으로 생성되어 보안이 강화됩니다.

옵션 A: 거버넌스 모드의 S3 객체 잠금은 문서에 필요한 불변성을 제공하지 않으므로 잠재적인 수정 또는 삭제가 허용됩니다.

옵션 C: SSE-S3 만으로는 서버 측 암호화가 명시적으로 지정된 암호화 키 순환 요구 사항을 충족하지 않습니다.

옵션 E: AWS KMS 고객 관리 키(옵션 D)를 사용할 수 있는 경우 고객 제공(가져온) 키(SSE-C)를 사용한 서버 측 암호화는 필요하지 않으며, 이는 보다 통합되고 관리 가능한 솔루션을 제공합니다.

Q190

A company has a web application that is based on Java and PHP. The company plans to move the application from on premises to AWS. The company needs the ability to test new site features frequently. The company also needs a highly available and managed solution that requires minimum operational overhead.
Which solution will meet these requirements?
A. Create an Amazon S3 bucket. Enable static web hosting on the S3 bucket. Upload the static content to the S3 bucket. Use AWS Lambda to process all dynamic content.
B. Deploy the web application to an AWS Elastic Beanstalk environment. Use URL swapping to switch between multiple Elastic Beanstalk environments for feature testing.
C. Deploy the web application to Amazon EC2 instances that are configured with Java and PHP. Use Auto Scaling groups and an Application Load Balancer to manage the website's availability.
D. Containerize the web application. Deploy the web application to Amazon EC2 instances. Use the AWS Load Balancer Controller to dynamically route traffic between containers that contain the new site features for testing.
Answer: B
https://www.examtopics.com/discussions/amazon/view/87536-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
Elastic Beanstalk 를 사용하면 애플리케이션을 실행하는 인프라에 대해 자세히 알지 못해도 AWS 클라우드에서 애플리케이션을 신속하게 배포하고 관리할 수 있습니다.
Elastic Beanstalk 는 Go, Java, .NET, Node.js, PHP, Python 및 Ruby 에서 개발된 애플리케이션을 지원합니다....애플리케이션을 생성 및 배포한 후에는 지표, 이벤트, 환경 상태 등의 애플리케이션 정보를 Elastic Beanstalk 콘솔, API 또는 통합된 AWS CLI 를 비롯한 명령줄 인터페이스를 통해 확인할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/elasticbeanstalk/latest/dg/Welcome.html

설명 2:
빈번한 기능 테스트 -
- 개발, 테스트 및 프로덕션 사용 사례를 위해 여러 Elastic Beanstalk 환경을 쉽게 생성할 수 있습니다.
- 간단한 URL 스와핑 기술을 사용하여 A/B 테스트 및 기능 반복을 위한 환경 간에 트래픽을 라우팅할 수 있습니다. 복잡한 라우팅 규칙이나 인프라 변경이 필요하지 않습니다.

Q191

A company has an ordering application that stores customer information in Amazon RDS for MySQL. During regular business hours, employees run one-time queries for reporting purposes. Timeouts are occurring during order processing because the reporting queries are taking a long time to run. The company needs to eliminate the timeouts without preventing employees from performing queries.

What should a solutions architect do to meet these requirements?

A. Create a read replica. Move reporting queries to the read replica.

B. Create a read replica. Distribute the ordering application to the primary DB instance and the read replica.

C. Migrate the ordering application to Amazon DynamoDB with on-demand capacity.

D. Schedule the reporting queries for non-peak hours.

Answer: A

https://www.examtopics.com/discussions/amazon/view/89077-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

A. 보고 쿼리를 읽기 전용 복제본으로 이동하면 주문 처리에 사용되는 기본 DB 인스턴스가 장기 실행 보고 쿼리의 영향을 받지 않습니다. 이렇게 하면 주문 처리 중 시간 초과를 제거하는 동시에 직원이 애플리케이션 성능에 영향을 주지 않고 쿼리를 수행할 수 있습니다.

B. 이것은 일정 수준의 부하 분산을 제공할 수 있지만 주문 처리 중 쿼리 보고로 인해 발생하는 시간 초과 문제를 구체적으로 다루지는 않습니다.

C. DynamoDB 는 확장성과 성능상의 이점을 제공하지만 애플리케이션의 데이터 모델 및 쿼리 접근 방식을 크게 변경해야 할 수 있습니다.

D. 이 접근 방식은 주문 처리에 미치는 영향을 완화하는 데 도움이 될 수 있지만 직원이 쿼리를 수행하는 것을 막지 않고 시간 초과를 제거해야 하는 요구 사항을 해결하지는 못합니다.

Q192

A hospital wants to create digital copies for its large collection of historical written records. The hospital will continue to add hundreds of new documents each day. The hospital's data team will scan the documents and will upload the documents to the AWS Cloud.

A solutions architect must implement a solution to analyze the documents, extract the

medical information, and store the documents so that an application can run SQL queries on the data. The solution must maximize scalability and operational efficiency.
Which combination of steps should the solutions architect take to meet these requirements? (Choose two)
A. Write the document information to an Amazon EC2 instance that runs a MySQL database.
B. Write the document information to an Amazon S3 bucket. Use Amazon Athena to query the data.
C. Create an Auto Scaling group of Amazon EC2 instances to run a custom application that processes the scanned files and extracts the medical information.
D. Create an AWS Lambda function that runs when new documents are uploaded. Use Amazon Rekognition to convert the documents to raw text. Use Amazon Transcribe Medical to detect and extract relevant medical information from the text.
E. Create an AWS Lambda function that runs when new documents are uploaded. Use Amazon Textract to convert the documents to raw text. Use Amazon Comprehend Medical to detect and extract relevant medical information from the text.
Answer: B, E
https://www.examtopics.com/discussions/amazon/view/89133-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : AWS 클라우드에 문서를 업로드할 거라고 했으니 적절치 않음. MySQL 이 아니라 Amazon RDS for MySQL 이 됐던지 했어야 함.
B(O) : S3 는 자료를 저장하는데 많이 사용되고, Athena 는 S3 에 쿼리하는 대화형 서비스임. Amazon Athena 는 표준 SQL 을 사용하여 Amazon S3(Amazon Simple Storage Service)에 있는 데이터를 직접 간편하게 분석할 수 있는 대화형 쿼리 서비스입니다.
https://docs.aws.amazon.com/ko_kr/athena/latest/ug/what-is.html
C(?) : 프로그램을 AWS 에서 돌려야한다는 말이 없어서 불명확.
D(X) : Amazon Rekognition 은 이미지나 비디오 분석 서비스인데, 문서라면 텍스트 위주라서 탈락. 그리고 Transcribe Medical 은 음성->텍스트 변환이지 텍스트->의료 정보 추출이 아님.
Amazon Transcribe Medical 은 사용자가 의료 관련 음성 데이터를 텍스트로 변환하는 기능을 사용자의 음성 지원 애플리케이션에 쉽게 추가할 수 있도록 하는 자동 음성 인식(ASR) 서비스입니다.
https://aws.amazon.com/ko/transcribe/medical/
E(O) : Lambda 로 Scalabilty 확보 가능. Amazon Textract 는 이미지 등에서 텍스트를 추출하는 OCR 서비스로 문서화에 적합. Amazon Comprehend Medical 은 미리 학습된 기계

학습을 사용하여 처방전, 처치, 진단과 같은 의료 텍스트에서 의료 데이터를 파악하고 추출하는 서비스로 병원에서 사용하기 적합.
확장성 : Lambda 는 코드를 실행하는 인프라를 관리하고 수신 요청에 대한 응답으로 자동 확장됩니다.
https://docs.aws.amazon.com/ko_kr/lambda/latest/dg/gettingstarted-features.html#gettingstarted-features-scaling
Amazon Textract 는 스캔한 문서에서 텍스트, 필기 및 데이터를 자동으로 추출하는 기계 학습(ML) 서비스입니다. 단순한 광학 문자 인식(OCR) 이상으로 양식 및 표의 데이터를 식별하고 이해하며 추출합니다.
https://aws.amazon.com/ko/textract/
Amazon Comprehend Medical 은 HIPAA 적격 자연어 처리(NLP) 서비스로, 미리 학습된 기계 학습을 사용하여 처방전, 처치, 진단과 같은 의료 텍스트에서 의료 데이터를 파악하고 추출합니다.
https://aws.amazon.com/ko/comprehend/medical/

설명 2:
이 솔루션은 애플리케이션이 데이터에 대해 SQL 쿼리를 실행할 수 있도록 문서를 분석하고 의료 정보를 추출하고 문서를 저장하는 대량의 과거 서면 기록 컬렉션을 위한 디지털 사본 생성 요구 사항을 충족합니다. 문서 정보를 Amazon S3 버킷에 쓰면 스캔한 파일을 위한 확장 가능하고 내구성 있는 스토리지를 제공할 수 있습니다. Amazon Athena 를 사용하여 데이터를 쿼리하면 S3 에 저장된 데이터에 대한 서버리스 및 대화형 SQL 분석을 제공할 수 있습니다. 새 문서가 업로드될 때 실행되는 AWS Lambda 함수를 생성하면 스캔한 파일의 이벤트 기반 및 서버리스 처리를 제공할 수 있습니다. Amazon Textract 를 사용하여 문서를 원시 텍스트로 변환하면 정확한 광학 문자 인식(OCR)을 제공하고 인공 지능(AI)을 사용하여 문서에서 테이블 및 양식과 같은 구조화된 데이터를 추출할 수 있습니다. Amazon Comprehend Medical 을 사용하여 텍스트에서 관련 의료 정보를 감지하고 추출하면 의료 텍스트에서 건강 데이터를 이해하고 추출하도록 사전 훈련된 기계 학습을 사용하는 자연어 처리(NLP) 서비스를 제공할 수 있습니다.

실행되는 Amazon EC2 인스턴스에 문서 정보를 쓰기 때문에 옵션 A 가 올바르지 않습니다. MySQL 데이터베이스는 인프라 오버헤드와 복잡성을 증가시킬 수 있으며 대량의 데이터를 처리하지 못할 수 있습니다.

스캔한 파일을 처리하고 의료 정보를 추출하는 사용자 지정 애플리케이션을 실행하기 위해 Amazon EC2 인스턴스의 Auto Scaling 그룹을 생성하면 인프라 오버헤드와 복잡성이 증가할 수 있고 기존 AI 및 NLP 서비스를 활용하지 못할 수 있으므로 옵션 C 는 올바르지

않습니다. Textract 및 Comprehend Medical 과 같은

Amazon Rekognition 을 사용하여 문서를 원시 텍스트로 변환하면 이미지 및 비디오 분석을 제공할 수 있지만 OCR 또는 문서에서 구조화된 데이터 추출을 지원하지 않기 때문에 옵션 D 는 올바르지 않습니다. Amazon Transcribe Medical 을 사용하여 텍스트에서 관련 의료 정보를 감지하고 추출하면 의료 대화를 위한 음성-텍스트 변환 서비스를 제공할 수 있지만 텍스트 분석이나 의료 텍스트에서 건강 데이터 추출은 지원하지 않습니다.
참조:
https://aws.amazon.com/s3/
https://aws.amazon.com/athena/
https://aws.amazon.com/lambda/
https://aws.amazon.com/texttract/
https://aws.amazon.com/comprehend/medical/

Q193
A company is running a batch application on Amazon EC2 instances. The application consists of a backend with multiple Amazon RDS databases. The application is causing a high number of reads on the databases. A solutions architect must reduce the number of database reads while ensuring high availability.
What should the solutions architect do to meet this requirement?
A. Add Amazon RDS read replicas.
B. Use Amazon ElastiCache for Redis.
C. Use Amazon Route 53 DNS caching
D. Use Amazon ElastiCache for Memcached.
Answer: A
https://www.examtopics.com/discussions/amazon/view/89134-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
이 솔루션은 여러 Amazon RDS 데이터베이스가 있는 백엔드로 구성된 배치 애플리케이션의 고가용성을 보장하면서 데이터베이스 읽기 수를 줄이는 요구 사항을 충족합니다.
Amazon RDS 읽기 전용 복제본은 읽기 전용 트래픽을 처리할 수 있는 기본 데이터베이스 인스턴스의 복사본입니다. 기본 데이터베이스 인스턴스에 대해 하나 이상의 읽기 전용 복제본을 만들고 특수 엔드포인트를 사용하여 연결할 수 있습니다. 읽기 전용 복제본은

기본 데이터베이스 인스턴스에서 읽기 쿼리를 오프로드하여 애플리케이션의 성능과 가용성을 향상시킬 수 있습니다.

Redis 용 Amazon ElastiCache 를 사용하면 자주 액세스하는 데이터를 캐시할 수 있는 빠른 인 메모리 데이터 스토어를 제공할 수 있지만 Amazon RDS 데이터베이스에서 복제를 지원하지 않기 때문에 옵션 B 는 올바르지 않습니다.

Amazon Route 53 DNS 캐싱을 사용하면 DNS 쿼리의 성능과 가용성을 개선할 수 있지만 데이터베이스 읽기 수는 줄어들지 않기 때문에 옵션 C 는 올바르지 않습니다.

Memcached 용 Amazon ElastiCache 를 사용하면 자주 액세스하는 데이터를 캐시할 수 있는 빠른 메모리 데이터 스토어를 제공할 수 있지만 Amazon RDS 데이터베이스에서 복제를 지원하지 않기 때문에 옵션 D 는 올바르지 않습니다.

설명 2:
Amazon RDS 데이터베이스에 읽기 전용 복제본을 추가하면 읽기 워크로드를 복제본으로 오프로드하여 데이터베이스 읽기 수를 줄이고 성능을 향상할 수 있습니다. 읽기 전용 복제본은 고가용성을 제공하고 읽기 트래픽을 독립적으로 처리하여 로드를 분산하고 기본 데이터베이스의 부담을 줄일 수 있습니다.
B. Redis 용 Amazon ElastiCache 는 주로 캐싱에 사용되는 인 메모리 데이터 스토어로, 읽기 성능을 향상시킬 수 있지만 데이터베이스 읽기 수를 직접적으로 줄이지는 않습니다.
C. Amazon Route 53 DNS 캐싱은 DNS 응답을 캐시하는 서비스로, 전체 네트워크 성능을 향상시킬 수 있지만 데이터베이스 읽기 감소를 구체적으로 다루지는 않습니다.
D. Memcached 용 Amazon ElastiCache 는 Redis 와 유사한 또 다른 캐싱 서비스이지만 데이터베이스 읽기 감소 문제를 직접적으로 해결하지는 않습니다.

참조:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

Q194
A company needs to run a critical application on AWS. The company needs to use Amazon EC2 for the application's database. The database must be highly available and must fail over automatically if a disruptive event occurs.
Which solution will meet these requirements?
A. Launch two EC2 instances, each in a different Availability Zone in the same AWS Region.

Install the database on both EC2 instances. Configure the EC2 instances as a cluster. Set up database replication.
B. Launch an EC2 instance in an Availability Zone. Install the database on the EC2 instance. Use an Amazon Machine Image (AMI) to back up the data. Use AWS CloudFormation to automate provisioning of the EC2 instance if a disruptive event occurs.
C. Launch two EC2 instances, each in a different AWS Region. Install the database on both EC2 instances. Set up database replication. Fail over the database to a second Region.
D. Launch an EC2 instance in an Availability Zone. Install the database on the EC2 instance. Use an Amazon Machine Image (AMI) to back up the data. Use EC2 automatic recovery to recover the instance if a disruptive event occurs.
Answer: A
https://www.examtopics.com/discussions/amazon/view/89136-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
서로 다른 가용 영역에서 두 개의 EC2 인스턴스를 시작하고 데이터베이스 복제가 있는 클러스터로 구성하면 데이터베이스에서 고가용성과 자동 장애 조치를 달성할 수 있습니다. 한 인스턴스 또는 가용 영역을 사용할 수 없게 되더라도 다른 인스턴스는 중단 없이 애플리케이션을 계속 제공할 수 있습니다.
B. 단일 EC2 인스턴스를 시작하고 백업 및 프로비저닝 자동화를 위해 AMI 를 사용하면 자동 장애 조치 또는 고가용성이 제공되지 않습니다.
C. 다른 AWS 리전에서 EC2 인스턴스를 시작하고 데이터베이스 복제를 설정하는 것은 재해 복구 기능을 제공할 수 있지만 단일 리전 내에서 자동 장애 조치를 제공하지 않는 다중 리전 설정입니다.
D. EC2 자동 복구를 사용하면 하드웨어 문제로 인해 인스턴스가 실패하는 경우 인스턴스를 복구할 수 있지만 여러 인스턴스 또는 가용 영역에서 자동 장애 조치 또는 고가용성을 제공하지는 않습니다.

Q195
A company's order system sends requests from clients to Amazon EC2 instances. The EC2 instances process the orders and then store the orders in a database on Amazon RDS. Users report that they must reprocess orders when the system fails. The company wants a resilient solution that can process orders automatically if a system outage occurs.
What should a solutions architect do to meet these requirements?
A. Move the EC2 instances into an Auto Scaling group. Create an Amazon EventBridge

(Amazon CloudWatch Events) rule to target an Amazon Elastic Container Service (Amazon ECS) task.
B. Move the EC2 instances into an Auto Scaling group behind an Application Load Balancer (ALB). Update the order system to send messages to the ALB endpoint.
C. Move the EC2 instances into an Auto Scaling group. Configure the order system to send messages to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the EC2 instances to consume messages from the queue.
D. Create an Amazon Simple Notification Service (Amazon SNS) topic. Create an AWS Lambda function, and subscribe the function to the SNS topic. Configure the order system to send messages to the SNS topic. Send a command to the EC2 instances to process the messages by using AWS Systems Manager Run Command.
Answer: C
https://www.examtopics.com/discussions/amazon/view/89138-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
SQS 는 Dead Letter Queue 등 다양한 옵션으로 메시지 처리가 실패했을 경우 해당 메시지를 보관했다가 다시 처리할 수 있게끔 하는 기능을 제공하고 있음.

설명 2:
시스템 중단 시 자동으로 주문을 처리할 수 있는 탄력적인 솔루션을 보유해야 한다는 회사의 요구 사항을 충족하려면 솔루션 설계자가 내결함성 아키텍처를 구현해야 합니다. 주어진 시나리오에 따라 가능한 솔루션은 EC2 인스턴스를 Auto Scaling 그룹으로 이동하고 메시지를 Amazon Simple Queue Service(Amazon SQS) 대기열로 보내도록 주문 시스템을 구성하는 것입니다. 그런 다음 EC2 인스턴스는 대기열의 메시지를 사용할 수 있습니다.

Q196
A company runs an application on a large fleet of Amazon EC2 instances. The application reads and writes entries into an Amazon DynamoDB table. The size of the DynamoDB table continuously grows, but the application needs only data from the last 30 days. The company needs a solution that minimizes cost and development effort.
Which solution meets these requirements?
A. Use an AWS CloudFormation template to deploy the complete solution. Redeploy the CloudFormation stack every 30 days, and delete the original stack.
B. Use an EC2 instance that runs a monitoring application from AWS Marketplace. Configure

the monitoring application to use Amazon DynamoDB Streams to store the timestamp when a new item is created in the table. Use a script that runs on the EC2 instance to delete items that have a timestamp that is older than 30 days.
C. Configure Amazon DynamoDB Streams to invoke an AWS Lambda function when a new item is created in the table. Configure the Lambda function to delete items in the table that are older than 30 days.
D. Extend the application to add an attribute that has a value of the current timestamp plus 30 days to each new item that is created in the table. Configure DynamoDB to use the attribute as the TTL attribute.
Answer: D
https://www.examtopics.com/discussions/amazon/view/89140-exam-aws-certified-solutions-architect-associate-saa-c03/

해설 1:
30 일 동안의 데이터만 필요하다고 했으니 30 일이 지나면 자동 삭제되도록 하는 기능이 필요.
A(X) : 30 일마다 재배포하는 것은 번거로움.
B(X) : 스크립트를 사용하는 것은 스크립트를 짜야하므로 번거로움.
C(X) : Lambda 함수를 매번 쓰는 것은 비용 효율성 면에서 좋지 않고 Lambda 코드 짜는 것도 번거로움.
D(O) : TTL 속성을 사용하면 별다른 코딩이나 노력 없이 설정만 해두면 자동으로 삭제되므로 간편함.
Amazon DynamoDB TTL(Time to Live)을 사용하면 항목별 타임스탬프를 정의하여 항목이 더 이상 필요하지 않은 시기를 결정할 수 있습니다. 지정된 타임스탬프의 날짜 및 시간 직후 DynamoDB 는 쓰기 처리량을 소모하지 않고 테이블에서 항목을 삭제합니다.
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html

설명 2:
Amazon DynamoDB TTL(Time to Live)을 사용하면 항목별 타임스탬프를 정의하여 항목이 더 이상 필요하지 않은 시기를 결정할 수 있습니다. 지정된 타임스탬프의 날짜 및 시간 직후 DynamoDB 는 쓰기 처리량을 소비하지 않고 테이블에서 항목을 삭제합니다. TTL 은 워크로드 요구 사항에 따라 최신 상태로 유지되는 항목만 유지하여 저장된 데이터 볼륨을 줄이는 수단으로 추가 비용 없이 제공됩니다. TTL 은 특정 시간이 지나면 관련성을 잃는 항목을 저장할 때 유용합니다.
다음은 TTL 사용 사례의 예입니다.
애플리케이션에서 1 년 동안 활동이 없으면 사용자 또는 센서 데이터를 제거합니다. 만료된

항목을 Amazon DynamoDB Streams 및 AWS Lambda 를 통해 Amazon S3 데이터 레이크에 보관합니다. 계약 또는 규제 의무에 따라 일정 기간 동안 민감한 데이터를 보관합니다.
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html

Q197
A company has a Microsoft.NET application that runs on an on-premises Windows Server. The application stores data by using an Oracle Database Standard
Edition server. The company is planning a migration to AWS and wants to minimize development changes while moving the application. The AWS application environment should be highly available.
Which combination of actions should the company take to meet these requirements? (Choose two)
A. Refactor the application as serverless with AWS Lambda functions running .NET Core.
B. Rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment.
C. Replatform the application to run on Amazon EC2 with the Amazon Linux Amazon Machine Image (AMI).
D. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Amazon DynamoDB in a Multi-AZ deployment.
E. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment.
Answer: B, E
https://www.examtopics.com/discussions/amazon/view/89068-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : 리팩터링은 코드 변경을 수반하므로 개발 변경 사항 최소화 조건 불충족.
B(O) : AWS Elastic Beanstalk.NET 용 에서 Amazon Web Services 를 사용하는 ASP.NET 웹 애플리케이션을 보다 쉽게 배포, 관리 및 조정할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/elasticbeanstalk/latest/dg/create_deploy_NET.html
C(X) : 재플랫폼화는 개발 변경 사항 최소화 조건 불충족.
D(X) : Oracle 데이터베이스는 관계형 데이터베이스이고, DynamoDB 는 비관계형 데이터베이스로 유형이 다름. 개발 변경 최소화 조건 불충족.
E(O) : 다중 AZ 배포로 고가용성 조건 충족. DMS 서비스로 데이터베이스 마이그레이션 가능. RDS for Oracle 로 개발 변경 최소화 가능.

설명 2:
애플리케이션을 AWS 로 이동하는 동안 개발 변경을 최소화하고 높은 수준의 가용성을 보장하기 위해 회사는 다중 AZ 배포에서 .NET 플랫폼을 사용하여 AWS Elastic Beanstalk 에서 애플리케이션을 다시 호스팅할 수 있습니다. 이렇게 하면 애플리케이션 코드를 변경할 필요 없이 고가용성 환경에서 애플리케이션을 실행할 수 있습니다.
또한 회사는 AWS Database Migration Service(AWS DMS)를 사용하여 다중 AZ 배포에서 Oracle 데이터베이스를 Amazon RDS 의 Oracle 로 마이그레이션할 수 있습니다. 이를 통해 회사는 여전히 높은 수준의 가용성을 달성하면서 기존 데이터베이스 플랫폼을 유지할 수 있습니다.

Q198
A company runs a containerized application on a Kubernetes cluster in an on-premises data center. The company is using a MongoDB database for data storage.
The company wants to migrate some of these environments to AWS, but no code changes or deployment method changes are possible at this time. The company needs a solution that minimizes operational overhead.
Which solution meets these requirements?
A. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 worker nodes for compute and MongoDB on EC2 for data storage.
B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute and Amazon DynamoDB for data storage.
C. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 worker nodes for compute and Amazon DynamoDB for data storage.
D. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute and Amazon DocumentDB (with MongoDB compatibility) for data storage.
Answer: D
https://www.examtopics.com/discussions/amazon/view/89078-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
Kubernetes 클러스터 = EKS
MongoDB 호환 = DocumentDB

설명 2:

Amazon DocumentDB(MongoDB 와 호환)는 빠르고 안정적이며 완벽하게 관리되는 데이터베이스 서비스입니다.
Amazon DocumentDB 를 사용하면 클라우드에서 MongoDB 호환 데이터베이스를 쉽게 설정, 운영 및 확장할 수 있습니다. Amazon DocumentDB 를 사용하면 동일한 애플리케이션 코드를 실행하고 MongoDB 에서 사용하는 것과 동일한 드라이버 및 도구를 사용할 수 있습니다.
https://docs.aws.amazon.com/documentdb/latest/developerguide/what-is.html

Q199
A telemarketing company is designing its customer call center functionality on AWS. The company needs a solution that provides multiple speaker recognition and generates transcript files. The company wants to query the transcript files to analyze the business patterns. The transcript files must be stored for 7 years for auditing purposes.
Which solution will meet these requirements?
A. Use Amazon Rekognition for multiple speaker recognition. Store the transcript files in Amazon S3. Use machine learning models for transcript file analysis.
B. Use Amazon Transcribe for multiple speaker recognition. Use Amazon Athena for transcript file analysis.
C. Use Amazon Translate for multiple speaker recognition. Store the transcript files in Amazon Redshift. Use SQL queries for transcript file analysis.
D. Use Amazon Rekognition for multiple speaker recognition. Store the transcript files in Amazon S3. Use Amazon Textract for transcript file analysis.
Answer: B
https://www.examtopics.com/discussions/amazon/view/89141-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : Amazon Rekognition 은 이미지/비디오 분석 서비스. 콜센터라고 했으므로 오디오를 다른 걸로 변환시켜주는 서비스가 필요하므로 오답.
Amazon Rekognition 은 애플리케이션에 강력한 시각 분석 기능을 쉽게 추가할 수 있게 해주는 서비스입니다. Rekognition Image 를 통해 수백만 개의 이미지를 검색, 확인 및 구성할 수 있는 강력한 애플리케이션을 쉽게 구축할 수 있습니다. Rekognition Video 를 통해 저장된 동영상 또는 실시간 스트림 동영상에서 동작 기반 컨텍스트를 추출하고 이를 분석할 수 있습니다. https://aws.amazon.com/ko/rekognition/faqs/
B(O) : Amazon Transcribe 로 다중 Speaker 인식 가능. 7 년 동안 저장해야한다고 했으므로

S3 같은 스토리지 서비스가 필요한데, 해당 선택지에서는 S3 가 언급은 되지 않았으나 S3 에 쿼리하는 Athena 가 있으므로 S3 를 사용하고 있다고 추측할 수 있음.
Amazon Transcribe 는 고객이 손쉽게 음성을 텍스트로 변환할 수 있게 해주는 AWS 서비스입니다. https://aws.amazon.com/ko/transcribe/faqs/
C(X) : Amazon Translate 는 기계 번역 서비스.
Amazon Translate 는 합리적인 가격으로 고품질의 사용자 지정 가능한 언어 번역을 빠르게 제공하는 신경망 기계 번역 서비스입니다. https://aws.amazon.com/ko/translate/
D(X) : A 와 동일한 이유로 오답.

설명 2:
Amazon Transcribe 는 이제 스트리밍 트랜스크립션을 위한 화자 레이블 지정을 지원합니다. Amazon Transcribe 는 음성을 텍스트로 쉽게 변환할 수 있는 자동 음성 인식(ASR) 서비스입니다.
라이브 오디오 전사에서 각 오디오 스트림에는 여러 명의 화자가 포함될 수 있습니다. 이제 화자에게 레이블을 지정하는 기능을 편리하게 켤 수 있으므로 출력 기록에서 누가 무엇을 말하는지 식별하는 데 도움이 됩니다.
https://aws.amazon.com/ko/about-aws/whats-new/2020/08/amazon-transcribe-supports-speaker-labeling-streaming-transcription/

Q200
A company hosts its application on AWS. The company uses Amazon Cognito to manage users. When users log in to the application, the application fetches required data from Amazon DynamoDB by using a REST API that is hosted in Amazon API Gateway. The company wants an AWS managed solution that will control access to the REST API to reduce development efforts.
Which solution will meet these requirements with the LEAST operational overhead?
A. Configure an AWS Lambda function to be an authorizer in API Gateway to validate which user made the request.
B. For each user, create and assign an API key that must be sent with each request. Validate the key by using an AWS Lambda function.
C. Send the user's email address in the header with every request. Invoke an AWS Lambda function to validate that the user with that email address has proper access.
D. Configure an Amazon Cognito user pool authorizer in API Gateway to allow Amazon Cognito to validate each request.
Answer: D

https://www.examtopics.com/discussions/amazon/view/89142-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
Amazon Cognito 콘솔, CLI/SDK 또는 API 를 사용하여 사용자 풀을 만들거나 다른 AWS 계정이 소유한 풀을 사용합니다.

설명 2:
https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-withcognito.html
REST API 에 대한 액세스를 제어하고 개발 노력을 줄이기 위해 회사는 API Gateway 에서 Amazon Cognito 사용자 풀 권한 부여자를 사용할 수 있습니다. 이를 통해 Amazon Cognito 는 각 요청을 검증하고 인증된 사용자만 API 에 액세스할 수 있도록 합니다. 이 솔루션은 회사가 추가 인프라나 코드를 개발하고 유지 관리할 필요가 없으므로 운영 오버헤드가 가장 적습니다.

Q201
A company is developing a marketing communications service that targets mobile app users. The company needs to send confirmation messages with Short Message Service (SMS) to its users. The users must be able to reply to the SMS messages. The company must store the responses for a year for analysis.
What should a solutions architect do to meet these requirements?
A. Create an Amazon Connect contact flow to send the SMS messages. Use AWS Lambda to process the responses.
B. Build an Amazon Pinpoint journey. Configure Amazon Pinpoint to send events to an Amazon Kinesis data stream for analysis and archiving.
C. Use Amazon Simple Queue Service (Amazon SQS) to distribute the SMS messages. Use AWS Lambda to process the responses.
D. Create an Amazon Simple Notification Service (Amazon SNS) FIFO topic. Subscribe an Amazon Kinesis data stream to the SNS topic for analysis and archiving.
Answer: B
https://www.examtopics.com/discussions/amazon/view/89080-exam-aws-certified-solutions-architect-associate-saa-c03/

설명

https://aws.amazon.com/pinpoint/product-details/sms/
양방향 메시징: 고객으로부터 SMS 메시지를 받고 채팅과 같은 대화형 환경에서 회신합니다. Amazon Pinpoint 를 사용하면 고객이 특정 키워드가 포함된 메시지를 보낼 때 자동 응답을 생성할 수 있습니다. Amazon Lex 를 사용하여 대화형 봇을 만들 수도 있습니다. 대부분의 휴대폰 사용자는 들어오는 SMS 메시지를 받은 직후에 읽습니다. 고객에게 긴급하거나 중요한 정보를 제공해야 하는 경우 SMS 메시징이 적합한 솔루션일 수 있습니다. Amazon Pinpoint 를 사용하여 대상 고객 그룹을 생성한 다음 캠페인 기반 메시지를 보낼 수 있습니다. Amazon Pinpoint 를 사용하여 약속 확인, 주문 업데이트, 일회용 암호와 같은 다이렉트 메시지를 보낼 수도 있습니다.

Q202
A company is planning to move its data to an Amazon S3 bucket. The data must be encrypted when it is stored in the S3 bucket. Additionally, the encryption key must be automatically rotated every year.
Which solution will meet these requirements with the LEAST operational overhead?
A. Move the data to the S3 bucket. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use the built-in key rotation behavior of SSE-S3 encryption keys.
B. Create an AWS Key Management Service (AWS KMS) customer managed key. Enable automatic key rotation. Set the S3 bucket's default encryption behavior to use the customer managed KMS key. Move the data to the S3 bucket.
C. Create an AWS Key Management Service (AWS KMS) customer managed key. Set the S3 bucket's default encryption behavior to use the customer managed KMS key. Move the data to the S3 bucket. Manually rotate the KMS key every year.
D. Encrypt the data with customer key material before moving the data to the S3 bucket. Create an AWS Key Management Service (AWS KMS) key without key material. Import the customer key material into the KMS key. Enable automatic key rotation.
Answer: B
https://www.examtopics.com/discussions/amazon/view/89081-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
・S3 버킷에 저장될 때 암호화되므로 SSE(서버 측 암호화). 만약 S3 버킷으로 보내기 전에 암호화하면 CSE(클라이언트 측 암호화)임.
・Amazon S3 버킷에 저장되는 모든 객체를 암호화하는 기본 암호화 동작을 버킷에 설정할

수 있습니다. 객체는 Amazon S3 관리형 키를 사용한 서버 측 암호화(SSE-S3) 또는 AWS Key Management Service(AWS KMS) 키를 사용한 서버 측 암호화를 사용하여 암호화됩니다.
https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/default-bucket-encryption.html
A(X) : 먼저 S3 버킷을 암호화한 게 아니라 데이터를 S3 버킷에 담아놓고 암호화를 했기 때문에 불필요한 배치 작업이 발생.
Amazon S3 기본 암호화를 사용하면 S3 버킷에 대한 기본 암호화 동작을 설정하여 모든 새 객체가 버킷에 저장될 때 암호화되도록 할 수 있습니다. Amazon S3 관리형 키를 사용한 서버 측 암호화(SSE-S3) 또는 AWS Key Management Service(AWS KMS)에 저장된 AWS KMS keys 를 사용한 서버 측 암호화(SSE-KMS)로 객체를 암호화합니다. 서버 측 암호화를 사용하는 경우 Amazon S3 에서는 객체를 디스크에 저장하기 전에 암호화하고 기존 Amazon S3 객체를 암호화하기 위해 Amazon S3 배치 작업을 사용할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/bucket-encryption.html
B(O) : AWS KMS CMK(고객 관리 키)는 원래 키 자동 교체(rotate)을 하진 않지만 이를 활성화할 수 있음.
https://docs.aws.amazon.com/ko_kr/kms/latest/developerguide/concepts.html#customer-cmk
C(X) : 암호화 키는 매년 자동 순환되어야 한다고 했는데 수동 순환이라 오답.
D(X) : S3 버킷으로 이동하기 전에 기본 암호화 동작을 설정하므로 SSE 가 아닌 CSE(클라이언트 측 암호화)임.

설명 2:
SSE-S3 - 무료이며 AWS 소유 CMK(CMK = 고객 마스터 키)를 사용합니다. 암호화 키는 AWS 에서 소유하고 관리하며 여러 계정 간에 공유됩니다. 회전은 여기 표에 표시된 대로 시간에 따라 자동으로 바뀝니다. 시간은 명시적으로 정의되지 않습니다.
SSE-KMS - 두 가지 특징이 있습니다.
AWS 관리형 CMK. 귀하의 계정에 대해서만 생성된 무료 CMK 입니다. 정책을 보고 사용량을 감사할 수만 있고 관리할 수는 없습니다. 교체는 자동입니다. 1095 일(3 년)당 한 번, 고객이 CMK 를 관리합니다. 이것은 사용자가 생성하고 관리할 수 있는 사용자 고유의 키를 사용합니다. 회전은 기본적으로 활성화되어 있지 않습니다. 그러나 활성화하면 1 년마다 자동으로 순환됩니다. 이 변형은 사용자가 가져온 키 자료를 사용할 수도 있습니다. 가져온 자료로 이러한 키를 생성하면 자동 회전이 없습니다. 수동 회전만 가능합니다.
SSE-C - 고객 제공 키. 암호화 키는 AWS 외부에서 사용자가 완전히 관리합니다. AWS 는 이를 교체하지 않습니다.

이 솔루션은 데이터를 Amazon S3 버킷으로 이동하고, 데이터가 S3 버킷에 저장될 때 데이터를 암호화하고, 최소한의 운영 오버헤드로 매년 암호화 키를 자동으로 교체하는 요구 사항을 충족합니다. AWS Key Management Service(AWS KMS)는 데이터의 암호화 키를 생성하고 관리할 수 있는 서비스입니다. 고객 관리형 키는 AWS KMS 에서 생성하고 관리하는 대칭 암호화 키입니다. 고객 관리형 키에 대해 자동 키 교체를 활성화할 수 있습니다. 즉, AWS KMS 는 매년 키에 대한 새로운 암호화 자료를 생성합니다. 고객 관리형 KMS 키를 사용하도록 S3 버킷의 기본 암호화 동작을 설정할 수 있습니다. 즉, 암호화 방법을 지정하지 않고 버킷에 업로드된 모든 객체는 해당 키로 암호화됩니다.
Amazon S3 관리형 암호화 키(SSE-S3)로 서버 측 암호화를 사용하면 암호화 키를 제어하거나 관리할 수 없으므로 옵션 A 는 올바르지 않습니다. SSE-S3 는 각 객체에 대해 고유한 키를 사용하고 S3 에서 정기적으로 순환하는 마스터 키로 해당 키를 암호화합니다. 그러나 SSE-S3 키에 대한 키 교체를 활성화 또는 비활성화하거나 교체 간격을 지정할 수 없습니다.
옵션 C 는 올바르지 않습니다. 매년 KMS 키를 수동으로 교체하면 운영 오버헤드와 복잡성이 증가할 수 있고 교체 프로세스를 잊어버리거나 지연하는 경우 매년 키 교체 요구 사항을 충족하지 못할 수 있기 때문입니다.
데이터를 S3 버킷으로 이동하기 전에 고객 키 자료로 데이터를 암호화하면 운영 오버헤드와 복잡성이 증가할 수 있고 버킷의 모든 객체에 대해 일관된 암호화를 제공하지 못할 수 있으므로 옵션 D 는 올바르지 않습니다. 키 자료 없이 KMS 키를 생성하고 고객 키 자료를 KMS 키로 가져오면 고유한 임의 비트 소스를 사용하여 KMS 키를 생성할 수 있지만 자동 키 순환은 지원하지 않습니다.
참조:
https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html
https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html
https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-encryption.html

Q203
The customers of a finance company request appointments with financial advisors by sending text messages. A web application that runs on Amazon EC2 instances accepts the appointment requests. The text messages are published to an Amazon Simple Queue Service (Amazon SQS) queue through the web application. Another application that runs on EC2 instances then sends meeting invitations and meeting confirmation email messages to the customers. After successful scheduling, this application stores the meeting information in an Amazon DynamoDB database.
As the company expands, customers report that their meeting invitations are taking longer to

arrive.
What should a solutions architect recommend to resolve this issue?
A. Add a DynamoDB Accelerator (DAX) cluster in front of the DynamoDB database.
B. Add an Amazon API Gateway API in front of the web application that accepts the appointment requests.
C. Add an Amazon CloudFront distribution. Set the origin as the web application that accepts the appointment requests.
D. Add an Auto Scaling group for the application that sends meeting invitations. Configure the Auto Scaling group to scale based on the depth of the SQS queue.
Answer: D
https://www.examtopics.com/discussions/amazon/view/89082-exam-aws-certified-solutions-architect-associate-saa-c03/

설명
회의 초대 전달 시간이 길어지는 문제를 해결하기 위해 솔루션 설계자는 회의 초대를 보내는 애플리케이션에 대해 Auto Scaling 그룹을 추가하고 SQS 대기열의 깊이에 따라 확장되도록 Auto Scaling 그룹을 구성하도록 권장할 수 있습니다. 이렇게 하면 약속 요청 수가 증가함에 따라 애플리케이션이 확장되어 회의 초대의 성능 및 배달 시간이 향상됩니다.

Q204
An online retail company has more than 50 million active customers and receives more than 25,000 orders each day. The company collects purchase data for customers and stores this data in Amazon S3. Additional customer data is stored in Amazon RDS.
The company wants to make all the data available to various teams so that the teams can perform analytics. The solution must provide the ability to manage fine-grained permissions for the data and must minimize operational overhead.
Which solution will meet these requirements?
A. Migrate the purchase data to write directly to Amazon RDS. Use RDS access controls to limit access.
B. Schedule an AWS Lambda function to periodically copy data from Amazon RDS to Amazon S3. Create an AWS Glue crawler. Use Amazon Athena to query the data. Use S3 policies to limit access.
C. Create a data lake by using AWS Lake Formation. Create an AWS Glue JDBC connection to Amazon RDS. Register the S3 bucket in Lake Formation. Use Lake Formation access

controls to limit access.
D. Create an Amazon Redshift cluster. Schedule an AWS Lambda function to periodically copy data from Amazon S3 and Amazon RDS to Amazon Redshift. Use Amazon Redshift access controls to limit access.
Answer: C
https://www.examtopics.com/discussions/amazon/view/89083-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(X) : 액세스 제어하는 것까지만 나왔고 어떻게 쿼리할 것인지는 언급 안 함.
B(X) : 처음부터 S3 에 다 저장할 것이지 결국 S3 에 저장할 거면서 왜 RDS 에 저장했다가 다시 S3 에 저장하는지?
C(O) : S3 버킷을 데이터레이크로 만들고 Glue 를 통해서 ETL 함으로서 S3 에 저장된 데이터를 RedShift 같은 서비스에서 사용할 수 있게끔 함. RDS 에 저장된 고객 데이터는 Glue JDBC 를 통해 변환
・S3 버킷을 AWS Lake Formation 을 사용해 데이터레이크로 만들고 Glue 기능 사용해 ETL.
AWS Lake Formation 콘솔, Lake Formation API 또는 AWS 명령줄 인터페이스(AWS CLI)를 사용하여 Amazon S3 위치를 등록할 수 있습니다.
https://docs.aws.amazon.com/lake-formation/latest/dg/register-location.html
Lake Formation 은 콘솔 제어, ETL 코드 생성, 작업 모니터링, 공통 데이터 카탈로그, 서버리스 아키텍처를 포함하여 AWS Glue 에서 공유 인프라를 활용합니다. AWS Glue 는 아직 이러한 유형의 기능에 초점을 맞추고 있는 반면, Lake Formation 은 AWS Glue 기능을 포함하면서, 동시에 데이터 레이크를 구축하고 보안하고 관리하는 데 유용한 추가 기능을 제공합니다.
https://aws.amazon.com/ko/glue/faqs/
・AWS RDS 에 저장된 데이터를 Glue 에서 사용
AWS Glue 는 기본적으로 Amazon Aurora, Amazon RDS for MySQL, Amazon RDS for Oracle, Amazon RDS for PostgreSQL, Amazon RDS for SQL Server, Amazon Redshift, DynamoDB 및 Amazon S3 뿐만 아니라 Amazon EC2 에서 실행되는 Virtual Private Cloud(Amazon VPC)에 있는 MySQL, Oracle, Microsoft SQL Server 및 PostgreSQL 데이터베이스에 저장된 데이터를 지원합니다.
https://aws.amazon.com/ko/glue/faqs/
AWS Glue 는 JDBC 연결을 통해 다음 데이터 스토어에 연결할 수 있습니다. ◎Amazon Redshift. ◎Amazon RDS for MariaDB
https://docs.aws.amazon.com/ko_kr/glue/latest/dg/connection-properties.html#connecti

on-properties-jdbc

・데이터에 대한 세분화된 권한 관리
AWS Lake Formation 은 간단한 권한 부여/취소 메커니즘을 기반으로 하는 권한 모델을 제공합니다. Lake Formation 권한은 AWS Identity and Access Management(IAM) 권한과 결합되어 데이터 레이크에 저장된 데이터 및 해당 데이터를 설명하는 메타데이터에 대한 액세스를 제어합니다.
https://docs.aws.amazon.com/lake-formation/latest/dg/security-data-access.html
D(X) : 주기적으로 처리하라는 요구 사항이 있지 않는 이상 바로바로 처리하는 게 보통인데, 주기적으로 처리하고 있음.

설명 2:
다양한 팀에서 모든 데이터를 사용할 수 있도록 하고 운영 오버헤드를 최소화하기 위해 회사는 AWS Lake Formation 을 사용하여 데이터 레이크를 생성할 수 있습니다. 이를 통해 회사는 모든 데이터를 한 곳에서 중앙 집중화하고 세분화된 액세스 제어를 사용하여 데이터에 대한 액세스를 관리할 수 있습니다. 회사의 요구 사항을 충족하기 위해 솔루션 설계자는 AWS Lake Formation 을 사용하여 데이터 레이크를 만들고, Amazon RDS 에 대한 AWS Glue JDBC 연결을 만들고, Lake Formation 에 S3 버킷을 등록할 수 있습니다. 그런 다음 솔루션 설계자는 Lake Formation 액세스 제어를 사용하여 데이터에 대한 액세스를 제한할 수 있습니다. 이 솔루션은 데이터에 대한 세분화된 권한을 관리하고 운영 오버헤드를 최소화하는 기능을 제공합니다.

Q205
A company hosts a marketing website in an on-premises data center. The website consists of static documents and runs on a single server. An administrator updates the website content infrequently and uses an SFTP client to upload new documents.
The company decides to host its website on AWS and to use Amazon CloudFront. The company's solutions architect creates a CloudFront distribution. The solutions architect must design the most cost-effective and resilient architecture for website hosting to serve as the CloudFront origin.
Which solution will meet these requirements?
A. Create a virtual server by using Amazon Lightsail. Configure the web server in the Lightsail instance. Upload website content by using an SFTP client.
B. Create an AWS Auto Scaling group for Amazon EC2 instances. Use an Application Load Balancer. Upload website content by using an SFTP client.

C. Create a private Amazon S3 bucket. Use an S3 bucket policy to allow access from a CloudFront origin access identity (OAI). Upload website content by using the AWS CLI.
D. Create a public Amazon S3 bucket. Configure AWS Transfer for SFTP. Configure the S3 bucket for website hosting. Upload website content by using the SFTP client.
Answer: C
https://www.examtopics.com/discussions/amazon/view/89085-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
프라이빗 S3 에서 웹사이트를 호스팅하면 정적 웹사이트 콘텐츠를 위한 비용 효율적이고 가용성이 높은 스토리지를 제공합니다. CloudFront OAI 의 액세스를 허용하도록 버킷 정책을 구성하면 CloudFront 를 통해서만 S3 에 안전하게 액세스할 수 있습니다. 이렇게 하면 웹사이트 콘텐츠가 S3 를 비공개로 유지하면서 CloudFront 를 통해 제공됩니다. AWS CLI 를 사용하여 웹 사이트 콘텐츠를 업로드하면 콘텐츠를 쉽고 효율적으로 관리할 수 있습니다.

A. Lightsail 가상 서버에서 웹 사이트를 호스팅하면 정적 콘텐츠 호스팅에 S3 를 직접 사용하는 것과 비교하여 추가 관리 오버헤드와 비용이 발생합니다.
B. 정적 웹 사이트 콘텐츠를 제공하기 위해 EC2 인스턴스 및 ALB 와 함께 AWS ASG 를 사용할 필요가 없습니다. 불필요한 복잡성과 비용이 추가됩니다.
D. AWS Transfer for SFTP 를 사용하면 SFTP 업로드가 가능하지만 AWS CLI 를 사용하여 콘텐츠를 S3 에 직접 업로드하는 것과 비교하여 추가 비용과 복잡성이 발생합니다. 또한 공용 S3 에서 웹 사이트 콘텐츠를 호스팅하는 것은 보안 관점에서 바람직하지 않을 수 있습니다.

참고:
https://docs.aws.amazon.com/cli/latest/reference/transfer/describe-server.html

Q206
A company wants to manage Amazon Machine Images (AMIs). The company currently copies AMIs to the same AWS Region where the AMIs were created. The company needs to design an application that captures AWS API calls and sends alerts whenever the Amazon EC2 CreateImage API operation is called within the company's account.
Which solution will meet these requirements with the LEAST operational overhead?
A. Create an AWS Lambda function to query AWS CloudTrail logs and to send an alert when a CreateImage API call is detected.

B. Configure AWS CloudTrail with an Amazon Simple Notification Service (Amazon SNS) notification that occurs when updated logs are sent to Amazon S3. Use Amazon Athena to create a new table and to query on CreateImage when an API call is detected.
C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for the CreateImage API call. Configure the target as an Amazon Simple Notification Service (Amazon SNS) topic to send an alert when a CreateImage API call is detected.
D. Configure an Amazon Simple Queue Service (Amazon SQS) FIFO queue as a target for AWS CloudTrail logs. Create an AWS Lambda function to send an alert to an Amazon Simple Notification Service (Amazon SNS) topic when a CreateImage API call is detected.
Answer: C
https://www.examtopics.com/discussions/amazon/view/89086-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/WindowsGuide/monitor-ami-events.html
CreateImage API 호출에 대한 Amazon EventBridge(Amazon CloudWatch Events) 규칙을 생성하고 CreateImage API 호출이 감지될 때 알림을 보내도록 대상을 Amazon Simple Notification Service(Amazon SNS) 주제로 구성하면 운영 오버헤드가 최소인 요구 사항을 충족합니다. .
Amazon EventBridge 는 자체 애플리케이션, 통합 SaaS(Software as a Service) 애플리케이션 및 AWS 서비스의 데이터를 사용하여 애플리케이션을 쉽게 함께 연결할 수 있게 해주는 서버리스 이벤트 버스입니다. CreateImage API 호출에 대한 EventBridge 규칙을 생성하여 회사는 계정 내에서 이 작업이 호출될 때마다 경고를 설정할 수 있습니다. 경고는 SNS 주제로 보낼 수 있으며, 그런 다음 회사의 이메일 또는 기타 원하는 대상으로 알림을 보내도록 구성할 수 있습니다.

참고
https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/WindowsGuide/monitor-ami-events.html

Q207
A company owns an asynchronous API that is used to ingest user requests and, based on the request type, dispatch requests to the appropriate microservice for processing. The company is using Amazon API Gateway to deploy the API front end, and an AWS Lambda

function that invokes Amazon DynamoDB to store user requests before dispatching them to the processing microservices.
The company provisioned as much DynamoDB throughput as its budget allows, but the company is still experiencing availability issues and is losing user requests.
What should a solutions architect do to address this issue without impacting existing users?
A. Add throttling on the API Gateway with server-side throttling limits.
B. Use DynamoDB Accelerator (DAX) and Lambda to buffer writes to DynamoDB.
C. Create a secondary index in DynamoDB for the table with the user requests.
D. Use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB.
Answer: D
https://www.examtopics.com/discussions/amazon/view/89087-exam-aws-certified-solutions-architect-associate-saa-c03/

설명
솔루션 설계자는 SQS 대기열과 Lambda 를 사용하여 처리 마이크로서비스에서 API 프런트 엔드를 분리하고 시스템의 전반적인 확장성과 가용성을 개선할 수 있습니다. SQS 대기열은 버퍼 역할을 하여 API 프런트 엔드가 마이크로서비스 처리에 높은 작업 부하가 발생하거나 일시적으로 사용할 수 없는 경우에도 사용자 요청을 계속 수락할 수 있도록 합니다. 그런 다음 Lambda 함수는 SQS 대기열에서 요청을 검색하고 DynamoDB 에 기록하여 모든 사용자 요청이 저장 및 처리되도록 할 수 있습니다. 이 접근 방식을 통해 회사는 API 프런트 엔드와 독립적으로 처리 마이크로서비스를 확장할 수 있으므로 수요가 많은 기간에도 사용자가 API 를 계속 사용할 수 있습니다.

즉 사용자 요청을 잃고 있음 = SQS 로 해결. 정답은 D.

Q208
A company needs to move data from an Amazon EC2 instance to an Amazon S3 bucket. The company must ensure that no API calls and no data are routed through public internet routes. Only the EC2 instance can have access to upload data to the S3 bucket.
Which solution will meet these requirements?
A. Create an interface VPC endpoint for Amazon S3 in the subnet where the EC2 instance is located. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
B. Create a gateway VPC endpoint for Amazon S3 in the Availability Zone where the EC2

instance is located. Attach appropriate security groups to the endpoint. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
C. Run the nslookup tool from inside the EC2 instance to obtain the private IP address of the S3 bucket's service API endpoint. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
D. Use the AWS provided, publicly available ip-ranges.json file to obtain the private IP address of the S3 bucket's service API endpoint. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
Answer: A
https://www.examtopics.com/discussions/amazon/view/89088-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
EC2 인스턴스-S3 버킷 간 통신이 인터넷에 노출되지 않음 = S3 Gateway Endpoint.

설명 2:
EC2 인스턴스와 동일한 서브넷에 Amazon S3 용 인터페이스 VPC 종단점을 생성하면 EC2 인스턴스와 S3 간의 데이터 전송이 공용 인터넷을 거치지 않고 Amazon 네트워크 내에서 비공개로 발생할 수 있습니다. 이렇게 하면 EC2 인스턴스와 S3 간의 안전하고 직접적인 통신이 보장됩니다. EC2 인스턴스와 연결된 IAM 역할의 액세스만 허용하는 리소스 정책을 S3 버킷에 연결하면 권한이 부여된 인스턴스에 대한 액세스만 추가로 제한됩니다.

B. Amazon S3 용 게이트웨이 VPC 종단점을 생성하려면 공용 인터넷을 통한 라우팅이 여전히 필요하므로 이 경우에는 바람직하지 않습니다.
C. nslookup 을 실행하거나 VPC 경로 테이블에서 특정 경로를 생성하면 트래픽이 여전히 공용 인터넷 경로를 통과할 수 있으므로 원하는 수준의 보안 및 개인 정보 보호를 제공하지 않습니다.
D. 공개적으로 사용 가능한 ip-ranges.json 파일을 사용하여 S3 버킷의 서비스 API 엔드포인트의 프라이빗 IP 주소를 얻는 것은 권장되는 접근 방식이 아닙니다. IP 주소는 시간이 지남에 따라 변경될 수 있고 동일한 수준의 보안을 제공하지 않기 때문입니다. VPC 엔드포인트를 사용합니다.

참고
https://aws.amazon.com/blogs/security/how-to-restrict-amazon-s3-bucket-access-to-

a-specific-iamrole/

Q209

A solutions architect is designing the architecture of a new application being deployed to the AWS Cloud. The application will run on Amazon EC2 On-Demand Instances and will automatically scale across multiple Availability Zones. The EC2 instances will scale up and down frequently throughout the day. An Application Load Balancer (ALB) will handle the load distribution. The architecture needs to support distributed session data management. The company is willing to make changes to code if needed.

What should the solutions architect do to ensure that the architecture supports distributed session data management?

A. Use Amazon ElastiCache to manage and store session data.

B. Use session affinity (sticky sessions) of the ALB to manage session data.

C. Use Session Manager from AWS Systems Manager to manage the session.

D. Use the GetSessionToken API operation in AWS Security Token Service (AWS STS) to manage the session.

Answer: A

https://www.examtopics.com/discussions/amazon/view/89089-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

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

확장성을 해결하고 개별 웹 서버에서 액세스할 수 있는 세션에 대한 공유 데이터 저장소를 제공하기 위해 웹 서버 자체에서 HTTP 세션을 추상화할 수 있습니다.

이에 대한 일반적인 솔루션은 Redis 및 Memcached 와 같은 메모리 내 키/값 저장소를 활용하는 것입니다. 메모리 내 키/값 저장소용 ElastiCache 제품에는 복제를 지원할 수 있는 Redis 용 ElastiCache 와 복제를 지원하지 않는 Memcached 용 ElastiCache 가 포함됩니다.

설명 2:

A(O) : 분산 세션 관리 : 확장성을 해결하고 개별 웹 서버에서 액세스할 수 있는 세션에 대한 공유 데이터 저장소를 제공하기 위해 웹 서버 자체에서 HTTP 세션을 추상화할 수 있습니다. 이에 대한 일반적인 솔루션은 Redis 및 Memcached 와 같은 메모리 내 키/값 저장소 를 활용하는 것 입니다.

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

Redis 용 Amazon ElastiCache 는 사용자 인증 토큰, 세션 상태 등 세션 정보를 관리하는 세션 스토어로 사용하기에 매우 적합합니다. Redis 용 Amazon ElastiCache 를 세션 키에 대한 적절한 TTL 과 함께 빠른 키-값 스토어로 사용하면 세션 정보를 관리할 수 있습니다.
https://aws.amazon.com/ko/elasticache/redis/?nc=sn&loc=2&dn=1#Session_Store
B(X) : EC2 인스턴스는 하루 종일 자주 확장 및 축소된다고 했는데 Session Affinity(=Sticky Session)은 이에 맞지 않음. ""개별 노드에 세션 저장을 사용할 때의 단점은 장애가 발생할 경우 장애가 발생한 노드에 있던 세션이 손실될 가능성이 있다는 것입니다. 또한 웹 서버 수가 변경되는 경우(예: 확장 시나리오) 활성 세션이 특정 서버에 존재할 수 있으므로 트래픽이 웹 서버 전체에 불균등하게 분산될 수 있습니다.
https://aws.amazon.com/ko/caching/session-management/
C(X) : Session Manager 는 접속 서비스이지 데이터 관리 서비스가 아님. Session Manager 는 인바운드 포트를 열거나, 배스천 호스트를 유지하거나, SSH 키를 관리할 필요 없이 안전하고 감사 가능한 노드 관리를 제공
https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html
D(X) : STS 는 임시 보안 자격 증명 서비스. ""AWS Security Token Service(AWS STS)를 사용하면 AWS 리소스에 대한 액세스를 제어할 수 있는 임시 보안 자격 증명을 생성하여 신뢰받는 사용자에게 제공할 수 있습니다.
https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/id_credentials_temp.html

Q210
A company offers a food delivery service that is growing rapidly. Because of the growth, the company's order processing system is experiencing scaling problems during peak traffic hours. The current architecture includes the following:
• A group of Amazon EC2 instances that run in an Amazon EC2 Auto Scaling group to collect orders from the application.
• Another group of EC2 instances that run in an Amazon EC2 Auto Scaling group to fulfill orders.
The order collection process occurs quickly, but the order fulfillment process can take longer. Data must not be lost because of a scaling event.
A solutions architect must ensure that the order collection process and the order fulfillment process can both scale properly during peak traffic hours. The solution must optimize utilization of the company's AWS resources.
Which solution meets these requirements?
A. Use Amazon CloudWatch metrics to monitor the CPU of each instance in the Auto Scaling groups. Configure each Auto Scaling group's minimum capacity according to peak workload

values.
B. Use Amazon CloudWatch metrics to monitor the CPU of each instance in the Auto Scaling groups. Configure a CloudWatch alarm to invoke an Amazon Simple Notification Service (Amazon SNS) topic that creates additional Auto Scaling groups on demand.
C. Provision two Amazon Simple Queue Service (Amazon SQS) queues: one for order collection and another for order fulfillment. Configure the EC2 instances to poll their respective queue. Scale the Auto Scaling groups based on notifications that the queues send.
D. Provision two Amazon Simple Queue Service (Amazon SQS) queues: one for order collection and another for order fulfillment. Configure the EC2 instances to poll their respective queue. Create a metric based on a backlog per instance calculation. Scale the Auto Scaling groups based on this metric.
Answer: D
https://www.examtopics.com/discussions/amazon/view/94992-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
Auto Scaling 그룹의 인스턴스 수는 메시지를 처리하는 데 걸리는 시간과 허용 가능한 지연 시간(대기열 지연)에 따라 결정될 수 있습니다. 해결책은 유지 관리할 인스턴스당 허용 가능한 백로그인 대상 값과 함께 인스턴스 메트릭당 백로그를 사용하는 것입니다.

설명 2:
A. 이 접근 방식은 CPU 사용률에만 초점을 맞추므로 주문 수집 및 이행 프로세스의 확장 요구 사항을 정확하게 반영하지 못할 수 있습니다. 분리 및 신뢰할 수 있는 메시지 처리에 대한 요구 사항은 다루지 않습니다.

B. 이 접근 방식은 경보를 통합하여 추가 Auto Scaling 그룹을 트리거하지만 SQS 대기열을 사용하여 제공되는 분리 및 안정적인 메시지 처리가 부족합니다. 비효율적인 확장 및 잠재적인 데이터 손실이 발생할 수 있습니다.

C. SQS 대기열을 사용하는 것이 올바른 방향으로 나아가는 단계이지만 대기열 알림만을 기준으로 확장하는 것은 최적의 리소스 활용을 제공하지 못할 수 있습니다. 인스턴스당 백로그를 고려하지 않으며 조정에 대한 세밀한 제어를 허용하지 않습니다.

전반적으로 주문 수집 및 이행을 위해 SQS 대기열을 사용하고, 인스턴스 계산당 백로그를 기반으로 메트릭을 생성하고, 이에 따라 Auto Scaling 그룹을 확장하는 옵션 D 는 리소스

활용을 최적화하고 보장하면서 확장 문제를 해결하는 가장 적합한 솔루션입니다. 신뢰할 수 있는 메시지 처리

Q211

A company hosts multiple production applications. One of the applications consists of resources from Amazon EC2, AWS Lambda, Amazon RDS, Amazon Simple Notification Service (Amazon SNS), and Amazon Simple Queue Service (Amazon SQS) across multiple AWS Regions. All company resources are tagged with a tag name of "application" and a value that corresponds to each application. A solutions architect must provide the quickest solution for identifying all of the tagged components.

Which solution meets these requirements?

A. Use AWS CloudTrail to generate a list of resources with the application tag.

B. Use the AWS CLI to query each service across all Regions to report the tagged components.

C. Run a query in Amazon CloudWatch Logs Insights to report on the components with the application tag.

D. Run a query with the AWS Resource Groups Tag Editor to report on the resources globally with the application tag.

Answer: D

https://www.examtopics.com/discussions/amazon/view/95145-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

CloudTrail 은 주로 API 활동 캡처 및 로깅에 중점을 두기 때문에 A 는 가장 빠른 솔루션이 아닙니다. 리소스 변경에 대한 정보를 제공할 수 있지만 여러 서비스 및 리전에서 태그가 지정된 모든 구성 요소를 식별하는 포괄적이고 빠른 방법을 제공하지 않을 수 있습니다.

B 에는 AWS CLI 를 사용하여 각 서비스를 수동으로 쿼리하는 작업이 포함되며, 이는 특히 여러 서비스 및 리전을 처리할 때 시간이 많이 걸리고 번거로울 수 있습니다. 태그가 지정된 구성 요소를 빠르게 식별하기 위한 가장 효율적인 솔루션은 아닙니다.

C 는 태그가 지정된 구성 요소를 직접 식별하기보다는 로그 분석에 중점을 둡니다. CloudWatch Logs Insights 는 로그에서 정보를 추출하는 데 도움이 될 수 있지만 여러 서비스 및 리전에서 태그가 지정된 모든 구성 요소의 통합 목록을 수집하는 간단하고 빠른 방법을 제공하지 않을 수 있습니다.

D 는 태그를 기반으로 리소스를 관리하고 구성하도록 특별히 설계된 Resource Groups Tag Editor 를 활용하므로 가장 빠른 솔루션입니다. 여러 서비스 및 리전에서 태그가 지정된 구성 요소에 대한 보고서를 생성하는 중앙 집중식의 효율적인 접근 방식을 제공합니다.

참고:
https://docs.aws.amazon.com/tag-editor/latest/userguide/tagging.html

Q212
A company needs to export its database once a day to Amazon S3 for other teams to access. The exported object size varies between 2 GB and 5 GB. The S3 access pattern for the data is variable and changes rapidly. The data must be immediately available and must remain accessible for up to 3 months. The company needs the most cost-effective solution that will not increase retrieval time.
Which S3 storage class should the company use to meet these requirements?
A. S3 Intelligent-Tiering
B. S3 Glacier Instant Retrieval
C. S3 Standard
D. S3 Standard-Infrequent Access (S3 Standard-IA)
Answer: A
https://www.examtopics.com/discussions/amazon/view/95300-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
옵션 A 는 액세스 패턴이 변화하는 개체를 위해 설계되었지만 특히 액세스 패턴이 가변적이고 빠르게 변경되는 경우 데이터의 장기 저장을 위한 가장 비용 효율적인 솔루션이 아닐 수 있습니다.

옵션 B 는 장기 아카이브 저장에 최적화되어 있으며 회사에서 요구하는 즉각적인 액세스를 제공하지 않을 수 있습니다. Glacier 스토리지에서 데이터를 검색하면 일반적으로 다른 스토리지 클래스에 비해 검색 시간이 더 오래 걸립니다.

옵션 C 는 즉각적인 가용성과 데이터에 대한 빠른 액세스를 위한 적절한 선택입니다. 높은 내구성, 가용성 및 낮은 대기 시간 액세스를 제공하므로 회사의 요구 사항에 적합합니다. 그러나 장기 보관을 위한 가장 비용 효율적인 옵션은 아닙니다.

옵션 D 는 특히 자주 액세스하지 않는 데이터의 경우 S3 Standard 에 비해 비용 효율적인 스토리지 클래스입니다. 그러나 데이터에 대한 액세스 패턴이 가변적이고 빠르게 변경되기 때문에 S3 Standard-IA 는 빈번한 액세스에 대한 추가 검색 비용이 발생하므로 가장 비용 효율적인 솔루션이 아닐 수 있습니다.

Q213

A company is developing a new mobile app. The company must implement proper traffic filtering to protect its Application Load Balancer (ALB) against common application-level attacks, such as cross-site scripting or SQL injection. The company has minimal infrastructure and operational staff. The company needs to reduce its share of the responsibility in managing, updating, and securing servers for its AWS environment.

What should a solutions architect recommend to meet these requirements?

A. Configure AWS WAF rules and associate them with the ALB.

B. Deploy the application using Amazon S3 with public hosting enabled.

C. Deploy AWS Shield Advanced and add the ALB as a protected resource.

D. Create a new ALB that directs traffic to an Amazon EC2 instance running a third-party firewall, which then passes the traffic to the current ALB.

Answer: A

https://www.examtopics.com/discussions/amazon/view/95301-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

솔루션 설계자는 AWS WAF 규칙을 구성하고 이를 ALB 와 연결하는 옵션 A 를 권장해야 합니다. 이를 통해 회사는 교차 사이트 스크립팅 또는 SQL 주입과 같은 일반적인 애플리케이션 수준 공격으로부터 ALB를 보호하는 데 필요한 애플리케이션 계층에서 트래픽 필터링을 적용할 수 있습니다. AWS WAF 는 애플리케이션 가용성에 영향을 미치거나 보안을 손상시키거나 과도한 리소스를 소비할 수 있는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션을 쉽게 보호할 수 있게 해주는 관리형 서비스입니다. 회사는 애플리케이션의 보안을 보장하기 위해 규칙을 쉽게 관리하고 업데이트할 수 있습니다.

설명 2:

AWS WAF 규칙을 구성하고 이를 ALB 와 연결함으로써 회사는 악성 트래픽이 애플리케이션에 도달하기 전에 필터링하고 차단할 수 있습니다. AWS WAF 는 사전 구성된 규칙 세트를 제공하고 사용자 지정 규칙 생성을 허용하여 XSS 및 SQL 주입과 같은

일반적인 취약성으로부터 보호합니다.

옵션 B 는 애플리케이션 수준 공격으로부터 보호하는 데 필요한 보안 및 트래픽 필터링 기능을 제공하지 않습니다. 보안 조치를 구현하는 것보다 정적 콘텐츠를 호스팅하는 데 더 적합합니다.
옵션 C 는 XSS 또는 SQL 주입과 같은 애플리케이션 수준 공격이 아닌 DDoS 보호에 중점을 둡니다. AWS Shield Advanced 는 시나리오에 언급된 특정 요구 사항을 다루지 않습니다.
옵션 D 는 추가 인프라를 유지하고 보호하는 것과 관련되며, 이는 책임을 줄이고 최소한의 운영 직원에 의존해야 한다는 요구 사항에 위배됩니다.

Q214
A company's reporting system delivers hundreds of .csv files to an Amazon S3 bucket each day. The company must convert these files to Apache Parquet format and must store the files in a transformed data bucket.
Which solution will meet these requirements with the LEAST development effort?
A. Create an Amazon EMR cluster with Apache Spark installed. Write a Spark application to transform the data. Use EMR File System (EMRFS) to write files to the transformed data bucket.
B. Create an AWS Glue crawler to discover the data. Create an AWS Glue extract, transform, and load (ETL) job to transform the data. Specify the transformed data bucket in the output step.
C. Use AWS Batch to create a job definition with Bash syntax to transform the data and output the data to the transformed data bucket. Use the job definition to submit a job. Specify an array job as the job type.
D. Create an AWS Lambda function to transform the data and output the data to the transformed data bucket. Configure an event notification for the S3 bucket. Specify the Lambda function as the destination for the event notification.
Answer: B
https://www.examtopics.com/discussions/amazon/view/95154-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
AWS Glue 는 분석을 위해 데이터를 준비하고 변환하는 프로세스를 간소화하는 완전 관리형 ETL 서비스입니다. AWS Glue 를 사용하려면 다른 옵션에 비해 최소한의 개발 노력이

필요합니다.

옵션 A 는 데이터 변환을 위한 Spark 애플리케이션 작성과 관련되므로 더 많은 개발 노력이 필요합니다. 또한 EMR 클러스터로 추가 인프라 관리를 소개합니다.

옵션 C 는 데이터 변환을 위한 사용자 지정 Bash 스크립트를 작성하고 관리해야 합니다. 수동 작업이 더 많이 필요하며 데이터 변환을 위한 AWS Glue 의 내장 기능을 제공하지 않습니다.

옵션 D 는 데이터 변환을 위해 사용자 지정 Lambda 를 개발하고 관리해야 합니다. Lambda 는 변환을 처리할 수 있지만 ETL 작업을 위해 특별히 설계된 AWS Glue 에 비해 더 많은 노력이 필요합니다.

따라서 옵션 B 는 AWS Glue 의 데이터 검색, 변환 및 변환된 데이터 버킷으로의 출력 기능을 활용하여 가장 쉽고 최소한의 개발 노력을 제공합니다.

참고:
https://docs.aws.amazon.com/ko_kr/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html

Q215
A company has 700 TB of backup data stored in network attached storage (NAS) in its data center. This backup data need to be accessible for infrequent regulatory requests and must be retained 7 years. The company has decided to migrate this backup data from its data center to AWS. The migration must be complete within 1 month. The company has 500 Mbps of dedicated bandwidth on its public internet connection available for data transfer.
What should a solutions architect do to migrate and store the data at the LOWEST cost?
A. Order AWS Snowball devices to transfer the data. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
B. Deploy a VPN connection between the data center and Amazon VPC. Use the AWS CLI to copy the data from on premises to Amazon S3 Glacier.
C. Provision a 500 Mbps AWS Direct Connect connection and transfer the data to Amazon S3. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
D. Use AWS DataSync to transfer the data and deploy a DataSync agent on premises. Use the DataSync task to copy files from the on-premises NAS storage to Amazon S3 Glacier.

Answer: A
https://www.examtopics.com/discussions/amazon/view/94983-exam-aws-certified-solutions-architect-associate-saa-c03/

해설:
700TB 나 되는 대용량을 Snowball Edge Device 를 사용하지 않고 네트워크 상으로 옮기는 것은 굉장히 많은 시간이 소요됨.
https://kindloveit.tistory.com/68
https://www.omnicalculator.com/other/data-transfer

Q216
A company has a serverless website with millions of objects in an Amazon S3 bucket. The company uses the S3 bucket as the origin for an Amazon CloudFront distribution. The company did not set encryption on the S3 bucket before the objects were loaded. A solutions architect needs to enable encryption for all existing objects and for all objects that are added to the S3 bucket in the future.
Which solution will meet these requirements with the LEAST amount of effort?
A. Create a new S3 bucket. Turn on the default encryption settings for the new S3 bucket. Download all existing objects to temporary local storage. Upload the objects to the new S3 bucket.
B. Turn on the default encryption settings for the S3 bucket. Use the S3 Inventory feature to create a .csv file that lists the unencrypted objects. Run an S3 Batch Operations job that uses the copy command to encrypt those objects.
C. Create a new encryption key by using AWS Key Management Service (AWS KMS). Change the settings on the S3 bucket to use server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Turn on versioning for the S3 bucket.
D. Navigate to Amazon S3 in the AWS Management Console. Browse the S3 bucket's objects. Sort by the encryption field. Select each unencrypted object. Use the Modify button to apply default encryption settings to every unencrypted object in the S3 bucket.
Answer: B
https://www.examtopics.com/discussions/amazon/view/95040-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
S3 에서 기본 암호화 설정을 활성화하면 새로 추가된 모든 객체가 자동으로 암호화됩니다.

기존 객체를 암호화하기 위해 S3 Inventory 기능을 사용하여 암호화되지 않은 객체 목록을 생성할 수 있습니다. 그런 다음 암호화를 적용하는 동안 해당 객체를 복사하기 위해 S3 배치 작업 작업을 실행할 수 있습니다.
A. 이 솔루션에는 새 S3 를 생성하고 모든 기존 개체를 수동으로 다운로드 및 업로드하는 작업이 포함됩니다. 수백만 개의 개체를 전송하는 데 상당한 노력과 시간이 필요하므로 효율성이 떨어지는 솔루션입니다.
C. AWS KMS 로 SSE 를 활성화하는 것은 S3 에서 객체를 암호화하는 유효한 접근 방식이지만 기존 객체를 암호화해야 하는 요구 사항을 해결하지는 않습니다. 버킷에 추가된 새 객체에만 암호화를 적용합니다.
D. 기본 암호화 설정을 적용하기 위해 S3 의 각 개체를 수동으로 수정하는 것은 노동 집약적이고 오류가 발생하기 쉬운 프로세스입니다. 암호화되지 않은 각 개체를 개별적으로 선택하고 수정해야 하므로 많은 수의 개체에 비실용적입니다.

참고:
https://spin.atomicobject.com/2020/09/15/aws-s3-encrypt-existing-objects/

Q217
A company runs a global web application on Amazon EC2 instances behind an Application Load Balancer. The application stores data in Amazon Aurora. The company needs to create a disaster recovery solution and can tolerate up to 30 minutes of downtime and potential data loss. The solution does not need to handle the load when the primary infrastructure is healthy.
What should a solutions architect do to meet these requirements?
A. Deploy the application with the required infrastructure elements in place. Use Amazon Route 53 to configure active-passive failover. Create an Aurora Replica in a second AWS Region.
B. Host a scaled-down deployment of the application in a second AWS Region. Use Amazon Route 53 to configure active-active failover. Create an Aurora Replica in the second Region.
C. Replicate the primary infrastructure in a second AWS Region. Use Amazon Route 53 to configure active-active failover. Create an Aurora database that is restored from the latest snapshot.
D. Back up data with AWS Backup. Use the backup to create the required infrastructure in a second AWS Region. Use Amazon Route 53 to configure active-passive failover. Create an Aurora second primary instance in the second Region.

Answer: A
https://www.examtopics.com/discussions/amazon/view/95015-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
솔루션은 기본 인프라가 정상일 때 부하를 처리할 필요가 없다고 했으므로 Active/Passive Failover 를 사용하면 됨. 따라서 A,D 둘 중 하나가 답.
A(O) : Q: Amazon Aurora 는 교차 리전 복제를 지원하나요? 예. 물리적 또는 논리적 복제를 사용하여 교차 리전 Aurora 복제본을 설정할 수 있습니다. Amazon RDS 콘솔에서 교차 리전 복제본을 새로운 기본 복제본으로 승격할 수 있습니다. 논리적(binlog) 복제의 경우, 승격 프로세스는 워크로드에 따라 다르지만 보통 몇 분 정도 걸립니다. 승격 프로세스를 시작하면 교차 리전 복제가 중단됩니다. https://aws.amazon.com/ko/rds/aurora/faqs/
D(X) : 굳이 AWS Backup 을 사용하지 않아도 오로라 교차 리전 복제본 (Aurora Cross Region Replica)를 사용하면 됨. 그리고 글로벌 웹 애플리케이션을 사용한다고 했는데 이런 경우엔 데이터를 복제해 인스턴스를 다른 리전에 생성하는 것보단 복제본을 사용해서 각 지역에서 읽기 쿼리를 할 때 지연시간을 줄이는 것이 더 좋음.

참고:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html

Q218
A company has a web server running on an Amazon EC2 instance in a public subnet with an Elastic IP address. The default security group is assigned to the EC2 instance. The default network ACL has been modified to block all traffic. A solutions architect needs to make the web server accessible from everywhere on port 443.
Which combination of steps will accomplish this task? (Choose two)
A. Create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0.
B. Create a security group with a rule to allow TCP port 443 to destination 0.0.0.0/0.
C. Update the network ACL to allow TCP port 443 from source 0.0.0.0/0.
D. Update the network ACL to allow inbound/outbound TCP port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0.
E. Update the network ACL to allow inbound TCP port 443 from source 0.0.0.0/0 and outbound TCP port 32768-65535 to destination 0.0.0.0/0.
Answer: A, E
https://www.examtopics.com/discussions/amazon/view/95056-exam-aws-certified-solut

ions-architect-associate-saa-c03/

설명:
포트 443 의 모든 위치에서 웹 서버에 액세스할 수 있도록 하는 작업을 수행하는 단계 조합은 소스 0.0.0.0/0(A)에서 TCP 포트 443 을 허용하고 네트워크 ACL 을 업데이트하는 규칙으로 보안 그룹을 생성하는 것입니다. 소스 0.0.0.0/0(C)에서 인바운드 TCP 포트 443 을 허용합니다.
이렇게 하면 포트 443 에 대한 트래픽이 보안 그룹 수준과 네트워크 ACL 수준 모두에서 허용되어 포트 443 의 모든 위치에서 웹 서버에 액세스할 수 있습니다.

Q219
A company's application is having performance issues. The application is stateful and needs to complete in-memory tasks on Amazon EC2 instances. The company used AWS CloudFormation to deploy infrastructure and used the M5 EC2 instance family. As traffic increased, the application performance degraded. Users are reporting delays when the users attempt to access the application.
Which solution will resolve these issues in the MOST operationally efficient way?
A. Replace the EC2 instances with T3 EC2 instances that run in an Auto Scaling group. Make the changes by using the AWS Management Console.
B. Modify the CloudFormation templates to run the EC2 instances in an Auto Scaling group. Increase the desired capacity and the maximum capacity of the Auto Scaling group manually when an increase is necessary.
C. Modify the CloudFormation templates. Replace the EC2 instances with R5 EC2 instances. Use Amazon CloudWatch built-in EC2 memory metrics to track the application performance for future capacity planning.
D. Modify the CloudFormation templates. Replace the EC2 instances with R5 EC2 instances. Deploy the Amazon CloudWatch agent on the EC2 instances to generate custom application latency metrics for future capacity planning.
Answer: D
https://www.examtopics.com/discussions/amazon/view/95162-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
M5 인스턴스를 메모리 집약적인 워크로드에 최적화된 R5 인스턴스로 교체하면 애플리케이션에서 메모리 용량과 성능을 높일 수 있습니다.

또한 EC2 인스턴스에 CloudWatch 에이전트를 배포하면 애플리케이션 성능에 대한 중요한 통찰력을 제공할 수 있는 사용자 지정 애플리케이션 대기 시간 메트릭을 생성할 수 있습니다.
이 솔루션은 적절한 인스턴스 유형을 활용하고 더 나은 모니터링 및 향후 용량 계획을 위해 사용자 지정 애플리케이션 메트릭을 수집하여 성능 문제를 효율적으로 해결합니다.

A. T3 인스턴스로 교체하면 인 메모리 작업에 충분한 메모리 용량을 제공하지 못할 수 있습니다.
B. ASG 의 용량을 수동으로 늘리면 성능 문제가 직접적으로 해결되지 않습니다.
C. 내장된 EC2 메모리 메트릭에만 의존하면 메모리 내 작업을 최적화하는 데 충분한 세분성을 제공하지 못할 수 있습니다.

가장 효율적인 솔루션은 CloudFormation 템플릿을 수정하고, R5 인스턴스로 교체하고, 사용자 지정 메트릭을 위해 CloudWatch 에이전트를 배포하는 것입니다.

Q220
A solutions architect is designing a new API using Amazon API Gateway that will receive requests from users. The volume of requests is highly variable; several hours can pass without receiving a single request. The data processing will take place asynchronously, but should be completed within a few seconds after a request is made.
Which compute service should the solutions architect have the API invoke to deliver the requirements at the lowest cost?
A. An AWS Glue job
B. An AWS Lambda function
C. A containerized service hosted in Amazon Elastic Kubernetes Service (Amazon EKS)
D. A containerized service hosted in Amazon ECS with Amazon EC2
Answer: B
https://www.examtopics.com/discussions/amazon/view/95306-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
API Gateway + Lambda 는 서버리스 아키텍처를 사용하는 최신 애플리케이션을 위한 완벽한 솔루션입니다.

설명 2:

Lambda 는 요청을 비동기식으로 처리하기 위해 API Gateway 에서 트리거할 수 있는 서버리스 컴퓨팅 서비스입니다. 들어오는 요청 볼륨에 따라 자동으로 확장되며 요청을 처리하는 데 사용된 실제 컴퓨팅 시간에 대해서만 요금을 부과하여 비용 최적화를 허용합니다.

A. Glue 는 완전히 관리되는 ETL 서비스입니다. API 요청을 제공하는 대신 데이터 처리 및 변환 작업을 위해 설계되었습니다. 가변적인 요청량을 처리하고 몇 초 내에 응답을 전달하는 데 적합하지 않을 수 있습니다.
C. EKS 는 확장성과 유연성을 제공하지만 가변적인 API 요청 볼륨을 처리하기 위해 인프라를 관리하고 확장하는 데 추가적인 복잡성과 오버헤드가 발생할 수 있습니다.
D. 이전 옵션과 마찬가지로 EC2 와 함께 ECS 를 사용하려면 인프라 관리 및 확장을 위한 추가 노력이 필요하며, 이는 간헐적이고 가변적인 API 요청 볼륨을 처리하는 데 필요하지 않을 수 있습니다.

Q221
A company runs an application on a group of Amazon Linux EC2 instances. For compliance reasons, the company must retain all application log files for 7 years. The log files will be analyzed by a reporting tool that must be able to access all the files concurrently.
Which storage solution meets these requirements MOST cost-effectively?
A. Amazon Elastic Block Store (Amazon EBS)
B. Amazon Elastic File System (Amazon EFS)
C. Amazon EC2 instance store
D. Amazon S3
Answer: D
https://www.examtopics.com/discussions/amazon/view/95307-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A. EBS 는 EC2 인스턴스와 함께 사용할 블록 수준 스토리지 볼륨을 제공합니다. 내구성과 지속성을 제공하지만 로그 파일의 장기 보존을 위한 가장 비용 효율적인 솔루션은 아닙니다. 또한 이 시나리오의 요구 사항인 파일에 대한 동시 액세스를 제공하지 않습니다.
B. EFS 는 여러 EC2 인스턴스에 동시에 탑재할 수 있는 확장 가능한 파일 스토리지 서비스입니다. 파일에 대한 동시 액세스를 제공하지만 S3 에 비해 가격이 높기 때문에 장기 보존을 위한 가장 비용 효율적인 옵션이 아닐 수 있습니다.
C. 인스턴스 스토어는 EC2 인스턴스에 물리적으로 연결된 임시 스토리지 옵션입니다. 규정

준수 목적에 필요한 내구성 및 장기 보존을 제공하지 않습니다. 또한 인스턴스 스토어는 연결된 특정 EC2 인스턴스 외부에서 액세스할 수 없으므로 보고 도구를 통한 동시 액세스가 불가능합니다.

따라서 장기보존, 동시접속, 가성비 등의 요구사항을 고려할 때 S3가 가장 적합하고 가성비 좋은 스토리지 솔루션입니다.

참고:
https://docs.aws.amazon.com/efs/latest/ug/transfer-data-to-efs.html

Q222
A company has hired an external vendor to perform work in the company's AWS account. The vendor uses an automated tool that is hosted in an AWS account that the vendor owns. The vendor does not have IAM access to the company's AWS account.
How should a solutions architect grant this access to the vendor?
A. Create an IAM role in the company's account to delegate access to the vendor's IAM role. Attach the appropriate IAM policies to the role for the permissions that the vendor requires.
B. Create an IAM user in the company's account with a password that meets the password complexity requirements. Attach the appropriate IAM policies to the user for the permissions that the vendor requires.
C. Create an IAM group in the company's account. Add the tool's IAM user from the vendor account to the group. Attach the appropriate IAM policies to the group for the permissions that the vendor requires.
D. Create a new identity provider by choosing "AWS account" as the provider type in the IAM console. Supply the vendor's AWS account ID and user name. Attach the appropriate IAM policies to the new provider for the permissions that the vendor requires.
Answer: A
https://www.examtopics.com/discussions/amazon/view/95160-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
IAM 역할을 생성하고 공급업체의 IAM 역할에 대한 액세스 권한을 위임함으로써 계정 간에 신뢰 관계를 설정합니다. 이렇게 하면 공급업체의 자동화 도구가 회사 계정의 역할을 맡고 필요한 리소스에 액세스할 수 있습니다.

적절한 IAM 정책을 역할에 연결하면 해당 도구가 작업을 수행하는 데 벤더가 요구하는 정확한 권한을 정의할 수 있습니다. 이렇게 하면 공급업체가 회사 계정에 대한 직접적인 IAM 액세스 권한을 부여하지 않고도 필요한 액세스 권한을 가질 수 있습니다.

B 는 암호가 있는 IAM 사용자를 생성하려면 벤더와 자격 증명을 공유해야 하므로 보안상의 이유로 권장되지 않습니다.

공급업체의 IAM 사용자를 회사 계정의 IAM 그룹에 추가하면 공급업체 도구에 대한 액세스를 위임하는 직접적이고 통제된 방법을 제공하지 않기 때문에 C 는 올바르지 않습니다.

공급업체의 AWS 계정에 대한 새 자격 증명 공급자를 생성하면 공급업체 도구에 대한 액세스 권한을 위임하는 간단한 방법이 제공되지 않기 때문에 D 는 틀렸습니다. ID 공급자는 일반적으로 외부 ID 시스템을 사용하는 연합 액세스에 사용됩니다.

참고:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html

Q223
A company has deployed a Java Spring Boot application as a pod that runs on Amazon Elastic Kubernetes Service (Amazon EKS) in private subnets. The application needs to write data to an Amazon DynamoDB table. A solutions architect must ensure that the application can interact with the DynamoDB table without exposing traffic to the internet.
Which combination of steps should the solutions architect take to accomplish this goal? (Choose two)
A. Attach an IAM role that has sufficient privileges to the EKS pod.
B. Attach an IAM user that has sufficient privileges to the EKS pod.
C. Allow outbound connectivity to the DynamoDB table through the private subnets' network ACLs.
D. Create a VPC endpoint for DynamoDB.
E. Embed the access keys in the Java Spring Boot code.
Answer: A, D
https://www.examtopics.com/discussions/amazon/view/95310-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A. IAM 역할을 EKS 포드에 연결하면 포드가 DynamoDB 에 액세스하는 데 필요한 권한을 부여할 수 있습니다. IAM 역할에는 DynamoDB 테이블에 대한 액세스를 허용하는 적절한 정책이 있어야 합니다.

D. DynamoDB 용 VPC 엔드포인트를 생성하면 EKS 포드가 인터넷 연결 없이도 VPC 내에서 비공개로 DynamoDB 에 액세스할 수 있습니다. VPC 엔드포인트는 DynamoDB 에 대한 직접적이고 안전한 연결을 제공하므로 트래픽이 인터넷을 통해 흐를 필요가 없습니다.

B 는 IAM 사용자를 포드에 연결하는 것이 권장되는 접근 방식이 아니기 때문에 올바르지 않습니다. IAM 사용자는 AWS Management Console 또는 AP 를 통해 AWS 서비스에 액세스하기 위한 것입니다.

네트워크 ACL 을 통한 아웃바운드 연결 구성은 DynamoDB 에 대한 안전하고 직접적인 연결을 제공하지 않기 때문에 C 는 올바르지 않습니다.

코드에 액세스 키를 포함하는 것은 권장되는 보안 방법이 아니기 때문에 E 는 올바르지 않습니다. 잠재적인 보안 취약성이 발생할 수 있습니다. AWS 서비스에 대한 액세스를 제공하기 위해 IAM 역할 또는 기타 보안 메커니즘을 사용하는 것이 좋습니다.

참고
https://docs.aws.amazon.com/ko_kr/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html
https://aws.amazon.com/ko/about-aws/whats-new/2019/09/amazon-eks-adds-support-to-assign-iam-permissions-to-kubernetes-service-accounts/

Q224
A company recently migrated its web application to AWS by rehosting the application on Amazon EC2 instances in a single AWS Region. The company wants to redesign its application architecture to be highly available and fault tolerant. Traffic must reach all running EC2 instances randomly.
Which combination of steps should the company take to meet these requirements? (Choose two)
A. Create an Amazon Route 53 failover routing policy.

B. Create an Amazon Route 53 weighted routing policy.
C. Create an Amazon Route 53 multivalue answer routing policy.
D. Launch three EC2 instances: two instances in one Availability Zone and one instance in another Availability Zone.
E. Launch four EC2 instances: two instances in one Availability Zone and two instances in another Availability Zone.
Answer: C, E
https://www.examtopics.com/discussions/amazon/view/95311-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
C. Route 53 의 다중 응답 라우팅 정책을 사용하면 DNS 레코드에 대한 다중 값을 구성할 수 있으며 Route 53 은 다중 임의 값으로 DNS 쿼리에 응답합니다. 이를 통해 사용 가능한 EC2 인스턴스 간에 트래픽을 무작위로 분산할 수 있습니다.
E. 다른 AZ 에서 EC2 인스턴스를 시작하면 고가용성과 내결함성을 얻을 수 있습니다. 4 개의 인스턴스(각 AZ 에 2 개)를 시작하면 트래픽 로드를 처리하고 원하는 수준의 가용성을 유지하기에 충분한 리소스가 있습니다.

A. 장애 조치 라우팅은 기본 리소스 또는 위치를 사용할 수 없는 경우에만 트래픽을 백업 리소스 또는 보조 위치로 보내도록 설계되었습니다.
B. 가중 라우팅 정책을 사용하면 여러 EC2 인스턴스에 트래픽을 분산할 수 있지만 무작위 분산이 보장되지는 않습니다.
D. 여러 AZ 에서 인스턴스를 시작하는 것은 내결함성을 위해 중요하지만 세 개의 인스턴스만 있으면 트래픽이 고르게 분산되지 않습니다. 인스턴스가 3 개뿐이면 트래픽이 고르게 분산되지 않아 리소스 활용이 불균형해질 수 있습니다.

참고
https://aws.amazon.com/premiumsupport/knowledge-center/multivalue-versus-simple-policies/

Q225
A media company collects and analyzes user activity data on premises. The company wants to migrate this capability to AWS. The user activity data store will continue to grow and will be petabytes in size. The company needs to build a highly available data ingestion solution that facilitates on-demand analytics of existing data and new data with SQL.

Which solution will meet these requirements with the LEAST operational overhead?
A. Send activity data to an Amazon Kinesis data stream. Configure the stream to deliver the data to an Amazon S3 bucket.
B. Send activity data to an Amazon Kinesis Data Firehose delivery stream. Configure the stream to deliver the data to an Amazon Redshift cluster.
C. Place activity data in an Amazon S3 bucket. Configure Amazon S3 to run an AWS Lambda function on the data as the data arrives in the S3 bucket.
D. Create an ingestion service on Amazon EC2 instances that are spread across multiple Availability Zones. Configure the service to forward data to an Amazon RDS Multi-AZ database.
Answer: B
https://www.examtopics.com/discussions/amazon/view/94985-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
Amazon Redshift 는 클라우드에서 완벽하게 관리되는 페타바이트 규모의 데이터 웨어하우스 서비스입니다. 수백 기가바이트의 데이터로 시작하여 페타바이트 이상으로 확장할 수 있습니다. 이를 통해 데이터를 사용하여 비즈니스와 고객에 대한 새로운 통찰력을 얻을 수 있습니다. 데이터 웨어하우스를 생성하는 첫 번째 단계는 Amazon Redshift 클러스터라는 노드 집합을 시작하는 것입니다. 클러스터를 프로비저닝한 후 데이터 세트를 업로드한 다음 데이터 분석 쿼리를 수행할 수 있습니다. 데이터 세트의 크기에 관계없이 Amazon Redshift 는 오늘날 사용하는 것과 동일한 SQL 기반 도구 및 비즈니스 인텔리전스 애플리케이션을 사용하여 빠른 쿼리 성능을 제공합니다.

설명 2:
B 는 데이터 수집 및 분석을 위한 완전히 관리되고 확장 가능한 솔루션을 제공합니다. KDF 는 대량의 스트리밍 데이터를 처리하도록 자동으로 확장하여 데이터 수집 프로세스를 간소화합니다. 강력하고 완전히 관리되는 데이터 웨어하우징 솔루션인 Redshift 클러스터에 데이터를 직접 로드할 수 있습니다.

A. Kinesis 는 스트리밍 데이터를 처리할 수 있지만 분석 솔루션에 데이터를 로드하려면 추가 처리가 필요합니다.
C. S3 및 Lambda 가 데이터 저장 및 처리를 처리할 수 있지만 KDF 및 Redshift 가 제공하는 완전관리형 솔루션에 비해 수동 구성 및 관리가 더 많이 필요합니다.
D. 이 옵션은 EC2 인스턴스 및 RDS 데이터베이스 인프라를 수동으로 관리하고 확장해야 하므로 더 많은 운영 오버헤드가 필요합니다.

따라서 Redshift 클러스터에 데이터를 제공하는 KDF 가 포함된 옵션 B 는 주어진 시나리오에서 사용자 활동 데이터를 수집하고 분석하기 위한 가장 간소화되고 운영상 효율적인 솔루션을 제공합니다.

Q226

A company collects data from thousands of remote devices by using a RESTful web services application that runs on an Amazon EC2 instance. The EC2 instance receives the raw data, transforms the raw data, and stores all the data in an Amazon S3 bucket. The number of remote devices will increase into the millions soon. The company needs a highly scalable solution that minimizes operational overhead.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two)

A. Use AWS Glue to process the raw data in Amazon S3.

B. Use Amazon Route 53 to route traffic to different EC2 instances.

C. Add more EC2 instances to accommodate the increasing amount of incoming data.

D. Send the raw data to Amazon Simple Queue Service (Amazon SQS). Use EC2 instances to process the data.

E. Use Amazon API Gateway to send the raw data to an Amazon Kinesis data stream. Configure Amazon Kinesis Data Firehose to use the data stream as a source to deliver the data to Amazon S3.

Answer: A, E

https://www.examtopics.com/discussions/amazon/view/95312-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

"RESTful 웹 서비스" => API 게이트웨이.

"EC2 인스턴스는 원시 데이터를 수신하고, 원시 데이터를 변환하고, 모든 데이터를 Amazon S3 버킷에 저장합니다."

=> (Extract - Transform - Load)가 있는 GLUE

설명 2:

A. 데이터의 스키마를 자동으로 발견하고 ETL 코드를 생성하여 변환합니다.

E. API Gateway 는 RESTful 웹 서비스를 통해 원격 장치에서 원시 데이터를 수신하는 데 사용할 수 있습니다. 들어오는 요청을 처리하기 위해 확장 가능하고 관리되는 인프라를

제공합니다. 그런 다음 데이터를 확장성과 내구성이 뛰어난 실시간 데이터 스트리밍 서비스인 Amazon Kinesis 데이터 스트림으로 보낼 수 있습니다. 여기에서 데이터 스트림을 소스로 사용하고 변환된 데이터를 Amazon S3 에 전달하도록 Amazon Kinesis Data Firehose 를 구성할 수 있습니다. 이러한 서비스 조합을 통해 운영 오버헤드를 최소화하면서 원활한 데이터 수집 및 처리가 가능합니다.

B. 확장 가능한 데이터 처리 및 저장의 필요성을 직접적으로 다루지는 않습니다. DNS 관리 및 트래픽을 다른 끝점으로 라우팅하는 데 중점을 둡니다.
C. 더 많은 EC2 를 추가하면 인스턴스 관리 및 확장 측면에서 운영 오버헤드가 증가할 수 있습니다.
D. 데이터 처리에 SQS 및 EC2 를 사용하면 더 복잡해지고 운영 오버헤드가 발생합니다.

Q227
A company needs to retain its AWS CloudTrail logs for 3 years. The company is enforcing CloudTrail across a set of AWS accounts by using AWS Organizations from the parent account. The CloudTrail target S3 bucket is configured with S3 Versioning enabled. An S3 Lifecycle policy is in place to delete current objects after 3 years.
After the fourth year of use of the S3 bucket, the S3 bucket metrics show that the number of objects has continued to rise. However, the number of new CloudTrail logs that are delivered to the S3 bucket has remained consistent.
Which solution will delete objects that are older than 3 years in the MOST cost-effective manner?
A. Configure the organization's centralized CloudTrail trail to expire objects after 3 years.
B. Configure the S3 Lifecycle policy to delete previous versions as well as current versions.
C. Create an AWS Lambda function to enumerate and delete objects from Amazon S3 that are older than 3 years.
D. Configure the parent account as the owner of all objects that are delivered to the S3 bucket.
Answer: B
https://www.examtopics.com/discussions/amazon/view/95314-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이전 버전과 현재 버전을 삭제하도록 S3 수명 주기 정책을 구성하면 이전 버전의 CloudTrail 로그가 삭제됩니다. 이렇게 하면 3 년 이상 된 객체가 S3 버킷에서 제거되어

객체 수를 줄이고 스토리지 비용을 제어할 수 있습니다.

A. 이 옵션은 S3 의 개체 관리와 직접적인 관련이 없습니다. S3 버킷에서 객체를 삭제해야 하는 필요성을 해결하지 못할 수 있는 CloudTrail 추적 만료 구성에 중점을 둡니다.
C. Lambda 를 생성하여 3 년 이상 된 객체를 삭제하는 것은 기술적으로 가능하지만 이 접근 방식은 복잡성과 운영 오버헤드를 추가로 도입합니다.
D. S3 버킷에 있는 객체의 소유권을 변경해도 3 년 이상 된 객체를 삭제해야 하는 필요성이 직접적으로 해결되지는 않습니다. 소유권은 개체의 삭제 동작에 영향을 주지 않습니다.

참고:
https://docs.aws.amazon.com/ko_kr/awscloudtrail/latest/userguide/best-practices-security.html

Q228
A company has an API that receives real-time data from a fleet of monitoring devices. The API stores this data in an Amazon RDS DB instance for later analysis. The amount of data that the monitoring devices send to the API fluctuates. During periods of heavy traffic, the API often returns timeout errors.
After an inspection of the logs, the company determines that the database is not capable of processing the volume of write traffic that comes from the API. A solutions architect must minimize the number of connections to the database and must ensure that data is not lost during periods of heavy traffic.
Which solution will meet these requirements?
A. Increase the size of the DB instance to an instance type that has more available memory.
B. Modify the DB instance to be a Multi-AZ DB instance. Configure the application to write to all active RDS DB instances.
C. Modify the API to write incoming data to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function that Amazon SQS invokes to write data from the queue to the database.
D. Modify the API to write incoming data to an Amazon Simple Notification Service (Amazon SNS) topic. Use an AWS Lambda function that Amazon SNS invokes to write data from the topic to the database.
Answer: C
https://www.examtopics.com/discussions/amazon/view/95318-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
Amazon SQS 를 사용하면 API 가 데이터를 데이터베이스에 직접 쓰지 않고 대기열에 쓰기 때문에 데이터베이스에 대한 연결 수를 최소화하는 데 도움이 됩니다. 또한 대기열에서 데이터베이스로 데이터를 쓰기 위해 Amazon SQS 가 호출하는 AWS Lambda 함수를 사용하면 대기열이 API 와 데이터베이스 사이에서 버퍼 역할을 하므로 트래픽이 많은 기간 동안 데이터가 손실되지 않도록 하는 데 도움이 됩니다.

설명 2:
SQS 를 버퍼로 활용하고 Lambda 를 사용하여 큐에서 데이터베이스로 데이터를 처리하고 기록함으로써 이 솔루션은 데이터베이스에 대한 연결 수를 최소화하면서 확장성, 분리 및 안정성을 제공합니다. 이 접근 방식은 트래픽 변동을 처리하고 트래픽이 많은 기간 동안 데이터 무결성을 보장합니다.

A. DB 인스턴스의 크기를 늘리면 더 많은 메모리를 제공할 수 있지만 높은 쓰기 트래픽을 효율적으로 처리하고 데이터베이스에 대한 연결을 최소화하는 문제는 해결되지 않습니다.
B. DB 인스턴스를 다중 AZ 인스턴스로 수정하고 모든 활성 인스턴스에 쓰면 가용성이 향상될 수 있지만 높은 쓰기 트래픽을 효율적으로 처리하고 데이터베이스에 대한 연결을 최소화하는 문제는 해결되지 않습니다.
D. SNS 와 Lambda 를 사용하면 디커플링과 확장성을 제공할 수 있지만 많은 쓰기 트래픽을 효율적으로 처리하고 데이터베이스에 대한 연결을 최소화하는 데 적합하지 않습니다.

Q229
A company manages its own Amazon EC2 instances that run MySQL databases. The company is manually managing replication and scaling as demand increases or decreases. The company needs a new solution that simplifies the process of adding or removing compute capacity to or from its database tier as needed. The solution also must offer improved performance, scaling, and durability with minimal effort from operations.
Which solution meets these requirements?
A. Migrate the databases to Amazon Aurora Serverless for Aurora MySQL.
B. Migrate the databases to Amazon Aurora Serverless for Aurora PostgreSQL.
C. Combine the databases into one larger MySQL database. Run the larger database on larger EC2 instances.
D. Create an EC2 Auto Scaling group for the database tier. Migrate the existing databases to the new environment.

Answer: A
https://www.examtopics.com/discussions/amazon/view/95319-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
데이터베이스를 Aurora Serverless 로 마이그레이션하면 자동 조정 및 복제 기능이 제공됩니다. Aurora Serverless 는 워크로드에 따라 자동으로 용량을 조정하므로 필요에 따라 컴퓨팅 용량을 원활하게 추가하거나 제거할 수 있습니다. 또한 복제 및 확장을 수동으로 관리할 필요 없이 향상된 성능, 내구성 및 고가용성을 제공합니다.

B. 호환성 문제가 발생할 수 있고 중요한 코드 수정이 필요할 수 있는 다른 데이터베이스 엔진으로의 마이그레이션을 제안하기 때문에 올바르지 않습니다.
C. 더 큰 EC2 인스턴스에서 더 큰 MySQL 데이터베이스로 통합하면 원하는 확장성과 자동화가 제공되지 않기 때문에 올바르지 않습니다.
D. 데이터베이스 계층에 대해 EC2 Auto Scaling 그룹을 사용하려면 여전히 복제 및 조정을 수동으로 관리해야 하기 때문에 올바르지 않습니다.

참고:
https://aws.amazon.com/rds/aurora/serverless/

Q230
A company is concerned that two NAT instances in use will no longer be able to support the traffic needed for the company's application. A solutions architect wants to implement a solution that is highly available, fault tolerant, and automatically scalable.
What should the solutions architect recommend?
A. Remove the two NAT instances and replace them with two NAT gateways in the same Availability Zone.
B. Use Auto Scaling groups with Network Load Balancers for the NAT instances in different Availability Zones.
C. Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones.
D. Replace the two NAT instances with Spot Instances in different Availability Zones and deploy a Network Load Balancer.
Answer: C
https://www.examtopics.com/discussions/amazon/view/95322-exam-aws-certified-solut

ions-architect-associate-saa-c03/

설명 1:
여러 가용 영역에 리소스가 있고 하나의 NAT 게이트웨이를 공유하는 경우 NAT 게이트웨이의 가용 영역이 다운되면 다른 가용 영역의 리소스가 인터넷에 액세스할 수 없게 됩니다. 가용 영역 독립적 아키텍처를 생성하려면 각 가용 영역에 NAT 게이트웨이를 생성하고 리소스가 동일한 가용 영역에서 NAT 게이트웨이를 사용하도록 라우팅을 구성합니다.
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html#nat-gateway-basics

설명 2:
이 권장 사항은 NAT 게이트웨이를 여러 AZ 에 분산하여 고가용성과 내결함성을 보장합니다. NAT 게이트웨이는 확장 가능하고 가용성이 높은 아웃바운드 NAT 기능을 제공하는 관리형 AWS 서비스입니다. 서로 다른 AZ 에 NAT 게이트웨이를 배포함으로써 회사는 중복성을 확보하고 단일 장애 지점을 방지할 수 있습니다. 또한 이 솔루션은 수동 개입 없이 증가하는 트래픽을 처리할 수 있는 자동 크기 조정을 제공합니다.

두 NAT 게이트웨이를 동일한 가용 영역에 배치하면 내결함성이 제공되지 않으므로 옵션 A 는 올바르지 않습니다.
옵션 B 는 Network Load Balancer 와 함께 Auto Scaling 그룹을 사용하는 것이 NAT 인스턴스에 권장되는 접근 방식이 아니기 때문에 올바르지 않습니다.
옵션 D 는 스팟 인스턴스가 NAT 인스턴스와 같은 중요한 인프라 구성 요소에 적합하지 않기 때문에 올바르지 않습니다.

Q231
An application runs on an Amazon EC2 instance that has an Elastic IP address in VPC A. The application requires access to a database in VPC B. Both VPCs are in the same AWS account.
Which solution will provide the required access MOST securely?
A. Create a DB instance security group that allows all traffic from the public IP address of the application server in VPC A.
B. Configure a VPC peering connection between VPC A and VPC B.
C. Make the DB instance publicly accessible. Assign a public IP address to the DB instance.
D. Launch an EC2 instance with an Elastic IP address into VPC B. Proxy all requests through

the new EC2 instance.
Answer: B
https://www.examtopics.com/discussions/amazon/view/95323-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
VPC 피어링 연결은 사용자가 프라이빗 IP 주소를 사용하여 트래픽을 라우팅할 수 있도록 하는 두 VPC 간의 네트워킹 연결입니다. 각 VPC 의 인스턴스는 마치 동일한 네트워크 내에 있는 것처럼 서로 통신할 수 있습니다. VPC 피어링 연결은 같거나 다른 AWS 계정과 Regions1 의 VPC 간에 생성할 수 있습니다. 솔루션은 VPC A 와 VPC B 간에 VPC 피어링 연결을 구성하여 필요한 액세스를 가장 안전하게 제공할 수 있습니다.
1. VPC A 에 있는 애플리케이션 서버의 퍼블릭 IP 주소에서 오는 모든 트래픽을 허용하는 DB 인스턴스 보안 그룹을 생성합니다. 이 솔루션은 DB 인스턴스를 퍼블릭 인터넷에 노출하고 액세스 제어를 위한 단일 IP 주소.
2. DB 인스턴스를 공개적으로 액세스할 수 있도록 합니다. 퍼블릭 IP 주소를 DB 인스턴스에 할당합니다. 이 솔루션은 DB 인스턴스를 퍼블릭 인터넷에 노출하고 모든 소스에 연결할 수 있도록 허용하므로 필요한 액세스를 가장 안전하게 제공하지 않습니다.
3. 탄력적 IP 주소가 있는 EC2 인스턴스를 VPC B 로 시작합니다. 새 EC2 인스턴스를 통해 모든 요청을 프록시합니다. 이 솔루션은 대기 시간과 복잡성을 유발할 수 있는 추가 리소스 생성 및 프록시 서버 구성과 관련되므로 필요한 액세스를 가장 안전하게 제공하지 않습니다.
참조 URL: https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html

설명 2:
VPC A 와 VPC B 간에 VPC 피어링 연결을 구성하면 VPC A 의 EC2 인스턴스와 VPC B 의 데이터베이스 간에 비공개 보안 통신을 설정할 수 있습니다. 공용 IP 주소가 필요하거나 데이터베이스를 인터넷에 노출해야 합니다.

옵션 A 는 덜 안전할 수 있는 응용 프로그램 서버의 공용 IP 주소에서 오는 모든 트래픽을 허용해야 하므로 최상의 솔루션이 아닙니다.
옵션 C 는 DB 인스턴스를 공개적으로 액세스 가능하게 만드는 것과 관련이 있으며, 이는 데이터베이스를 인터넷에 직접 노출함으로써 보안 위험을 초래합니다.
옵션 D 는 VPC B 에서 추가 EC2 인스턴스를 시작하고 이를 통해 모든 요청을 프록시하여 불필요한 복잡성을 추가합니다. 이는 이 시나리오에서 가장 효율적이고 안전한 접근 방식이 아닙니다.

Q232

A company runs demonstration environments for its customers on Amazon EC2 instances. Each environment is isolated in its own VPC. The company's operations team needs to be notified when RDP or SSH access to an environment has been established.

A. Configure Amazon CloudWatch Application Insights to create AWS Systems Manager OpsItems when RDP or SSH access is detected.

B. Configure the EC2 instances with an IAM instance profile that has an IAM role with the AmazonSSMManagedInstanceCore policy attached.

C. Publish VPC flow logs to Amazon CloudWatch Logs. Create required metric filters. Create an Amazon CloudWatch metric alarm with a notification action for when the alarm is in the ALARM state.

D. Configure an Amazon EventBridge rule to listen for events of type EC2 Instance State-change Notification. Configure an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the operations team to the topic.

Answer: C

https://www.examtopics.com/discussions/amazon/view/95324-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

CloudWatch Logs 에 VPC 흐름 로그를 게시하고 RDP 또는 SSH 액세스를 감지하는 지표 필터를 생성함으로써 운영 팀은 경보가 트리거될 때 이를 알리도록 CloudWatch 지표 경보를 구성할 수 있습니다. 이렇게 하면 환경에 대한 RDP 또는 SSH 액세스가 설정될 때 원하는 알림이 제공됩니다.

CloudWatch Application Insights 는 RDP 또는 SSH 액세스를 감지하도록 설계되지 않았기 때문에 옵션 A 는 올바르지 않습니다.

옵션 B 도 올바르지 않습니다. AmazonSSMManagedInstanceCore 정책으로 IAM 인스턴스 프로필을 구성하면 RDP 또는 SSH 액세스가 발생할 때 운영 팀에 알려야 하는 요구 사항이 직접 해결되지 않기 때문입니다.

EC2 인스턴스 상태 변경 알림 이벤트를 수신하도록 EventBridge 규칙을 구성하고 SNS 주제를 대상으로 사용하면 운영 팀에 인스턴스 시작 또는 중지와 같은 인스턴스 상태 변경 사항을 알릴 수 있으므로 옵션 D 는 잘못된 것입니다. 그러나 질문에 명시된 요구 사항인 RDP 또는 SSH 액세스가 설정된 시기를 구체적으로 감지하거나 알리지는 않습니다.

참고:
https://aws.amazon.com/blogs/security/how-to-monitor-and-visualize-failed-ssh-access-attemptsto-amazon-ec2-linux-instances/

Q233
A solutions architect has created a new AWS account and must secure AWS account root user access.
Which combination of actions will accomplish this? (Choose two)
A. Ensure the root user uses a strong password.
B. Enable multi-factor authentication to the root user.
C. Store root user access keys in an encrypted Amazon S3 bucket.
D. Add the root user to a group containing administrative permissions.
E. Apply the required permissions to the root user with an inline policy document.
Answer: A, B
https://www.examtopics.com/discussions/amazon/view/95084-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A. 루트 사용자에 대해 강력한 암호를 설정하는 것은 무단 액세스를 방지하기 위한 필수 보안 조치입니다.
B. MFA 를 활성화하면 암호 외에 모바일 앱의 코드 또는 하드웨어 토큰과 같은 추가 인증 요소를 요구하여 추가 보안 계층을 추가합니다.
C. 루트 사용자 액세스 키는 가능하면 피해야 하며 대신 권한이 제한된 IAM 사용자를 사용하는 것이 가장 좋습니다.
D. 루트 사용자는 이미 계정의 모든 리소스 및 서비스에 대한 무제한 액세스 권한을 가지고 있으므로 추가 관리 권한을 부여하면 무단 작업의 위험이 높아질 수 있습니다.
E. 대신 적절한 권한을 가진 IAM 사용자를 생성하고 해당 사용자를 일상적인 작업에 사용하는 동시에 루트 사용자를 보호하고 필요한 관리 작업에만 사용하는 것이 좋습니다.

설명 2:
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html
https://docs.aws.amazon.com/accounts/latest/reference/best-practices-root-user.html
* AWS 계정 루트 사용자에서 AWS Multi-Factor Authentication(MFA)을 활성화합니다. 자세한 내용은 IAM 사용 설명서의 AWS 에서 멀티 팩터 인증(MFA) 사용을 참조하십시오.

* AWS 계정 루트 사용자 암호 또는 액세스 키를 누구와도 공유하지 마십시오.
* 강력한 암호를 사용하여 AWS Management Console 에 대한 액세스를 보호하십시오. AWS 계정 루트 사용자 암호 관리에 대한 자세한 내용은 루트 사용자 암호 변경 단원을 참조하십시오.

Q234
A company is building a new web-based customer relationship management application. The application will use several Amazon EC2 instances that are backed by Amazon Elastic Block Store (Amazon EBS) volumes behind an Application Load Balancer (ALB). The application will also use an Amazon Aurora database. All data for the application must be encrypted at rest and in transit.
Which solution will meet these requirements?
A. Use AWS Key Management Service (AWS KMS) certificates on the ALB to encrypt data in transit. Use AWS Certificate Manager (ACM) to encrypt the EBS volumes and Aurora database storage at rest.
B. Use the AWS root account to log in to the AWS Management Console. Upload the company's encryption certificates. While in the root account, select the option to turn on encryption for all data at rest and in transit for the account.
C. Use AWS Key Management Service (AWS KMS) to encrypt the EBS volumes and Aurora database storage at rest. Attach an AWS Certificate Manager (ACM) certificate to the ALB to encrypt data in transit.
D. Use BitLocker to encrypt all data at rest. Import the company's TLS certificate keys to AWS Key Management Service (AWS KMS) Attach the KMS keys to the ALB to encrypt data in transit.
Answer: C
https://www.examtopics.com/discussions/amazon/view/95325-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 옵션은 AWS Key Management Service(AWS KMS)를 사용하기 때문에 가장 효율적입니다. 이 서비스는 암호화 키를 쉽게 생성 및 관리하고 다양한 AWS 서비스와 실행 중인 애플리케이션에서 키 사용을 제어할 수 있게 해줍니다. AWS 에서. 또한 AWS KMS 를 사용하여 EBS 볼륨과 유휴 Aurora 데이터베이스 스토리지를 암호화하여 관리하는 암호화 키로 데이터를 암호화하여 데이터 보호를 제공합니다. 또한 AWS 서비스 및 내부 연결 리소스와 함께 사용할 공용 및 개인 SSL/TLS(Secure Sockets Layer/Transport Layer

Security) 인증서를 쉽게 프로비저닝, 관리 및 배포할 수 있는 서비스인 AWS Certificate Manager(ACM)를 사용합니다. . 또한 ACM 인증서를 ALB 에 연결하여 전송 중인 데이터를 암호화합니다. 이는 클라이언트와 로드 밸런서 간의 연결에 SSL/TLS 암호화를 활성화하여 데이터 보호를 제공합니다. 이 솔루션은 미사용 및 전송 중인 애플리케이션의 모든 데이터를 암호화해야 한다는 요구 사항을 충족합니다.

옵션 A 는 ALB 에서 AWS KMS 인증서를 사용하여 전송 중인 데이터를 암호화하기 때문에 효율성이 떨어집니다. 이는 AWS KMS 가 인증서를 제공하지 않고 키만 제공하기 때문에 불가능합니다. 또한 AWS Certificate Manager(ACM)를 사용하여 유휴 EBS 볼륨 및 Aurora 데이터베이스 스토리지를 암호화합니다. 이는 ACM 이 암호화를 제공하지 않고 인증서만 제공하기 때문에 불가능합니다.

옵션 B 는 AWS 루트 계정을 사용하여 AWS Management Console 에 로그인하기 때문에 효율성이 떨어집니다. 이 방법은 계정의 모든 리소스에 대한 무제한 액세스 권한이 있으므로 권장되지 않습니다. 또한 회사의 암호화 인증서를 업로드하는데 ACM 은 인증서를 무료로 제공할 수 있으므로 필요하지 않습니다. 또한 계정에 대해 저장 및 전송 중인 모든 데이터에 대해 암호화를 켜는 옵션을 선택합니다. 이는 암호화 설정이 각 서비스 및 리소스에 따라 다르기 때문에 불가능합니다.

옵션 D 는 Windows 서버의 볼륨에 대한 암호화를 제공하는 Windows 기능인 BitLocker 를 사용하여 미사용 데이터를 모두 암호화하기 때문에 효율성이 떨어집니다. 그러나 이것은 Aurora 가 Linux 서버에서 실행되기 때문에 미사용 Aurora 데이터베이스 스토리지에 대한 암호화를 제공하지 않습니다. 또한 회사의 TLS 인증서 키를 AWS KMS 로 가져오는데, 이는 ACM 이 인증서를 무료로 제공할 수 있으므로 필요하지 않습니다. 또한 KMS 키를 ALB 에 연결하여 전송 중인 데이터를 암호화합니다. ALB 에는 키가 아닌 인증서가 필요하기 때문에 불가능합니다.

설명 2:
AWS KMS 를 사용하여 유휴 상태의 EBS 및 Aurora 데이터베이스 스토리지를 암호화할 수 있습니다.
ACM 을 사용하여 SSL/TLS 인증서를 가져와 ALB 에 연결할 수 있습니다. 이는 클라이언트와 ALB 간에 전송 중인 데이터를 암호화합니다.

A 는 EBS 를 암호화하기 위한 올바른 서비스가 아닌 EBS 를 암호화하기 위해 ACM 을 사용하도록 제안하기 때문에 올바르지 않습니다.

B 는 정답이 아닙니다. AWS 루트 계정에 의존하고 AWS Management Console 에서 유휴 및 전송 중인 모든 데이터에 대한 암호화를 활성화하는 옵션을 선택하는 것은 유효한 접근 방식이 아니기 때문입니다.

BitLocker 는 AWS 서비스에서 데이터를 암호화하는 데 적합한 솔루션이 아니기 때문에 D 는 틀렸습니다. 주로 Windows 기반 운영 체제에서 데이터를 암호화하는 데 사용됩니다. 또한 TLS 인증서 키를 AWS KMS 로 가져와 ALB 에 연결하는 것은 전송 중인 데이터를 암호화하는 데 권장되는 접근 방식이 아닙니다.

Q235

A company is moving its on-premises Oracle database to Amazon Aurora PostgreSQL. The database has several applications that write to the same tables. The applications need to be migrated one by one with a month in between each migration. Management has expressed concerns that the database has a high number of reads and writes. The data must be kept in sync across both databases throughout the migration.

What should a solutions architect recommend?

A. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a change data capture (CDC) replication task and a table mapping to select all tables.

B. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.

C. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a memory optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.

D. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a compute optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select the largest tables.

Answer: C

https://www.examtopics.com/discussions/amazon/view/95326-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

AWS SCT 는 Oracle 데이터베이스의 스키마와 코드를 Aurora PostgreSQL 과 호환되도록 변환하는 데 사용됩니다. AWS DMS 는 Oracle 데이터베이스에서 Aurora PostgreSQL 로

데이터를 마이그레이션하는 데 활용됩니다. 마이그레이션 프로세스 중에 많은 수의 읽기 및 쓰기를 처리하려면 메모리 최적화 복제 인스턴스를 사용하는 것이 좋습니다.
전체 로드 및 CDC 복제 작업을 생성하면 초기 데이터 마이그레이션이 수행되고 Oracle 데이터베이스의 진행 중인 변경 사항이 지속적으로 캡처되어 Aurora PostgreSQL 데이터베이스에 적용됩니다. 테이블 매핑을 위해 모든 테이블을 선택하면 동일한 테이블에 쓰는 모든 응용 프로그램이 마이그레이션됩니다.

AWS DataSync 를 단독으로 사용하는 것은 데이터베이스 마이그레이션 및 데이터 동기화에 충분하지 않기 때문에 옵션 A 및 B 는 올바르지 않습니다.

계산에 최적화된 복제 인스턴스를 사용하는 것이 많은 수의 읽기 및 쓰기를 처리하는 데 가장 적합한 선택이 아니기 때문에 옵션 D 는 올바르지 않습니다.

참고
https://repost.aws/ko/knowledge-center/dms-memory-optimization

Q236
A company has a three-tier application for image sharing. The application uses an Amazon EC2 instance for the front-end layer, another EC2 instance for the application layer, and a third EC2 instance for a MySQL database. A solutions architect must design a scalable and highly available solution that requires the least amount of change to the application.
Which solution meets these requirements?
A. Use Amazon S3 to host the front-end layer. Use AWS Lambda functions for the application layer. Move the database to an Amazon DynamoDB table. Use Amazon S3 to store and serve users' images.
B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS DB instance with multiple read replicas to serve users' images.
C. Use Amazon S3 to host the front-end layer. Use a fleet of EC2 instances in an Auto Scaling group for the application layer. Move the database to a memory optimized instance type to store and serve users' images.
D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS Multi-AZ DB instance. Use Amazon S3 to store and serve users' images.
Answer: D

https://www.examtopics.com/discussions/amazon/view/94990-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
로드 밸런싱된 다중 AZ AWS EBS 를 사용하면 애플리케이션을 크게 변경하지 않고도 두 계층 모두에 대한 확장성과 고가용성을 얻을 수 있습니다. DB 를 RDS 다중 AZ DB 로 이동하면 고가용성과 자동 장애 조치가 보장됩니다. S3 를 통해 사용자 이미지를 저장하고 제공하면 확장 가능하고 가용성이 높은 솔루션을 제공합니다.

프런트 엔드 계층에 S3 를 사용하고 애플리케이션 계층에 Lambda 를 사용하려면 애플리케이션 아키텍처를 크게 변경해야 하므로 A 는 정답이 아닙니다. DB 를 DynamoDB 로 이동하려면 DB 관련 코드를 다시 작성해야 합니다.

이미지를 제공하기 위해 로드 밸런싱된 다중 AZ AWS EBS 환경과 읽기 전용 복제본이 있는 RDS DB 를 사용하는 것이 더 적합한 솔루션이기 때문에 B 는 틀렸습니다. 읽기 전용 복제본이 있는 RDS 는 이러한 용도로 S3 를 사용하는 것보다 이미지 제공 워크로드를 더 효율적으로 처리할 수 있습니다.

프런트 엔드 계층에 S3 를 사용하고 애플리케이션 계층에 EC2 의 ASG 를 사용하려면 애플리케이션 아키텍처를 수정해야 하므로 C 는 올바르지 않습니다. 메모리 최적화 EC2 유형의 이미지를 저장하고 제공하는 것은 S3 를 사용할 때보다 가장 효율적이고 확장 가능한 접근 방식이 아닐 수 있습니다.

설명 2:
AWS Fargate 는 Amazon EC2 인스턴스의 서버 또는 클러스터를 관리할 필요 없이 컨테이너를 실행하기 위해 Amazon ECS 와 함께 사용할 수 있는 기술입니다. Fargate 를 사용하면 더 이상 컨테이너를 실행하기 위해 가상 머신의 클러스터를 프로비저닝, 구성 또는 확장할 필요가 없습니다.
https://docs.aws.amazon.com/AmazonECS/latest/userguide/what-is-fargate.html

"고가용성"의 경우: 다중 AZ 및 "애플리케이션에 대한 최소 변경 사항"의 경우: Elastic Beanstalk 는 용량 프로비저닝, 로드 밸런싱, 자동 확장에서 애플리케이션 상태 모니터링에 이르기까지 배포를 자동으로 처리합니다.

Q237

An application running on an Amazon EC2 instance in VPC-A needs to access files in another EC2 instance in VPC-B. Both VPCs are in separate AWS accounts. The network administrator needs to design a solution to configure secure access to EC2 instance in VPC-B from VPC-A. The connectivity should not have a single point of failure or bandwidth concerns.

Which solution will meet these requirements?

A. Set up a VPC peering connection between VPC-A and VPC-B.

B. Set up VPC gateway endpoints for the EC2 instance running in VPC-B.

C. Attach a virtual private gateway to VPC-B and set up routing from VPC-A.

D. Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-A.

Answer: A

https://www.examtopics.com/discussions/amazon/view/95144-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

VPC 피어링 연결을 사용하면 인터넷 게이트웨이, VPN 연결 또는 NAT 장치 없이 프라이빗 IP 주소를 사용하여 서로 다른 VPC 의 인스턴스 간에 안전한 통신이 가능합니다. 이를 설정하면 VPC-A 에서 실행 중인 애플리케이션이 공용 인터넷이나 단일 장애 지점을 거치지 않고 VPC-B 의 EC2 에 직접 액세스할 수 있습니다.

B 는 VPC 게이트웨이 엔드포인트가 인터넷을 통하지 않고 VPC 에서 S3 또는 DynamoDB 에 액세스하는 데 사용되기 때문에 올바르지 않습니다. 서로 다른 VPC 에 있는 EC2 인스턴스 간에 연결을 설정하도록 설계되지 않았습니다.

C 는 VPC 간에 VPN 연결을 구성해야 하므로 올바르지 않습니다. 이로 인해 추가적인 복잡성과 잠재적인 단일 실패 지점이 발생합니다.

D 는 프라이빗 VIF 를 생성하고 경로를 추가하면 Direct Connect 를 사용하여 온프레미스 인프라와 VPC-B 간에 직접 연결을 설정하는 데 적용할 수 있기 때문에 올바르지 않지만 서로 다른 VPC 내의 별도 VPC 에 있는 EC2 인스턴스 간의 통신 시나리오에는 적합하지 않습니다. AWS 계정.

설명 2:

AWS 는 VPC 의 기존 인프라를 사용하여 VPC 피어링 연결을 생성합니다. 게이트웨이나 VPN 연결이 아니며 별도의 물리적 하드웨어에 의존하지 않습니다. 통신 또는 대역폭 병목

현상에 대한 단일 장애 지점이 없습니다.
https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html

Q238
A company wants to experiment with individual AWS accounts for its engineer team. The company wants to be notified as soon as the Amazon EC2 instance usage for a given month exceeds a specific threshold for each account.
What should a solutions architect do to meet this requirement MOST cost-effectively?
A. Use Cost Explorer to create a daily report of costs by service. Filter the report by EC2 instances. Configure Cost Explorer to send an Amazon Simple Email Service (Amazon SES) notification when a threshold is exceeded.
B. Use Cost Explorer to create a monthly report of costs by service. Filter the report by EC2 instances. Configure Cost Explorer to send an Amazon Simple Email Service (Amazon SES) notification when a threshold is exceeded.
C. Use AWS Budgets to create a cost budget for each account. Set the period to monthly. Set the scope to EC2 instances. Set an alert threshold for the budget. Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded.
D. Use AWS Cost and Usage Reports to create a report with hourly granularity. Integrate the report data with Amazon Athena. Use Amazon EventBridge to schedule an Athena query. Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded.
Answer: C
https://www.examtopics.com/discussions/amazon/view/94996-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
각 계정에 대한 비용 예산을 생성하고 기간을 월 단위로 지정하고 범위를 EC2 로 지정하면 EC2 와 관련된 비용을 구체적으로 추적하고 모니터링할 수 있습니다. 예산에 경고 임계값을 설정하면 지정된 임계값이 초과될 때 알림이 트리거됩니다. 알림을 받도록 SNS 를 구성합니다. 회사에서 구독하면 즉시 알림을 받을 수 있습니다.

A 와 B 는 Cost Explorer 를 사용하여 임계값을 초과할 때 실시간 알림을 제공하지 않을 수 있는 보고서를 생성하기 때문에 가장 비용 효율적인 솔루션이 아닙니다. 또한 A.는 일일 보고서 사용을 제안하고 B.는 월별 보고서 사용을 제안합니다. 이는 즉각적인 알림에 대해

원하는 수준의 세분성을 제공하지 않을 수 있습니다.

D 는 Athena 및 EventBridge 와 함께 비용 및 사용 보고서를 사용하는 것과 관련됩니다. 이 솔루션은 더 많은 유연성과 데이터 분석 기능을 제공하며 더 복잡하고 Athena 를 사용하고 시간별 보고서를 생성하는 데 추가 비용이 발생할 수 있습니다.

설명 2:
AWS 예산을 사용하면 AWS 계정에 대한 예산을 생성하고 사용량이 특정 임계값을 초과할 때 알림을 설정할 수 있습니다. 각 계정에 대한 예산을 생성하고 기간을 월 단위로 지정하고 범위를 EC2 인스턴스로 지정하면 각 계정의 EC2 사용량을 효과적으로 추적하고 임계값을 초과할 때 알림을 받을 수 있습니다. 이 솔루션은 Amazon Athena 또는 Amazon EventBridge 와 같은 추가 리소스가 필요하지 않기 때문에 가장 비용 효율적인 옵션입니다.

Q239
A solutions architect needs to design a new microservice for a company's application. Clients must be able to call an HTTPS endpoint to reach the microservice. The microservice also must use AWS Identity and Access Management (IAM) to authenticate calls. The solutions architect will write the logic for this microservice by using a single AWS Lambda function that is written in Go 1.x.
Which solution will deploy the function in the MOST operationally efficient way?
A. Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API.
B. Create a Lambda function URL for the function. Specify AWS_IAM as the authentication type.
C. Create an Amazon CloudFront distribution. Deploy the function to Lambda@Edge. Integrate IAM authentication logic into the Lambda@Edge function.
D. Create an Amazon CloudFront distribution. Deploy the function to CloudFront Functions. Specify AWS_IAM as the authentication type.
Answer: A
https://www.examtopics.com/discussions/amazon/view/95365-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
API Gateway REST API 를 생성하면 클라이언트가 마이크로서비스에 도달하기 위해 호출할 수 있는 HTTPS 엔드포인트를 정의할 수 있습니다. API 에서 IAM 인증을 활성화하여 API

호출에 대한 인증을 적용합니다. 이렇게 하면 인증된 요청만 마이크로서비스에 도달할 수 있습니다. 이 솔루션은 API 게이트웨이의 기본 제공 기능을 활용하여 HTTP 엔드포인트, 요청 라우팅 및 IAM 인증을 처리하므로 운영상 효율적입니다. 추가 인프라 구성 요소 없이 확장 가능하고 관리되는 솔루션을 제공합니다.

B 는 Lambda URL 을 생성하고 인증 유형으로 AWS IAM 을 지정할 것을 제안합니다. 이것은 IAM 인증을 제공할 수 있지만 요청 유효성 검사, 속도 제한 및 API 구성의 손쉬운 관리와 같은 API Gateway 의 이점이 없습니다.

C 와 D 에는 CloudFront, Lambda@Edge 및 CloudFront 함수 사용이 포함됩니다. 이러한 서비스는 유연성과 에지 위치에서 논리를 실행할 수 있는 기능을 제공하지만 추가적인 복잡성을 야기하며 지정된 요구 사항에 필요하지 않을 수 있습니다.

Q240

A company previously migrated its data warehouse solution to AWS. The company also has an AWS Direct Connect connection. Corporate office users query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 50 MB and each webpage sent by the visualization tool is approximately 500 KB. Result sets returned by the data warehouse are not cached.

Which solution provides the LOWEST data transfer egress cost for the company?

A. Host the visualization tool on premises and query the data warehouse directly over the internet.

B. Host the visualization tool in the same AWS Region as the data warehouse. Access it over the internet.

C. Host the visualization tool on premises and query the data warehouse directly over a Direct Connect connection at a location in the same AWS Region.

D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection at a location in the same Region.

Answer: D

https://www.examtopics.com/discussions/amazon/view/94998-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

데이터 웨어하우스와 동일한 AWS 리전에서 시각화 도구를 호스팅하고 동일한 리전 내에서 Direct Connect 연결을 통해 액세스하면 데이터 전송 비용이 없어지고 지연 시간이 짧은

고대역폭 연결이 보장됩니다.

A. 온프레미스에서 시각화 도구를 호스팅하고 인터넷을 통해 데이터 웨어하우스를 쿼리하면 모든 쿼리 결과에 대한 데이터 전송 비용과 잠재적 대기 시간 및 대역폭 제한이 발생합니다.

B. 데이터 웨어하우스와 동일한 AWS 리전에서 시각화 도구를 호스팅하지만 인터넷을 통해 액세스하면 여전히 각 쿼리 결과에 대한 데이터 전송 비용이 발생합니다.

C. 온프레미스에서 시각화 도구를 호스팅하고 동일한 AWS 리전 내에서 Direct Connect 연결을 통해 데이터 웨어하우스를 쿼리하면 모든 쿼리 결과에 대한 데이터 전송 비용이 발생하고 온프레미스 인프라가 필요하여 복잡성이 추가됩니다.

참고:
https://aws.amazon.com/directconnect/pricing/
https://aws.amazon.com/blogs/aws/aws-data-transfer-prices-reduced/

Q241
An online learning company is migrating to the AWS Cloud. The company maintains its student records in a PostgreSQL database. The company needs a solution in which its data is available and online across multiple AWS Regions at all times.
Which solution will meet these requirements with the LEAST amount of operational overhead?
A. Migrate the PostgreSQL database to a PostgreSQL cluster on Amazon EC2 instances.
B. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance with the Multi-AZ feature turned on.
C. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Create a read replica in another Region.
D. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Set up DB snapshots to be copied to another Region.
Answer: C
https://www.examtopics.com/discussions/amazon/view/95000-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

PostgreSQL 데이터베이스를 PostgreSQL DB 유지용 RDS 로 늘리고 다른 AWS 리전에 읽기 전용 복제본을 생성하면 여러 리전에서 데이터 가용성과 온라인 액세스를 충분히 할 수 있습니다. 이 솔루션은 EC2 폐쇄에서 PostgreSQL 클러스터를 관리하거나(옵션 A) 스냅샷을 사용하여 수동 복제를 설정하는 것(옵션 D)에 비해 연산된 헤드가 적입니다. 또한 Amazon RDS 는 기본 복원 및 복제 설정을 처리하여 회사의 운영 문제를 줄입니다.

B 는 단일 AWS 리전 내에서 고가용성을 누릴 수 있습니다. 그러나 질문에 여러 개의 AWS 리전에서 항상 데이터를 온라인으로 사용할 수 있어야만 요구 사항을 충족할 수 없습니다. RDS 의 다중 AZ 기능은 동일한 리전 내에서 자동으로 조치를 취하지만 데이터를 여러 리전으로 복제하지 않습니다.

설명 2:
"항상 여러 AWS 리전에서 온라인으로". 현재 읽기 전용 복제본만 지역 간 지원, 다중 AZ 는 지역 간 지원하지 않음(동일한 지역에서만 작동)
https://aws.amazon.com/ko/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/

Q242
A company hosts its web application on AWS using seven Amazon EC2 instances. The company requires that the IP addresses of all healthy EC2 instances be returned in response to DNS queries.
Which policy should be used to meet this requirement?
A. Simple routing policy
B. Latency routing policy
C. Multi-value routing policy
D. Geolocation routing policy
Answer: C
https://www.examtopics.com/discussions/amazon/view/95001-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
다중 응답 라우팅 정책을 사용하여 여러 리소스에 DNS 응답을 배포할 수 있습니다.
예를 들어 라우팅 레코드를 Route 53 상태 확인과 연결하려는 경우 다중값 응답 라우팅을 사용합니다. 예를 들어 DNS 쿼리에 대해 여러 값을 반환하고 트래픽을 여러 IP 주소로 라우팅해야 하는 경우 다중 값 응답 라우팅을 사용합니다.

https://aws.amazon.com/premiumsupport/knowledge-center/multivalue-versus-simple-policies/

설명 2:
다중값 라우팅 정책은 Route 53 이 동일한 리소스에 대한 여러 정상 IP 주소로 DNS 쿼리에 응답하도록 허용합니다. 이는 여러 인스턴스가 동일한 용도로 사용되며 부하 분산 또는 장애 조치가 가능한 시나리오에서 특히 유용합니다. 다중 값 라우팅 정책을 사용하면 Route 53 은 여러 IP 주소를 무작위 순서로 반환하여 모든 정상 인스턴스에 트래픽을 분산합니다.

옵션 A(단순 라우팅 정책)는 DNS 쿼리에 대한 응답으로 단일 IP 주소만 반환하며 여러 주소 반환을 지원하지 않습니다.

옵션 B(대기 시간 라우팅 정책)는 리소스에 대한 최저 대기 시간을 기반으로 트래픽을 라우팅하는 데 사용되며 모든 정상 IP 주소를 반환해야 하는 요구 사항을 충족하지 않습니다.

옵션 D(Geolocation 라우팅 정책)는 사용자의 지리적 위치를 기반으로 트래픽을 라우팅하는 데 사용되며 정상 IP 주소를 모두 반환해야 하는 요구 사항을 충족하지 않습니다.

따라서 다중 값 라우팅 정책은 DNS 쿼리에 대한 응답으로 모든 정상 EC2 인스턴스의 IP 주소를 반환하는 데 가장 적합한 옵션입니다.

Q243
A medical research lab produces data that is related to a new study. The lab wants to make the data available with minimum latency to clinics across the country for their on-premises, file-based applications. The data files are stored in an Amazon S3 bucket that has read-only permissions for each clinic.
What should a solutions architect recommend to meet these requirements?
A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic.
B. Migrate the files to each clinic's on-premises applications by using AWS DataSync for processing.
C. Deploy an AWS Storage Gateway volume gateway as a virtual machine (VM) on premises

at each clinic.
D. Attach an Amazon Elastic File System (Amazon EFS) file system to each clinic's on-premises servers.
Answer: A
https://www.examtopics.com/discussions/amazon/view/95002-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
AWS Storage Gateway 는 온프레미스 소프트웨어 어플라이언스와 클라우드 기반 스토리지를 연결하여 조직의 온프레미스 IT 환경과 AWS 스토리지 인프라 간의 원활하고 안전한 통합을 제공하는 서비스입니다. 각 진료소 구내에 파일 게이트웨이를 가상 머신으로 배포함으로써 의료 연구실은 각 진료소에 대한 읽기 전용 권한을 유지하면서 S3 버킷에 저장된 데이터에 대한 짧은 대기 시간 액세스를 제공할 수 있습니다. 이 솔루션을 통해 클리닉은 데이터 전송이나 마이그레이션 없이 온프레미스 파일 기반 애플리케이션에서 직접 데이터 파일에 액세스할 수 있습니다.

설명 2:
A. 클리닉에서 파일 인터페이스를 통해 S3 버킷에 저장된 데이터 파일에 액세스할 수 있습니다. 파일 게이트웨이는 자주 액세스하는 데이터를 로컬로 캐시하여 대기 시간을 줄이고 데이터에 대한 빠른 액세스를 제공합니다.

B. AWS DataSync 를 사용하여 Amazon S3 버킷에서 각 클리닉의 온프레미스 애플리케이션으로 데이터 파일을 전송하는 작업이 포함됩니다. 이렇게 하면 데이터 마이그레이션이 가능하지만 실시간 액세스를 제공하지 않을 수 있으며 추가 대기 시간이 발생할 수 있습니다.

C. 파일 수준의 접근보다는 데이터에 대한 블록 수준의 접근에 적합하다. 파일 기반 애플리케이션을 위한 가장 효율적인 솔루션이 아닐 수도 있습니다.

D. 확장 가능한 파일 스토리지 서비스인 Amazon EFS 를 사용하여 데이터에 대한 파일 수준 액세스를 제공합니다. 그러나 파일 게이트웨이 솔루션을 사용할 때보다 복잡성과 대기 시간이 추가로 발생할 수 있습니다.

Q244
A company is using a content management system that runs on a single Amazon EC2

instance. The EC2 instance contains both the web server and the database software. The company must make its website platform highly available and must enable the website to scale to meet user demand.

What should a solutions architect recommend to meet these requirements?

A. Move the database to Amazon RDS, and enable automatic backups. Manually launch another EC2 instance in the same Availability Zone. Configure an Application Load Balancer in the Availability Zone, and set the two instances as targets.

B. Migrate the database to an Amazon Aurora instance with a read replica in the same Availability Zone as the existing EC2 instance. Manually launch another EC2 instance in the same Availability Zone. Configure an Application Load Balancer, and set the two EC2 instances as targets.

C. Move the database to Amazon Aurora with a read replica in another Availability Zone. Create an Amazon Machine Image (AMI) from the EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

D. Move the database to a separate EC2 instance, and schedule backups to Amazon S3. Create an Amazon Machine Image (AMI) from the original EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

Answer: C

https://www.examtopics.com/discussions/amazon/view/95336-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

이 접근 방식은 웹 사이트 플랫폼에 고가용성과 확장성을 모두 제공합니다. 데이터베이스를 다른 가용 영역에 있는 읽기 전용 복제본이 있는 Amazon Aurora 로 이동하면 데이터베이스에 대한 장애 조치 옵션이 제공됩니다. 두 가용 영역에서 Application Load Balancer 및 Auto Scaling 그룹을 사용하면 증가하는 사용자 수요를 충족하기 위해 웹 사이트를 자동으로 확장할 수 있습니다. 또한 원래 EC2 인스턴스에서 AMI 를 생성하면 장애 발생 시 인스턴스를 쉽게 복제할 수 있습니다.

설명 2:

옵션 A 는 고가용성 또는 확장성을 위한 솔루션을 제공하지 않습니다. 동일한 AZ 에서 다른 EC2 인스턴스를 수동으로 시작하면 해당 AZ 에 장애가 발생하면 다운타임이 발생하므로 고가용성이 보장되지 않을 수 있습니다.

옵션 B 는 데이터베이스 성능을 개선하고 내결함성 수준을 제공하지만 웹 사이트 플랫폼의 확장성 측면을 다루지는 않습니다.

옵션 C 는 고가용성과 내결함성을 모두 제공합니다. AMI 를 생성하면 AZ 간에 EC2 인스턴스를 쉽게 복제할 수 있습니다. 두 AZ 에서 ALB 를 구성하고 ASG 를 연결하면 여러 인스턴스에 걸쳐 확장성과 부하 분산이 보장됩니다.

옵션 D 는 회사에서 요구하는 고가용성 및 확장성을 제공하지 않습니다. S3 에 예약된 백업은 데이터 보호를 다루지만 웹사이트 가용성이나 확장성에 기여하지는 않습니다.

Q245

A company is launching an application on AWS. The application uses an Application Load Balancer (ALB) to direct traffic to at least two Amazon EC2 instances in a single target group. The instances are in an Auto Scaling group for each environment. The company requires a development environment and a production environment. The production environment will have periods of high traffic.

Which solution will configure the development environment MOST cost-effectively?

A. Reconfigure the target group in the development environment to have only one EC2 instance as a target.

B. Change the ALB balancing algorithm to least outstanding requests.

C. Reduce the size of the EC2 instances in both environments.

D. Reduce the maximum number of EC2 instances in the development environment's Auto Scaling group.

Answer: A

https://www.examtopics.com/discussions/amazon/view/95337-exam-aws-certified-solutions-architect-associate-saa-c03/

설명

대상으로 하나의 EC2 인스턴스만 포함하도록 개발 환경에서 대상 그룹을 구성하면 해당 환경에 할당된 리소스를 효과적으로 줄일 수 있습니다. 이렇게 하면 더 적은 수의 EC2 인스턴스 및 관련 리소스를 활용하여 비용을 최소화할 수 있습니다.

옵션 B 는 개발 환경의 비용 효율성을 직접 다루지 않습니다. 비용 최적화보다는 로드 밸런싱 전략에 중점을 둡니다.

옵션 C 는 현재 인스턴스 크기가 과도하게 프로비저닝되거나 애플리케이션 요구 사항에 불필요하지 않는 한 가장 비용 효율적인 솔루션이 아닐 수 있습니다.

옵션 D 는 비용 절감에 도움이 될 수 있지만 특히 부하가 증가하는 기간 동안 트래픽을 처리하고 효율적으로 확장하는 환경의 기능에 영향을 미칠 수 있습니다.

전반적으로 옵션 A 는 기능 설정을 유지하면서 개발 환경에 할당된 리소스를 최소화함으로써 비용 효율적인 접근 방식을 제공합니다.

Q246

A company runs a web application on Amazon EC2 instances in multiple Availability Zones. The EC2 instances are in private subnets. A solutions architect implements an internet-facing Application Load Balancer (ALB) and specifies the EC2 instances as the target group. However, the internet traffic is not reaching the EC2 instances.

How should the solutions architect reconfigure the architecture to resolve this issue?

A. Replace the ALB with a Network Load Balancer. Configure a NAT gateway in a public subnet to allow internet traffic.

B. Move the EC2 instances to public subnets. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0.

C. Update the route tables for the EC2 instances' subnets to send 0.0.0.0/0 traffic through the internet gateway route. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0.

D. Create public subnets in each Availability Zone. Associate the public subnets with the ALB. Update the route tables for the public subnets with a route to the private subnets.

Answer: D

https://www.examtopics.com/discussions/amazon/view/95003-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

A. 다른 유형의 로드 밸런서를 사용하고 NAT 게이트웨이를 구성할 것을 제안하지만 EC2 인스턴스에 도달하는 인터넷 트래픽 문제는 다루지 않습니다.

B.는 EC2 인스턴스를 퍼블릭 인터넷에 노출할 것을 제안합니다. 이는 보안 위험을 초래할 수 있으며 인스턴스에 도달하는 인바운드 인터넷 트래픽 문제를 해결하지 않습니다.

C.는 아웃바운드 인터넷 액세스를 갖도록 EC2 인스턴스를 구성할 것을 제안하지만 인스턴스에 도달하는 인바운드 인터넷 트래픽 문제를 해결하지는 않습니다.

D.가 정답입니다. 퍼블릭 서브넷을 생성하고 이를 ALB 와 연결하면 인바운드 인터넷 트래픽이 ALB 에 도달할 수 있습니다. 프라이빗 서브넷에 대한 경로를 포함하도록 퍼블릭 서브넷의 라우팅 테이블이 업데이트되어 트래픽이 프라이빗 서브넷의 EC2 인스턴스에 도달할 수 있습니다. 이 설정을 사용하면 인터넷 트래픽이 ALB 를 통해 EC2 인스턴스에 도달하도록 허용하면서 애플리케이션에 대한 보안 액세스가 가능합니다.

참고:
https://repost.aws/ko/knowledge-center/public-load-balancer-private-ec2

Q247
A company has deployed a database in Amazon RDS for MySQL. Due to increased transactions, the database support team is reporting slow reads against the DB instance and recommends adding a read replica.
Which combination of actions should a solutions architect take before implementing this change? (Choose two)
A. Enable binlog replication on the RDS primary node.
B. Choose a failover priority for the source DB instance.
C. Allow long-running transactions to complete on the source DB instance.
D. Create a global table and specify the AWS Regions where the table will be available.
E. Enable automatic backups on the source instance by setting the backup retention period to a value other than 0.
Answer: C, E
https://www.examtopics.com/discussions/amazon/view/95004-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A. 읽기 복제본 설정에 필요한 RDS 기본 노드에서 이진 로그 복제 기능을 활성화합니다.

B. 장애 조치 시나리오 중에 DB 인스턴스가 기본 역할로 승격되는 순서를 결정합니다. 느린 읽기 문제를 해결하기 위해 읽기 전용 복제본을 추가하는 것과 직접적인 관련이 없습니다.

C. 원본 DB 인스턴스에서 진행 중인 모든 트랜잭션이 변경 사항을 구현하기 전에 완료되도록 합니다. 읽기 전용 복제본으로 전환하는 동안 데이터 무결성과 일관성을 유지하는 데 도움이 됩니다.

D.는 DynamoDB 전용 기능입니다. DynamoDB 에서 다중 리전 복제 및 고가용성을 허용하지만 이 시나리오에는 적용할 수 없습니다.

E. 원본 DB 인스턴스에 대해 정기적인 백업이 수행되는지 확인합니다. 이는 읽기 전용 복제본을 추가하는 동안 또는 이후에 문제가 발생할 경우 특정 시점 복원을 허용하므로 데이터 보호 및 복구 목적에 중요합니다.

설명 2:
"오래 실행되는 활성 트랜잭션은 읽기 전용 복제본 생성 프로세스를 느리게 할 수 있습니다. 읽기 전용 복제본을 생성하기 전에 장기 실행 트랜잭션이 완료될 때까지 기다리는 것이 좋습니다. 동일한 원본 DB 인스턴스에서 여러 읽기 전용 복제본을 병렬로 생성하는 경우 , Amazon RDS 는 첫 번째 생성 작업 시작 시 하나의 스냅샷만 찍습니다. 읽기 전용 복제본을 생성할 때 고려해야 할 몇 가지 사항이 있습니다. 먼저 백업 보존 기간을 0 이외의 값.
이 요구 사항은 다른 읽기 전용 복제본의 원본 DB 인스턴스인 읽기 전용 복제본에도 적용됩니다."
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

Q248
A company runs analytics software on Amazon EC2 instances. The software accepts job requests from users to process data that has been uploaded to Amazon S3. Users report that some submitted data is not being processed Amazon CloudWatch reveals that the EC2 instances have a consistent CPU utilization at or near 100%. The company wants to improve system performance and scale the system based on user load.
What should a solutions architect do to meet these requirements?
A. Create a copy of the instance. Place all instances behind an Application Load Balancer.
B. Create an S3 VPC endpoint for Amazon S3. Update the software to reference the endpoint.
C. Stop the EC2 instances. Modify the instance type to one with a more powerful CPU and more memory. Restart the instances.
D. Route incoming requests to Amazon Simple Queue Service (Amazon SQS). Configure an EC2 Auto Scaling group based on queue size. Update the software to read from the queue.

Answer: D
https://www.examtopics.com/discussions/amazon/view/95329-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A. 인스턴스 사본을 생성하고 모든 인스턴스를 ALB 뒤에 배치하는 것은 높은 CPU 사용률 문제를 해결하거나 사용자 부하에 따라 확장성을 제공하지 않습니다.

B. S3 용 S3 VPC 엔드포인트를 생성하고 엔드포인트를 참조하도록 소프트웨어를 업데이트하면 네트워크 성능이 향상되지만 높은 CPU 사용률 문제를 해결하거나 사용자 부하에 따라 확장성을 제공하지 않습니다.

C. EC2 인스턴스를 중지하고 인스턴스 유형을 더 강력한 CPU 와 더 많은 메모리를 가진 인스턴스 유형으로 수정하면 성능이 향상될 수 있지만 사용자 부하에 따른 확장성은 해결되지 않습니다.

D. 들어오는 요청을 SQS 로 라우팅하고, 대기열 크기에 따라 EC2 ASG 를 구성하고, 대기열에서 읽을 수 있도록 소프트웨어를 업데이트하면 시스템 성능이 향상되고 사용자 로드에 따라 확장성이 제공됩니다.

따라서 옵션 D 는 높은 CPU 사용률을 해결하고 시스템 성능을 개선하며 사용자 부하에 따라 확장성을 활성화하므로 올바른 선택입니다.

Q249
A company is implementing a shared storage solution for a media application that is hosted in the AWS Cloud. The company needs the ability to use SMB clients to access data. The solution must be fully managed.
Which AWS solution meets these requirements?
A. Create an AWS Storage Gateway volume gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
B. Create an AWS Storage Gateway tape gateway. Configure tapes to use Amazon S3. Connect the application server to the tape gateway.
C. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
D. Create an Amazon FSx for Windows File Server file system. Attach the file system to the

origin server. Connect the application server to the file system.
Answer: D
https://www.examtopics.com/discussions/amazon/view/95006-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A. Storage Gateway 사용과 관련이 있지만 SMB 클라이언트에 대한 지원을 구체적으로 언급하지는 않습니다. SMB 클라이언트를 사용하여 데이터에 액세스해야 하는 요구 사항을 충족하지 못할 수 있습니다.

B. S3 에 데이터를 보관하는 데 주로 사용되는 테이프 게이트웨이 구성과 함께 Storage Gateway 를 사용하는 것과 관련됩니다. SMB 클라이언트가 데이터에 액세스할 수 있도록 기본 지원을 제공하지 않습니다.

C. EC2 Windows 인스턴스에서 Windows 파일 공유를 수동으로 설정하고 구성하는 작업이 포함됩니다. SMB 클라이언트가 데이터에 액세스할 수 있지만 수동 설정 및 유지 관리가 필요하므로 완전히 관리되는 솔루션은 아닙니다.

D. SMB 클라이언트를 지원하는 완전히 관리되는 Windows 파일 시스템인 FSx for Windows 파일 서버 파일 시스템 생성이 포함됩니다. 기본 SMB 를 지원하는 사용하기 쉬운 공유 스토리지 솔루션을 제공합니다.

SMB 클라이언트를 사용하고 완전히 관리되는 솔루션이 필요한 요구 사항을 기반으로 옵션 D 가 가장 적합한 선택입니다.

설명 2:
https://aws.amazon.com/fsx/lustre/
Amazon FSx 는 Windows 파일 시스템 기능과 업계 표준 서버를 기본적으로 지원합니다.
네트워크를 통해 파일 저장소에 액세스하기 위한 메시지 블록(SMB) 프로토콜.
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html

온프레미스-AWS 간 스토리지 서비스 중 SMB 지원하는 건 Storage Gateway File Gateway 나 Amazon FSx for Windows 라고 보면 됨.

Q250

A company's security team requests that network traffic be captured in VPC Flow Logs. The logs will be frequently accessed for 90 days and then accessed intermittently.
What should a solutions architect do to meet these requirements when configuring the logs?
A. Use Amazon CloudWatch as the target. Set the CloudWatch log group with an expiration of 90 days.
B. Use Amazon Kinesis as the target. Configure the Kinesis stream to always retain the logs for 90 days.
C. Use AWS CloudTrail as the target. Configure CloudTrail to save to an Amazon S3 bucket, and enable S3 Intelligent-Tiering.
D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days.
Answer: D
https://www.examtopics.com/discussions/amazon/view/95007-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A. CloudWatch 를 VPC 흐름 로그의 대상으로 사용할 것을 제안합니다. 그러나 90 일 동안 로그 보존을 관리한 다음 간헐적으로 액세스하는 메커니즘을 제공하지 않습니다.

B. Kinesis 를 VPC 흐름 로그의 대상으로 사용할 것을 제안합니다. 90 일 동안 로그를 보관할 수 있지만 로그에 대한 간헐적 액세스 요구 사항은 다루지 않습니다.

C. CloudTrail 을 VPC 흐름 로그의 대상으로 사용할 것을 제안합니다. 그러나 CloudTrail 은 네트워크 트래픽 로그 캡처가 아니라 API 활동을 감사 및 모니터링하도록 설계되었습니다. VPC 흐름 로그 캡처 요구 사항을 충족하지 않습니다.

D. S3 를 VPC 흐름 로그의 대상으로 사용하고 S3 수명 주기 정책을 활용하여 90 일 후에 로그를 비용 효율적인 스토리지 클래스로 전환할 것을 제안합니다. 90 일 동안 로그를 유지해야 하는 요구 사항을 충족하고 스토리지 비용을 최적화하면서 간헐적인 액세스에 대한 유연성을 제공합니다.

설명 2:
여기에는 VPC 흐름 로그가 S3 로 직접 이동할 수 있음을 지정하는 표가 있습니다. CloudTrail 을 거쳐 S3 로 이동할 필요가 없습니다. CW 를 통해서도 아닙니다.
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AWS-logs-and-resourcepolicy.html#AWS-logs-i

Q251

An Amazon EC2 instance is located in a private subnet in a new VPC. This subnet does not have outbound internet access, but the EC2 instance needs the ability to download monthly security updates from an outside vendor.

What should a solutions architect do to meet these requirements?

A. Create an internet gateway, and attach it to the VPC. Configure the private subnet route table to use the internet gateway as the default route.

B. Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.

C. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the NAT instance as the default route.

D. Create an internet gateway, and attach it to the VPC. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the internet gateway as the default route.

Answer: B

https://www.examtopics.com/discussions/amazon/view/95023-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

A. 사설 서브넷에 직접 인터넷 액세스를 제공합니다. 이는 아웃바운드 인터넷 액세스를 제한하는 것이 목표이므로 이 경우에는 바람직하지 않습니다.

B. 프라이빗 서브넷의 EC2 가 프록시 역할을 하는 NAT 게이트웨이를 통해 인터넷에 액세스할 수 있습니다. 프라이빗 서브넷의 보안을 유지하면서 통제된 아웃바운드 인터넷 액세스를 제공합니다.

C. NAT 게이트웨이를 사용하는 것과 유사하지만 NAT 인스턴스를 사용하는 것과 관련이 있습니다. NAT 인스턴스는 NAT 게이트웨이에 비해 더 많은 수동 구성 및 관리가 필요하므로 덜 선호되는 옵션입니다.

D. 필요하지 않은 인터넷 게이트웨이와 NAT 인스턴스의 사용을 결합합니다. 불필요한 복잡성이 발생하고 추가 관리가 필요한 NAT 인스턴스가 추가됩니다.

전반적으로 옵션 B 는 퍼블릭 서브넷에 배치된 NAT 게이트웨이를 활용하여 프라이빗

서브넷의 EC2 인스턴스에 대해 제어된 아웃바운드 인터넷 액세스를 활성화하므로 가장 적합한 솔루션입니다.

NAT 게이트웨이는 AWS 및 일반적으로 NAT 인스턴스보다 선호됩니다.

설명 2:
이 접근 방식을 사용하면 EC2 인스턴스가 여전히 프라이빗 서브넷에 있는 동안 인터넷에 액세스하고 월별 보안 업데이트를 다운로드할 수 있습니다. NAT 게이트웨이를 만들어 퍼블릭 서브넷에 배치하면 프라이빗 서브넷의 인스턴스가 NAT 게이트웨이를 통해 인터넷에 액세스할 수 있습니다. 그런 다음 NAT 게이트웨이를 기본 경로로 사용하도록 프라이빗 서브넷 경로 테이블을 구성합니다. 이렇게 하면 모든 아웃바운드 트래픽이 NAT 게이트웨이를 통해 전달되어 EC2 인스턴스가 프라이빗 서브넷의 보안을 유지하면서 인터넷에 액세스할 수 있습니다.

Q252
A solutions architect needs to design a system to store client case files. The files are core company assets and are important. The number of files will grow over time.
The files must be simultaneously accessible from multiple application servers that run on Amazon EC2 instances. The solution must have built-in redundancy.
Which solution meets these requirements?
A. Amazon Elastic File System (Amazon EFS)
B. Amazon Elastic Block Store (Amazon EBS)
C. Amazon S3 Glacier Deep Archive
D. AWS Backup
Answer: A
https://www.examtopics.com/discussions/amazon/view/95024-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
EFS 는 여러 EC2 에서 동시에 액세스할 수 있는 확장 가능하고 완벽하게 관리되는 파일 스토리지 서비스를 제공합니다. 리전 내의 여러 AZ 에 데이터를 저장하여 기본 제공 중복성을 제공합니다. EFS 를 사용하면 여러 애플리케이션 서버에서 클라이언트 사례 파일에 동시에 액세스할 수 있으므로 시간이 지남에 따라 파일 수가 증가함에 따라 고가용성과 확장성이 보장됩니다.

옵션 B 인 EBS 는 일반적으로 개별 EC2 에 연결하는 데 사용되는 블록 수준 스토리지 서비스이며 여러 인스턴스에 대한 동시 액세스를 제공하지 않으므로 이 시나리오에 적합하지 않습니다.

옵션 C, S3 Glacier Deep Archive 는 장기 아카이브 스토리지 서비스이며 활성 파일 액세스 및 여러 애플리케이션 서버의 동시 액세스에 적합하지 않을 수 있습니다.

옵션 D, AWS Backup 은 중앙 집중식 백업 관리 서비스이며 필요한 동시 파일 액세스 및 중복 기능을 제공하지 않습니다.

따라서 가장 적합한 솔루션은 Amazon EFS(옵션 A)입니다.

설명 2:
Amazon EFS 는 여러 EC2 인스턴스에서 동시에 액세스할 수 있는 간단하고 확장 가능한 완전 관리형 파일 시스템을 제공하며 내장된 중복성을 제공합니다. 동일한 파일에 액세스하기 위해 여러 EC2 인스턴스에 최적화되어 있으며 가용성, 내구성 및 보안성이 우수하도록 설계되었습니다. 데이터를 페타바이트까지 확장할 수 있고 수천 개의 동시 연결을 처리할 수 있으며 대량의 데이터를 저장하고 액세스하기 위한 비용 효율적인 솔루션입니다.

Q253
A solutions architect has created two IAM policies: Policy1 and Policy2. Both policies are attached to an IAM group.

Policy 1

```
{
  "Version": "2012-10-17",  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:Get*",
        "iam:List*",
        "kms:List*",
        "ec2:*",
        "ds:*",
        "logs:Get*",
        "logs:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

Policy 2

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ds:Delete*",
      "Resource": "*"
    }
  ]
}
```

A cloud engineer is added as an IAM user to the IAM group. Which action will the cloud engineer be able to perform?

A. Deleting IAM users

B. Deleting directories

C. Deleting Amazon EC2 instances

D. Deleting logs from Amazon CloudWatch Logs

Answer: C

https://www.examtopics.com/discussions/amazon/view/95008-exam-aws-certified-solutions-architect-associate-saa-c03/

Q254

A company is reviewing a recent migration of a three-tier application to a VPC. The security team discovers that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.

What should a solutions architect do to correct this issue?

A. Create security group rules using the instance ID as the source or destination.

B. Create security group rules using the security group ID as the source or destination.

C. Create security group rules using the VPC CIDR blocks as the source or destination.

D. Create security group rules using the subnet CIDR blocks as the source or destination.

Answer: B

https://www.examtopics.com/discussions/amazon/view/95009-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

A. 특정 인스턴스를 기반으로 트래픽을 제한하므로 애플리케이션 계층 간에 최소 권한 원칙을 적용하는 데 가장 적합한 솔루션이 아닐 수 있습니다.

B. 규칙에서 보안 그룹 ID 를 사용하면 필요한 통신만 허용하고 최소 권한 원칙을 준수하여 애플리케이션 계층 간의 트래픽을 정밀하게 제어할 수 있습니다.

C. 전체 VPC CIDR 블록을 기반으로 광범위한 규칙을 적용하여 특정 애플리케이션 계층 간의 보안 통신에 필요한 수준의 세분성을 제공하지 못할 수 있습니다.

D. 서브넷 CIDR 블록을 기반으로 트래픽을 제한하므로 애플리케이션 계층 간의 적절한 보안을 보장하기에 충분하지 않을 수 있습니다.

요약하면 보안 그룹 ID(옵션 B)를 사용하면 최소 권한 원칙에 따라 애플리케이션 계층 간의 트래픽을 정밀하게 제어할 수 있으므로 권장되는 접근 방식입니다.

참고

https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/security-group-rules.html

Q255

A company has an ecommerce checkout workflow that writes an order to a database and

calls a service to process the payment. Users are experiencing timeouts during the checkout process. When users resubmit the checkout form, multiple unique orders are created for the same desired transaction.

How should a solutions architect refactor this workflow to prevent the creation of multiple orders?

A. Configure the web application to send an order message to Amazon Kinesis Data Firehose. Set the payment service to retrieve the message from Kinesis Data Firehose and process the order.

B. Create a rule in AWS CloudTrail to invoke an AWS Lambda function based on the logged application path request. Use Lambda to query the database, call the payment service, and pass in the order information.

C. Store the order in the database. Send a message that includes the order number to Amazon Simple Notification Service (Amazon SNS). Set the payment service to poll Amazon SNS, retrieve the message, and process the order.

D. Store the order in the database. Send a message that includes the order number to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the payment service to retrieve the message and process the order. Delete the message from the queue.

Answer: D

https://www.examtopics.com/discussions/amazon/view/95026-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

A. 다중 주문 생성 방지에 적합한 솔루션이 아닙니다. 이 접근 방식은 순차적이고 안정적인 주문 처리를 보장하지 않습니다.

B. 다중 주문 생성을 방지하기 위한 적절한 해결책이 아닙니다. CloudTrail 은 주로 API 활동을 기록하고 감사하는 데 사용되며 기록된 요청을 기반으로 Lambda 를 호출하면 올바른 주문 처리가 보장되지 않습니다.

C.는 적절한 솔루션이 아닙니다. SNS 는 게시-구독 메시징 서비스이며 이를 폴링하면 처리가 지연되고 잠재적인 주문 중복이 발생할 수 있습니다.

D.가 정답입니다. SQS FIFO 를 사용하면 주문이 순차적이고 안정적인 방식으로 처리되어 동일한 거래에 대해 여러 주문이 생성되는 것을 방지할 수 있습니다.

설명 2:

VPC 내에 있는 프라이빗 서브넷의 EC2 인스턴스와 DynamoDB 간 가장 안전한 AWS 네트워크 통신 = VPC Gateway Endpoint.

게이트웨이 엔드포인트는 VPC 용 인터넷 게이트웨이 또는 NAT 디바이스가 없어도 Amazon

S3 및 DynamoDB 에 대한 안정적인 연결을 제공합니다.
https://docs.aws.amazon.com/ko_kr/vpc/latest/privatelink/vpce-gateway.html#vpc-endpoints-limitations

설명 3:
DynamoDB 용 VPC 엔드포인트를 사용하면 VPC 의 Amazon EC2 인스턴스가 프라이빗 IP 주소를 사용하여 퍼블릭 인터넷에 노출되지 않고 DynamoDB 에 액세스할 수 있습니다. EC2 인스턴스에는 퍼블릭 IP 주소가 필요하지 않으며 VPC 에 인터넷 게이트웨이, NAT 디바이스 또는 가상 프라이빗 게이트웨이가 필요하지 않습니다. 엔드포인트 정책을 사용하여 DynamoDB 에 대한 액세스를 제어합니다. VPC 와 AWS 서비스 간의 트래픽은 Amazon 네트워크를 벗어나지 않습니다.

Q256
A solutions architect is implementing a document review application using an Amazon S3 bucket for storage. The solution must prevent accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to download, modify, and upload documents.
Which combination of actions should be taken to meet these requirements? (Choose two)
A. Enable a read-only bucket ACL.
B. Enable versioning on the bucket.
C. Attach an IAM policy to the bucket.
D. Enable MFA Delete on the bucket.
E. Encrypt the bucket using AWS KMS.
Answer: B, D
https://www.examtopics.com/discussions/amazon/view/95460-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
B. S3 버킷에 여러 버전의 객체를 저장할 수 있습니다. 이렇게 하면 문서를 실수로 덮어쓰거나 삭제하더라도 모든 버전의 문서를 사용할 수 있습니다.

D. 버킷의 객체를 우발적으로 삭제하지 않도록 추가 보호 계층을 추가합니다. MFA 삭제가 활성화된 상태에서 사용자는 버킷에서 객체를 성공적으로 삭제하려면 추가 인증 요소를 제공해야 합니다. 이를 통해 우발적 삭제 또는 무단 삭제를 방지하고 중요한 문서에 대한

추가 보안 수준을 제공합니다.

A. 사용자가 문서를 수정하거나 업로드하는 것을 제한합니다. 사용자가 문서를 다운로드, 수정 및 업로드할 수 있도록 허용하는 요구 사항을 충족하지 않습니다.

C. 버킷에 대한 액세스 권한을 제어할 수 있지만 우발적인 삭제를 방지하거나 문서의 모든 버전의 가용성을 보장하는 요구 사항을 구체적으로 다루지는 않습니다.

E. 암호화는 버전 관리 및 삭제 방지보다는 데이터 보호에 중점을 둡니다.

Q257

A company is building a solution that will report Amazon EC2 Auto Scaling events across all the applications in an AWS account. The company needs to use a serverless solution to store the EC2 Auto Scaling status data in Amazon S3. The company then will use the data in Amazon S3 to provide near-real-time updates in a dashboard. The solution must not affect the speed of EC2 instance launches.

How should the company move the data to Amazon S3 to meet these requirements?

A. Use an Amazon CloudWatch metric stream to send the EC2 Auto Scaling status data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.

B. Launch an Amazon EMR cluster to collect the EC2 Auto Scaling status data and send the data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.

C. Create an Amazon EventBridge rule to invoke an AWS Lambda function on a schedule. Configure the Lambda function to send the EC2 Auto Scaling status data directly to Amazon S3.

D. Use a bootstrap script during the launch of an EC2 instance to install Amazon Kinesis Agent. Configure Kinesis Agent to collect the EC2 Auto Scaling status data and send the data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.

Answer: A

https://www.examtopics.com/discussions/amazon/view/95027-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

B. EC2 Auto Scaling 상태 데이터를 수집하고 S3 로 보내는 데 불필요한 복잡성과 오버헤드가 발생합니다. 이 특정 요구 사항에 가장 효율적인 서버리스 솔루션은 아닙니다.

C. 실시간으로 트리거되지 않기 때문에 데이터 업데이트가 지연될 수 있습니다. 또한 직접 데이터 스트림을 사용하는 것과 비교할 때 불필요한 오버헤드와 복잡성이 추가됩니다.

D. 추가 종속성 및 관리 오버헤드를 도입합니다. 또한 피해야 할 요구 사항인 EC2 인스턴스 시작 속도에 영향을 미칠 수 있습니다.

전반적으로 옵션 A 는 CloudWatch 지표 스트림과 Kinesis Data Firehose 를 활용하여 EC2 인스턴스 시작 속도에 영향을 주지 않고 S3 에서 EC2 Auto Scaling 상태 데이터를 효율적으로 캡처하고 저장함으로써 간소화된 서버리스 솔루션을 제공합니다.

설명 2:
지표 스트림을 사용하여 CloudWatch 지표를 거의 실시간으로 제공하고 낮은 지연 시간으로 선택한 대상으로 지속적으로 스트리밍할 수 있습니다. 사용 사례 중 하나는 데이터 레이크입니다. 지표 스트림을 생성하고 CloudWatch 지표를 Amazon S3 와 같은 데이터 레이크에 전달하는 Amazon Kinesis Data Firehose 전달 스트림으로 보냅니다.
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Metric-Streams.html

Q258
A company has an application that places hundreds of .csv files into an Amazon S3 bucket every hour. The files are 1 GB in size. Each time a file is uploaded, the company needs to convert the file to Apache Parquet format and place the output file into an S3 bucket.
Which solution will meet these requirements with the LEAST operational overhead?
A. Create an AWS Lambda function to download the .csv files, convert the files to Parquet format, and place the output files in an S3 bucket. Invoke the Lambda function for each S3 PUT event.
B. Create an Apache Spark job to read the .csv files, convert the files to Parquet format, and place the output files in an S3 bucket. Create an AWS Lambda function for each S3 PUT event to invoke the Spark job.
C. Create an AWS Glue table and an AWS Glue crawler for the S3 bucket where the application places the .csv files. Schedule an AWS Lambda function to periodically use Amazon Athena to query the AWS Glue table, convert the query results into Parquet format, and place the output files into an S3 bucket.
D. Create an AWS Glue extract, transform, and load (ETL) job to convert the .csv files to Parquet format and place the output files into an S3 bucket. Create an AWS Lambda function

for each S3 PUT event to invoke the ETL job.
Answer: D
https://www.examtopics.com/discussions/amazon/view/95028-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A. 상당한 운영 오버헤드가 발생합니다. 이 접근 방식에는 Lambda 관리, 동시성 처리, 큰 파일 크기에 대한 적절한 오류 처리 보장이 필요하며 이는 어려울 수 있습니다.
B. 불필요한 복잡성과 운영 오버헤드를 추가합니다. Spark 작업 관리, 확장성 처리 및 각 파일 업로드에 대한 Lambda 호출 조정은 번거로울 수 있습니다.
C. 추가 복잡성을 도입하고 가장 효율적인 솔루션이 아닐 수 있습니다. 여기에는 Glue 리소스 관리, Lambda 예약, 새 파일이 업로드되지 않은 경우에도 데이터 쿼리가 포함됩니다.

옵션 D 는 AWS Glue 의 ETL 기능을 활용하여 규모에 맞게 데이터 변환 작업을 정의하고 실행할 수 있습니다. 각 S3 PUT 이벤트에 대해 Lambda 함수를 사용하여 ETL 작업을 호출하면 수동 개입 없이 파일이 Parquet 형식으로 효율적으로 변환되도록 할 수 있습니다. 이 접근 방식은 운영 오버헤드를 최소화하고 간소화되고 확장 가능한 솔루션을 제공합니다.

참고:
https://docs.aws.amazon.com/ko_kr/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html

Q259
A company is implementing new data retention policies for all databases that run on Amazon RDS DB instances. The company must retain daily backups for a minimum period of 2 years. The backups must be consistent and restorable.
Which solution should a solutions architect recommend to meet these requirements?
A. Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan.
B. Configure a backup window for the RDS DB instances for daily snapshots. Assign a snapshot retention policy of 2 years to each RDS DB instance. Use Amazon Data Lifecycle Manager (Amazon DLM) to schedule snapshot deletions.
C. Configure database transaction logs to be automatically backed up to Amazon CloudWatch Logs with an expiration period of 2 years.

D. Configure an AWS Database Migration Service (AWS DMS) replication task. Deploy a replication instance, and configure a change data capture (CDC) task to stream database changes to Amazon S3 as the target. Configure S3 Lifecycle policies to delete the snapshots after 2 years.
Answer: A
https://www.examtopics.com/discussions/amazon/view/95030-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A. 중앙 집중식 백업 관리 서비스인 AWS Backup 을 사용하여 RDS 백업을 유지할 것을 제안합니다. 백업 볼트가 생성되고 일일 일정과 2 년의 백업 보존 기간으로 백업 계획이 정의됩니다. RDS DB 인스턴스가 이 백업 계획에 할당됩니다.
B. 일관되고 복원 가능한 백업에 대한 요구 사항을 다루지 않습니다. 스냅샷은 시점 백업이며 원하는 수준의 일관성을 제공하지 못할 수 있습니다.
C. 데이터베이스에 필요한 백업 및 복원 기능을 제공하도록 설계되지 않았습니다. 백업의 일관성을 보장하거나 쉬운 복원 메커니즘을 제공하지 않습니다.
D. 일일 백업 및 일관된 백업 보존에 대한 요구 사항을 다루지 않습니다. 백업 및 복원보다는 복제 및 변경 데이터 캡처에 더 중점을 둡니다.

설명 2:
AWS Backup 은 사용자가 AWS 서비스 전체에서 데이터 백업을 중앙 집중화하고 자동화할 수 있는 완전 관리형 서비스입니다. 백업 빈도 및 보존 기간을 지정하는 백업 계획을 생성하고 관리할 수 있습니다. 또한 백업 데이터를 저장하는 컨테이너인 백업 볼트에 백업 리소스를 할당할 수도 있습니다 1. 솔루션은 AWS Backup 을 사용하여 RDS 백업이 일관되고 복원 가능하며 최소 2 년 동안 유지되도록 할 수 있습니다.
1. 일일 스냅샷을 위해 RDS DB 인스턴스의 백업 기간을 구성합니다. 각 RDS DB 인스턴스에 2 년의 스냅샷 보존 정책을 할당합니다. Amazon DLM(Amazon Data Lifecycle Manager)을 사용하여 스냅샷 삭제를 예약합니다. Amazon DLM 은 RDS 스냅샷과 호환되지 않고 스냅샷 삭제를 예약하는 데 사용할 수 없기 때문에 이 솔루션은 백업의 일관성과 복원 가능성을 보장해야 하는 요구 사항을 충족하지 않습니다.
2. 만료 기간이 2 년인 Amazon CloudWatch Logs 에 자동으로 백업되도록 데이터베이스 트랜잭션 로그를 구성합니다. 이 솔루션은 데이터베이스를 특정 시점으로 복원하는 데 데이터베이스 트랜잭션 로그가 충분하지 않기 때문에 백업이 일관되고 복원 가능한지 확인해야 하는 요구 사항을 충족하지 않습니다. 데이터베이스의 전체 상태가 아니라 데이터베이스에 대한 변경 사항만 캡처합니다.
3. AWS Database Migration Service(AWS DMS) 복제 작업을 구성합니다. 복제 인스턴스를

배포하고 변경 데이터 캡처(CDC) 작업을 구성하여 데이터베이스 변경 사항을 대상으로 Amazon S3 에 스트리밍합니다. 2 년 후 스냅샷을 삭제하도록 S3 수명 주기 정책을 구성합니다. AWS DMS 는 사용자가 데이터베이스를 백업하는 것이 아니라 AWS 로 데이터베이스를 마이그레이션하는 데 도움이 되는 서비스이므로 이 솔루션은 백업의 일관성과 복원 가능성을 보장해야 하는 요구 사항을 충족하지 않습니다. 또한 복제 인스턴스 및 CDC 작업과 같은 추가 리소스 및 구성이 필요합니다.
참조 URL:
https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html

Q260
A company's compliance team needs to move its file shares to AWS. The shares run on a Windows Server SMB file share. A self-managed on-premises Active Directory controls access to the files and folders.
The company wants to use Amazon FSx for Windows File Server as part of the solution. The company must ensure that the on-premises Active Directory groups restrict access to the FSx for Windows File Server SMB compliance shares, folders, and files after the move to AWS. The company has created an FSx for Windows File Server file system.
Which solution will meet these requirements?
A. Create an Active Directory Connector to connect to the Active Directory. Map the Active Directory groups to IAM groups to restrict access.
B. Assign a tag with a Restrict tag key and a Compliance tag value. Map the Active Directory groups to IAM groups to restrict access.
C. Create an IAM service-linked role that is linked directly to FSx for Windows File Server to restrict access.
D. Join the file system to the Active Directory to restrict access.
Answer: D
https://www.examtopics.com/discussions/amazon/view/95343-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
D. 파일 시스템이 인증 및 액세스 제어를 위해 기존 AD 인프라를 활용할 수 있습니다.

이 시나리오에서는 AD 그룹을 IAM 그룹에 매핑하는 것이 적용되지 않기 때문에 옵션 A 가 올바르지 않습니다. IAM 은 주로 AWS 리소스에 대한 액세스를 관리하는 데 사용되지만 요구 사항은 액세스 제어를 위해 온프레미스 AD 와 통합하는 것입니다.

Restrict 태그 키와 규정 준수 태그 값이 있는 태그를 할당하면 액세스 제어를 위해 온프레미스 AD 와의 필수 통합이 제공되지 않기 때문에 옵션 B 는 올바르지 않습니다. 태그는 리소스를 구성하고 분류하는 데 사용되며 인증 또는 액세스 제어 메커니즘을 제공하지 않습니다.

FSx for Windows File Server 에 직접 연결된 IAM 서비스 연결 역할 생성이 온프레미스 AD 와 통합되지 않기 때문에 옵션 C 는 올바르지 않습니다. IAM 역할은 권한 관리를 위해 AWS 내에서 사용되며 외부 AD 시스템과의 필수 통합을 제공하지 않습니다.

설명 2:
FSx for Windows File Server 파일 시스템을 온프레미스 Active Directory 에 결합하면 회사에서 기존 Active Directory 그룹을 사용하여 AWS 로 이동한 후 파일 공유, 폴더 및 파일에 대한 액세스를 제한할 수 있습니다. 이 옵션을 사용하면 회사는 기존 액세스 제어 및 관리 구조를 계속 사용하여 AWS 로 보다 원활하게 전환할 수 있습니다.

Q261
A company recently announced the deployment of its retail website to a global audience. The website runs on multiple Amazon EC2 instances behind an Elastic Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones.
The company wants to provide its customers with different versions of content based on the devices that the customers use to access the website.
Which combination of actions should a solutions architect take to meet these requirements? (Choose two)
A. Configure Amazon CloudFront to cache multiple versions of the content.
B. Configure a host header in a Network Load Balancer to forward traffic to different instances.
C. Configure a Lambda@Edge function to send specific objects to users based on the User-Agent header.
D. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up host-based routing to different EC2 instances.
E. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up path-based routing to different EC2 instances.
Answer: A, C
https://www.examtopics.com/discussions/amazon/view/95011-exam-aws-certified-solut

ions-architect-associate-saa-c03/

설명 1:
A. 고객이 위치 및 장치 유형에 따라 적절한 버전의 콘텐츠를 받을 수 있습니다.
C. Lambda@Edge 를 생성하면 들어오는 요청의 User-Agent 헤더를 검사하고 사용 중인 장치 유형을 확인할 수 있습니다. 이 정보를 기반으로 응답을 사용자 지정하고 적절한 버전의 콘텐츠를 사용자에게 보낼 수 있습니다.
B. 장치 유형에 따라 다른 콘텐츠 버전을 제공해야 하는 요구 사항을 다루지 않습니다.
D. & E.는 장치별 콘텐츠 요구 사항을 다루지 않습니다.

따라서 옵션 A 와 C 는 고객이 웹 사이트에 액세스하는 데 사용하는 장치에 따라 다양한 버전의 콘텐츠를 제공해야 하는 요구 사항을 충족하기 위한 올바른 작업 조합입니다.

설명
C 의 경우: 향상된 사용자 경험 Lambda@Edge 는 성능 저하 없이 콘텐츠를 개인화할 수 있도록 하여 전 세계 웹 사이트 및 웹 애플리케이션에 대한 사용자 경험을 개선하는 데 도움을 줄 수 있습니다. 실시간 이미지 변환 사용자 특성에 따라 즉시 이미지를 변환하여 사용자 경험을 사용자 정의할 수 있습니다. 예를 들어 뷰어의 장치 유형(모바일, 데스크톱 또는 태블릿)에 따라 이미지 크기를 조정할 수 있습니다. 또한 CloudFront Edge 위치에서 변환된 이미지를 캐싱하여 이미지를 제공할 때 성능을 더욱 향상시킬 수 있습니다.
https://aws.amazon.com/lambda/edge/

Q262
A company plans to use Amazon ElastiCache for its multi-tier web application. A solutions architect creates a Cache VPC for the ElastiCache cluster and an App VPC for the application's Amazon EC2 instances. Both VPCs are in the us-east-1 Region.
The solutions architect must implement a solution to provide the application's EC2 instances with access to the ElastiCache cluster.
Which solution will meet these requirements MOST cost-effectively?
A. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.
B. Create a Transit VPC. Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.

C. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the peering connection's security group to allow inbound connection from the application's security group.
D. Create a Transit VPC. Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC. Configure an inbound rule for the Transit VPC's security group to allow inbound connection from the application's security group.
Answer: A
https://www.examtopics.com/discussions/amazon/view/95463-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
VPC 간에 피어링 연결을 생성하는 것은 연결을 설정하는 비용 효율적인 방법입니다. 두 VPC 에서 피어링 연결을 위한 라우팅 테이블 항목을 추가하면 두 VPC 간에 트래픽이 흐를 수 있습니다. ElastiCache 클러스터의 보안 그룹에서 인바운드 규칙을 구성하면 애플리케이션 보안 그룹의 인바운드 연결이 허용되어 앱 VPC 의 EC2 인스턴스에서 ElastiCache 클러스터에 액세스할 수 있습니다.
옵션 B 는 이 시나리오에 불필요한 복잡성과 비용을 추가하는 Transit VPC 생성을 제안합니다.
옵션 C 는 인바운드 연결을 제어하는 데 ElastiCache 클러스터의 보안 그룹을 사용해야 하므로 필요하지 않은 피어링 연결의 보안 그룹에 대한 인바운드 규칙 구성을 제안합니다.
옵션 D 는 Transit VPC 의 보안 그룹에 대한 인바운드 규칙 구성을 제안하며, 이는 이 경우에 필요하지 않으며 불필요한 복잡성을 추가합니다.
따라서 옵션 A 는 애플리케이션의 EC2 인스턴스에 ElastiCache 클러스터에 대한 액세스 권한을 제공하는 가장 비용 효율적인 솔루션입니다.

설명 2:
두 VPC 간에 피어링 연결을 생성하고 ElastiCache 클러스터의 보안 그룹에 대한 인바운드 규칙을 구성하여 애플리케이션의 보안 그룹에서 인바운드 연결을 허용하는 것이 가장 비용 효율적인 솔루션입니다. 피어링 연결은 무료이며 보안 그룹 규칙을 구성하는 비용만 발생합니다. Transit VPC 솔루션에는 추가 비용이 발생하는 추가 VPC 및 관련 리소스가 필요합니다.
https://aws.amazon.com/certification/policies/before-testing/

Q263
A company is building an application that consists of several microservices. The company

has decided to use container technologies to deploy its software on AWS. The company needs a solution that minimizes the amount of ongoing effort for maintenance and scaling. The company cannot manage additional infrastructure.

Which combination of actions should a solutions architect take to meet these requirements? (Choose two)

A. Deploy an Amazon Elastic Container Service (Amazon ECS) cluster.

B. Deploy the Kubernetes control plane on Amazon EC2 instances that span multiple Availability Zones.

C. Deploy an Amazon Elastic Container Service (Amazon ECS) service with an Amazon EC2 launch type. Specify a desired task number level of greater than or equal to 2.

D. Deploy an Amazon Elastic Container Service (Amazon ECS) service with a Fargate launch type. Specify a desired task number level of greater than or equal to 2.

E. Deploy Kubernetes worker nodes on Amazon EC2 instances that span multiple Availability Zones. Create a deployment that specifies two or more replicas for each microservice.

Answer: A, D

https://www.examtopics.com/discussions/amazon/view/95012-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

옵션 B 와 E 는 Kubernetes 컨트롤 플레인과 작업자 노드를 EC2 인스턴스에 배포할 것을 제안합니다. 이렇게 하려면 노력을 최소화해야 한다는 요구 사항과 달리 인프라를 관리하고 지속적인 유지 관리 오버헤드를 추가해야 합니다.

옵션 C 는 ECS 에 대해 Amazon EC2 시작 유형을 사용할 것을 제안합니다. 이 유형은 여전히 EC2 인스턴스 관리가 필요하고 Fargate 를 사용하는 것만큼 비용 효율적이고 확장 가능하지 않습니다.

따라서 Amazon ECS 클러스터와 ECS 서비스를 Fargate 시작 유형(옵션 A 및 D)으로 배포하는 조합은 추가 인프라를 관리하지 않고 유지 관리 및 확장 노력을 최소화하는 데 가장 적합합니다.

설명 2:

AWS Fargate 는 Amazon EC2 인스턴스의 서버 또는 클러스터를 관리할 필요 없이 컨테이너를 실행하기 위해 Amazon ECS 와 함께 사용할 수 있는 기술입니다. Fargate 를 사용하면 더 이상 컨테이너를 실행하기 위해 가상 머신의 클러스터를 프로비저닝, 구성

또는 확장할 필요가 없습니다.
https://docs.aws.amazon.com/AmazonECS/latest/userguide/what-is-fargate.html

Q264
A company has a web application hosted over 10 Amazon EC2 instances with traffic directed by Amazon Route 53. The company occasionally experiences a timeout error when attempting to browse the application. The networking team finds that some DNS queries return IP addresses of unhealthy instances, resulting in the timeout error.
What should a solutions architect implement to overcome these timeout errors?
A. Create a Route 53 simple routing policy record for each EC2 instance. Associate a health check with each record.
B. Create a Route 53 failover routing policy record for each EC2 instance. Associate a health check with each record.
C. Create an Amazon CloudFront distribution with EC2 instances as its origin. Associate a health check with the EC2 instances.
D. Create an Application Load Balancer (ALB) with a health check in front of the EC2 instances. Route to the ALB from Route 53.
Answer: D
https://www.examtopics.com/discussions/amazon/view/95345-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
설계자는 ALB 를 생성하고 상태 확인을 구성하여 정상 인스턴스만 트래픽을 수신하도록 합니다. ALB 는 구성된 상태 확인 설정을 기반으로 EC2 인스턴스의 상태를 주기적으로 확인합니다.
Route 53 에서 ALB 로 트래픽을 라우팅하면 DNS 쿼리가 개별 인스턴스 대신 ALB 의 IP 주소를 반환합니다. 이를 통해 ALB 는 정상 인스턴스에만 트래픽을 분산하여 비정상 인스턴스로 인한 시간 초과를 방지할 수 있습니다.
A & B: 상태 확인을 각 레코드와 연결하면 비정상 인스턴스를 식별하는 데 도움이 될 수 있지만 자동 로드 밸런싱 및 정상 인스턴스에 대한 트래픽 배포를 제공하지 않습니다.
C: CloudFront 는 성능과 가용성을 향상시킬 수 있지만 기본적으로 CDN 이며 로드 밸런싱 및 정상 인스턴스에 대한 트래픽 분산 문제를 직접적으로 해결하지 못할 수 있습니다.
따라서 옵션 D 는 상태 확인이 포함된 ALB 를 구현하고 Route 53 을 통해 트래픽을 라우팅하여 시간 초과 오류를 극복하는 데 가장 적합한 솔루션입니다.

설명 2:
ALB(Application Load Balancer)를 사용하면 들어오는 트래픽을 여러 백엔드 인스턴스에 분산하고 비정상 인스턴스에서 트래픽을 제거하면서 정상 인스턴스로 트래픽을 자동으로 라우팅할 수 있습니다. EC2 인스턴스 앞에 ALB 를 사용하고 Route 53 에서 ALB 로 트래픽을 라우팅함으로써 로드 밸런서는 인스턴스에 대한 상태 확인을 수행하고 정상 인스턴스로만 트래픽을 라우팅할 수 있으므로 비정상 인스턴스로 인한 시간 초과 오류를 줄이거나 제거하는 데 도움이 됩니다.

Q265
A solutions architect needs to design a highly available application consisting of web, application, and database tiers. HTTPS content delivery should be as close to the edge as possible, with the least delivery time.
Which solution meets these requirements and is MOST secure?
A. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
B. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.
C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
D. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.
Answer: C
https://www.examtopics.com/discussions/amazon/view/95013-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A. EC2 인스턴스를 퍼블릭 인터넷에 직접 노출하므로 보안이 손상될 수 있습니다.
B. 효율적인 부하 분산과 고가용성을 위해 필요한 퍼블릭 서브넷의 부하 분산 장치가 부족합니다.
D. 로드 밸런싱 및 HTTPS 콘텐츠 전송을 제공하며 EC2 인스턴스를 공용 인터넷에 직접 노출하므로 보안 위험이 발생할 수 있습니다.

C. 퍼블릭 ALB 를 오리진으로 하는 CloudFront 를 사용하여 고가용성, 프라이빗 서브넷을 통한 보안 액세스 및 최적화된 HTTPS 콘텐츠 전송을 제공합니다.

설명 2:
이 솔루션은 웹, 애플리케이션 및 데이터베이스 계층이 있는 고가용성 애플리케이션에 대한 요구 사항을 충족할 뿐만 아니라 에지 기반 콘텐츠 전달을 제공합니다. 또한 웹 서버에 대한 직접 액세스를 제한하는 프라이빗 서브넷에 ALB 를 두어 보안을 최대화하는 동시에 퍼블릭 ALB 를 통해 인터넷을 통해 트래픽을 제공할 수 있습니다. 이렇게 하면 웹 서버가 공용 인터넷에 노출되지 않으므로 공격 표면이 줄어들고 애플리케이션에 안전하게 액세스할 수 있습니다.

Q266
A company has a popular gaming platform running on AWS. The application is sensitive to latency because latency can impact the user experience and introduce unfair advantages to some players. The application is deployed in every AWS Region. It runs on Amazon EC2 instances that are part of Auto Scaling groups configured behind Application Load Balancers (ALBs). A solutions architect needs to implement a mechanism to monitor the health of the application and redirect traffic to healthy endpoints.
Which solution meets these requirements?
A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on, and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.
B. Create an Amazon CloudFront distribution and specify the ALB as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
C. Create an Amazon CloudFront distribution and specify Amazon S3 as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
D. Configure an Amazon DynamoDB database to serve as the data store for the application. Create a DynamoDB Accelerator (DAX) cluster to act as the in-memory cache for DynamoDB hosting the application data.
Answer: A
https://www.examtopics.com/discussions/amazon/view/95014-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
B. CloudFront 는 캐싱 및 콘텐츠 전송에 도움이 될 수 있지만 애플리케이션의 상태를 모니터링하거나 상태 확인을 기반으로 트래픽 리디렉션을 수행하는 메커니즘을 제공하지 않습니다.
C. 이 구성은 정적 콘텐츠 전달에 적합하지만 응용 프로그램의 상태 모니터링 및 트래픽 리디렉션 요구 사항을 다루지 않습니다.
D. 이렇게 하면 성능이 향상될 수 있지만 애플리케이션의 상태를 모니터링하거나 상태 확인을 기반으로 트래픽을 리디렉션하지 않습니다.
따라서 옵션 A 는 AWS Global Accelerator 를 활용하여 애플리케이션 상태를 모니터링하고, 트래픽을 정상 엔드포인트로 라우팅하고, 지연 시간 문제를 해결하면서 사용자 경험을 최적화하므로 가장 적합한 솔루션입니다.

설명 2:
AWS Global Accelerator 는 상태 확인을 기반으로 최적의 정상 엔드포인트로 트래픽을 전달하고 클라이언트의 지리적 위치를 기반으로 가장 가까운 정상 엔드포인트로 트래픽을 라우팅할 수도 있습니다. 액셀러레이터를 구성하고 이를 각 리전의 지역 엔드포인트에 연결하고 ALB 를 엔드포인트로 추가함으로써 솔루션은 트래픽을 정상 엔드포인트로 리디렉션하여 대기 시간을 줄이고 애플리케이션이 최적으로 실행되도록 함으로써 사용자 경험을 개선합니다. 이 솔루션은 트래픽이 가장 가까운 정상 엔드포인트로 전달되도록 하고 전반적인 사용자 경험을 개선하는 데 도움이 됩니다.

Q267
A company has one million users that use its mobile app. The company must analyze the data usage in near-real time. The company also must encrypt the data in near-real time and must store the data in a centralized location in Apache Parquet format for further processing.
Which solution will meet these requirements with the LEAST operational overhead?
A. Create an Amazon Kinesis data stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data. Invoke an AWS Lambda function to send the data to the Kinesis Data Analytics application.
B. Create an Amazon Kinesis data stream to store the data in Amazon S3. Create an Amazon EMR cluster to analyze the data. Invoke an AWS Lambda function to send the data to the EMR cluster.
C. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon EMR cluster to analyze the data.

D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data.
Answer: D
https://www.examtopics.com/discussions/amazon/view/95347-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A. 데이터를 분석 애플리케이션으로 보내려면 Lambda 를 호출해야 합니다. 이로 인해 추가적인 운영 오버헤드와 복잡성이 발생합니다.

B. EMR 은 빅 데이터 처리를 위한 강력한 도구이지만 Kinesis Data Analytics 에 비해 더 많은 운영 관리 및 구성이 필요합니다.

C. Kinesis Data Analytics 가 보다 간소화되고 자동화된 방식으로 분석을 수행할 때 데이터 분석에 EMR 을 포함하여 불필요한 복잡성을 도입합니다.

따라서 옵션 D 는 데이터 수집에 Kinesis Data Firehose 를 활용하고 S3 에 데이터를 저장하며 거의 실시간 분석을 위해 Kinesis Data Analytics 를 활용하여 데이터 사용 분석 및 암호화를 위한 운영 오버헤드가 낮은 솔루션을 제공하므로 가장 적합한 솔루션입니다. .

설명 2:
이 솔루션은 거의 실시간으로 데이터 수집, 데이터 변환, 암호화 및 데이터 저장을 자동으로 처리할 수 있는 완전관리형 서비스인 Amazon Kinesis Data Firehose 를 사용하므로 최소한의 운영 오버헤드로 요구 사항을 충족합니다. Kinesis Data Firehose 는 추가 처리를 위해 Amazon S3 에 Apache Parquet 형식으로 데이터를 자동으로 저장할 수 있습니다.
또한 Amazon Kinesis Data Analytics 애플리케이션을 생성하여 인프라를 관리하거나 Lambda 함수를 호출할 필요 없이 거의 실시간으로 데이터를 분석할 수 있습니다. 이렇게 하면 최소한의 운영 오버헤드로 많은 양의 데이터를 처리할 수 있습니다.

Q268
A gaming company has a web application that displays scores. The application runs on Amazon EC2 instances behind an Application Load Balancer. The application stores data in an Amazon RDS for MySQL database. Users are starting to experience long delays and interruptions that are caused by database read performance. The company wants to

improve the user experience while minimizing changes to the application's architecture.
What should a solutions architect do to meet these requirements?
A. Use Amazon ElastiCache in front of the database.
B. Use RDS Proxy between the application and the database.
C. Migrate the application from EC2 instances to AWS Lambda.
D. Migrate the database from Amazon RDS for MySQL to Amazon DynamoDB.
Answer: B
https://www.examtopics.com/discussions/amazon/view/95016-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A. ElastiCache 는 자주 액세스하는 데이터를 캐싱하여 읽기 성능을 향상시킬 수 있지만 애플리케이션 아키텍처를 변경해야 합니다. 또한 특히 애플리케이션의 데이터베이스 사용에 복잡한 쿼리 또는 빈번한 데이터 업데이트가 포함되는 경우 RDS Proxy 와 동일한 수준의 읽기 성능 향상을 제공하지 못할 수 있습니다.
C. Lambda 는 확장성 및 운영 오버헤드 감소와 같은 이점을 제공할 수 있지만 데이터베이스 읽기 성능 문제를 직접 해결하지 못할 수 있습니다. Lambda 로 마이그레이션하려면 애플리케이션의 아키텍처 및 코드베이스를 크게 변경해야 합니다.
D. DynamoDB 는 확장 가능한 고성능 NoSQL 데이터베이스이지만 MySQL 과 같은 관계형 데이터베이스에서 DynamoDB 로 마이그레이션하려면 애플리케이션의 데이터 모델과 쿼리 패턴을 크게 변경해야 합니다.
따라서 옵션 B 는 RDS Proxy 를 활용하여 데이터베이스 연결을 최적화하고 읽기 성능을 개선하고 애플리케이션 아키텍처의 변경을 최소화하며 데이터베이스 읽기 성능 문제를 해결하기 위한 확장 가능하고 효율적인 솔루션을 제공하므로 가장 적합한 솔루션입니다.

Q269
An ecommerce company has noticed performance degradation of its Amazon RDS based web application. The performance degradation is attributed to an increase in the number of read-only SQL queries triggered by business analysts. A solutions architect needs to solve the problem with minimal changes to the existing web application.
What should the solutions architect recommend?
A. Export the data to Amazon DynamoDB and have the business analysts run their queries.
B. Load the data into Amazon ElastiCache and have the business analysts run their queries.
C. Create a read replica of the primary database and have the business analysts run their queries.

D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries.
Answer: C
https://www.examtopics.com/discussions/amazon/view/95032-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A. DynamoDB 는 확장 가능한 NoSQL 데이터베이스이지만 애플리케이션의 데이터 모델 및 쿼리 패턴을 변경해야 합니다.
B. ElastiCache 는 쿼리 성능을 향상시킬 수 있는 인메모리 데이터 저장소이지만 주로 복잡한 쿼리를 실행하기보다는 캐싱에 사용됩니다.
D. Redshift 는 강력한 데이터 웨어하우징 솔루션이지만 데이터를 마이그레이션하고 쿼리를 Redshift 의 열 기반 아키텍처에 적용하려면 애플리케이션 및 쿼리 논리를 크게 변경해야 합니다.
따라서 옵션 C 는 RDS 의 읽기 전용 복제본을 활용하여 기본 데이터베이스에서 읽기 전용 쿼리 트래픽을 오프로드하므로 비즈니스 분석가가 웹 애플리케이션의 성능에 영향을 주지 않고 쿼리를 실행할 수 있으므로 가장 적합한 권장 사항입니다. 기존 웹 애플리케이션에 대한 최소한의 변경으로 확장 가능하고 효율적인 솔루션을 제공합니다.

설명 2:
기본 RDS 데이터베이스의 읽기 복제본을 생성하면 기본 데이터베이스에서 읽기 전용 SQL 쿼리를 오프로드하여 웹 애플리케이션의 성능을 향상시키는 데 도움이 됩니다. 읽기 복제본은 읽기 전용 트래픽을 처리하는 데 사용할 수 있는 기본 데이터베이스의 정확한 복사본으로, 기본 데이터베이스의 부하를 줄이고 웹 애플리케이션의 성능을 향상시킵니다.
이 솔루션은 기존 웹 애플리케이션에 대한 최소한의 변경으로 구현할 수 있습니다.
분석가는 코드를 수정하지 않고 읽기 복제본에서 쿼리를 계속 실행할 수 있습니다.

Q270
A company is using a centralized AWS account to store log data in various Amazon S3 buckets. A solutions architect needs to ensure that the data is encrypted at rest before the data is uploaded to the S3 buckets. The data also must be encrypted in transit.
Which solution meets these requirements?
A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.
B. Use server-side encryption to encrypt the data that is being uploaded to the S3 buckets.
C. Create bucket policies that require the use of server-side encryption with S3 managed

encryption keys (SSE-S3) for S3 uploads.
D. Enable the security option to encrypt the S3 buckets through the use of a default AWS Key Management Service (AWS KMS) key.
Answer: A
https://www.examtopics.com/discussions/amazon/view/95031-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
클라이언트 측 암호화는 데이터를 Amazon S3 에 업로드하기 전에 데이터를 암호화하는 방법입니다. 이를 통해 사용자는 암호화 프로세스, 암호화 키 및 관련 도구를 관리할 수 있습니다. 클라이언트 측 암호화를 사용하면 Amazon S3 가 암호화 키나 암호화되지 않은 데이터에 액세스할 수 없기 때문에 솔루션은 유휴 및 전송 중에 데이터를 암호화할 수 있습니다.

Q271
A solutions architect observes that a nightly batch processing job is automatically scaled up for 1 hour before the desired Amazon EC2 capacity is reached. The peak capacity is the ‘same every night and the batch jobs always start at 1 AM. The solutions architect needs to find a cost-effective solution that will allow for the desired EC2 capacity to be reached quickly and allow the Auto Scaling group to scale down after the batch jobs are complete. What should the solutions architect do to meet these requirements?
A. Increase the minimum capacity for the Auto Scaling group.
B. Increase the maximum capacity for the Auto Scaling group.
C. Configure scheduled scaling to scale up to the desired compute level.
D. Change the scaling policy to add more EC2 instances during each scaling operation.
Answer: C
https://www.examtopics.com/discussions/amazon/view/95018-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
예약된 조정을 구성하여 솔루션 설계자는 배치 작업이 시작될 때 특정 시간(IAM)에 원하는 컴퓨팅 수준으로 자동으로 확장한 다음 작업이 완료되면 자동으로 축소하도록 Auto Scaling 그룹을 설정할 수 있습니다. 이렇게 하면 원하는 EC2 용량에 빠르게 도달할 수 있고 비용 절감에도 도움이 됩니다.

Q272

A company serves a dynamic website from a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The website needs to support multiple languages to serve customers around the world. The website's architecture is running in the us-west-1 Region and is exhibiting high request latency for users that are located in other parts of the world. The website needs to serve requests quickly and efficiently regardless of a user's location. However, the company does not want to recreate the existing architecture across multiple Regions.

What should a solutions architect do to meet these requirements?

A. Replace the existing architecture with a website that is served from an Amazon S3 bucket. Configure an Amazon CloudFront distribution with the S3 bucket as the origin. Set the cache behavior settings to cache based on the Accept-Language request header.

B. Configure an Amazon CloudFront distribution with the ALB as the origin. Set the cache behavior settings to cache based on the Accept-Language request header.

C. Create an Amazon API Gateway API that is integrated with the ALB. Configure the API to use the HTTP integration type. Set up an API Gateway stage to enable the API cache based on the Accept-Language request header.

D. Launch an EC2 instance in each additional Region and configure NGINX to act as a cache server for that Region. Put all the EC2 instances and the ALB behind an Amazon Route 53 record set with a geolocation routing policy.

Answer: B

https://www.examtopics.com/discussions/amazon/view/99865-exam-aws-certified-solutions-architect-associate-saa-c03/

Q273

A rapidly growing ecommerce company is running its workloads in a single AWS Region. A solutions architect must create a disaster recovery (DR) strategy that includes a different AWS Region. The company wants its database to be up to date in the DR Region with the least possible latency. The remaining infrastructure in the DR Region needs to run at reduced capacity and must be able to scale up if necessary.

Which solution will meet these requirements with the LOWEST recovery time objective (RTO)?

A. Use an Amazon Aurora global database with a pilot light deployment.

B. Use an Amazon Aurora global database with a warm standby deployment.

C. Use an Amazon RDS Multi-AZ DB instance with a pilot light deployment.
D. Use an Amazon RDS Multi-AZ DB instance with a warm standby deployment.
Answer: B
https://www.examtopics.com/discussions/amazon/view/99505-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
▪ 웜 스탠바이는 감소된 수준의 트래픽을 즉시 처리할 수 있습니다. 그런 다음 이 기존 배포를 확장해야 하므로 파일럿 라이트보다 RTO 시간이 더 짧습니다. 파일럿 라이트를 사용하려면 먼저 인프라를 배포한 다음 워크로드가 요청을 처리할 수 있기 전에 리소스를 확장해야 하기 때문입니다.
https://aws.amazon.com/ko/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iii-pilot-light-and-warm-standby/
A(X) : 파일럿 라이트를 사용하기 때문에 오답.
B(O) : Amazon Aurora 글로벌 데이터베이스는 여러 리전에 걸쳐 자동으로 복제를 진행
Amazon Aurora Global Database 는 단일 Amazon Aurora 데이터베이스를 여러 AWS 리전으로 확장할 수 있는 기능입니다. 데이터베이스 성능에 전혀 영향을 주지 않고 데이터를 복제하고, 각 리전에서 보통 1 초 미만의 짧은 대기 시간으로 빠른 로컬 읽기를 지원하며, 리전 규모의 가동 중단 발생 시 재해 복구를 제공합니다.""
https://aws.amazon.com/ko/rds/aurora/faqs/
C(X) : 파일럿 라이트를 사용하기 때문에 오답.
D(X) : RDS Multi AZ 는 동일 리전 내로 한정됨.
Amazon RDS 다중 AZ 배포는 단일 AWS 리전 내의 데이터베이스 인스턴스에 대한 향상된 가용성을 제공합니다.
https://aws.amazon.com/ko/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/

Q274
A company runs an application on Amazon EC2 instances. The company needs to implement a disaster recovery (DR) solution for the application. The DR solution needs to have a recovery time objective (RTO) of less than 4 hours. The DR solution also needs to use the fewest possible AWS resources during normal operations.
Which solution will meet these requirements in the MOST operationally efficient way?
A. Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by

using AWS Lambda and custom scripts.
B. Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS CloudFormation.
C. Launch EC2 instances in a secondary AWS Region. Keep the EC2 instances in the secondary Region active at all times.
D. Launch EC2 instances in a secondary Availability Zone. Keep the EC2 instances in the secondary Availability Zone active at all times.
Answer: B
https://www.examtopics.com/discussions/amazon/view/99459-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이를 통해 회사는 RTO(복구 시간 목표)가 4 시간 미만이고 정상 운영 중에 AWS 리소스를 최대한 적게 사용하는 애플리케이션에 대한 재해 복구(DR) 솔루션을 구현할 수 있습니다. Amazon 머신 이미지(AMI)를 생성하여 EC2 인스턴스를 백업하고 AMI 를 보조 AWS 리전에 복사함으로써 회사는 애플리케이션의 특정 시점 스냅샷을 생성하고 이를 다른 지리적 위치에 저장할 수 있습니다. AWS CloudFormation 을 사용하여 보조 지역의 인프라 배포를 자동화함으로써 회사는 재해 발생 시 템플릿에서 리소스 스택을 신속하게 시작할 수 있습니다. 이는 EC2 인스턴스용 DR 솔루션을 구현하는 비용 효율적이고 운영 효율적인 방법입니다.

Q275
A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours, but scales down to 2 instances overnight. Staff are complaining that the application is very slow when the day begins, although it runs well by mid-morning.
How should the scaling be changed to address the staff complaints and keep costs to a minimum?
A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.
B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.

C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period.
D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens.
Answer: C
https://www.examtopics.com/discussions/amazon/view/99584-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 옵션은 아침에 용량을 더 빠르게 확장하여 성능을 개선하지만 작업 외 시간에도 여전히 용량을 축소할 수 있습니다. 다음과 같이 이를 달성합니다.
* 대상 추적 작업은 CPU 사용률 대상에 따라 확장됩니다. 아침에 더 낮은 CPU 임계값에서 트리거함으로써 Auto Scaling 그룹은 트래픽이 증가함에 따라 더 빨리 확장을 시작하여 사용률이 너무 높아져 성능에 영향을 미치기 전에 인스턴스를 시작합니다.
* 휴지 기간을 줄이면 Auto Scaling 이 보다 적극적으로 확장하여 목표에 도달할 때까지 더 많은 인스턴스를 더 빠르게 시작할 수 있습니다. 이렇게 하면 용량 증가 속도가 빨라집니다.
* 그러나 고정된 최소/최대 용량을 설정하는 예약된 작업과 달리 대상 추적을 사용하면 수요에 따라 근무 외 시간에도 그룹을 축소할 수 있습니다. 이는 비용을 최소화하는 데 도움이 됩니다.

Q276
A company has a multi-tier application deployed on several Amazon EC2 instances in an Auto Scaling group. An Amazon RDS for Oracle instance is the application's data layer that uses Oracle-specific PL/SQL functions. Traffic to the application has been steadily increasing. This is causing the EC2 instances to become overloaded and the RDS instance to run out of storage. The Auto Scaling group does not have any scaling metrics and defines the minimum healthy instance count only. The company predicts that traffic will continue to increase at a steady but unpredictable rate before leveling off.
What should a solutions architect do to ensure the system can automatically scale for the increased traffic? (Choose two)
A. Configure storage Auto Scaling on the RDS for Oracle instance.
B. Migrate the database to Amazon Aurora to use Auto Scaling storage.
C. Configure an alarm on the RDS for Oracle instance for low free storage space.
D. Configure the Auto Scaling group to use the average CPU as the scaling metric.

E. Configure the Auto Scaling group to use the average free memory as the scaling metric.
Answer: A, D
https://www.examtopics.com/discussions/amazon/view/99739-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Auto Scaling Storage RDS 는 스토리지 문제를 완화하고 Oracle Pl/Sql 을 Aurora 로 마이그레이션하는 것은 번거롭습니다. 또한 Aurora 에는 기본적으로 자동 스토리지 확장 기능이 있습니다.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIOPS.StorageTypes.html#USER_PIOPS.Autoscaling

Q277
A company provides an online service for posting video content and transcoding it for use by any mobile platform. The application architecture uses Amazon Elastic File System (Amazon EFS) Standard to collect and store the videos so that multiple Amazon EC2 Linux instances can access the video content for processing. As the popularity of the service has grown over time, the storage costs have become too expensive.
Which storage solution is MOST cost-effective?
A. Use AWS Storage Gateway for files to store and process the video content.
B. Use AWS Storage Gateway for volumes to store and process the video content.
C. Use Amazon EFS for storing the video content. Once processing is complete, transfer the files to Amazon Elastic Block Store (Amazon EBS).
D. Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon Elastic Block Store (Amazon EBS) volume attached to the server for processing.
Answer: D
https://www.examtopics.com/discussions/amazon/view/99509-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
* 비디오 콘텐츠의 대규모, 내구성 및 저렴한 스토리지를 위한 Amazon S3. S3 스토리지 비용은 EFS 보다 훨씬 저렴합니다.
* Amazon EBS 는 처리 중에 일시적으로만 가능합니다. 비디오를 처리해야 할 때만 EBS 볼륨을 마운트하고 그 후에 마운트를 해제함으로써 컨텐츠가 고가의 EBS 스토리지에 소요되는 시간을 최소화합니다.

* EBS 볼륨은 활성 처리에 필요한 워크로드에 맞게 크기를 조정하여 비용을 낮출 수 있습니다. 볼륨은 전체 비디오 라이브러리를 장기간 저장할 필요가 없습니다.

Q278

A company wants to create an application to store employee data in a hierarchical structured relationship. The company needs a minimum-latency response to high-traffic queries for the employee data and must protect any sensitive data. The company also needs to receive monthly email messages if any financial information is present in the employee data.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two)

A. Use Amazon Redshift to store the employee data in hierarchies. Unload the data to Amazon S3 every month.

B. Use Amazon DynamoDB to store the employee data in hierarchies. Export the data to Amazon S3 every month.

C. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly events to AWS Lambda.

D. Use Amazon Athena to analyze the employee data in Amazon S3. Integrate Athena with Amazon QuickSight to publish analysis dashboards and share the dashboards with users.

E. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon Simple Notification Service (Amazon SNS) subscription.

Answer: B, E

https://www.examtopics.com/discussions/amazon/view/99940-exam-aws-certified-solutions-architect-associate-saa-c03/

참고:

https://docs.aws.amazon.com/ko_kr/prescriptive-guidance/latest/dynamodb-hierarchical-data-model/introduction.html

Q279

A company has an application that is backed by an Amazon DynamoDB table. The company's compliance requirements specify that database backups must be taken every month, must be available for 6 months, and must be retained for 7 years.

Which solution will meet these requirements?

A. Create an AWS Backup plan to back up the DynamoDB table on the first day of each month. Specify a lifecycle policy that transitions the backup to cold storage after 6 months. Set the retention period for each backup to 7 years.

B. Create a DynamoDB on-demand backup of the DynamoDB table on the first day of each month. Transition the backup to Amazon S3 Glacier Flexible Retrieval after 6 months. Create an S3 Lifecycle policy to delete backups that are older than 7 years.

C. Use the AWS SDK to develop a script that creates an on-demand backup of the DynamoDB table. Set up an Amazon EventBridge rule that runs the script on the first day of each month. Create a second script that will run on the second day of each month to transition DynamoDB backups that are older than 6 months to cold storage and to delete backups that are older than 7 years.

D. Use the AWS CLI to create an on-demand backup of the DynamoDB table. Set up an Amazon EventBridge rule that runs the command on the first day of each month with a cron expression. Specify in the command to transition the backups to cold storage after 6 months and to delete the backups after 7 years.

Answer: A

https://www.examtopics.com/discussions/amazon/view/99793-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

이 솔루션은 다음과 같은 요구 사항을 충족합니다.

* AWS Backup 은 백업 계획에 정의된 일정(매월 1 일)에 따라 DynamoDB 테이블의 전체 백업을 자동으로 수행합니다.

* 수명 주기 정책은 6 개월 후에 백업을 콜드 스토리지로 전환하여 해당 요구 사항을 충족할 수 있습니다.

* 백업 계획에서 7 년 보존 기간을 설정하면 필요에 따라 각 백업이 7 년 동안 보존됩니다.

* AWS Backup 은 백업 작업 및 수명 주기 정책을 관리하므로 사용자 지정 스크립팅 또는 관리가 필요하지 않습니다.

Q280

A company is using Amazon CloudFront with its website. The company has enabled logging on the CloudFront distribution, and logs are saved in one of the company's Amazon S3 buckets. The company needs to perform advanced analyses on the logs and build visualizations.

What should a solutions architect do to meet these requirements?

A. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 bucket. Visualize the results with AWS Glue.

B. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 bucket. Visualize the results with Amazon QuickSight.

C. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs in the S3 bucket. Visualize the results with AWS Glue.

D. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs in the S3 bucket. Visualize the results with Amazon QuickSight.

Answer: B

https://www.examtopics.com/discussions/amazon/view/99508-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

https://docs.aws.amazon.com/quicksight/latest/user/welcome.html

Athena 를 사용하여 S3 버킷의 CloudFront 로그를 쿼리하고 QuickSight 를 사용하여 결과를 시각화하는 것이 비용 효율적이고 확장 가능하며 인프라 설정이 필요하지 않기 때문에 최상의 솔루션입니다. 또한 전담 개발자 팀 없이 회사에서 고급 분석을 수행하고 대화형 시각화를 구축할 수 있는 강력한 솔루션을 제공합니다.

Q281

A company runs a fleet of web servers using an Amazon RDS for PostgreSQL DB instance. After a routine compliance check, the company sets a standard that requires a recovery point objective (RPO) of less than 1 second for all its production databases.

Which solution meets these requirements?

A. Enable a Multi-AZ deployment for the DB instance.

B. Enable auto scaling for the DB instance in one Availability Zone.

C. Configure the DB instance in one Availability Zone, and create multiple read replicas in a separate Availability Zone.

D. Configure the DB instance in one Availability Zone, and configure AWS Database Migration Service (AWS DMS) change data capture (CDC) tasks.

Answer: A

https://www.examtopics.com/discussions/amazon/view/99511-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 옵션은 다른 가용 영역에 있는 대기 인스턴스에 데이터를 자동으로 복제하여 RDS 데이터베이스 인스턴스에 향상된 가용성과 내구성을 제공하는 DB 인스턴스용 다중 AZ 배포를 사용하기 때문에 가장 효율적입니다. 또한 대기 인스턴스가 동기식 물리적 복제를 사용하여 기본 인스턴스와 동기화 상태를 유지하므로 모든 프로덕션 데이터베이스에 대해 1 초 미만의 복구 지점 목표(RPO)를 제공합니다. 이 솔루션은 모든 프로덕션 데이터베이스에 대해 1 초 미만의 RPO 요구 사항을 충족합니다.
옵션 B 는 로드 또는 일정에 따라 DB 인스턴스의 컴퓨팅 용량을 자동으로 조정하는 방법인 하나의 가용 영역에서 DB 인스턴스에 대해 Auto Scaling 을 사용하기 때문에 효율성이 떨어집니다.
그러나 이것은 데이터를 다른 가용 영역에 복제하지 않기 때문에 모든 프로덕션 데이터베이스에 대해 1 초 미만의 RPO 를 제공하지 않습니다.
옵션 C 는 읽기 트래픽을 제공하고 조정을 지원할 수 있는 기본 데이터베이스의 읽기 전용 복사본인 별도의 가용 영역에서 읽기 전용 복제본을 사용하기 때문에 효율성이 떨어집니다. 그러나 읽기 전용 복제본은 비동기식 복제를 사용하고 기본 데이터베이스보다 지연될 수 있으므로 모든 프로덕션 데이터베이스에 대해 1 초 미만의 RPO 를 제공하지 않습니다.
옵션 D 는 원본 데이터에 대한 변경 사항을 캡처하고 대상 데이터에 적용하는 작업인 AWS DMS(AWS Database Migration Service) 변경 데이터 캡처(CDC) 작업을 사용하기 때문에 효율성이 떨어집니다. 그러나 AWS DMS 는 비동기식 복제를 사용하고 소스 데이터베이스보다 지연될 수 있으므로 모든 프로덕션 데이터베이스에 대해 1 초 미만의 RPO 를 제공하지 않습니다.

Q282
A company runs a web application that is deployed on Amazon EC2 instances in the private subnet of a VPC. An Application Load Balancer (ALB) that extends across the public subnets directs web traffic to the EC2 instances. The company wants to implement new security measures to restrict inbound traffic from the ALB to the EC2 instances while preventing access from any other source inside or outside the private subnet of the EC2 instances.
Which solution will meet these requirements?
A. Configure a route in a route table to direct traffic from the internet to the private IP addresses of the EC2 instances.
B. Configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB.
C. Move the EC2 instances into the public subnet. Give the EC2 instances a set of Elastic IP addresses.

D. Configure the security group for the ALB to allow any TCP traffic on any port.
Answer: B
https://www.examtopics.com/discussions/amazon/view/99660-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
ALB 에서 EC2 인스턴스로의 인바운드 트래픽을 제한하려면 EC2 인스턴스의 보안 그룹은 ALB 의 보안 그룹에서 들어오는 트래픽만 허용해야 합니다. 이렇게 하면 EC2 인스턴스는 ALB 에서만 요청을 받을 수 있으며 프라이빗 서브넷 내부 또는 외부의 다른 소스에서는 요청을 받을 수 없습니다.

Q283
A research company runs experiments that are powered by a simulation application and a visualization application. The simulation application runs on Linux and outputs intermediate data to an NFS share every 5 minutes. The visualization application is a Windows desktop application that displays the simulation output and requires an SMB file system.
The company maintains two synchronized file systems. This strategy is causing data duplication and inefficient resource usage. The company needs to migrate the applications to AWS without making code changes to either application.
Which solution will meet these requirements?
A. Migrate both applications to AWS Lambda. Create an Amazon S3 bucket to exchange data between the applications.
B. Migrate both applications to Amazon Elastic Container Service (Amazon ECS). Configure Amazon FSx File Gateway for storage.
C. Migrate the simulation application to Linux Amazon EC2 instances. Migrate the visualization application to Windows EC2 instances. Configure Amazon Simple Queue Service (Amazon SQS) to exchange data between the applications.
D. Migrate the simulation application to Linux Amazon EC2 instances. Migrate the visualization application to Windows EC2 instances. Configure Amazon FSx for NetApp ONTAP for storage.
Answer: D
https://www.examtopics.com/discussions/amazon/view/99512-exam-aws-certified-solutions-architect-associate-saa-c03/

Q284

As part of budget planning, management wants a report of AWS billed items listed by user. The data will be used to create department budgets. A solutions architect needs to determine the most efficient way to obtain this report information.

Which solution meets these requirements?

A. Run a query with Amazon Athena to generate the report.

B. Create a report in Cost Explorer and download the report.

C. Access the bill details from the billing dashboard and download the bill.

D. Modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES).

Answer: B

https://www.examtopics.com/discussions/amazon/view/99513-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

이 옵션은 시간 경과에 따른 AWS 비용 및 사용량을 시각화, 이해 및 관리할 수 있는 도구인 Cost Explorer 를 사용하기 때문에 가장 효율적입니다. 비용 탐색기에서 사용자 이름 태그를 필터로 사용하여 사용자별로 AWS 청구 항목을 나열하는 보고서를 생성할 수 있습니다. 그런 다음 보고서를 CSV 파일로 다운로드하여 예산 계획에 사용할 수 있습니다.

옵션 A 는 표준 SQL 을 사용하여 Amazon S3 의 데이터를 분석할 수 있는 서버리스 대화형 쿼리 서비스인 Amazon Athena 를 사용하기 때문에 효율성이 떨어집니다. S3 에서 AWS 비용 및 사용 보고서 데이터를 가리키는 Athena 테이블을 설정한 다음 쿼리를 실행하여 보고서를 생성해야 합니다. 이렇게 하면 추가 비용과 복잡성이 발생합니다.

옵션 C 는 AWS 비용 및 사용량에 대한 높은 수준의 요약을 제공하는 결제 대시보드를 사용하기 때문에 효율성이 떨어집니다. 청구 대시보드에서 청구 세부 정보에 액세스하고 청구서를 통해 다운로드할 수 있지만 사용자별로 청구 항목이 나열되지 않습니다. 추가 단계가 필요한 사용자 이름별로 비용을 그룹화하려면 태그를 사용해야 합니다.

옵션 D 는 서비스 사용량, 서비스 비용 및 인스턴스 예약을 계획할 수 있는 도구인 AWS 예산을 사용하기 때문에 효율성이 떨어집니다. Amazon Simple Email Service(Amazon SES)로 알리도록 AWS 예산에서 비용 예산을 수정할 수 있지만 이렇게 하면 사용자별로 AWS 청구 항목 보고서가 생성되지 않습니다. 이는 실제 또는 예상 비용이 예산 금액을 초과하거나 초과할 것으로 예상되는 경우에만 알려줍니다.

Q285

A company hosts its static website by using Amazon S3. The company wants to add a contact form to its webpage. The contact form will have dynamic server-side components for users to input their name, email address, phone number, and user message. The company anticipates that there will be fewer than 100 site visits each month.

Which solution will meet these requirements MOST cost-effectively?

A. Host a dynamic contact form page in Amazon Elastic Container Service (Amazon ECS). Set up Amazon Simple Email Service (Amazon SES) to connect to any third-party email provider.

B. Create an Amazon API Gateway endpoint with an AWS Lambda backend that makes a call to Amazon Simple Email Service (Amazon SES).

C. Convert the static webpage to dynamic by deploying Amazon Lightsail. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail.

D. Create a t2.micro Amazon EC2 instance. Deploy a LAMP (Linux, Apache, MySQL, PHP/Perl/Python) stack to host the webpage. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail.

Answer: B

https://www.examtopics.com/discussions/amazon/view/99680-exam-aws-certified-solutions-architect-associate-saa-c03/

Q286

A company has a static website that is hosted on Amazon CloudFront in front of Amazon S3. The static website uses a database backend. The company notices that the website does not reflect updates that have been made in the website's Git repository. The company checks the continuous integration and continuous delivery (CI/CD) pipeline between the Git repository and Amazon S3. The company verifies that the webhooks are configured properly and that the CI/CD pipeline is sending messages that indicate successful deployments.

A solutions architect needs to implement a solution that displays the updates on the website.

Which solution will meet these requirements?

A. Add an Application Load Balancer.

B. Add Amazon ElastiCache for Redis or Memcached to the database layer of the web application.

C. Invalidate the CloudFront cache.

D. Use AWS Certificate Manager (ACM) to validate the website's SSL certificate.
Answer: C
https://www.examtopics.com/discussions/amazon/view/99669-exam-aws-certified-solutions-architect-associate-saa-c03/

Q287
A company wants to migrate a Windows-based application from on premises to the AWS Cloud. The application has three tiers: an application tier, a business tier, and a database tier with Microsoft SQL Server. The company wants to use specific features of SQL Server such as native backups and Data Quality Services. The company also needs to share files for processing between the tiers.
How should a solutions architect design the architecture to meet these requirements?
A. Host all three tiers on Amazon EC2 instances. Use Amazon FSx File Gateway for file sharing between the tiers.
B. Host all three tiers on Amazon EC2 instances. Use Amazon FSx for Windows File Server for file sharing between the tiers.
C. Host the application tier and the business tier on Amazon EC2 instances. Host the database tier on Amazon RDS. Use Amazon Elastic File System (Amazon EFS) for file sharing between the tiers.
D. Host the application tier and the business tier on Amazon EC2 instances. Host the database tier on Amazon RDS. Use a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume for file sharing between the tiers.
Answer: B
https://www.examtopics.com/discussions/amazon/view/99670-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 솔루션을 통해 회사는 Amazon FSx for Windows File Server 를 사용하여 계층 간에 Windows 기반 파일 공유를 제공하면서 Amazon EC2 인스턴스에서 세 계층을 모두 호스팅할 수 있습니다. 이를 통해 회사는 기본 백업 및 데이터 품질 서비스와 같은 SQL Server 의 특정 기능을 사용하면서 계층 간에 처리를 위해 파일을 공유할 수 있습니다.

Q288
A company is migrating a Linux-based web server group to AWS. The web servers must

access files in a shared file store for some content. The company must not make any changes to the application.

What should a solutions architect do to meet these requirements?

A. Create an Amazon S3 Standard bucket with access to the web servers.

B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.

C. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers.

D. Configure a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume to all web servers.

Answer: C

https://www.examtopics.com/discussions/amazon/view/99671-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

Amazon Elastic File System(Amazon EFS) 파일 시스템을 생성합니다. 모든 웹 서버에 EFS 파일 시스템을 마운트합니다. 애플리케이션을 변경하지 않고 Linux 기반 웹 서버용 공유 파일 스토어를 제공해야 한다는 요구 사항을 충족하려면 Amazon EFS 파일 시스템을 사용하는 것이 가장 좋은 솔루션입니다.

Amazon EFS 는 여러 Linux 기반 인스턴스에서 파일에 대한 공유 액세스를 제공하는 관리형 NFS 파일 시스템 서비스이므로 이 사용 사례에 적합합니다. Amazon S3 는 파일 시스템이 아닌 객체 스토리지 서비스이고 S3 버킷을 파일 시스템으로 탑재하려면 추가 도구 또는 라이브러리가 필요하기 때문에 이 시나리오에 적합하지 않습니다. Amazon CloudFront 는 콘텐츠 전송 성능을 개선하는 데 사용할 수 있지만 이 요구 사항에는 필요하지 않습니다. 또한 Amazon EBS 볼륨은 한 번에 하나의 인스턴스에만 탑재할 수 있으므로 여러 인스턴스에서 파일을 공유하는 데 적합하지 않습니다.

Q289

A company has an AWS Lambda function that needs read access to an Amazon S3 bucket that is located in the same AWS account.

Which solution will meet these requirements in the MOST secure manner?

A. Apply an S3 bucket policy that grants read access to the S3 bucket.

B. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to the S3 bucket.

C. Embed an access key and a secret key in the Lambda function's code to grant the required IAM permissions for read access to the S3 bucket.

D. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to all S3 buckets in the account.
Answer: B
https://www.examtopics.com/discussions/amazon/view/99756-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 옵션은 최소 권한 원칙을 따르고 코드의 자격 증명을 노출하지 않고 Lambda 함수에 필요한 권한만 부여하기 때문에 가장 안전합니다. IAM 역할은 Lambda 함수의 실행 역할로 구성할 수 있으며 IAM 정책은 S3 버킷 ARN 및 s3:GetObject 작업을 지정할 수 있습니다.
옵션 A 는 Lambda 함수보다 더 많은 S3 버킷에 대한 액세스 권한이 있는 보안 주체에게 읽기 액세스 권한을 부여하기 때문에 덜 안전합니다.
옵션 C 는 손상되거나 노출될 수 있는 자격 증명을 코드에 내장하기 때문에 덜 안전합니다.
옵션 D 는 계정의 모든 S3 버킷에 대한 읽기 액세스 권한을 부여하기 때문에 덜 안전합니다. 이는 Lambda 함수에 필요한 것보다 많을 수 있습니다.

Q290
A company hosts a web application on multiple Amazon EC2 instances. The EC2 instances are in an Auto Scaling group that scales in response to user demand. The company wants to optimize cost savings without making a long-term commitment.
Which EC2 instance purchasing option should a solutions architect recommend to meet these requirements?
A. Dedicated Instances only
B. On-Demand Instances only
C. A mix of On-Demand Instances and Spot Instances
D. A mix of On-Demand Instances and Reserved Instances
Answer: C
https://www.examtopics.com/discussions/amazon/view/100006-exam-aws-certified-solutions-architect-associate-saa-c03/

참고
https://docs.aws.amazon.com/ko_kr/autoscaling/ec2/userguide/ec2-auto-scaling-mixed-instances-groups.html

Q291

A media company uses Amazon CloudFront for its publicly available streaming video content. The company wants to secure the video content that is hosted in Amazon S3 by controlling who has access. Some of the company's users are using a custom HTTP client that does not support cookies. Some of the company's users are unable to change the hardcoded URLs that they are using for access.

Which services or methods will meet these requirements with the LEAST impact to the users? (Choose two)

A. Signed cookies

B. Signed URLs

C. AWS AppSync

D. JSON Web Token (JWT)

E. AWS Secrets Manager

Answer: A, B

https://www.examtopics.com/discussions/amazon/view/99831-exam-aws-certified-solutions-architect-associate-saa-c03/

Q292

A company is preparing a new data platform that will ingest real-time streaming data from multiple sources. The company needs to transform the data before writing the data to Amazon S3. The company needs the ability to use SQL to query the transformed data.

Which solutions will meet these requirements? (Choose two.)

A. Use Amazon Kinesis Data Streams to stream the data. Use Amazon Kinesis Data Analytics to transform the data. Use Amazon Kinesis Data Firehose to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.

B. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to stream the data. Use AWS Glue to transform the data and to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.

C. Use AWS Database Migration Service (AWS DMS) to ingest the data. Use Amazon EMR to transform the data and to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.

D. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to stream the data. Use Amazon Kinesis Data Analytics to transform the data and to write the data to Amazon S3. Use the Amazon RDS query editor to query the transformed data from Amazon S3.

E. Use Amazon Kinesis Data Streams to stream the data. Use AWS Glue to transform the

data. Use Amazon Kinesis Data Firehose to write the data to Amazon S3. Use the Amazon RDS query editor to query the transformed data from Amazon S3.
Answer: A, B
https://www.examtopics.com/discussions/amazon/view/99834-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
여러 소스에서 실시간 스트리밍 데이터를 수집, 변환 및 쿼리하려면 Amazon Kinesis 와 Amazon MSK 가 적합한 솔루션입니다. Amazon Kinesis Data Streams 는 다양한 소스의 데이터를 스트리밍하고 다른 AWS 서비스와 통합할 수 있습니다. Amazon Kinesis Data Analytics 는 SQL 또는 Apache Flink 를 사용하여 데이터를 변환할 수 있습니다. Amazon Kinesis Data Firehose 는 Amazon S3 또는 다른 대상에 데이터를 쓸 수 있습니다. Amazon Athena 는 표준 SQL 을 사용하여 Amazon S3 에서 변환된 데이터를 쿼리할 수 있습니다.
Amazon MSK 는 데이터 스트리밍을 위한 인기 있는 오픈 소스 플랫폼인 Apache Kafka 를 사용하여 데이터를 스트리밍할 수 있습니다. AWS Glue 는 Apache Spark 또는 Python 스크립트를 사용하여 데이터를 변환하고 Amazon S3 또는 기타 대상에 데이터를 쓸 수 있습니다. Amazon Athena 는 표준 SQL 을 사용하여 Amazon S3 에서 변환된 데이터를 쿼리할 수도 있습니다.

Q293
A company has an on-premises volume backup solution that has reached its end of life. The company wants to use AWS as part of a new backup solution and wants to maintain local access to all the data while it is backed up on AWS. The company wants to ensure that the data backed up on AWS is automatically and securely transferred.
Which solution meets these requirements?
A. Use AWS Snowball to migrate data out of the on-premises solution to Amazon S3. Configure on-premises systems to mount the Snowball S3 endpoint to provide local access to the data.
B. Use AWS Snowball Edge to migrate data out of the on-premises solution to Amazon S3. Use the Snowball Edge file interface to provide on-premises systems with local access to the data.
C. Use AWS Storage Gateway and configure a cached volume gateway. Run the Storage Gateway software appliance on premises and configure a percentage of data to cache locally. Mount the gateway storage volumes to provide local access to the data.
D. Use AWS Storage Gateway and configure a stored volume gateway. Run the Storage

Gateway software appliance on premises and map the gateway storage volumes to on-premises storage. Mount the gateway storage volumes to provide local access to the data.
Answer: D
https://www.examtopics.com/discussions/amazon/view/99692-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 옵션은 온프레미스 소프트웨어 어플라이언스와 클라우드 기반 스토리지를 연결하여 온프레미스 IT 환경과 AWS 스토리지 인프라 간의 데이터 보안 기능과의 원활한 통합을 제공하는 서비스인 AWS Storage Gateway 를 사용하기 때문에 가장 효율적입니다. . 또한 기본 데이터를 로컬에 저장하고 데이터의 특정 시점 스냅샷을 Amazon S3 에 비동기식으로 백업하는 볼륨 게이트웨이 유형인 저장된 볼륨 게이트웨이를 사용합니다. 또한 온프레미스에서 Storage Gateway 소프트웨어 애플리케이션을 실행하고 게이트웨이 스토리지 볼륨을 온프레미스 스토리지에 매핑하므로 기존 스토리지 하드웨어 및 네트워크 인프라를 사용할 수 있습니다. 또한 게이트웨이 스토리지 볼륨을 탑재하여 데이터에 대한 로컬 액세스를 제공하므로 온프레미스에서 지연 시간이 짧은 액세스를 위해 데이터를 사용할 수 있으며 동시에 AWS 에 백업할 수 있습니다. 이 솔루션은 AWS 에 백업되는 동안 모든 데이터에 대한 로컬 액세스를 유지하고 AWS 에 백업된 데이터가 자동으로 안전하게 전송되도록 하는 요구 사항을 충족합니다.
옵션 A 는 대량의 데이터를 AWS 안팎으로 전송할 수 있는 물리적 장치인 AWS Snowball 을 사용하기 때문에 효율성이 떨어집니다. 그러나 이것은 장치의 수동 취급 및 배송을 필요로 하기 때문에 주기적인 백업 솔루션을 제공하지 않습니다. 또한 데이터에 대한 로컬 액세스를 제공하기 위해 Snowball S3 엔드포인트를 탑재하도록 온프레미스 시스템을 구성하므로 추가적인 복잡성과 지연 시간이 발생할 수 있습니다.
옵션 B 는 일부 AWS 기능을 위한 온보드 스토리지 및 컴퓨팅 기능이 있는 물리적 디바이스인 AWS Snowball Edge 를 사용하기 때문에 효율성이 떨어집니다. 그러나 이것은 장치의 수동 취급 및 배송을 필요로 하기 때문에 주기적인 백업 솔루션을 제공하지 않습니다. 또한 Snowball Edge 파일 인터페이스를 사용하여 온프레미스 시스템에 데이터에 대한 로컬 액세스를 제공하므로 추가적인 복잡성과 지연 시간이 발생할 수 있습니다.
옵션 C 는 AWS Storage Gateway 를 사용하고 기본 데이터를 Amazon S3 에 저장하고 자주 액세스하는 데이터 하위 집합의 복사본을 로컬에 보관하는 일종의 볼륨 게이트웨이인 캐시된 볼륨 게이트웨이를 구성하기 때문에 효율성이 떨어집니다. 그러나 일부 데이터 하위 집합만 로컬로 캐시되기 때문에 모든 데이터에 대한 로컬 액세스를 제공하지는 않습니다. 또한 로컬로 캐시할 데이터의 비율을 구성하므로 저장된 볼륨 게이트웨이를 사용하는 것보다 더 높은 비용과 복잡성이 발생할 수 있습니다.

Q294

An application that is hosted on Amazon EC2 instances needs to access an Amazon S3 bucket. Traffic must not traverse the internet.

How should a solutions architect configure access to meet these requirements?

A. Create a private hosted zone by using Amazon Route 53.

B. Set up a gateway VPC endpoint for Amazon S3 in the VPC.

C. Configure the EC2 instances to use a NAT gateway to access the S3 bucket.

D. Establish an AWS Site-to-Site VPN connection between the VPC and the S3 bucket.

Answer: B

https://www.examtopics.com/discussions/amazon/view/99954-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

이 옵션은 인터넷 게이트웨이나 VPC 용 NAT 장치 없이 Amazon S3 에 대한 안정적인 연결을 제공하는 Amazon S3 용 게이트웨이 VPC 엔드포인트를 사용하기 때문에 가장 효율적입니다. 게이트웨이 VPC 엔드포인트는 서비스의 접두사 목록을 사용하여 VPC 에서 Amazon S3 로 트래픽을 라우팅하고 AWS 네트워크를 벗어나지 않습니다. 이것은 인터넷을 통과하지 않는다는 요구 사항을 충족합니다.

옵션 A 는 VPC 내의 리소스에 대한 사용자 지정 도메인 이름을 생성할 수 있는 DNS 서비스인 Amazon Route 53 을 사용하여 프라이빗 호스팅 영역을 사용하기 때문에 효율성이 떨어집니다. 그러나 이것은 인터넷 게이트웨이나 NAT 장치 없이는 Amazon S3 에 대한 연결을 제공하지 않습니다.

옵션 C 는 NAT 게이트웨이를 사용하여 S3 버킷에 액세스하기 때문에 효율성이 떨어집니다. S3 버킷은 개인 서브넷의 인스턴스가 인터넷 또는 다른 AWS 서비스에 연결할 수 있도록 지원하지만 인터넷이 이러한 인스턴스와의 연결을 시작하지 못하도록 하는 고가용성 관리형 NAT(Network Address Translation) 서비스입니다. 그러나 이것은 인터넷을 통과하지 않는 요구 사항을 충족하지 못합니다.그러나 이것은 인터넷을 통과하지 않는다는 요구 사항을 충족하지 않습니다.

옵션 D는 온프레미스 네트워크와 VPC 간의 안전하고 암호화된 네트워크 연결인 S3 버킷과 VPC 간에 AWS Site-to-Site VPN 연결을 사용하기 때문에 효율성이 떨어집니다. 그러나 이것은 인터넷을 통과하지 않는다는 요구 사항을 충족하지 않습니다.

Q295

An ecommerce company stores terabytes of customer data in the AWS Cloud. The data contains personally identifiable information (PII). The company wants to use the data in three applications. Only one of the applications needs to process the PII. The PII must be removed before the other two applications process the data.

Which solution will meet these requirements with the LEAST operational overhead?

A. Store the data in an Amazon DynamoDB table. Create a proxy application layer to intercept and process the data that each application requests.

B. Store the data in an Amazon S3 bucket. Process and transform the data by using S3 Object Lambda before returning the data to the requesting application.

C. Process the data and store the transformed data in three separate Amazon S3 buckets so that each application has its own custom dataset. Point each application to its respective S3 bucket.

D. Process the data and store the transformed data in three separate Amazon DynamoDB tables so that each application has its own custom dataset. Point each application to its respective DynamoDB table.

Answer: B

https://www.examtopics.com/discussions/amazon/view/99956-exam-aws-certified-solutions-architect-associate-saa-c03/

Q296

A development team has launched a new application that is hosted on Amazon EC2 instances inside a development VPC. A solutions architect needs to create a new VPC in the same account. The new VPC will be peered with the development VPC. The VPC CIDR block for the development VPC is 192.168.0.0/24. The solutions architect needs to create a CIDR block for the new VPC. The CIDR block must be valid for a VPC peering connection to the development VPC.

What is the SMALLEST CIDR block that meets these requirements?

A. 10.0.1.0/32

B. 192.168.0.0/24

C. 192.168.1.0/32

D. 10.0.1.0/24

Answer: D

https://www.examtopics.com/discussions/amazon/view/99651-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
허용되는 블록 크기는 /28 넷마스크와 /16 넷마스크 사이입니다. CIDR 블록은 VPC 와 연결된 기존 CIDR 블록과 겹치지 않아야 합니다.
https://docs.aws.amazon.com/vpc/latest/userguide/configure-your-vpc.html

Q297
A company deploys an application on five Amazon EC2 instances. An Application Load Balancer (ALB) distributes traffic to the instances by using a target group. The average CPU usage on each of the instances is below 10% most of the time, with occasional surges to 65%.
A solutions architect needs to implement a solution to automate the scalability of the application. The solution must optimize the cost of the architecture and must ensure that the application has enough CPU resources when surges occur.
Which solution will meet these requirements?
A. Create an Amazon CloudWatch alarm that enters the ALARM state when the CPUUtilization metric is less than 20%. Create an AWS Lambda function that the CloudWatch alarm invokes to terminate one of the EC2 instances in the ALB target group.
B. Create an EC2 Auto Scaling group. Select the existing ALB as the load balancer and the existing target group as the target group. Set a target tracking scaling policy that is based on the ASGAverageCPUUtilization metric. Set the minimum instances to 2, the desired capacity to 3, the maximum instances to 6, and the target value to 50%. Add the EC2 instances to the Auto Scaling group.
C. Create an EC2 Auto Scaling group. Select the existing ALB as the load balancer and the existing target group as the target group. Set the minimum instances to 2, the desired capacity to 3, and the maximum instances to 6. Add the EC2 instances to the Auto Scaling group.
D. Create two Amazon CloudWatch alarms. Configure the first CloudWatch alarm to enter the ALARM state when the average CPUUtilization metric is below 20%. Configure the second CloudWatch alarm to enter the ALARM state when the average CPUUtilization matric is above 50%. Configure the alarms to publish to an Amazon Simple Notification Service (Amazon SNS) topic to send an email message. After receiving the message, log in to decrease or increase the number of EC2 instances that are running.
Answer: B
https://www.examtopics.com/discussions/amazon/view/99652-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
* Auto Scaling 그룹은 수요 변화에 맞춰 EC2 인스턴스를 자동으로 확장합니다. 이는 필요한 만큼의 인스턴스만 실행하여 비용을 최적화합니다.
* 대상 추적 조정 정책은 ASGAverageCPUUtilization 지표를 모니터링하고 평균 CPU 를 약 50% 대상 값으로 유지하도록 조정합니다. 이렇게 하면 CPU 가 급증하는 동안 리소스가 충분해집니다.
* ALB 와 대상 그룹은 재사용되므로 애플리케이션 아키텍처가 변경되지 않습니다. Auto Scaling 그룹은 기존 로드 밸런서 설정에 연결됩니다.
* 최소 2 개에서 최대 6 개의 인스턴스는 수요에 따라 필요에 따라 3 개에서 6 개 사이의 인스턴스를 확장할 수 있는 기능을 제공합니다.
* 단 3 개의 인스턴스(원하는 용량)로 시작하고 필요에 따라 확장하여 비용을 최적화합니다. CPU 사용량이 떨어지면 원하는 용량에 맞게 인스턴스가 종료됩니다.

Q298
A company is running a critical business application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances run in an Auto Scaling group and access an Amazon RDS DB instance.
The design did not pass an operational review because the EC2 instances and the DB instance are all located in a single Availability Zone. A solutions architect must update the design to use a second Availability Zone.
Which solution will make the application highly available?
A. Provision a subnet in each Availability Zone. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance with connections to each network.
B. Provision two subnets that extend across both Availability Zones. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance with connections to each network.
C. Provision a subnet in each Availability Zone. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance for Multi-AZ deployment.
D. Provision a subnet that extends across both Availability Zones. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance for Multi-AZ deployment.
Answer: C

https://www.examtopics.com/discussions/amazon/view/99653-exam-aws-certified-solutions-architect-associate-saa-c03/

참고:
https://aws.amazon.com/ko/vpc/faqs/#:~:text=Can%20a%20subnet%20span%20Availability

Q299
A research laboratory needs to process approximately 8 TB of data. The laboratory requires sub-millisecond latencies and a minimum throughput of 6 GBps for the storage subsystem. Hundreds of Amazon EC2 instances that run Amazon Linux will distribute and process the data.
Which solution will meet the performance requirements?
A. Create an Amazon FSx for NetApp ONTAP file system. Sat each volume' tiering policy to ALL. Import the raw data into the file system. Mount the fila system on the EC2 instances.
B. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent SSD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances.
C. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent HDD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances.
D. Create an Amazon FSx for NetApp ONTAP file system. Set each volume's tiering policy to NONE. Import the raw data into the file system. Mount the file system on the EC2 instances.
Answer: B
https://www.examtopics.com/discussions/amazon/view/99676-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
원시 데이터를 저장할 Amazon S3 버킷 생성 영구 SSD 스토리지를 사용하는 Amazon FSx for Lustre 파일 시스템 생성 Amazon S3 에서 데이터를 가져오고 내보내는 옵션 선택 EC2 인스턴스에 파일 시스템을 탑재합니다. Amazon FSx for Lustre 는 밀리초 미만의 지연 시간과 최대 6GBps 의 처리량을 위해 SSD 스토리지를 사용하고 Amazon S3 에서 데이터를 가져오고 내보낼 수 있습니다. 또한 영구 SSD 스토리지를 선택하는 옵션은 데이터가 디스크에 저장되고 파일 시스템이 중지되어도 손실되지 않도록 합니다.

Q300

A company needs to migrate a legacy application from an on-premises data center to the AWS Cloud because of hardware capacity constraints. The application runs 24 hours a day, 7 days a week. The application's database storage continues to grow over time.

What should a solutions architect do to meet these requirements MOST cost-effectively?

A. Migrate the application layer to Amazon EC2 Spot Instances. Migrate the data storage layer to Amazon S3.

B. Migrate the application layer to Amazon EC2 Reserved Instances. Migrate the data storage layer to Amazon RDS On-Demand Instances.

C. Migrate the application layer to Amazon EC2 Reserved Instances. Migrate the data storage layer to Amazon Aurora Reserved Instances.

D. Migrate the application layer to Amazon EC2 On-Demand Instances. Migrate the data storage layer to Amazon RDS Reserved Instances.

Answer: C

https://www.examtopics.com/discussions/amazon/view/99948-exam-aws-certified-solutions-architect-associate-saa-c03/

참고:

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.AuroraMySQL.html

Q301

A university research laboratory needs to migrate 30 TB of data from an on-premises Windows file server to Amazon FSx for Windows File Server. The laboratory has a 1 Gbps network link that many other departments in the university share.

The laboratory wants to implement a data migration service that will maximize the performance of the data transfer. However, the laboratory needs to be able to control the amount of bandwidth that the service uses to minimize the impact on other departments. The data migration must take place within the next 5 days.

Which AWS solution will meet these requirements?

A. AWS Snowcone

B. Amazon FSx File Gateway

C. AWS DataSync

D. AWS Transfer Family

Answer: C
https://www.examtopics.com/discussions/amazon/view/99659-exam-aws-certified-solutions-architect-associate-saa-c03/

Q302
A company wants to create a mobile app that allows users to stream slow-motion video clips on their mobile devices. Currently, the app captures video clips and uploads the video clips in raw format into an Amazon S3 bucket. The app retrieves these video clips directly from the S3 bucket. However, the videos are large in their raw format.
Users are experiencing issues with buffering and playback on mobile devices. The company wants to implement solutions to maximize the performance and scalability of the app while minimizing operational overhead.
Which combination of solutions will meet these requirements? (Choose two)
A. Deploy Amazon CloudFront for content delivery and caching.
B. Use AWS DataSync to replicate the video files across AW'S Regions in other S3 buckets.
C. Use Amazon Elastic Transcoder to convert the video files to more appropriate formats.
D. Deploy an Auto Sealing group of Amazon EC2 instances in Local Zones for content delivery and caching.
E. Deploy an Auto Scaling group of Amazon EC2 instances to convert the video files to more appropriate formats.
Answer: A, C
https://www.examtopics.com/discussions/amazon/view/99693-exam-aws-certified-solutions-architect-associate-saa-c03/

Q303
A company is launching a new application deployed on an Amazon Elastic Container Service (Amazon ECS) cluster and is using the Fargate launch type for ECS tasks. The company is monitoring CPU and memory usage because it is expecting high traffic to the application upon its launch. However, the company wants to reduce costs when utilization decreases. What should a solutions architect recommend?
A. Use Amazon EC2 Auto Scaling to scale at certain periods based on previous traffic patterns.
B. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm.

C. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.
D. Use AWS Application Auto Scaling with target tracking policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.
Answer: D
https://www.examtopics.com/discussions/amazon/view/99813-exam-aws-certified-solutions-architect-associate-saa-c03/

참고
https://docs.aws.amazon.com/ko_kr/autoscaling/application/userguide/what-is-application-auto-scaling.html

Q304
A company recently created a disaster recovery site in a different AWS Region. The company needs to transfer large amounts of data back and forth between NFS file systems in the two Regions on a periodic basis.
Which solution will meet these requirements with the LEAST operational overhead?
A. Use AWS DataSync.
B. Use AWS Snowball devices.
C. Set up an SFTP server on Amazon EC2.
D. Use AWS Database Migration Service (AWS DMS).
Answer: A
https://www.examtopics.com/discussions/amazon/view/99949-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 옵션은 온프레미스와 AWS 스토리지 서비스 간에 데이터 이동을 자동화하고 가속화하는 안전한 온라인 서비스인 AWS DataSync 를 사용하기 때문에 가장 효율적입니다. 또한 DataSync 를 사용하여 정기적으로 두 리전의 NFS 파일 시스템 간에 대량의 데이터를 주고받으며 최소한의 운영 오버헤드로 데이터 전송 프로세스를 단순화하고 가속화합니다. 이 솔루션은 최소한의 운영 오버헤드로 정기적으로 두 리전의 NFS 파일 시스템 간에 대량의 데이터를 주고받는 요구 사항을 충족합니다.

옵션 B 는 대량의 데이터를 AWS 안팎으로 전송할 수 있는 물리적 디바이스인 AWS Snowball 디바이스를 사용하기 때문에 효율성이 떨어집니다. 그러나 이것은 장치의 수동

취급 및 배송을 필요로 하기 때문에 주기적인 데이터 전송 솔루션을 제공하지 않습니다.

옵션 C 는 Amazon S33 에 저장된 파일에 대한 보안 파일 전송 프로토콜(SFTP) 액세스를 제공하는 방법인 Amazon EC2 에 SFTP 서버를 설정하기 때문에 효율성이 떨어집니다. 그러나 파일 전송을 수동으로 시작하고 모니터링해야 하므로 주기적인 데이터 전송 솔루션을 제공하지 않습니다.

옵션 D 는 데이터베이스를 AWS 로 빠르고 안전하게 마이그레이션하는 데 도움이 되는 서비스인 AWS DMS(AWS Database Migration Service)를 사용하기 때문에 효율성이 떨어집니다. 그러나 이것은 관계형 데이터베이스 및 비관계형 데이터 저장소만 지원하므로 NFS 파일 시스템용 데이터 전송 솔루션을 제공하지 않습니다.

Q305

A company is designing a shared storage solution for a gaming application that is hosted in the AWS Cloud. The company needs the ability to use SMB clients to access data. The solution must be fully managed.

Which AWS solution meets these requirements?

A. Create an AWS DataSync task that shares the data as a mountable file system. Mount the file system to the application server.

B. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.

C. Create an Amazon FSx for Windows File Server file system. Attach the file system to the origin server. Connect the application server to the file system.

D. Create an Amazon S3 bucket. Assign an IAM role to the application to grant access to the S3 bucket. Mount the S3 bucket to the application server.

Answer: C

https://www.examtopics.com/discussions/amazon/view/99809-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

Amazon FSx for Windows File Server(Amazon FSx)는 서버 메시지 블록(SMB) 프로토콜을 사용하는 Windows Server 에 구축된 완전 관리형, 고가용성 및 확장 가능한 파일 스토리지 솔루션입니다. 다른 중요한 엔터프라이즈 기능 중에서 Microsoft Active Directory 통합, 데이터 중복 제거 및 완전히 관리되는 백업을 허용합니다.

https://aws.amazon.com/blogs/storage/accessing-smb-fileshares-remotely-with-amazo

n-fsx-for-windows-file-server/

Q306

A company wants to run an in-memory database for a latency-sensitive application that runs on Amazon EC2 instances. The application processes more than 100,000 transactions each minute and requires high network throughput. A solutions architect needs to provide a cost-effective network design that minimizes data transfer charges.

Which solution meets these requirements?

A. Launch all EC2 instances in the same Availability Zone within the same AWS Region. Specify a placement group with cluster strategy when launching EC2 instances.

B. Launch all EC2 instances in different Availability Zones within the same AWS Region. Specify a placement group with partition strategy when launching EC2 instances.

C. Deploy an Auto Scaling group to launch EC2 instances in different Availability Zones based on a network utilization target.

D. Deploy an Auto Scaling group with a step scaling policy to launch EC2 instances in different Availability Zones.

Answer: A

https://www.examtopics.com/discussions/amazon/view/99807-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

* 단일 AZ 내에서 인스턴스를 시작하고 클러스터 배치 그룹을 사용하면 네트워크 대기 시간이 가장 짧고 인스턴스 간 대역폭이 가장 높습니다. 이는 메모리 데이터베이스 및 처리량이 많은 애플리케이션의 성능을 최대화합니다.

* 동일한 AZ 에 있는 인스턴스와 배치 그룹 간의 통신은 무료이므로 데이터 전송 요금이 최소화됩니다. AZ 간 및 퍼블릭 IP 트래픽에는 요금이 발생할 수 있습니다.

* 클러스터 배치 그룹을 사용하면 인스턴스를 AZ 내에서 서로 가깝게 배치할 수 있으므로 필요한 높은 네트워크 처리량이 가능합니다. 파티션 그룹은 AZ 에 걸쳐 있으므로 대역폭이 줄어듭니다.

* 영역 간 Auto Scaling 은 AZ 에서 인스턴스를 시작하여 데이터 전송 요금을 증가시킬 수 있습니다. 네트워크 처리량이 줄어들어 성능에 영향을 미칠 수 있습니다.

Q307

A company that primarily runs its application servers on premises has decided to migrate to

AWS. The company wants to minimize its need to scale its Internet Small Computer Systems Interface (iSCSI) storage on premises. The company wants only its recently accessed data to remain stored locally.

Which AWS solution should the company use to meet these requirements?

A. Amazon S3 File Gateway

B. AWS Storage Gateway Tape Gateway

C. AWS Storage Gateway Volume Gateway stored volumes

D. AWS Storage Gateway Volume Gateway cached volumes

Answer: D

https://www.examtopics.com/discussions/amazon/view/99611-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

AWS Storage Gateway Volume Gateway 는 iSCSI 스토리지에 연결하기 위한 두 가지 구성, 즉 저장 볼륨과 캐시 볼륨을 제공합니다. 저장된 볼륨 구성은 전체 데이터 세트를 온프레미스에 저장하고 데이터를 AWS 에 비동기식으로 백업합니다. 캐싱된 볼륨 구성은 최근에 액세스한 데이터를 온프레미스에 저장하고 나머지 데이터는 Amazon S3 에 저장합니다. 회사는 최근에 액세스한 데이터만 로컬에 저장하기를 원하므로 캐시된 볼륨 구성이 가장 적절할 것입니다. 이를 통해 회사는 자주 액세스하는 데이터를 온프레미스에 보관하고 iSCSI 스토리지 확장의 필요성을 줄이면서 AWS 클라우드를 통해 모든 데이터에 대한 액세스를 계속 제공할 수 있습니다. 또한 이 구성은 자주 액세스하는 데이터에 대한 짧은 대기 시간 액세스와 자주 액세스하지 않는 데이터에 대한 비용 효율적인 오프사이트 백업을 제공합니다.

https://docs.amazonaws.cn/en_us/storagegateway/latest/vgw/StorageGatewayConcepts.html#stora

Q308

A company has multiple AWS accounts that use consolidated billing. The company runs several active high performance Amazon RDS for Oracle On-Demand DB instances for 90 days. The company's finance team has access to AWS Trusted Advisor in the consolidated billing account and all other AWS accounts.

The finance team needs to use the appropriate AWS account to access the Trusted Advisor check recommendations for RDS. The finance team must review the appropriate Trusted Advisor check to reduce RDS costs.

Which combination of steps should the finance team take to meet these requirements?

(Choose two)
A. Use the Trusted Advisor recommendations from the account where the RDS instances are running.
B. Use the Trusted Advisor recommendations from the consolidated billing account to see all RDS instance checks at the same time.
C. Review the Trusted Advisor check for Amazon RDS Reserved Instance Optimization.
D. Review the Trusted Advisor check for Amazon RDS Idle DB Instances.
E. Review the Trusted Advisor check for Amazon Redshift Reserved Node Optimization.
Answer: B, D
https://www.examtopics.com/discussions/amazon/view/99936-exam-aws-certified-solutions-architect-associate-saa-c03/

Q309
A solutions architect needs to optimize storage costs. The solutions architect must identify any Amazon S3 buckets that are no longer being accessed or are rarely accessed.
Which solution will accomplish this goal with the LEAST operational overhead?
A. Analyze bucket access patterns by using the S3 Storage Lens dashboard for advanced activity metrics.
B. Analyze bucket access patterns by using the S3 dashboard in the AWS Management Console.
C. Turn on the Amazon CloudWatch BucketSizeBytes metric for buckets. Analyze bucket access patterns by using the metrics data with Amazon Athena.
D. Turn on AWS CloudTrail for S3 object monitoring. Analyze bucket access patterns by using CloudTrail logs that are integrated with Amazon CloudWatch Logs.
Answer: A
https://www.examtopics.com/discussions/amazon/view/99803-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
S3 Storage Lens 는 객체 스토리지 사용량, 활동 추세 및 비용 최적화를 위한 권장 사항에 대한 종합적인 보기를 제공하는 완전관리형 S3 스토리지 분석 솔루션입니다. Storage Lens 를 사용하면 모든 S3 버킷에서 객체 액세스 패턴을 분석하고 자세한 지표와 보고서를 생성할 수 있습니다.

Q310

A company sells datasets to customers who do research in artificial intelligence and machine learning (AI/ML). The datasets are large, formatted files that are stored in an Amazon S3 bucket in the us-east-1 Region. The company hosts a web application that the customers use to purchase access to a given dataset. The web application is deployed on multiple Amazon EC2 instances behind an Application Load Balancer. After a purchase is made, customers receive an S3 signed URL that allows access to the files.

The customers are distributed across North America and Europe. The company wants to reduce the cost that is associated with data transfers and wants to maintain or improve performance.

What should a solutions architect do to meet these requirements?

A. Configure S3 Transfer Acceleration on the existing S3 bucket. Direct customer requests to the S3 Transfer Acceleration endpoint. Continue to use S3 signed URLs for access control.

B. Deploy an Amazon CloudFront distribution with the existing S3 bucket as the origin. Direct customer requests to the CloudFront URL. Switch to CloudFront signed URLs for access control.

C. Set up a second S3 bucket in the eu-central-1 Region with S3 Cross-Region Replication between the buckets. Direct customer requests to the closest Region. Continue to use S3 signed URLs for access control.

D. Modify the web application to enable streaming of the datasets to end users. Configure the web application to read the data from the existing S3 bucket. Implement access control directly in the application.

Answer: B

https://www.examtopics.com/discussions/amazon/view/99697-exam-aws-certified-solutions-architect-associate-saa-c03/

참고:

https://docs.aws.amazon.com/ko_kr/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html

Q311

A company is using AWS to design a web application that will process insurance quotes. Users will request quotes from the application. Quotes must be separated by quote type, must be responded to within 24 hours, and must not get lost. The solution must maximize

operational efficiency and must minimize maintenance.
Which solution meets these requirements?
A. Create multiple Amazon Kinesis data streams based on the quote type. Configure the web application to send messages to the proper data stream. Configure each backend group of application servers to use the Kinesis Client Library (KCL) to pool messages from its own data stream.
B. Create an AWS Lambda function and an Amazon Simple Notification Service (Amazon SNS) topic for each quote type. Subscribe the Lambda function to its associated SNS topic. Configure the application to publish requests for quotes to the appropriate SNS topic.
C. Create a single Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon Simple Queue Service (Amazon SQS) queues to the SNS topic. Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type. Configure each backend application server to use its own SQS queue.
D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon OpenSearch Service cluster. Configure the application to send messages to the proper delivery stream. Configure each backend group of application servers to search for the messages from OpenSearch Service and process them accordingly.
Answer: C
https://www.examtopics.com/discussions/amazon/view/99627-exam-aws-certified-solutions-architect-associate-saa-c03/

참고:
https://aws.amazon.com/getting-started/hands-on/filter-messages-published-to-topics/

Q312
A company has an application that runs on several Amazon EC2 instances. Each EC2 instance has multiple Amazon Elastic Block Store (Amazon EBS) data volumes attached to it. The application's EC2 instance configuration and data need to be backed up nightly. The application also needs to be recoverable in a different AWS Region.
Which solution will meet these requirements in the MOST operationally efficient way?
A. Write an AWS Lambda function that schedules nightly snapshots of the application's EBS volumes and copies the snapshots to a different Region.
B. Create a backup plan by using AWS Backup to perform nightly backups. Copy the

backups to another Region. Add the application's EC2 instances as resources.
C. Create a backup plan by using AWS Backup to perform nightly backups. Copy the backups to another Region. Add the application's EBS volumes as resources.
D. Write an AWS Lambda function that schedules nightly snapshots of the application's EBS volumes and copies the snapshots to a different Availability Zone.
Answer: B
https://www.examtopics.com/discussions/amazon/view/99785-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이러한 요구 사항을 충족하는 운영상 가장 효율적인 솔루션은 AWS Backup 을 사용하여 야간 백업을 수행하고 백업을 다른 리전에 복사하는 백업 계획을 만드는 것입니다. 애플리케이션의 EBS 볼륨을 리소스로 추가하면 애플리케이션의 EC2 인스턴스 구성 및 데이터가 백업되고 백업을 다른 리전에 복사하면 애플리케이션을 다른 AWS 리전에서 복구할 수 있습니다.

Q313
A company is building a mobile app on AWS. The company wants to expand its reach to millions of users. The company needs to build a platform so that authorized users can watch the company's content on their mobile devices.
What should a solutions architect recommend to meet these requirements?
A. Publish content to a public Amazon S3 bucket. Use AWS Key Management Service (AWS KMS) keys to stream content.
B. Set up IPsec VPN between the mobile app and the AWS environment to stream content.
C. Use Amazon CloudFront. Provide signed URLs to stream content.
D. Set up AWS Client VPN between the mobile app and the AWS environment to stream content.
Answer: C
https://www.examtopics.com/discussions/amazon/view/100130-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Amazon CloudFront 는 짧은 지연 시간과 높은 전송 속도로 데이터, 비디오, 애플리케이션 및 API 를 전 세계 고객에게 안전하게 전달하는 콘텐츠 전송 네트워크(CDN)입니다. CloudFront 는 콘텐츠에 대한 인증된 액세스를 제공하는 서명된 URL 을 지원합니다. 이

기능을 통해 회사는 콘텐츠에 액세스할 수 있는 사람과 기간을 제어하여 수백만 명의 사용자에게 안전하고 확장 가능한 솔루션을 제공할 수 있습니다.

Q314

A company has an on-premises MySQL database used by the global sales team with infrequent access patterns. The sales team requires the database to have minimal downtime. A database administrator wants to migrate this database to AWS without selecting a particular instance type in anticipation of more users in the future.

Which service should a solutions architect recommend?

A. Amazon Aurora MySQL

B. Amazon Aurora Serverless for MySQL

C. Amazon Redshift Spectrum

D. Amazon RDS for MySQL

Answer: B

https://www.examtopics.com/discussions/amazon/view/99769-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

Amazon Aurora Serverless for MySQL 은 애플리케이션 수요에 따라 자동으로 확장 또는 축소되는 완전관리형 자동 확장 관계형 데이터베이스 서비스입니다. 이 서비스는 고객이 데이터베이스 인스턴스를 프로비저닝할 필요 없이 고가용성, 내구성 및 보안과 같은 Amazon Aurora 의 모든 기능을 제공합니다. Amazon Aurora Serverless for MySQL 을 사용하면 증가한 트래픽을 수용할 수 있도록 데이터베이스가 자동으로 확장되도록 설계되었기 때문에 영업 팀은 다운타임을 최소화할 수 있습니다. 또한 이 서비스를 통해 고객은 사용한 용량에 대해서만 비용을 지불할 수 있으므로 자주 사용하지 않는 액세스 패턴에 대해 비용 효율적입니다. Amazon RDS for MySQL 도 옵션이 될 수 있지만 고객이 인스턴스 유형을 선택해야 하고 데이터베이스 관리자는 증가하는 트래픽을 수용하기 위해 수동으로 인스턴스 크기를 모니터링하고 조정해야 합니다.

Q315

A company experienced a breach that affected several applications in its on-premises data center. The attacker took advantage of vulnerabilities in the custom applications that were running on the servers. The company is now migrating its applications to run on Amazon EC2 instances. The company wants to implement a solution that actively scans for

vulnerabilities on the EC2 instances and sends a report that details the findings.
Which solution will meet these requirements?
A. Deploy AWS Shield to scan the EC2 instances for vulnerabilities. Create an AWS Lambda function to log any findings to AWS CloudTrail.
B. Deploy Amazon Macie and AWS Lambda functions to scan the EC2 instances for vulnerabilities. Log any findings to AWS CloudTrail.
C. Turn on Amazon GuardDuty. Deploy the GuardDuty agents to the EC2 instances. Configure an AWS Lambda function to automate the generation and distribution of reports that detail the findings.
D. Turn on Amazon Inspector. Deploy the Amazon Inspector agent to the EC2 instances. Configure an AWS Lambda function to automate the generation and distribution of reports that detail the findings.
Answer: D
https://www.examtopics.com/discussions/amazon/view/99808-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Amazon Inspector(Amazon 검사기):
* EC2 인스턴스의 활성 취약성 스캔을 수행합니다. 소프트웨어 취약성, 의도하지 않은 네트워크 접근성 및 기타 보안 문제를 찾습니다.
* 스캔을 수행하려면 EC2 인스턴스에 에이전트를 설치해야 합니다. 에이전트는 각 인스턴스에 배포되어야 합니다.
* 보안 위험 또는 취약점에 대한 발견 사항을 자세히 설명하는 예약 검사 보고서를 제공합니다. 이러한 보고서는 문제를 패치하거나 수정하는 데 사용할 수 있습니다.
* AWS 환경에서 보안 취약점 및 잘못된 구성을 사전에 감지하는 데 가장 적합합니다.

Q316
A company uses an Amazon EC2 instance to run a script to poll for and process messages in an Amazon Simple Queue Service (Amazon SQS) queue. The company wants to reduce operational costs while maintaining its ability to process a growing number of messages that are added to the queue.
What should a solutions architect recommend to meet these requirements?
A. Increase the size of the EC2 instance to process messages faster.
B. Use Amazon EventBridge to turn off the EC2 instance when the instance is underutilized.
C. Migrate the script on the EC2 instance to an AWS Lambda function with the appropriate

runtime.
D. Use AWS Systems Manager Run Command to run the script on demand.
Answer: C
https://www.examtopics.com/discussions/amazon/view/99698-exam-aws-certified-solutions-architect-associate-saa-c03/

Q317
A company uses a legacy application to produce data in CSV format. The legacy application stores the output data in Amazon S3. The company is deploying a new commercial off-the-shelf (COTS) application that can perform complex SQL queries to analyze data that is stored in Amazon Redshift and Amazon S3 only. However, the COTS application cannot process the .csv files that the legacy application produces.
The company cannot update the legacy application to produce data in another format. The company needs to implement a solution so that the COTS application can use the data that the legacy application produces.
Which solution will meet these requirements with the LEAST operational overhead?
A. Create an AWS Glue extract, transform, and load (ETL) job that runs on a schedule. Configure the ETL job to process the .csv files and store the processed data in Amazon Redshift.
B. Develop a Python script that runs on Amazon EC2 instances to convert the .csv files to .sql files. Invoke the Python script on a cron schedule to store the output files in Amazon S3.
C. Create an AWS Lambda function and an Amazon DynamoDB table. Use an S3 event to invoke the Lambda function. Configure the Lambda function to perform an extract, transform, and load (ETL) job to process the .csv files and store the processed data in the DynamoDB table.
D. Use Amazon EventBridge to launch an Amazon EMR cluster on a weekly schedule. Configure the EMR cluster to perform an extract, transform, and load (ETL) job to process the .csv files and store the processed data in an Amazon Redshift table.
Answer: A
https://www.examtopics.com/discussions/amazon/view/99817-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 솔루션은 COTS 애플리케이션이 최소한의 운영 오버헤드로 레거시 애플리케이션이

생성하는 데이터를 사용할 수 있도록 솔루션 구현 요구 사항을 충족합니다. AWS Glue 는 분석을 위해 데이터를 준비하고 로드하는 서버리스 ETL 플랫폼을 제공하는 완전 관리형 서비스입니다.
AWS Glue 는 .csv 파일을 비롯한 다양한 형식의 데이터를 처리하고 복잡한 SQL 쿼리를 지원하는 완전관리형 데이터 웨어하우스 서비스인 Amazon Redshift 에 처리된 데이터를 저장할 수 있습니다. AWS Glue 는 데이터 처리 및 로드 프로세스를 자동화할 수 있는 일정에 따라 ETL 작업을 실행할 수 있습니다.

옵션 B 는 올바르지 않습니다. Amazon EC2 인스턴스에서 실행되는 Python 스크립트를 개발하여 .csv 파일을 sql 파일로 변환하면 운영 오버헤드와 복잡성이 증가하고 COTS 애플리케이션에 일관된 데이터 처리 및 로드를 제공하지 못할 수 있기 때문입니다.

.csv 파일을 처리하고 처리된 데이터를 DynamoDB 테이블에 저장하기 위해 AWS Lambda 함수 및 Amazon DynamoDB 테이블을 생성하는 것은 Amazon Redshift 를 COTS 애플리케이션의 데이터 소스로 사용하기 위한 요구 사항을 충족하지 않기 때문에 옵션 C 는 올바르지 않습니다.

Amazon EventBridge(Amazon CloudWatch Events)를 사용하여 주간 일정에 따라 Amazon EMR 클러스터를 시작하여 .csv 파일을 처리하고 처리된 데이터를 Amazon Redshift 테이블에 저장할 수 있으므로 옵션 D 는 올바르지 않습니다. COTS 애플리케이션에 적시에 데이터 처리 및 로드를 제공하지 않습니다.
참조:
https://aws.amazon.com/glue/
https://aws.amazon.com/redshift/

Q318
A company recently migrated its entire IT environment to the AWS Cloud. The company discovers that users are provisioning oversized Amazon EC2 instances and modifying security group rules without using the appropriate change control process. A solutions architect must devise a strategy to track and audit these inventory and configuration changes.
Which actions should the solutions architect take to meet these requirements? (Choose two)
A. Enable AWS CloudTrail and use it for auditing.
B. Use data lifecycle policies for the Amazon EC2 instances.
C. Enable AWS Trusted Advisor and reference the security dashboard.

D. Enable AWS Config and create rules for auditing and compliance purposes.
E. Restore previous resource configurations with an AWS CloudFormation template.
Answer: A, D
https://www.examtopics.com/discussions/amazon/view/99804-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A) AWS CloudTrail 을 활성화하고 감사에 사용합니다. AWS CloudTrail 은 API 호출 기록을 제공하며 EC2 인스턴스 및 보안 그룹에 대한 변경 사항을 감사하는 데 사용할 수 있습니다. 솔루션 설계자는 CloudTrail 로그를 분석하여 적절한 승인 없이 누가 대규모 인스턴스를 프로비저닝했거나 보안 그룹을 수정했는지 추적할 수 있습니다.
D) AWS Config 를 활성화하고 감사 및 규정 준수를 위한 규칙을 생성합니다. AWS Config 는 EC2 인스턴스 및 보안 그룹과 같은 리소스에 대한 구성 변경 사항을 기록할 수 있습니다. 솔루션 설계자는 특정 인스턴스 유형을 시작하거나 권한 없이 보안 그룹 포트를 여는 것과 같은 비준수 변경 사항을 모니터링하기 위해 AWS Config 규칙을 생성할 수 있습니다. AWS Config 는 이러한 규칙 위반에 대해 경고합니다.

Q319
A company has hundreds of Amazon EC2 Linux-based instances in the AWS Cloud. Systems administrators have used shared SSH keys to manage the instances. After a recent audit, the company's security team is mandating the removal of all shared keys. A solutions architect must design a solution that provides secure access to the EC2 instances.
Which solution will meet this requirement with the LEAST amount of administrative overhead?
A. Use AWS Systems Manager Session Manager to connect to the EC2 instances.
B. Use AWS Security Token Service (AWS STS) to generate one-time SSH keys on demand.
C. Allow shared SSH access to a set of bastion instances. Configure all other instances to allow only SSH access from the bastion instances.
D. Use an Amazon Cognito custom authorizer to authenticate users. Invoke an AWS Lambda function to generate a temporary SSH key.
Answer: A
https://www.examtopics.com/discussions/amazon/view/99628-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

Session Manager 는 완전히 관리되는 AWS Systems Manager 기능입니다. Session Manager 를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스, 에지 장치, 온프레미스 서버 및 가상 머신(VM)을 관리할 수 있습니다. 대화형 원클릭 브라우저 기반 셸 또는 AWS Command Line Interface(AWS CLI)를 사용할 수 있습니다. Session Manager 는 인바운드 포트를 열거나 배스천 호스트를 유지하거나 SSH 키를 관리할 필요 없이 안전하고 감사 가능한 노드 관리를 제공합니다.
또한 Session Manager 를 사용하면 관리 노드에 대한 제어된 액세스, 엄격한 보안 관행, 노드 액세스 세부 정보가 포함된 완전히 감사 가능한 로그가 필요한 기업 정책을 준수하는 동시에 최종 사용자에게 관리 노드에 대한 간단한 원클릭 교차 플랫폼 액세스를 제공할 수 있습니다.
https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html

Q320
A company is using a fleet of Amazon EC2 instances to ingest data from on-premises data sources. The data is in JSON format and ingestion rates can be as high as 1 MB/s. When an EC2 instance is rebooted, the data in-flight is lost. The company's data science team wants to query ingested data in near-real time.
Which solution provides near-real-time data querying that is scalable with minimal data loss?
A. Publish data to Amazon Kinesis Data Streams, Use Kinesis Data Analytics to query the data.
B. Publish data to Amazon Kinesis Data Firehose with Amazon Redshift as the destination. Use Amazon Redshift to query the data.
C. Store ingested data in an EC2 instance store. Publish data to Amazon Kinesis Data Firehose with Amazon S3 as the destination. Use Amazon Athena to query the data.
D. Store ingested data in an Amazon Elastic Block Store (Amazon EBS) volume. Publish data to Amazon ElastiCache for Redis. Subscribe to the Redis channel to query the data.
Answer: A
https://www.examtopics.com/discussions/amazon/view/99752-exam-aws-certified-solutions-architect-associate-saa-c03/

참고
https://docs.aws.amazon.com/ko_kr/kinesisanalytics/latest/dev/what-is.html

Q321

What should a solutions architect do to ensure that all objects uploaded to an Amazon S3 bucket are encrypted?

A. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set.

B. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set to private.

C. Update the bucket policy to deny if the PutObject does not have an aws:SecureTransport header set to true.

D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-side-encryption header set.

Answer: D

https://www.examtopics.com/discussions/amazon/view/99685-exam-aws-certified-solutions-architect-associate-saa-c03/

Q322

A solutions architect is designing a multi-tier application for a company. The application's users upload images from a mobile device. The application generates a thumbnail of each image and returns a message to the user to confirm that the image was uploaded successfully.

The thumbnail generation can take up to 60 seconds, but the company wants to provide a faster response time to its users to notify them that the original image was received. The solutions architect must design the application to asynchronously dispatch requests to the different application tiers.

What should the solutions architect do to meet these requirements?

A. Write a custom AWS Lambda function to generate the thumbnail and alert the user. Use the image upload process as an event source to invoke the Lambda function.

B. Create an AWS Step Functions workflow. Configure Step Functions to handle the orchestration between the application tiers and alert the user when thumbnail generation is complete.

C. Create an Amazon Simple Queue Service (Amazon SQS) message queue. As images are uploaded, place a message on the SQS queue for thumbnail generation. Alert the user through an application message that the image was received.

D. Create Amazon Simple Notification Service (Amazon SNS) notification topics and subscriptions. Use one subscription with the application to generate the thumbnail after the

image upload is complete. Use a second subscription to message the user's mobile app by way of a push notification after thumbnail generation is complete.
Answer: C
https://www.examtopics.com/discussions/amazon/view/99753-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 옵션은 메시지 손실이나 다른 서비스를 사용할 필요 없이 모든 볼륨의 소프트웨어 구성 요소 간에 메시지를 전송, 저장 및 수신할 수 있는 완전 관리형 메시지 대기열 서비스인 Amazon SQS 를 사용하기 때문에 가장 효율적입니다. 또한 SQS 메시지 대기열을 사용하여 서로 다른 애플리케이션 계층에 요청을 비동기식으로 전달하여 썸네일 생성 프로세스에서 이미지 업로드 프로세스를 분리하고 확장성과 안정성을 활성화합니다. 또한 이미지가 수신되었다는 애플리케이션 메시지를 통해 사용자에게 경고하므로 섬네일 생성이 완료될 때까지 기다리는 것보다 사용자에게 더 빠른 응답 시간을 제공합니다.

옵션 A 는 서버를 프로비저닝하거나 관리하지 않고 코드를 실행하는 방법인 사용자 지정 AWS Lambda 함수를 사용하여 썸네일을 생성하고 사용자에게 경고하기 때문에 효율성이 떨어집니다.
그러나 이것은 썸네일 생성 프로세스에서 이미지 업로드 프로세스를 분리하기 위해 비동기 디스패치 메커니즘을 사용하지 않습니다. 또한 이미지 업로드 프로세스를 이벤트 소스로 사용하여 Lambda 함수를 호출하므로 한 번에 업로드된 이미지가 많은 경우 동시성 문제가 발생할 수 있습니다.

옵션 B 는 애플리케이션의 구성 요소를 일련의 단계로 배열하고 시각화하는 그래픽 콘솔을 제공하는 완전관리형 서비스인 AWS Step Functions 를 사용하기 때문에 효율성이 떨어집니다. 그러나 이것은 썸네일 생성 프로세스에서 이미지 업로드 프로세스를 분리하기 위해 비동기 디스패치 메커니즘을 사용하지 않습니다. 또한 Step Functions 를 사용하여 애플리케이션 계층 간의 오케스트레이션을 처리하고 썸네일 생성이 완료되면 사용자에게 경고하므로 추가적인 복잡성과 대기 시간이 발생할 수 있습니다.

옵션 D 는 SMS 문자 메시지 또는 이메일을 통해 메시지 또는 알림을 사용자에게 직접 보낼 수 있는 완전 관리형 메시징 서비스인 Amazon SNS 를 사용하기 때문에 효율성이 떨어집니다. 그러나 이것은 썸네일 생성 프로세스에서 이미지 업로드 프로세스를 분리하기 위해 비동기 디스패치 메커니즘을 사용하지 않습니다. 또한 SNS 알림 주제 및 구독을 사용하여 이미지 업로드가 완료된 후 썸네일을 생성하고 썸네일 생성이 완료된 후 푸시 알림을 통해 사용자의 모바일 앱에 메시지를 보내므로 추가적인 복잡성과 대기 시간이

발생할 수 있습니다.

Q323

A company's facility has badge readers at every entrance throughout the building. When badges are scanned, the readers send a message over HTTPS to indicate who attempted to access that particular entrance.

A solutions architect must design a system to process these messages from the sensors. The solution must be highly available, and the results must be made available for the company's security team to analyze.

Which system architecture should the solutions architect recommend?

A. Launch an Amazon EC2 instance to serve as the HTTPS endpoint and to process the messages. Configure the EC2 instance to save the results to an Amazon S3 bucket.

B. Create an HTTPS endpoint in Amazon API Gateway. Configure the API Gateway endpoint to invoke an AWS Lambda function to process the messages and save the results to an Amazon DynamoDB table.

C. Use Amazon Route 53 to direct incoming sensor messages to an AWS Lambda function. Configure the Lambda function to process the messages and save the results to an Amazon DynamoDB table.

D. Create a gateway VPC endpoint for Amazon S3. Configure a Site-to-Site VPN connection from the facility network to the VPC so that sensor data can be written directly to an S3 bucket by way of the VPC endpoint.

Answer: B

https://www.examtopics.com/discussions/amazon/view/99699-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

Amazon API Gateway 를 HTTPS 엔드포인트로 배포하고 AWS Lambda 를 배포하여 메시지를 처리하고 Amazon DynamoDB 테이블에 저장합니다. 이 옵션은 대량의 데이터를 쉽게 처리할 수 있는 가용성과 확장성이 뛰어난 솔루션을 제공합니다. 또한 다른 AWS 서비스와 통합되어 보안 팀의 데이터를 보다 쉽게 분석하고 시각화할 수 있습니다.

Q324

A company wants to implement a disaster recovery plan for its primary on-premises file storage volume. The file storage volume is mounted from an Internet Small Computer

Systems Interface (iSCSI) device on a local storage server. The file storage volume holds hundreds of terabytes (TB) of data.
The company wants to ensure that end users retain immediate access to all file types from the on-premises systems without experiencing latency.
Which solution will meet these requirements with the LEAST amount of change to the company's existing infrastructure?
A. Provision an Amazon S3 File Gateway as a virtual machine (VM) that is hosted on premises. Set the local cache to 10 TB. Modify existing applications to access the files through the NFS protocol. To recover from a disaster, provision an Amazon EC2 instance and mount the S3 bucket that contains the files.
B. Provision an AWS Storage Gateway tape gateway. Use a data backup solution to back up all existing data to a virtual tape library. Configure the data backup solution to run nightly after the initial backup is complete. To recover from a disaster, provision an Amazon EC2 instance and restore the data to an Amazon Elastic Block Store (Amazon EBS) volume from the volumes in the virtual tape library.
C. Provision an AWS Storage Gateway Volume Gateway cached volume. Set the local cache to 10 TB. Mount the Volume Gateway cached volume to the existing file server by using iSCSI, and copy all files to the storage volume. Configure scheduled snapshots of the storage volume. To recover from a disaster, restore a snapshot to an Amazon Elastic Block Store (Amazon EBS) volume and attach the EBS volume to an Amazon EC2 instance.
D. Provision an AWS Storage Gateway Volume Gateway stored volume with the same amount of disk space as the existing file storage volume. Mount the Volume Gateway stored volume to the existing file server by using iSCSI, and copy all files to the storage volume. Configure scheduled snapshots of the storage volume. To recover from a disaster, restore a snapshot to an Amazon Elastic Block Store (Amazon EBS) volume and attach the EBS volume to an Amazon EC2 instance.
Answer: D
https://www.examtopics.com/discussions/amazon/view/99711-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
"회사는 최종 사용자가 온프레미스 시스템의 모든 파일 유형에 즉시 액세스할 수 있기를 원합니다."
- 캐싱된 볼륨(Cached volumes): 가장 최근 데이터에 대한 액세스 대기 시간이 짧습니다.
- 저장 볼륨(Stored volumes): 전체 데이터 세트는 온프레미스이며 S3 로 예약 백업되므로 볼륨 게이트웨이 저장 볼륨이 적절한 선택입니다.

Q325

A company is hosting a web application from an Amazon S3 bucket. The application uses Amazon Cognito as an identity provider to authenticate users and return a JSON Web Token (JWT) that provides access to protected resources that are stored in another S3 bucket. Upon deployment of the application, users report errors and are unable to access the protected content. A solutions architect must resolve this issue by providing proper permissions so that users can access the protected content.

Which solution meets these requirements?

A. Update the Amazon Cognito identity pool to assume the proper IAM role for access to the protected content.

B. Update the S3 ACL to allow the application to access the protected content.

C. Redeploy the application to Amazon S3 to prevent eventually consistent reads in the S3 bucket from affecting the ability of users to access the protected content.

D. Update the Amazon Cognito pool to use custom attribute mappings within the identity pool and grant users the proper permissions to access the protected content.

Answer: A

https://www.examtopics.com/discussions/amazon/view/99754-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

Amazon Cognito 자격 증명 풀은 인증된 사용자에게 AWS 리소스에 액세스할 수 있는 권한이 제한된 임시 자격 증명 세트를 할당합니다. 각 사용자의 권한은 생성한 IAM 역할을 통해 제어됩니다.

https://docs.aws.amazon.com/cognito/latest/developerguide/role-basedaccess-control.html

Q326

An image hosting company uploads its large assets to Amazon S3 Standard buckets. The company uses multipart upload in parallel by using S3 APIs and overwrites if the same object is uploaded again. For the first 30 days after upload, the objects will be accessed frequently. The objects will be used less frequently after 30 days, but the access patterns for each object will be inconsistent. The company must optimize its S3 storage costs while maintaining high availability and resiliency of stored assets.

Which combination of actions should a solutions architect recommend to meet these requirements? (Choose two.)

A. Move assets to S3 Intelligent-Tiering after 30 days.

B. Configure an S3 Lifecycle policy to clean up incomplete multipart uploads.

C. Configure an S3 Lifecycle policy to clean up expired object delete markers.

D. Move assets to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.

E. Move assets to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

Answer: A, B

https://www.examtopics.com/discussions/amazon/view/99755-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

S3 Intelligent-Tiering 은 성능 영향, 검색 비용 또는 운영 오버헤드 없이 액세스 빈도에 따라 가장 비용 효율적인 액세스 계층으로 데이터를 자동으로 이동하는 스토리지 클래스입니다. 회사 자산과 같이 액세스 패턴을 알 수 없거나 변경하는 데이터에 이상적입니다. 30 일 후에 자산을 S3 Intelligent-Tiering 으로 이동함으로써 회사는 저장된 자산의 고가용성과 복원력을 유지하면서 스토리지 비용을 최적화할 수 있습니다.

S3 수명 주기는 개체가 수명 주기 동안 비용 효율적으로 저장되도록 개체를 관리할 수 있게 해주는 기능입니다. 수명 주기 규칙을 생성하여 Amazon S3 가 객체 그룹에 적용하는 작업을 정의할 수 있습니다. 작업 중 하나는 업로드가 중단될 때 발생할 수 있는 불완전한 멀티파트 업로드를 중단하는 것입니다. 불완전한 멀티파트 업로드를 정리하도록 S3 수명 주기 정책을 구성함으로써 회사는 스토리지 비용을 줄이고 사용하지 않는 부분에 대한 비용 지불을 피할 수 있습니다.

만료된 객체 삭제 마커는 Amazon S3 에서 자동으로 삭제되고 스토리지 비용이 발생하지 않기 때문에 옵션 C 는 올바르지 않습니다. 따라서 만료된 객체 삭제 마커를 정리하도록 S3 수명 주기 정책을 구성해도 회사의 스토리지 비용에는 영향을 미치지 않습니다.

옵션 D 는 올바르지 않습니다. S3 Standard-IA 는 자주 액세스하지 않지만 필요할 때 신속하게 액세스해야 하는 데이터용 스토리지 클래스이기 때문입니다. S3 Standard 보다 저장 비용은 낮지만 검색 비용은 더 높고 최소 저장 기간 요금은 30 일입니다. 따라서 30 일 후에 자산을 S3 Standard-IA 로 이동해도 자산에 여전히 가끔 액세스하는 경우 회사의 스토리지 비용이 최적화되지 않을 수 있습니다.

옵션 E 는 올바르지 않습니다. S3 One Zone-IA 는 자주 액세스하지 않지만 필요할 때 신속하게 액세스해야 하는 데이터용 스토리지 클래스이기 때문입니다. S3 Standard-IA 보다 스토리지 비용이 저렴하지만 하나의 가용 영역에만 데이터를 저장하고 다른 스토리지 클래스보다 복원력이 떨어집니다. 또한 검색 비용이 더 높고 최소 저장 기간 요금이 30 일입니다. 따라서 30 일 후에 자산을 S3 One Zone-IA 로 이동하면 자산이 여전히 가끔씩

액세스되거나 고가용성이 필요한 경우 회사의 스토리지 비용이 최적화되지 않을 수 있습니다.
참조 URL:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html
https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html
https://docs.aws.amazon.com/AmazonS3/latest/userguide/delete-or-empty-bucket.html#deletebucket-considerations
https://docs.aws.amazon.com/AmazonS3/latest/userguide/mpuoverview.html
https://aws.amazon.com/certification/certified-solutions-architect-associate/

Q327
A solutions architect must secure a VPC network that hosts Amazon EC2 instances. The EC2 instances contain highly sensitive data and run in a private subnet. According to company policy, the EC2 instances that run in the VPC can access only approved third-party software repositories on the internet for software product updates that use the third party's URL. Other internet traffic must be blocked.
Which solution meets these requirements?
A. Update the route table for the private subnet to route the outbound traffic to an AWS Network Firewall firewall. Configure domain list rule groups.
B. Set up an AWS WAF web ACL. Create a custom set of rules that filter traffic requests based on source and destination IP address range sets.
C. Implement strict inbound security group rules. Configure an outbound rule that allows traffic only to the authorized software repositories on the internet by specifying the URLs.
D. Configure an Application Load Balancer (ALB) in front of the EC2 instances. Direct all outbound traffic to the ALB. Use a URL-based rule listener in the ALB's target group for outbound access to the internet.
Answer: A
https://www.examtopics.com/discussions/amazon/view/99795-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
EC2 에서 네트워크 방화벽으로 아웃바운드 연결을 보냅니다. 네트워크 방화벽에서 소프트웨어 패치 다운로드를 위해 특정 도메인을 허용하고 다른 모든 도메인을 거부하는 상태 저장 아웃바운드 규칙을 생성합니다.

Q328

A company is hosting a three-tier ecommerce application in the AWS Cloud. The company hosts the website on Amazon S3 and integrates the website with an API that handles sales requests. The company hosts the API on three Amazon EC2 instances behind an Application Load Balancer (ALB). The API consists of static and dynamic front-end content along with backend workers that process sales requests asynchronously.

The company is expecting a significant and sudden increase in the number of sales requests during events for the launch of new products.

What should a solutions architect recommend to ensure that all the requests are processed successfully?

A. Add an Amazon CloudFront distribution for the dynamic content. Increase the number of EC2 instances to handle the increase in traffic.

B. Add an Amazon CloudFront distribution for the static content. Place the EC2 instances in an Auto Scaling group to launch new instances based on network traffic.

C. Add an Amazon CloudFront distribution for the dynamic content. Add an Amazon ElastiCache instance in front of the ALB to reduce traffic for the API to handle.

D. Add an Amazon CloudFront distribution for the static content. Add an Amazon Simple Queue Service (Amazon SQS) queue to receive requests from the website for later processing by the EC2 instances.

Answer: D

https://www.examtopics.com/discussions/amazon/view/99704-exam-aws-certified-solutions-architect-associate-saa-c03/

Q329

A security audit reveals that Amazon EC2 instances are not being patched regularly. A solutions architect needs to provide a solution that will run regular security scans across a large fleet of EC2 instances. The solution should also patch the EC2 instances on a regular schedule and provide a report of each instance's patch status.

Which solution will meet these requirements?

A. Set up Amazon Macie to scan the EC2 instances for software vulnerabilities. Set up a cron job on each EC2 instance to patch the instance on a regular schedule.

B. Turn on Amazon GuardDuty in the account. Configure GuardDuty to scan the EC2 instances for software vulnerabilities. Set up AWS Systems Manager Session Manager to patch the EC2 instances on a regular schedule.

C. Set up Amazon Detective to scan the EC2 instances for software vulnerabilities. Set up an Amazon EventBridge scheduled rule to patch the EC2 instances on a regular schedule.
D. Turn on Amazon Inspector in the account. Configure Amazon Inspector to scan the EC2 instances for software vulnerabilities. Set up AWS Systems Manager Patch Manager to patch the EC2 instances on a regular schedule.
Answer: D
https://www.examtopics.com/discussions/amazon/view/99796-exam-aws-certified-solutions-architect-associate-saa-c03/

Q330
A company is planning to store data on Amazon RDS DB instances. The company must encrypt the data at rest.
What should a solutions architect do to meet this requirement?
A. Create a key in AWS Key Management Service (AWS KMS). Enable encryption for the DB instances.
B. Create an encryption key. Store the key in AWS Secrets Manager. Use the key to encrypt the DB instances.
C. Generate a certificate in AWS Certificate Manager (ACM). Enable SSL/TLS on the DB instances by using the certificate.
D. Generate a certificate in AWS Identity and Access Management (IAM). Enable SSL/TLS on the DB instances by using the certificate.
Answer: A
https://www.examtopics.com/discussions/amazon/view/99702-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Amazon RDS 의 유휴 데이터를 암호화하려면 AWS Key Management Service(AWS KMS)를 사용하는 Amazon RDS 의 암호화 기능을 사용할 수 있습니다. 이 기능을 통해 Amazon RDS 는 고유한 키로 각 데이터베이스 인스턴스를 암호화합니다. 이 키는 AWS KMS 에 의해 안전하게 저장됩니다. 자체 키를 관리하거나 기본 AWS 관리형 키를 사용할 수 있습니다. DB 인스턴스에 대한 암호화를 활성화하면 Amazon RDS 가 자동 백업, 읽기 전용 복제본 및 스냅샷을 비롯한 기본 스토리지를 암호화합니다.

Q331

A company must migrate 20 TB of data from a data center to the AWS Cloud within 30 days. The company's network bandwidth is limited to 15 Mbps and cannot exceed 70% utilization. What should a solutions architect do to meet these requirements?

A. Use AWS Snowball.

B. Use AWS DataSync.

C. Use a secure VPN connection.

D. Use Amazon S3 Transfer Acceleration.

Answer: A

https://www.examtopics.com/discussions/amazon/view/99603-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

AWS Snowball 은 AWS 클라우드 안팎으로 대량의 데이터 이동을 가속화하는 안전한 데이터 전송 솔루션입니다. 한 번에 최대 80TB 의 데이터를 이동할 수 있고 최대 50Mbps 의 네트워크 대역폭을 제공하므로 작업에 적합합니다. 또한 안전하고 사용하기 쉬우므로 이 마이그레이션에 이상적인 솔루션입니다.

Q332

A company needs to provide its employees with secure access to confidential and sensitive files. The company wants to ensure that the files can be accessed only by authorized users. The files must be downloaded securely to the employees' devices.

The files are stored in an on-premises Windows file server. However, due to an increase in remote usage, the file server is running out of capacity.

Which solution will meet these requirements?

A. Migrate the file server to an Amazon EC2 instance in a public subnet. Configure the security group to limit inbound traffic to the employees' IP addresses.

B. Migrate the files to an Amazon FSx for Windows File Server file system. Integrate the Amazon FSx file system with the on-premises Active Directory. Configure AWS Client VPN.

C. Migrate the files to Amazon S3, and create a private VPC endpoint. Create a signed URL to allow download.

D. Migrate the files to Amazon S3, and create a public VPC endpoint. Allow employees to sign on with AWS IAM Identity Center (AWS Single Sign-On).

Answer: B

https://www.examtopics.com/discussions/amazon/view/99792-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Windows 파일 서버는 온프레미스이며 데이터를 클라우드에 복제할 무언가가 필요합니다. 우리가 가진 유일한 옵션은 Windows 파일 서버용 AWS FSx 입니다. 또한 정보가 기밀이고 민감하기 때문에 적절한 사용자가 안전한 방식으로 정보에 액세스할 수 있도록 해야 합니다.
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html

Q333
A company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight, the application becomes much slower when the month-end financial calculation batch runs. This causes the CPU utilization of the EC2 instances to immediately peak to 100%, which disrupts the application. What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?
A. Configure an Amazon CloudFront distribution in front of the ALB.
B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.
C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.
D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances.
Answer: C
https://www.examtopics.com/discussions/amazon/view/99791-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
월별 일정을 기반으로 EC2 Auto Scaling 예약 조정 정책을 구성하는 것이 가장 좋은 옵션입니다. 이는 월별 배치 실행이 시작되기 전에 EC2 인스턴스의 사전 조정을 허용하기 때문입니다. 이렇게 하면 애플리케이션이 다운타임 없이 증가된 워크로드를 처리할 수 있습니다. 예약된 조정 정책은 배치 실행 몇 시간 전에 Auto Scaling 그룹의 인스턴스 수를 늘리고 배치 실행이 완료된 후 인스턴스 수를 줄이도록 구성할 수 있습니다. 이렇게 하면 필요할 때 리소스를 사용할 수 있고 필요하지 않을 때 리소스를 낭비하지 않을 수 있습니다. 월별 배치 실행 중에 증가된 워크로드를 처리하고 다운타임을 방지하는 가장 적절한 솔루션은 월별 일정을 기반으로 EC2 Auto Scaling 예약 조정 정책을 구성하는 것입니다.
https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html

Q334

A company wants to give a customer the ability to use on-premises Microsoft Active Directory to download files that are stored in Amazon S3. The customer's application uses an SFTP client to download the files.

Which solution will meet these requirements with the LEAST operational overhead and no changes to the customer's application?

A. Set up AWS Transfer Family with SFTP for Amazon S3. Configure integrated Active Directory authentication.

B. Set up AWS Database Migration Service (AWS DMS) to synchronize the on-premises client with Amazon S3. Configure integrated Active Directory authentication.

C. Set up AWS DataSync to synchronize between the on-premises location and the S3 location by using AWS IAM Identity Center (AWS Single Sign-On).

D. Set up a Windows Amazon EC2 instance with SFTP to connect the on-premises client with Amazon S3. Integrate AWS Identity and Access Management (IAM).

Answer: A

https://www.examtopics.com/discussions/amazon/view/99703-exam-aws-certified-solutions-architect-associate-saa-c03/

Q335

A company is experiencing sudden increases in demand. The company needs to provision large Amazon EC2 instances from an Amazon Machine Image (AMI). The instances will run in an Auto Scaling group. The company needs a solution that provides minimum initialization latency to meet the demand.

Which solution meets these requirements?

A. Use the aws ec2 register-image command to create an AMI from a snapshot. Use AWS Step Functions to replace the AMI in the Auto Scaling group.

B. Enable Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot. Provision an AMI by using the snapshot. Replace the AMI in the Auto Scaling group with the new AMI.

C. Enable AMI creation and define lifecycle rules in Amazon Data Lifecycle Manager (Amazon DLM). Create an AWS Lambda function that modifies the AMI in the Auto Scaling group.

D. Use Amazon EventBridge to invoke AWS Backup lifecycle policies that provision AMIs.

Configure Auto Scaling group capacity limits as an event source in EventBridge.
Answer: B
https://www.examtopics.com/discussions/amazon/view/99686-exam-aws-certified-solutions-architect-associate-saa-c03/

설명
스냅샷에서 Amazon Elastic Block Store(Amazon EBS) 빠른 스냅샷 복원을 활성화하면 스냅샷에서 새 Amazon Machine Image(AMI)를 빠르게 생성할 수 있으므로 새 인스턴스를 프로비저닝할 때 초기화 지연 시간을 줄이는 데 도움이 됩니다. AMI 가 프로비저닝되면 Auto Scaling 그룹의 AMI 를 새 AMI 로 교체할 수 있습니다. 이렇게 하면 업데이트된 AMI 에서 새 인스턴스가 시작되고 증가된 수요를 신속하게 충족할 수 있습니다.

Q336
A company hosts a multi-tier web application that uses an Amazon Aurora MySQL DB cluster for storage. The application tier is hosted on Amazon EC2 instances. The company's IT security guidelines mandate that the database credentials be encrypted and rotated every 14 days.
What should a solutions architect do to meet this requirement with the LEAST operational effort?
A. Create a new AWS Key Management Service (AWS KMS) encryption key. Use AWS Secrets Manager to create a new secret that uses the KMS key with the appropriate credentials. Associate the secret with the Aurora DB cluster. Configure a custom rotation period of 14 days.
B. Create two parameters in AWS Systems Manager Parameter Store: one for the user name as a string parameter and one that uses the SecureString type for the password. Select AWS Key Management Service (AWS KMS) encryption for the password parameter, and load these parameters in the application tier. Implement an AWS Lambda function that rotates the password every 14 days.
C. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system in all EC2 instances of the application tier. Restrict the access to the file on the file system so that the application can read the file and that only super users can modify the file. Implement an AWS Lambda function that rotates the key in Aurora every 14 days and writes new credentials into the file.
D. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS)

encrypted Amazon S3 bucket that the application uses to load the credentials. Download the file to the application regularly to ensure that the correct credentials are used. Implement an AWS Lambda function that rotates the Aurora credentials every 14 days and uploads these credentials to the file in the S3 bucket.

Answer: A

https://www.examtopics.com/discussions/amazon/view/99790-exam-aws-certified-solutions-architect-associate-saa-c03/

Q337

A company has deployed a web application on AWS. The company hosts the backend database on Amazon RDS for MySQL with a primary DB instance and five read replicas to support scaling needs. The read replicas must lag no more than 1 second behind the primary DB instance. The database routinely runs scheduled stored procedures.

As traffic on the website increases, the replicas experience additional lag during periods of peak load. A solutions architect must reduce the replication lag as much as possible. The solutions architect must minimize changes to the application code and must minimize ongoing operational overhead.

Which solution will meet these requirements?

A. Migrate the database to Amazon Aurora MySQL. Replace the read replicas with Aurora Replicas, and configure Aurora Auto Scaling. Replace the stored procedures with Aurora MySQL native functions.

B. Deploy an Amazon ElastiCache for Redis cluster in front of the database. Modify the application to check the cache before the application queries the database. Replace the stored procedures with AWS Lambda functions.

C. Migrate the database to a MySQL database that runs on Amazon EC2 instances. Choose large, compute optimized EC2 instances for all replica nodes. Maintain the stored procedures on the EC2 instances.

D. Migrate the database to Amazon DynamoDB. Provision a large number of read capacity units (RCUs) to support the required throughput, and configure on-demand capacity scaling. Replace the stored procedures with DynamoDB streams.

Answer: A

https://www.examtopics.com/discussions/amazon/view/99871-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

옵션 A 는 애플리케이션 코드를 크게 변경하지 않고 복제 지연을 줄이고 진행 중인 운영 오버헤드를 최소화하는 가장 적합한 솔루션입니다. 데이터베이스를 Amazon Aurora MySQL 로 마이그레이션하면 MySQL 용 Amazon RDS 에 비해 복제 성능과 확장성이 향상됩니다. Aurora 복제본은 더 빠른 복제를 제공하여 복제 지연을 줄이고 Aurora Auto Scaling 은 들어오는 트래픽을 처리하기에 충분한 Aurora 복제본이 있는지 확인합니다. 또한 Aurora MySQL 기본 기능은 저장 프로시저를 대체하여 데이터베이스의 부하를 줄이고 성능을 향상시킬 수 있습니다.

Q338

A solutions architect must create a disaster recovery (DR) plan for a high-volume software as a service (SaaS) platform. All data for the platform is stored in an Amazon Aurora MySQL DB cluster.

The DR plan must replicate data to a secondary AWS Region.

Which solution will meet these requirements MOST cost-effectively?

A. Use MySQL binary log replication to an Aurora cluster in the secondary Region. Provision one DB instance for the Aurora cluster in the secondary Region.

B. Set up an Aurora global database for the DB cluster. When setup is complete, remove the DB instance from the secondary Region.

C. Use AWS Database Migration Service (AWS DMS) to continuously replicate data to an Aurora cluster in the secondary Region. Remove the DB instance from the secondary Region.

D. Set up an Aurora global database for the DB cluster. Specify a minimum of one DB instance in the secondary Region.

Answer: D

https://www.examtopics.com/discussions/amazon/view/99758-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

기본 DB 클러스터에서 모든 보조로의 복제는 데이터베이스 엔진이 아닌 Aurora 스토리지 계층에서 처리하므로 변경 사항 복제 지연 시간은 일반적으로 1 초 미만으로 최소화됩니다. 데이터베이스 엔진을 복제 프로세스에서 제외한다는 것은 데이터베이스 엔진이 워크로드 처리 전용임을 의미합니다. 또한 Aurora MySQL binlog(이진 로깅) 복제를 구성하거나 관리할 필요가 없음을 의미합니다.

Q339

A company has a custom application with embedded credentials that retrieves information from an Amazon RDS MySQL DB instance. Management says the application must be made more secure with the least amount of programming effort.

What should a solutions architect do to meet these requirements?

A. Use AWS Key Management Service (AWS KMS) to create keys. Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation.

B. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Create an AWS Lambda function that rotates the credentials in Secret Manager.

C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.

D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

Answer: C

https://www.examtopics.com/discussions/amazon/view/99705-exam-aws-certified-solutions-architect-associate-saa-c03/

Q340

A media company hosts its website on AWS. The website application's architecture includes a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) and a database that is hosted on Amazon Aurora. The company's cybersecurity team reports that the application is vulnerable to SQL injection.

How should the company resolve this issue?

A. Use AWS WAF in front of the ALB. Associate the appropriate web ACLs with AWS WAF.

B. Create an ALB listener rule to reply to SQL injections with a fixed response.

C. Subscribe to AWS Shield Advanced to block all SQL injection attempts automatically.

D. Set up Amazon Inspector to block all SQL injection attempts automatically.

Answer: A

https://www.examtopics.com/discussions/amazon/view/99708-exam-aws-certified-solut

ions-architect-associate-saa-c03/

Q341

A company has an Amazon S3 data lake that is governed by AWS Lake Formation. The company wants to create a visualization in Amazon QuickSight by joining the data in the data lake with operational data that is stored in an Amazon Aurora MySQL database. The company wants to enforce column-level authorization so that the company's marketing team can access only a subset of columns in the database.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use Amazon EMR to ingest the data directly from the database to the QuickSight SPICE engine. Include only the required columns.

B. Use AWS Glue Studio to ingest the data from the database to the S3 data lake. Attach an IAM policy to the QuickSight users to enforce column-level access control. Use Amazon S3 as the data source in QuickSight.

C. Use AWS Glue Elastic Views to create a materialized view for the database in Amazon S3. Create an S3 bucket policy to enforce column-level access control for the QuickSight users. Use Amazon S3 as the data source in QuickSight.

D. Use a Lake Formation blueprint to ingest the data from the database to the S3 data lake. Use Lake Formation to enforce column-level access control for the QuickSight users. Use Amazon Athena as the data source in QuickSight.

Answer: D

https://www.examtopics.com/discussions/amazon/view/99710-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

Amazon QuickSight 및 AWS Lake Formation 을 사용하여 열 수준 권한 부여를 시행합니다.

https://aws.amazon.com/ko/blogs/big-data/enforce-column-level-authorization-with-amazon-quicksight-and-aws-lake-formation/

Q342

A transaction processing company has weekly scripted batch jobs that run on Amazon EC2 instances. The EC2 instances are in an Auto Scaling group. The number of transactions can vary, but the baseline CPU utilization that is noted on each run is at least 60%. The company needs to provision the capacity 30 minutes before the jobs run.

Currently, engineers complete this task by manually modifying the Auto Scaling group parameters. The company does not have the resources to analyze the required capacity trends for the Auto Scaling group counts. The company needs an automated way to modify the Auto Scaling group's desired capacity.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create a dynamic scaling policy for the Auto Scaling group. Configure the policy to scale based on the CPU utilization metric. Set the target value for the metric to 60%.

B. Create a scheduled scaling policy for the Auto Scaling group. Set the appropriate desired capacity, minimum capacity, and maximum capacity. Set the recurrence to weekly. Set the start time to 30 minutes before the batch jobs run.

C. Create a predictive scaling policy for the Auto Scaling group. Configure the policy to scale based on forecast. Set the scaling metric to CPU utilization. Set the target value for the metric to 60%. In the policy, set the instances to pre-launch 30 minutes before the jobs run.

D. Create an Amazon EventBridge event to invoke an AWS Lambda function when the CPU utilization metric value for the Auto Scaling group reaches 60%. Configure the Lambda function to increase the Auto Scaling group's desired capacity and maximum capacity by 20%.

Answer: C

https://www.examtopics.com/discussions/amazon/view/100204-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

이 옵션은 기계 학습을 사용하여 CloudWatch 의 기록 데이터를 기반으로 용량 요구 사항을 예측하는 일종의 조정 정책인 Auto Scaling 그룹에 대한 예측 조정 정책을 사용하기 때문에 가장 효율적입니다. 또한 Auto Scaling 그룹이 트래픽 변경에 앞서 용량을 조정할 수 있도록 예측을 기반으로 확장하도록 정책을 구성합니다. 또한 조정 메트릭을 CPU 사용률로 설정하고 메트릭의 대상 값을 60%로 설정합니다. 이는 각 실행에서 기록되는 기준 CPU 사용률과 일치합니다. 또한 작업이 실행되기 30 분 전에 인스턴스를 사전 실행하도록 설정하여 매주 스크립팅된 배치 작업이 시작되기 전에 충분한 용량이 프로비저닝되도록 합니다. 이 솔루션은 최소한의 운영 오버헤드로 작업이 실행되기 30 분 전에 용량을 프로비저닝해야 하는 요구 사항을 충족합니다.

옵션 A 는 변화하는 수요에 대응하여 Auto Scaling 그룹의 용량을 조정하는 일종의 조정 정책인 Auto Scaling 그룹에 대한 동적 조정 정책을 사용하기 때문에 효율성이 떨어집니다. 그러나 이것은 변화하는 트래픽에만 반응하기 때문에 작업 실행 30 분 전에 용량을 프로비저닝하는 방법을 제공하지 않습니다.

옵션 B 는 생성한 일정에 따라 Auto Scaling 그룹을 조정할 수 있는 조정 정책 유형인 Auto Scaling 그룹에 대해 예약된 조정 정책을 사용하기 때문에 효율성이 떨어집니다. 그러나 미리 정의된 지표 및 정책에 따라서만 확장되므로 예측 또는 CPU 사용률을 기반으로 확장하는 방법을 제공하지 않습니다.

옵션 D 는 Auto Scaling 그룹의 CPU 사용률 지표 값이 60%에 도달할 때 Amazon EventBridge 이벤트를 사용하여 AWS Lambda 함수를 호출하기 때문에 효율성이 떨어집니다. 이는 이벤트를 기반으로 서버리스 함수를 트리거하는 방법입니다. 그러나 이것은 변화하는 트래픽에만 반응하기 때문에 작업 실행 30 분 전에 용량을 프로비저닝하는 방법을 제공하지 않습니다.

Q343

A solution architect is designing a company's disaster recovery (DR) architecture. The company has a MySQL database that runs on an Amazon EC2 instance in a private subnet with scheduled backup. The DR design needs to include multiple AWS Regions.

Which solution will meet these requirements with the LEAST operational overhead?

A. Migrate the MySQL database to multiple EC2 instances. Configure a standby EC2 instance in the DR Region. Turn on replication.

B. Migrate the MySQL database to Amazon RDS. Use a Multi-AZ deployment. Turn on read replication for the primary DB instance in the different Availability Zones.

C. Migrate the MySQL database to an Amazon Aurora global database. Host the primary DB cluster in the primary Region. Host the secondary DB cluster in the DR Region.

D. Store the scheduled backup of the MySQL database in an Amazon S3 bucket that is configured for S3 Cross-Region Replication (CRR). Use the data backup to restore the database in the DR Region.

Answer: C

https://www.examtopics.com/discussions/amazon/view/100302-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

MySQL 데이터베이스를 Amazon Aurora 글로벌 데이터베이스로 마이그레이션하는 것이 최소한의 운영 오버헤드가 필요하기 때문에 최상의 솔루션입니다. Aurora 는 자동 장애 조치를 제공하는 관리형 서비스이므로 대기 인스턴스를 수동으로 구성할 필요가 없습니다. 기본 DB 클러스터는 기본 리전에서 호스팅할 수 있고 보조 DB 클러스터는 DR 리전에서

호스팅할 수 있습니다. 이 접근 방식을 통해 상당한 수동 개입 없이 데이터를 여러 리전에서 항상 사용 가능하고 최신 상태로 유지할 수 있습니다.

Q344

A company has a Java application that uses Amazon Simple Queue Service (Amazon SQS) to parse messages. The application cannot parse messages that are larger than 256 KB in size. The company wants to implement a solution to give the application the ability to parse messages as large as 50 MB.

Which solution will meet these requirements with the FEWEST changes to the code?

A. Use the Amazon SQS Extended Client Library for Java to host messages that are larger than 256 KB in Amazon S3.

B. Use Amazon EventBridge to post large messages from the application instead of Amazon SQS.

C. Change the limit in Amazon SQS to handle messages that are larger than 256 KB.

D. Store messages that are larger than 256 KB in Amazon Elastic File System (Amazon EFS). Configure Amazon SQS to reference this location in the messages.

Answer: A

https://www.examtopics.com/discussions/amazon/view/100202-exam-aws-certified-solutions-architect-associate-saa-c03/

Q345

A company wants to restrict access to the content of one of its main web applications and to protect the content by using authorization techniques available on AWS. The company wants to implement a serverless architecture and an authentication solution for fewer than 100 users. The solution needs to integrate with the main web application and serve web content globally. The solution must also scale as the company's user base grows while providing the lowest login latency possible.

Which solution will meet these requirements MOST cost-effectively?

A. Use Amazon Cognito for authentication. Use Lambda@Edge for authorization. Use Amazon CloudFront to serve the web application globally.

B. Use AWS Directory Service for Microsoft Active Directory for authentication. Use AWS Lambda for authorization. Use an Application Load Balancer to serve the web application globally.

C. Use Amazon Cognito for authentication. Use AWS Lambda for authorization. Use Amazon

S3 Transfer Acceleration to serve the web application globally.

D. Use AWS Directory Service for Microsoft Active Directory for authentication. Use Lambda@Edge for authorization. Use AWS Elastic Beanstalk to serve the web application globally.

Answer: A

https://www.examtopics.com/discussions/amazon/view/100341-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

https://aws.amazon.com/blogs/networking-and-content-delivery/adding-http-security-headersusing-lambdaedge-and-amazon-cloudfront/

Amazon CloudFront 는 웹 콘텐츠, 비디오 및 API 를 대규모로 안전하게 전송할 수 있는 글로벌 콘텐츠 전송 네트워크(CDN) 서비스입니다. 인증을 위해 Cognito 와 통합하고 인증을 위해 Lambda@Edge 와 통합하므로 전 세계적으로 웹 콘텐츠를 제공하는 데 이상적인 선택입니다. Lambda@Edge 는 AWS Lambda 기능을 사용자에게 더 가까운 곳에서 전역적으로 실행할 수 있는 서비스로, 지연 시간을 줄이고 응답 시간을 단축합니다. 또한 CloudFront 의 콘텐츠를 보호하기 위해 에지에서 인증 로직을 처리할 수 있습니다. 이 시나리오에서 Lambda@Edge 는 에지에서 실행하는 짧은 대기 시간 이점을 활용하면서 웹 애플리케이션에 대한 권한 부여를 제공할 수 있습니다.

Q346

A company has an aging network-attached storage (NAS) array in its data center. The NAS array presents SMB shares and NFS shares to client workstations. The company does not want to purchase a new NAS array. The company also does not want to incur the cost of renewing the NAS array's support contract. Some of the data is accessed frequently, but much of the data is inactive.

A solutions architect needs to implement a solution that migrates the data to Amazon S3, uses S3 Lifecycle policies, and maintains the same look and feel for the client workstations. The solutions architect has identified AWS Storage Gateway as part of the solution.

Which type of storage gateway should the solutions architect provision to meet these requirements?

A. Volume Gateway

B. Tape Gateway

C. Amazon FSx File Gateway

D. Amazon S3 File Gateway

Answer: D
https://www.examtopics.com/discussions/amazon/view/100220-exam-aws-certified-solutions-architect-associate-saa-c03/

Q347
A company has an application that is running on Amazon EC2 instances. A solutions architect has standardized the company on a particular instance family and various instance sizes based on the current needs of the company.
The company wants to maximize cost savings for the application over the next 3 years. The company needs to be able to change the instance family and sizes in the next 6 months based on application popularity and usage.
Which solution will meet these requirements MOST cost-effectively?
A. Compute Savings Plan
B. EC2 Instance Savings Plan
C. Zonal Reserved Instances
D. Standard Reserved Instances
Answer: A
https://www.examtopics.com/discussions/amazon/view/100221-exam-aws-certified-solutions-architect-associate-saa-c03/

Q348
A company collects data from a large number of participants who use wearable devices. The company stores the data in an Amazon DynamoDB table and uses applications to analyze the data. The data workload is constant and predictable. The company wants to stay at or below its forecasted budget for DynamoDB.
Which solution will meet these requirements MOST cost-effectively?
A. Use provisioned mode and DynamoDB Standard-Infrequent Access (DynamoDB Standard-IA). Reserve capacity for the forecasted workload.
B. Use provisioned mode. Specify the read capacity units (RCUs) and write capacity units (WCUs).
C. Use on-demand mode. Set the read capacity units (RCUs) and write capacity units (WCUs) high enough to accommodate changes in the workload.
D. Use on-demand mode. Specify the read capacity units (RCUs) and write capacity units (WCUs) with reserved capacity.

Answer: B
https://www.examtopics.com/discussions/amazon/view/100222-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 옵션은 테이블에서 읽기 및 쓰기를 처리하기 위한 읽기/쓰기 용량 모드인 프로비저닝 모드를 사용하기 때문에 가장 효율적입니다. 이를 통해 애플리케이션이 수행할 것으로 예상되는 읽기 및 쓰기 처리량을 지정할 수 있습니다. 또한 애플리케이션이 초당 읽거나 써야 하는 데이터의 양인 RCU(읽기 용량 단위) 및 WCU(쓰기 용량 단위)를 지정합니다. 또한 프로비저닝 모드는 예측 가능한 워크로드에 대해 온디맨드 모드보다 비용이 낮기 때문에 DynamoDB 에 대한 예상 예산 이하로 유지해야 하는 요구 사항을 충족합니다.
이 솔루션은 일정하고 예측 가능한 데이터 워크로드가 있는 웨어러블 장치를 사용하는 많은 참여자로부터 데이터를 수집해야 하는 요구 사항을 충족합니다.

옵션 A 는 프로비저닝 모드와 DynamoDB Standard-Infrequent Access(DynamoDB Standard-IA)를 사용하기 때문에 덜 효율적입니다. DynamoDB Standard-Infrequent Access 는 밀리초의 지연 시간이 필요한 자주 액세스하지 않는 항목을 위한 스토리지 클래스입니다. 그러나 이는 일정하고 예측 가능한 데이터 워크로드가 있는 웨어러블 장치를 사용하는 많은 참여자로부터 데이터를 수집해야 하는 요구 사항을 충족하지 않습니다. DynamoDB Standard-IA 는 액세스 빈도가 30 일에 한 번 미만인 항목에 더 적합하기 때문입니다.

옵션 C 는 수요 변화에 따라 테이블 용량을 자동으로 조정하여 사용한 만큼만 비용을 지불하는 읽기/쓰기 용량 모드인 온디맨드 모드를 사용하기 때문에 효율성이 떨어집니다. 그러나 온디맨드 모드는 예측 가능한 워크로드에 대해 프로비저닝된 모드보다 비용이 높기 때문에 DynamoDB 에 대한 예상 예산 이하로 유지해야 하는 요구 사항을 충족하지 않습니다.

옵션 D 는 온디맨드 모드를 사용하고 예약 용량이 있는 RCU 및 WCU 를 지정하기 때문에 효율성이 떨어집니다. 이는 할인된 시간당 요금과 교환하여 테이블에 대한 읽기 및 쓰기 용량을 예약하는 방법입니다. 그러나 온디맨드 모드는 예측 가능한 워크로드에 대해 프로비저닝된 모드보다 비용이 높기 때문에 DynamoDB 에 대한 예상 예산 이하로 유지해야 하는 요구 사항을 충족하지 않습니다. 또한 예약된 용량이 있는 RCU 및 WCU 를 지정하는 것은 프로비저닝 모드에만 적용되므로 온디맨드 모드에서는 불가능합니다.

Q349

A company stores confidential data in an Amazon Aurora PostgreSQL database in the ap-southeast-3 Region. The database is encrypted with an AWS Key Management Service (AWS KMS) customer managed key. The company was recently acquired and must securely share a backup of the database with the acquiring company's AWS account in ap-southeast-3.

What should a solutions architect do to meet these requirements?

A. Create a database snapshot. Copy the snapshot to a new unencrypted snapshot. Share the new snapshot with the acquiring company's AWS account.

B. Create a database snapshot. Add the acquiring company's AWS account to the KMS key policy. Share the snapshot with the acquiring company's AWS account.

C. Create a database snapshot that uses a different AWS managed KMS key. Add the acquiring company's AWS account to the KMS key alias. Share the snapshot with the acquiring company's AWS account.

D. Create a database snapshot. Download the database snapshot. Upload the database snapshot to an Amazon S3 bucket. Update the S3 bucket policy to allow access from the acquiring company's AWS account.

Answer: B

https://www.examtopics.com/discussions/amazon/view/100299-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

https://docs.aws.amazon.com/ko_kr/kms/latest/developerguide/key-policy-modifying-external-accounts.html

다른 사용자 지정 AWS KMS 키를 생성할 필요가 없습니다.

https://aws.amazon.com/premiumsupport/knowledge-center/aurora-share-encrypted-snapshot/

원본 계정 내에서 대상 계정에 사용자 지정 AWS KMS 키에 대한 액세스 권한을 부여합니다.

1. 원본 계정에 로그인하고 DB 클러스터 스냅샷과 동일한 리전의 AWS KMS 콘솔로 이동합니다.

2. 탐색 창에서 고객 관리형 키를 선택합니다.

3. 사용자 지정 AWS KMS 키(이미 생성됨)를 선택합니다.

4. 다른 AWS 계정 섹션에서 다른 AWS 계정 추가를 선택한 다음 대상 계정의 AWS 계정 번호를 입력합니다.

그런 다음 DB 클러스터 스냅샷을 복사하고 공유합니다.

Q350

A company uses a 100 GB Amazon RDS for Microsoft SQL Server Single-AZ DB instance in the us-east-1 Region to store customer transactions. The company needs high availability and automatic recovery for the DB instance.

The company must also run reports on the RDS database several times a year. The report process causes transactions to take longer than usual to post to the customers' accounts. The company needs a solution that will improve the performance of the report process.

Which combination of steps will meet these requirements? (Choose two)

A. Modify the DB instance from a Single-AZ DB instance to a Multi-AZ deployment.

B. Take a snapshot of the current DB instance. Restore the snapshot to a new RDS deployment in another Availability Zone.

C. Create a read replica of the DB instance in a different Availability Zone. Point all requests for reports to the read replica.

D. Migrate the database to RDS Custom.

E. Use RDS Proxy to limit reporting requests to the maintenance window.

Answer: A, C

https://www.examtopics.com/discussions/amazon/view/100300-exam-aws-certified-solutions-architect-associate-saa-c03/

Q351

A company is moving its data management application to AWS. The company wants to transition to an event-driven architecture. The architecture needs to be more distributed and to use serverless concepts while performing the different aspects of the workflow. The company also wants to minimize operational overhead.

Which solution will meet these requirements?

A. Build out the workflow in AWS Glue. Use AWS Glue to invoke AWS Lambda functions to process the workflow steps.

B. Build out the workflow in AWS Step Functions. Deploy the application on Amazon EC2 instances. Use Step Functions to invoke the workflow steps on the EC2 instances.

C. Build out the workflow in Amazon EventBridge. Use EventBridge to invoke AWS Lambda functions on a schedule to process the workflow steps.

D. Build out the workflow in AWS Step Functions. Use Step Functions to create a state machine. Use the state machine to invoke AWS Lambda functions to process the workflow

steps.
Answer: D
https://www.examtopics.com/discussions/amazon/view/100371-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 대답은 서버리스 개념을 사용하고 운영 오버헤드를 최소화하는 이벤트 기반 아키텍처로의 전환 요구 사항을 충족하기 때문에 정확합니다. AWS Step Functions 는 상태 시스템을 사용하여 여러 AWS 서비스를 워크플로로 조정할 수 있는 서버리스 서비스입니다. 상태 머신은 워크플로 단계의 실행 논리와 순서를 정의하는 작업 및 전환으로 구성됩니다. AWS Lambda 는 서버를 프로비저닝하거나 관리하지 않고도 코드를 실행할 수 있는 서버리스 FaaS(function-as-a-service) 플랫폼입니다. Lambda 함수는 Step Functions 에서 상태 시스템의 작업으로 호출할 수 있으며 데이터 수집, 변환, 검증 및 분석과 같은 데이터 관리 워크플로의 다양한 측면을 수행할 수 있습니다. Step Functions 및 Lambda 를 사용함으로써 회사는 다음과 같은 이점을 얻을 수 있습니다.
이벤트 기반: Step Functions 는 타이머, API 호출 또는 기타 AWS 서비스 이벤트와 같은 이벤트를 기반으로 Lambda 함수를 트리거할 수 있습니다. Lambda 함수는 이벤트 기반 아키텍처를 생성하여 다른 서비스나 상태 시스템에 이벤트를 내보낼 수도 있습니다.
서버리스: Step Functions 및 Lambda 는 AWS 에서 완전히 관리하므로 회사에서 서버 또는 인프라를 프로비저닝하거나 관리할 필요가 없습니다. 회사는 워크플로 및 기능에서 사용하는 리소스에 대해서만 비용을 지불하고 수요에 따라 자동으로 확장 또는 축소할 수 있습니다.
운영 오버헤드: Step Functions 및 Lambda 는 모니터링, 로깅, 추적, 오류 처리, 재시도 논리 및 보안과 같은 기본 제공 기능을 제공하므로 워크플로 및 기능의 개발 및 배포를 단순화합니다. 회사는 운영 세부 사항보다는 비즈니스 논리 및 데이터 처리에 집중할 수 있습니다.

Q352
A company is designing the network for an online multi-player game. The game uses the UDP networking protocol and will be deployed in eight AWS Regions. The network architecture needs to minimize latency and packet loss to give end users a high-quality gaming experience.
Which solution will meet these requirements?
A. Setup a transit gateway in each Region. Create inter-Region peering attachments between each transit gateway.

B. Set up AWS Global Accelerator with UDP listeners and endpoint groups in each Region.
C. Set up Amazon CloudFront with UDP turned on. Configure an origin in each Region.
D. Set up a VPC peering mesh between each Region. Turn on UDP for each VPC.
Answer: B
https://www.examtopics.com/discussions/amazon/view/100197-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 상황에 가장 적합한 솔루션은 각 리전에서 UDP 리스너 및 엔드포인트 그룹으로 AWS Global Accelerator 를 설정하는 옵션 B 입니다. AWS Global Accelerator 는 사용자 요청을 가장 가까운 AWS 지역[1]으로 라우팅하여 인터넷 애플리케이션의 가용성과 성능을 향상시키는 네트워킹 서비스입니다. 또한 대기 시간이 짧고 패킷 손실이 적은 더 빠르고 안정적인 데이터 전송을 제공하여 UDP 응용 프로그램의 성능을 향상시킵니다. 각 리전에서 UDP 리스너와 엔드포인트 그룹을 설정함으로써 Global Accelerator 는 더 빠른 응답 시간과 더 나은 사용자 경험을 위해 가장 가까운 리전으로 트래픽을 라우팅합니다.

Q353
A company hosts a three-tier web application on Amazon EC2 instances in a single Availability Zone. The web application uses a self-managed MySQL database that is hosted on an EC2 instance to store data in an Amazon Elastic Block Store (Amazon EBS) volume. The MySQL database currently uses a 1 TB Provisioned IOPS SSD (io2) EBS volume. The company expects traffic of 1,000 IOPS for both reads and writes at peak traffic.
The company wants to minimize any disruptions, stabilize performance, and reduce costs while retaining the capacity for double the IOPS. The company wants to move the database tier to a fully managed solution that is highly available and fault tolerant.
Which solution will meet these requirements MOST cost-effectively?
A. Use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with an io2 Block Express EBS volume.
B. Use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with a General Purpose SSD (gp2) EBS volume.
C. Use Amazon S3 Intelligent-Tiering access tiers.
D. Use two large EC2 instances to host the database in active-passive mode.
Answer: B
https://www.examtopics.com/discussions/amazon/view/100225-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
RDS 지원 스토리지:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html
GP2 최대 IOPS:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose.html#gp2-performance
Amazon RDS 는 범용 SSD(gp2 및 gp3 라고도 함), 프로비저닝된 IOPS SSD(io1 이라고도 함) 및 마그네틱(표준이라고도 함)의 세 가지 스토리지 유형을 제공합니다. 성능 특성과 가격이 다르기 때문에 스토리지 성능과 비용을 데이터베이스 워크로드의 요구 사항에 맞게 조정할 수 있습니다. 최대 64TiB 의 스토리지로 MySQL, MariaDB, Oracle 및 PostgreSQL RDS DB 인스턴스를 생성할 수 있습니다. 최대 16TiB 의 스토리지로 SQL Server RDS DB 인스턴스를 생성할 수 있습니다. 이 스토리지 용량에는 프로비저닝된 IOPS SSD 및 범용 SSD 스토리지 유형을 사용하십시오.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

Q354
A company hosts a serverless application on AWS. The application uses Amazon API Gateway, AWS Lambda, and an Amazon RDS for PostgreSQL database. The company notices an increase in application errors that result from database connection timeouts during times of peak traffic or unpredictable traffic. The company needs a solution that reduces the application failures with the least amount of change to the code.
What should a solutions architect do to meet these requirements?
A. Reduce the Lambda concurrency rate.
B. Enable RDS Proxy on the RDS DB instance.
C. Resize the RDS DB instance class to accept more connections.
D. Migrate the database to Amazon DynamoDB with on-demand scaling.
Answer: B
https://www.examtopics.com/discussions/amazon/view/100198-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
RDS Proxy 를 사용하면 예측할 수 없는 데이터베이스 트래픽 급증을 처리할 수 있습니다. 그렇지 않으면 이러한 급증으로 인해 연결 초과 구독 또는 빠른 속도로 새 연결 생성으로 인해 문제가 발생할 수 있습니다. RDS Proxy 는 데이터베이스 연결 풀을 설정하고 이

풀에서 연결을 재사용합니다. 이 접근 방식은 매번 새 데이터베이스 연결을 여는 메모리 및 CPU 오버헤드를 방지합니다. 초과 구독으로부터 데이터베이스를 보호하기 위해 생성되는 데이터베이스 연결 수를 제어할 수 있습니다.
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html

Q355
A company is migrating an old application to AWS. The application runs a batch job every hour and is CPU intensive. The batch job takes 15 minutes on average with an on-premises server. The server has 64 virtual CPU (vCPU) and 512 GiB of memory.
Which solution will run the batch job within 15 minutes with the LEAST operational overhead?
A. Use AWS Lambda with functional scaling.
B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate.
C. Use Amazon Lightsail with AWS Auto Scaling.
D. Use AWS Batch on Amazon EC2.
Answer: D
https://www.examtopics.com/discussions/amazon/view/100227-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Amazon EC2 에서 AWS Batch 를 사용합니다. AWS Batch 는 Amazon EC2 인스턴스에서 배치 작업을 쉽게 실행하는 데 사용할 수 있는 완전 관리형 배치 처리 서비스입니다. 워크로드에 맞게 인스턴스 수를 확장할 수 있으므로 최소한의 운영 오버헤드로 원하는 시간 내에 배치 작업을 완료할 수 있습니다.
Amazon API Gateway 에서 AWS Lambda 사용 - AWS Lambda
https://docs.aws.amazon.com/lambda/latest/dg/services-apigateway.html
AWS Lambda FAQ
https://aws.amazon.com/lambda/faqs/

Q356
A company stores its data objects in Amazon S3 Standard storage. A solutions architect has found that 75% of the data is rarely accessed after 30 days. The company needs all the data to remain immediately accessible with the same high availability and resiliency, but the company wants to minimize storage costs.
Which storage solution will meet these requirements?

A. Move the data objects to S3 Glacier Deep Archive after 30 days.
B. Move the data objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
C. Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
D. Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately.
Answer: B
https://www.examtopics.com/discussions/amazon/view/100229-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
30 일 후에 데이터 객체를 S3 Standard-Infrequent Access(S3 Standard-IA)로 이동하면 스토리지 비용을 최소화하면서 고가용성 및 복원력으로 데이터에 즉시 액세스할 수 있어야 한다는 요구 사항을 충족합니다. S3 Standard-IA 는 자주 액세스하지 않는 데이터를 위해 설계되었으며 S3 Standard 보다 낮은 스토리지 비용을 제공하는 동시에 S3 Standard 와 동일한 짧은 지연 시간, 높은 처리량 및 높은 내구성을 제공합니다.

Q357
A gaming company is moving its public scoreboard from a data center to the AWS Cloud. The company uses Amazon EC2 Windows Server instances behind an Application Load Balancer to host its dynamic application. The company needs a highly available storage solution for the application. The application consists of static files and dynamic server-side code.
Which combination of steps should a solutions architect take to meet these requirements? (Choose two)
A. Store the static files on Amazon S3. Use Amazon CloudFront to cache objects at the edge.
B. Store the static files on Amazon S3. Use Amazon ElastiCache to cache objects at the edge.
C. Store the server-side code on Amazon Elastic File System (Amazon EFS). Mount the EFS volume on each EC2 instance to share the files.
D. Store the server-side code on Amazon FSx for Windows File Server. Mount the FSx for Windows File Server volume on each EC2 instance to share the files.
E. Store the server-side code on a General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on each EC2 instance to share the files.

Answer: A, D
https://www.examtopics.com/discussions/amazon/view/100230-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
A: Elasticache 는 Amazon 당 순위표에 이상적임에도 불구하고 에지 위치에서 캐싱하지 않기 때문입니다.
D: FSx 가 대기 시간이 짧은 요구 사항에 대해 더 높은 성능을 제공하기 때문입니다.
https://www.techtarget.com/searchaws/tip/Amazon-FSx-vs-EFS-Compare-the-AWS-file-services
FSx 는 솔리드 스테이트 드라이브 스토리지 볼륨을 사용하여 고성능 및 1 밀리초 미만의 대기 시간을 위해 구축되었습니다. 이 설계를 통해 사용자는 스토리지 용량과 대기 시간을 독립적으로 선택할 수 있습니다. 따라서 테라바이트 이하의 파일 시스템도 256Mbps 이상의 처리량을 가질 수 있으며 최대 64TB 의 볼륨을 지원할 수 있습니다. Amazon S3 는 이미지, 동영상, 문서 등과 같은 정적 파일을 저장할 수 있는 객체 스토리지 서비스입니다. Amazon EFS 는 파일을 계층 구조로 저장할 수 있는 파일 스토리지 서비스이며 NFS 프로토콜을 지원합니다.
Amazon FSx for Windows File Server 는 파일을 계층 구조로 저장할 수 있고 SMB 프로토콜을 지원하는 파일 스토리지 서비스입니다. Amazon EBS 는 데이터를 고정 크기 블록에 저장하고 EC2 인스턴스에 연결할 수 있는 블록 스토리지 서비스입니다.
이러한 정의에 따라 요구 사항을 충족하기 위해 취해야 하는 단계 조합은 다음과 같습니다.
1. 정적 파일을 Amazon S3 에 저장합니다. Amazon CloudFront 를 사용하여 엣지에서 객체를 캐싱합니다.
2. Windows File Server 용 Amazon FSx 에 서버 측 코드를 저장합니다. 파일을 공유할 각 EC2 인스턴스에 FSx for Windows File Server 볼륨을 탑재합니다.

Q358
A social media company runs its application on Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is the origin for an Amazon CloudFront distribution. The application has more than a billion images stored in an Amazon S3 bucket and processes thousands of images each second. The company wants to resize the images dynamically and serve appropriate formats to clients.
Which solution will meet these requirements with the LEAST operational overhead?
A. Install an external image management library on an EC2 instance. Use the image management library to process the images.

B. Create a CloudFront origin request policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.
C. Use a Lambda@Edge function with an external image management library. Associate the Lambda@Edge function with the CloudFront behaviors that serve the images.
D. Create a CloudFront response headers policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.
Answer: C
https://www.examtopics.com/discussions/amazon/view/100231-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Lambda@Edge 는 CloudFront 엣지 위치에서 Lambda 함수를 실행할 수 있게 해주는 서비스입니다. CloudFront 를 통과하는 요청 및 응답을 수정하는 데 사용할 수 있습니다. CloudFront 오리진 요청 정책은 CloudFront 가 오리진으로 보내는 요청에 포함된 값(URL 쿼리 문자열, HTTP 헤더 및 쿠키)을 제어하는 정책입니다. 오리진에서 추가 정보를 수집하거나 오리진 응답을 사용자 정의하는 데 사용할 수 있습니다. CloudFront 응답 헤더 정책은 CloudFront 가 최종 사용자에게 보내는 응답에서 제거하거나 추가하는 HTTP 헤더를 지정하는 정책입니다. 응답에 보안 또는 사용자 지정 헤더를 추가하는 데 사용할 수 있습니다.
이러한 정의에 따라 최소한의 운영 오버헤드로 요구 사항을 충족하는 솔루션은 다음과 같습니다.
외부 이미지 관리 라이브러리와 함께 Lambda@Edge 함수를 사용합니다. Lambda@Edge 함수를 이미지를 제공하는 CloudFront 동작과 연결합니다.
이 솔루션을 사용하면 애플리케이션이 Lambda@Edge 함수를 사용하여 이미지 크기를 동적으로 조정하고 요청의 User-Agent HTTP 헤더를 기반으로 클라이언트에 적절한 형식을 제공할 수 있습니다. Lambda@Edge 기능은 엣지 위치에서 실행되어 오리진의 대기 시간과 부하를 줄입니다. 애플리케이션 코드는 이미지 조작 작업을 수행할 수 있는 외부 이미지 관리 라이브러리만 포함하면 됩니다.

Q359
A hospital needs to store patient records in an Amazon S3 bucket. The hospital's compliance team must ensure that all protected health information (PHI) is encrypted in transit and at rest. The compliance team must administer the encryption key for data at rest. Which solution will meet these requirements?

A. Create a public SSL/TLS certificate in AWS Certificate Manager (ACM). Associate the certificate with Amazon S3. Configure default encryption for each S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Assign the compliance team to manage the KMS keys.
B. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Configure default encryption for each S3 bucket to use server-side encryption with S3 managed encryption keys (SSE-S3). Assign the compliance team to manage the SSE-S3 keys.
C. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Configure default encryption for each S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Assign the compliance team to manage the KMS keys.
D. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Use Amazon Macie to protect the sensitive data that is stored in Amazon S3. Assign the compliance team to manage Macie.
Answer: C
https://www.examtopics.com/discussions/amazon/view/100232-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이를 통해 규정 준수 팀은 서버 측 암호화에 사용되는 KMS 키를 관리할 수 있으므로 암호화 키에 필요한 제어 기능을 제공합니다. 또한 버킷 정책에서 "aws:SecureTransport" 조건을 사용하면 S3 버킷에 대한 모든 연결이 전송 중에 암호화됩니다.

Q360
A company uses Amazon API Gateway to run a private gateway with two REST APIs in the same VPC. The BuyStock RESTful web service calls the CheckFunds RESTful web service to ensure that enough funds are available before a stock can be purchased. The company has noticed in the VPC flow logs that the BuyStock RESTful web service calls the CheckFunds RESTful web service over the internet instead of through the VPC. A solutions architect must implement a solution so that the APIs communicate through the VPC.
Which solution will meet these requirements with the FEWEST changes to the code?
A. Add an X-API-Key header in the HTTP header for authorization.
B. Use an interface endpoint.
C. Use a gateway endpoint.

D. Add an Amazon Simple Queue Service (Amazon SQS) queue between the two REST APIs.
Answer: B
https://www.examtopics.com/discussions/amazon/view/100238-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
인터페이스 엔드포인트를 사용하면 BuyStock RESTful 웹 서비스와 CheckFunds RESTful 웹 서비스가 코드를 변경하지 않고도 VPC 를 통해 통신할 수 있습니다. 인터페이스 엔드포인트는 고객의 VPC 에 탄력적 네트워크 인터페이스(ENI)를 생성한 다음 API 에서 ENI 로 트래픽을 라우팅하도록 라우팅 테이블을 구성합니다. 이렇게 하면 코드를 변경하지 않고도 두 API 가 VPC 를 통해 통신할 수 있습니다.

Q361
A company hosts a multiplayer gaming application on AWS. The company wants the application to read data with sub-millisecond latency and run one-time queries on historical data.
Which solution will meet these requirements with the LEAST operational overhead?
A. Use Amazon RDS for data that is frequently accessed. Run a periodic custom script to export the data to an Amazon S3 bucket.
B. Store the data directly in an Amazon S3 bucket. Implement an S3 Lifecycle policy to move older data to S3 Glacier Deep Archive for long-term storage. Run one-time queries on the data in Amazon S3 by using Amazon Athena.
C. Use Amazon DynamoDB with DynamoDB Accelerator (DAX) for data that is frequently accessed. Export the data to an Amazon S3 bucket by using DynamoDB table export. Run one-time queries on the data in Amazon S3 by using Amazon Athena.
D. Use Amazon DynamoDB for data that is frequently accessed. Turn on streaming to Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to read the data from Kinesis Data Streams. Store the records in an Amazon S3 bucket.
Answer: C
https://www.examtopics.com/discussions/amazon/view/102119-exam-aws-certified-solutions-architect-associate-saa-c03/

Q362
A company uses a payment processing system that requires messages for a particular

payment ID to be received in the same order that they were sent. Otherwise, the payments might be processed incorrectly.

Which actions should a solutions architect take to meet this requirement? (Choose two)

A. Write the messages to an Amazon DynamoDB table with the payment ID as the partition key.

B. Write the messages to an Amazon Kinesis data stream with the payment ID as the partition key.

C. Write the messages to an Amazon ElastiCache for Memcached cluster with the payment ID as the key.

D. Write the messages to an Amazon Simple Queue Service (Amazon SQS) queue. Set the message attribute to use the payment ID.

E. Write the messages to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the message group to use the payment ID.

Answer: B, E

https://www.examtopics.com/discussions/amazon/view/102121-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

1) SQS FIFO 대기열은 메시지가 전송된 정확한 순서대로 수신되도록 보장합니다. 지불 ID를 메시지 그룹으로 사용하면 지불 ID에 대한 모든 메시지가 순차적으로 수신됩니다.

2) Kinesis 데이터 스트림은 파티션 키별로 순서를 지정할 수도 있습니다. 지불 ID를 파티션 키로 사용하면 각 지불 ID에 대한 메시지의 엄격한 순서가 보장됩니다.

Q363

A company is building a game system that needs to send unique events to separate leaderboard, matchmaking, and authentication services concurrently. The company needs an AWS event-driven system that guarantees the order of the events.

Which solution will meet these requirements?

A. Amazon EventBridge event bus

B. Amazon Simple Notification Service (Amazon SNS) FIFO topics

C. Amazon Simple Notification Service (Amazon SNS) standard topics

D. Amazon Simple Queue Service (Amazon SQS) FIFO queues

Answer: B

https://www.examtopics.com/discussions/amazon/view/102124-exam-aws-certified-solutions-architect-associate-saa-c03/

Q364

A hospital is designing a new application that gathers symptoms from patients. The hospital has decided to use Amazon Simple Queue Service (Amazon SQS) and Amazon Simple Notification Service (Amazon SNS) in the architecture.

A solutions architect is reviewing the infrastructure design. Data must be encrypted at rest and in transit. Only authorized personnel of the hospital should be able to access the data. Which combination of steps should the solutions architect take to meet these requirements? (Choose two)

A. Turn on server-side encryption on the SQS components. Update the default key policy to restrict key usage to a set of authorized principals.

B. Turn on server-side encryption on the SNS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply a key policy to restrict key usage to a set of authorized principals.

C. Turn on encryption on the SNS components. Update the default key policy to restrict key usage to a set of authorized principals. Set a condition in the topic policy to allow only encrypted connections over TLS.

D. Turn on server-side encryption on the SQS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply a key policy to restrict key usage to a set of authorized principals. Set a condition in the queue policy to allow only encrypted connections over TLS.

E. Turn on server-side encryption on the SQS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply an IAM policy to restrict key usage to a set of authorized principals. Set a condition in the queue policy to allow only encrypted connections over TLS.

Answer: B, D

https://www.examtopics.com/discussions/amazon/view/102125-exam-aws-certified-solutions-architect-associate-saa-c03/

참고:

https://docs.aws.amazon.com/sns/latest/dg/sns-server-side-encryption.html

https://docs.aws.amazon.com/ko_kr/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-server-side-encryption.html

Q365

A company runs a web application that is backed by Amazon RDS. A new database administrator caused data loss by accidentally editing information in a database table. To help recover from this type of incident, the company wants the ability to restore the database to its state from 5 minutes before any change within the last 30 days.

Which feature should the solutions architect include in the design to meet this requirement?

A. Read replicas

B. Manual snapshots

C. Automated backups

D. Multi-AZ deployments

Answer: C

https://www.examtopics.com/discussions/amazon/view/102127-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

https://aws.amazon.com/rds/features/backup/

자동 백업은 요구 사항을 충족합니다. Amazon RDS 를 사용하면 DB 인스턴스의 백업을 자동으로 생성할 수 있습니다. 자동 백업을 사용하면 DB 인스턴스에 대한 PITR(특정 시점 복구)을 보존 기간(최대 35 일) 내의 특정 초 단위로 낮출 수 있습니다. 보존 기간을 30 일로 설정하면 최근 30 일 이내 변경 전 최대 5 분 전의 상태로 데이터베이스를 복원할 수 있습니다.

Q366

A company's web application consists of an Amazon API Gateway API in front of an AWS Lambda function and an Amazon DynamoDB database. The Lambda function handles the business logic, and the DynamoDB table hosts the data. The application uses Amazon Cognito user pools to identify the individual users of the application. A solutions architect needs to update the application so that only users who have a subscription can access premium content.

Which solution will meet this requirement with the LEAST operational overhead?

A. Enable API caching and throttling on the API Gateway API.

B. Set up AWS WAF on the API Gateway API. Create a rule to filter users who have a subscription.

C. Apply fine-grained IAM permissions to the premium content in the DynamoDB table.

D. Implement API usage plans and API keys to limit the access of users who do not have a

subscription.
Answer: D
https://www.examtopics.com/discussions/amazon/view/102128-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 옵션은 API 사용 계획 및 API 키를 사용하기 때문에 가장 효율적입니다. API 에 액세스할 수 있는 사람과 API 에 액세스할 수 있는 양과 속도를 제어할 수 있는 Amazon API Gateway 의 기능입니다. 또한 API 사용 계획 및 API 키를 구현하여 구독하지 않은 사용자의 액세스를 제한하므로 API 에 대한 다양한 액세스 계층을 생성하고 그에 따라 사용자에게 요금을 청구할 수 있습니다. 이 솔루션은 구독이 있는 사용자만 프리미엄 콘텐츠에 액세스할 수 있도록 애플리케이션 업데이트 요구 사항을 충족합니다.
옵션 A 는 Amazon API Gateway 의 기능인 API Gateway API 에서 API 캐싱 및 제한을 사용하기 때문에 효율성이 떨어집니다.
API 의 성능과 가용성을 개선하고 트래픽 급증으로부터 백엔드 시스템을 보호할 수 있습니다. 그러나 이는 가입하지 않은 사용자의 액세스를 제한하는 방법을 제공하지 않습니다.
옵션 B 는 가용성에 영향을 미치거나 보안을 손상시키거나 과도한 리소스를 소비할 수 있는 일반적인 웹 악용으로부터 웹 애플리케이션 또는 API 를 보호하는 웹 애플리케이션 방화벽 서비스인 API Gateway API 에서 AWS WAF 를 사용하기 때문에 효율성이 떨어집니다. 그러나 이는 가입하지 않은 사용자의 액세스를 제한하는 방법을 제공하지 않습니다.
옵션 C 는 테이블 내의 특정 항목 또는 속성에 대한 액세스를 제어할 수 있는 권한인 DynamoDB 테이블의 프리미엄 콘텐츠에 대한 세분화된 IAM 권한을 사용하기 때문에 효율성이 떨어집니다. 그러나 이는 API 수준에서 구독하지 않은 사용자의 액세스를 제한하는 방법을 제공하지 않습니다.

Q367
A company is using Amazon Route 53 latency-based routing to route requests to its UDP-based application for users around the world. The application is hosted on redundant servers in the company's on-premises data centers in the United States, Asia, and Europe. The company's compliance requirements state that the application must be hosted on premises. The company wants to improve the performance and availability of the application.
What should a solutions architect do to meet these requirements?
A. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the

on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the NLBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
B. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the ALBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
C. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three NLBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.
D. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three ALBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.
Answer: A
https://www.examtopics.com/discussions/amazon/view/102131-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
https://aws.amazon.com/ko/step-functions/#:~:text=AWS%20Step%20Functions%20is%20a
AWS Step Functions 의 일반적인 사용 사례는 사람의 개입이 필요한 작업입니다(예: 승인 프로세스). Step Functions 를 사용하면 분산 애플리케이션의 구성 요소를 상태 머신이라고 하는 시각적 워크플로의 일련의 단계로 쉽게 조정할 수 있습니다. 안정적이고 확장 가능한 방식으로 애플리케이션의 단계를 실행하기 위해 상태 시스템을 신속하게 구축하고 실행할 수 있습니다.

Q368
A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods for IAM user passwords.
What should the solutions architect do to accomplish this?
A. Set an overall password policy for the entire AWS account.
B. Set a password policy for each IAM user in the AWS account.
C. Use third-party vendor software to set password requirements.

D. Attach an Amazon CloudWatch rule to the Create_newuser event to set the password with the appropriate requirements.
Answer: A
https://www.examtopics.com/discussions/amazon/view/102132-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 옵션은 IAM 사용자 암호에 대한 복잡성 요구 사항 및 필수 교체 기간을 지정하는 방법인 전체 AWS 계정에 대한 전체 암호 정책을 설정하기 때문에 가장 효율적입니다. 또한 암호 정책은 계정의 모든 IAM 사용자에게 적용되므로 모든 새 사용자에 대한 암호 정책 설정 요구 사항을 충족합니다. 이 솔루션은 IAM 사용자 암호에 대한 특정 복잡성 요구 사항 및 필수 교체 기간 설정 요구 사항을 충족합니다.
옵션 B 는 AWS 계정의 각 IAM 사용자에 대해 암호 정책을 설정하기 때문에 효율성이 떨어집니다. 암호 정책은 계정 수준에서만 설정할 수 있으므로 불가능합니다.
옵션 C 는 타사 공급업체 소프트웨어를 사용하여 암호 요구 사항을 설정하기 때문에 효율성이 떨어집니다. IAM 은 암호 정책을 설정하는 기본 제공 방법을 제공하므로 필요하지 않습니다.
옵션 D 는 Amazon CloudWatch 규칙을 Create_newuser 이벤트에 연결하여 적절한 요구 사항으로 암호를 설정하기 때문에 효율성이 떨어집니다. 이는 CloudWatch 규칙이 IAM 사용자 암호를 수정할 수 없기 때문에 불가능합니다.

Q369
A company has migrated an application to Amazon EC2 Linux instances. One of these EC2 instances runs several 1-hour tasks on a schedule. These tasks were written by different teams and have no common programming language. The company is concerned about performance and scalability while these tasks run on a single instance. A solutions architect needs to implement a solution to resolve these concerns.
Which solution will meet these requirements with the LEAST operational overhead?
A. Use AWS Batch to run the tasks as jobs. Schedule the jobs by using Amazon EventBridge (Amazon CloudWatch Events).
B. Convert the EC2 instance to a container. Use AWS App Runner to create the container on demand to run the tasks as jobs.
C. Copy the tasks into AWS Lambda functions. Schedule the Lambda functions by using Amazon EventBridge (Amazon CloudWatch Events).
D. Create an Amazon Machine Image (AMI) of the EC2 instance that runs the tasks. Create

an Auto Scaling group with the AMI to run multiple copies of the instance.
Answer: A
https://www.examtopics.com/discussions/amazon/view/102133-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
AWS Batch 는 사용자가 AWS 에서 배치 작업을 실행할 수 있게 해주는 완전관리형 서비스입니다. 다른 언어로 작성된 다양한 유형의 작업을 처리하고 EC2 인스턴스에서 실행할 수 있습니다. 또한 Amazon EventBridge(Amazon CloudWatch Events)와 통합되어 시간 또는 이벤트 트리거를 기반으로 작업을 예약합니다. 이 솔루션은 성능, 확장성 및 낮은 운영 오버헤드 요구 사항을 충족합니다.
1. EC2 인스턴스를 컨테이너로 변환합니다. AWS App Runner 를 사용하여 작업을 작업으로 실행할 온디맨드 컨테이너를 생성합니다. 이 솔루션은 EC2 인스턴스를 컨테이너로 변환하고 웹 애플리케이션을 자동으로 빌드 및 배포하고 트래픽 부하를 분산하는 서비스인 AWS App Runner 를 사용하므로 낮은 운영 오버헤드 요구 사항을 충족하지 않습니다. 배치 작업을 실행하는 데는 필요하지 않습니다.
2. 작업을 AWS Lambda 함수에 복사합니다. Amazon EventBridge(Amazon CloudWatch Events)를 사용하여 Lambda 함수를 예약합니다. AWS Lambda 에는 실행 시간이 15 분, 메모리 할당이 10GB 로 제한되어 있으므로 이 솔루션은 성능 요구 사항을 충족하지 않습니다. 이러한 제한은 1 시간 작업을 실행하는 데 충분하지 않을 수 있습니다.
3. 작업을 실행하는 EC2 인스턴스의 Amazon 머신 이미지(AMI)를 생성합니다. AMI 로 Auto Scaling 그룹을 생성하여 인스턴스의 여러 복사본을 실행합니다. 이 솔루션은 구성 및 관리가 필요한 추가 리소스인 AMI 및 Auto Scaling 그룹을 생성하고 유지 관리하므로 낮은 운영 오버헤드 요구 사항을 충족하지 않습니다.
참조 URL:
https://docs.aws.amazon.com/ko_kr/whitepapers/latest/aws-overview/compute-services.html

Q370
A company runs a public three-tier web application in a VPC. The application runs on Amazon EC2 instances across multiple Availability Zones. The EC2 instances that run in private subnets need to communicate with a license server over the internet. The company needs a managed solution that minimizes operational maintenance.
Which solution meets these requirements?
A. Provision a NAT instance in a public subnet. Modify each private subnet's route table with

a default route that points to the NAT instance.
B. Provision a NAT instance in a private subnet. Modify each private subnet's route table with a default route that points to the NAT instance.
C. Provision a NAT gateway in a public subnet. Modify each private subnet's route table with a default route that points to the NAT gateway.
D. Provision a NAT gateway in a private subnet. Modify each private subnet's route table with a default route that points to the NAT gateway.
Answer: C
https://www.examtopics.com/discussions/amazon/view/102134-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
NAT 게이트웨이는 프라이빗 서브넷의 인스턴스가 인터넷이나 다른 AWS 서비스에 연결할 수 있게 해주지만 인터넷이 해당 인스턴스와의 연결을 시작하지 못하도록 하는 네트워크 주소 변환(NAT) 장치 유형입니다. NAT 게이트웨이는 최소한의 운영 유지 관리가 필요하고 최대 45Gbps 의 버스트 트래픽을 처리할 수 있는 관리형 서비스입니다. NAT 게이트웨이는 시나리오의 3 계층 웹 애플리케이션과 같이 프라이빗 서브넷의 EC2 인스턴스가 인터넷을 통해 라이선스 서버와 통신해야 하는 시나리오에 적합합니다.
시나리오의 요구 사항을 충족하려면 솔루션 설계자가 퍼블릭 서브넷에서 NAT 게이트웨이를 프로비저닝해야 합니다. 솔루션 설계자는 또한 NAT 게이트웨이를 가리키는 기본 경로로 각 프라이빗 서브넷의 경로 테이블을 수정해야 합니다. 이렇게 하면 프라이빗 서브넷에서 실행되는 EC2 인스턴스가 NAT 게이트웨이를 통해 인터넷을 통해 라이선스 서버에 액세스할 수 있습니다.

Q371
A company needs to create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster to host a digital media streaming application. The EKS cluster will use a managed node group that is backed by Amazon Elastic Block Store (Amazon EBS) volumes for storage. The company must encrypt all data at rest by using a customer managed key that is stored in AWS Key Management Service (AWS KMS).
Which combination of actions will meet this requirement with the LEAST operational overhead? (Choose two)
A. Use a Kubernetes plugin that uses the customer managed key to perform data encryption.
B. After creation of the EKS cluster, locate the EBS volumes. Enable encryption by using the customer managed key.

C. Enable EBS encryption by default in the AWS Region where the EKS cluster will be created. Select the customer managed key as the default key.
D. Create the EKS cluster. Create an IAM role that has a policy that grants permission to the customer managed key. Associate the role with the EKS cluster.
E. Store the customer managed key as a Kubernetes secret in the EKS cluster. Use the customer managed key to encrypt the EBS volumes.
Answer: B, D
https://www.examtopics.com/discussions/amazon/view/102135-exam-aws-certified-solutions-architect-associate-saa-c03/

Q372
A company wants to migrate an Oracle database to AWS. The database consists of a single table that contains millions of geographic information systems (GIS) images that are high resolution and are identified by a geographic code.
When a natural disaster occurs, tens of thousands of images get updated every few minutes. Each geographic code has a single image or row that is associated with it. The company wants a solution that is highly available and scalable during such events.
Which solution meets these requirements MOST cost-effectively?
A. Store the images and geographic codes in a database table. Use Oracle running on an Amazon RDS Multi-AZ DB instance.
B. Store the images in Amazon S3 buckets. Use Amazon DynamoDB with the geographic code as the key and the image S3 URL as the value.
C. Store the images and geographic codes in an Amazon DynamoDB table. Configure DynamoDB Accelerator (DAX) during times of high load.
D. Store the images in Amazon S3 buckets. Store geographic codes and image S3 URLs in a database table. Use Oracle running on an Amazon RDS Multi-AZ DB
Answer: B
https://www.examtopics.com/discussions/amazon/view/102136-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Amazon S3 는 수백만 개의 이미지 1 를 저장할 수 있는 확장성과 내구성이 뛰어나고 비용 효율적인 객체 스토리지 서비스입니다. Amazon DynamoDB 는 키-값 및 문서 데이터에 대해 높은 처리량과 짧은 지연 시간을 처리할 수 있는 완전관리형 NoSQL 데이터베이스입니다. S3 를 사용하여 이미지를 저장하고 DynamoDB 를 사용하여 지리적

코드와 이미지 S3 URL 을 저장함으로써 솔루션은 자연 재해 중에 고가용성과 확장성을 달성할 수 있습니다. 또한 캐싱, 자동 확장, 글로벌 테이블과 같은 DynamoDB 의 기능을 활용하여 성능을 개선하고 비용을 절감할 수 있습니다.

1. 데이터베이스 테이블에 이미지와 지리적 코드를 저장합니다. Amazon RDS 다중 AZ DB 인스턴스에서 실행되는 Oracle 을 사용합니다. Oracle 은 이미지와 같은 대량의 비정형 데이터를 효율적으로 처리하지 못할 수 있는 관계형 데이터베이스이므로 이 솔루션은 확장성 및 비용 효율성 요구 사항을 충족하지 않습니다. 또한 S3 및 DynamoDB 보다 라이선스 및 운영 비용이 더 많이 듭니다.

2. Amazon DynamoDB 테이블에 이미지와 지리적 코드를 저장합니다. 로드가 많은 시간 동안 DynamoDB Accelerator(DAX)를 구성합니다. 이 솔루션은 DynamoDB 에 이미지를 저장하면 S312 에 저장하는 것보다 더 많은 스토리지 공간을 사용하고 더 많은 비용이 발생하므로 비용 효율성 요구 사항을 충족하지 않습니다. 또한 높은 부하를 처리하기 위해 DAX 클러스터의 추가 구성 및 관리가 필요합니다.

3. Amazon S3 버킷에 이미지를 저장합니다. 지리적 코드와 이미지 S3 URL 을 데이터베이스 테이블에 저장합니다. Amazon RDS 다중 AZ DB 인스턴스에서 실행되는 Oracle 을 사용합니다. Oracle 은 지리적 코드와 같은 키-값 데이터에 대한 높은 처리량과 낮은 대기 시간을 효율적으로 처리하지 못할 수 있는 관계형 데이터베이스이므로 이 솔루션은 확장성 및 비용 효율성 요구 사항을 충족하지 않습니다. 또한 DynamoDB2 보다 라이선스 및 운영 비용이 더 많이 듭니다.

참조 URL: https://dynobase.dev/dynamodb-vs-s3/

Q373

A company has an application that collects data from IoT sensors on automobiles. The data is streamed and stored in Amazon S3 through Amazon Kinesis Data
Firehose. The data produces trillions of S3 objects each year. Each morning, the company uses the data from the previous 30 days to retrain a suite of machine learning (ML) models. Four times each year, the company uses the data from the previous 12 months to perform analysis and train other ML models. The data must be available with minimal delay for up to 1 year. After 1 year, the data must be retained for archival purposes.

A. Use the S3 Intelligent-Tiering storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.

B. Use the S3 Intelligent-Tiering storage class. Configure S3 Intelligent-Tiering to automatically move objects to S3 Glacier Deep Archive after 1 year.

C. Use the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.

D. Use the S3 Standard storage class. Create an S3 Lifecycle policy to transition objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days, and then to S3 Glacier Deep Archive after 1 year.

Answer: D

https://www.examtopics.com/discussions/amazon/view/102137-exam-aws-certified-solutions-architect-associate-saa-c03/

Q374

A company is running several business applications in three separate VPCs within the us-east-1 Region. The applications must be able to communicate between VPCs. The applications also must be able to consistently send hundreds of gigabytes of data each day to a latency-sensitive application that runs in a single on-premises data center.

A solutions architect needs to design a network connectivity solution that maximizes cost-effectiveness.

Which solution meets these requirements?

A. Configure three AWS Site-to-Site VPN connections from the data center to AWS. Establish connectivity by configuring one VPN connection for each VPC.

B. Launch a third-party virtual network appliance in each VPC. Establish an IPsec VPN tunnel between the data center and each virtual appliance.

C. Set up three AWS Direct Connect connections from the data center to a Direct Connect gateway in us-east-1. Establish connectivity by configuring each VPC to use one of the Direct Connect connections.

D. Set up one AWS Direct Connect connection from the data center to AWS. Create a transit gateway, and attach each VPC to the transit gateway. Establish connectivity between the Direct Connect connection and the transit gateway.

Answer: D

https://www.examtopics.com/discussions/amazon/view/102138-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

A(X) : VPC-온프레미스 간 통신은 이루어지나 VPC 간 통신은 이루어지지 않고 있음.

B(X) : A 와 같은 이유로 오답.

C(X) : A 와 같은 이유로 오답.

D(O) : Transit Gateway 는 동일한 리전 내에 있는 여러 VPC 들을 연결하는 전송 '허브'이므로 Transit Gateway 를 거쳐 VPC 끼리 통신이 가능

AWS Transit Gateway 는 동일한 리전의 VPC 를 상호 연결하여 Amazon VPC 라우팅 구성을 한 곳에 통합하는 네트워크 전송 허브입니다.
https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway.html

Q375
An ecommerce company is building a distributed application that involves several serverless functions and AWS services to complete order-processing tasks. These tasks require manual approvals as part of the workflow. A solutions architect needs to design an architecture for the order-processing application. The solution must be able to combine multiple AWS Lambda functions into responsive serverless applications. The solution also must orchestrate data and services that run on Amazon EC2 instances, containers, or on-premises servers.
Which solution will meet these requirements with the LEAST operational overhead?
A. Use AWS Step Functions to build the application.
B. Integrate all the application components in an AWS Glue job.
C. Use Amazon Simple Queue Service (Amazon SQS) to build the application.
D. Use AWS Lambda functions and Amazon EventBridge events to build the application.
Answer: A
https://www.examtopics.com/discussions/amazon/view/102139-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
AWS Step Functions 는 시각적 워크플로를 사용하여 분산 애플리케이션 및 마이크로서비스의 구성 요소를 조정하여 애플리케이션을 쉽게 구축할 수 있게 해주는 완전 관리형 서비스입니다.
Step Functions 를 사용하면 여러 AWS Lambda 함수를 반응형 서버리스 애플리케이션에 결합하고 Amazon EC2 인스턴스, 컨테이너 또는 온프레미스 서버에서 실행되는 데이터 및 서비스를 오케스트레이션할 수 있습니다. Step Functions 는 또한 워크플로의 일부로 수동 승인을 허용합니다. 이 솔루션은 최소한의 운영 오버헤드로 모든 요구 사항을 충족합니다.
https://aws.amazon.com/ko/step-functions/#:~:text=AWS%20Step%20Functions%20is%20a

Q376

A company has launched an Amazon RDS for MySQL DB instance. Most of the connections to the database come from serverless applications. Application traffic to the database changes significantly at random intervals. At times of high demand, users report that their applications experience database connection rejection errors.

Which solution will resolve this issue with the LEAST operational overhead?

A. Create a proxy in RDS Proxy. Configure the users' applications to use the DB instance through RDS Proxy.

B. Deploy Amazon ElastiCache for Memcached between the users' applications and the DB instance.

C. Migrate the DB instance to a different instance class that has higher I/O capacity. Configure the users' applications to use the new DB instance.

D. Configure Multi-AZ for the DB instance. Configure the users' applications to switch between the DB instances.

Answer: A

https://www.examtopics.com/discussions/amazon/view/102140-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

최신 서버리스 아키텍처에 구축된 애플리케이션을 포함하여 많은 애플리케이션은 데이터베이스 서버에 대해 많은 수의 열린 연결을 가질 수 있으며 빠른 속도로 데이터베이스 연결을 열고 닫을 수 있으므로 데이터베이스 메모리와 컴퓨팅 리소스가 고갈될 수 있습니다. Amazon RDS Proxy 를 사용하면 애플리케이션이 데이터베이스와 설정된 연결을 풀링하고 공유하여 데이터베이스 효율성과 애플리케이션 확장성을 개선할 수 있습니다.

(https://aws.amazon.com/pt/rds/proxy/)

Q377

A company recently deployed a new auditing system to centralize information about operating system versions, patching, and installed software for Amazon EC2 instances. A solutions architect must ensure all instances provisioned through EC2 Auto Scaling groups successfully send reports to the auditing system as soon as they are launched and terminated.

Which solution achieves these goals MOST efficiently?

A. Use a scheduled AWS Lambda function and run a script remotely on all EC2 instances to send data to the audit system.

B. Use EC2 Auto Scaling lifecycle hooks to run a custom script to send data to the audit system when instances are launched and terminated.
C. Use an EC2 Auto Scaling launch configuration to run a custom script through user data to send data to the audit system when instances are launched and terminated.
D. Run a custom script on the instance operating system to send data to the audit system. Configure the script to be invoked by the EC2 Auto Scaling group when the instance starts and is terminated.
Answer: B
https://www.examtopics.com/discussions/amazon/view/102142-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Amazon EC2 Auto Scaling 은 Auto Scaling 그룹에 수명 주기 후크를 추가하는 기능을 제공합니다. 이러한 후크를 사용하면 Auto Scaling 인스턴스 수명 주기의 이벤트를 인식하는 솔루션을 생성한 다음 해당 수명 주기 이벤트가 발생할 때 인스턴스에서 사용자 지정 작업을 수행할 수 있습니다.
(https://docs.aws.amazon.com/autoscaling/ec2/userguide/lifecycle-hooks.html)

Q378
A company is developing a real-time multiplayer game that uses UDP for communications between the client and servers in an Auto Scaling group. Spikes in demand are anticipated during the day, so the game server platform must adapt accordingly. Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention.
Which solution should a solutions architect recommend?
A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage.
B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.
C. Use a Network Load Balancer for traffic distribution and Amazon Aurora Global Database for data storage.
D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage.
Answer: B
https://www.examtopics.com/discussions/amazon/view/102143-exam-aws-certified-sol

utions-architect-associate-saa-c03/

설명:
Network Load Balancer 는 연결 수준(계층 4)에서 작동하고 TCP 및 UDP 트래픽 모두의 부하를 분산할 수 있는 일종의 부하 분산 장치입니다. Network Load Balancer 는 실시간 멀티플레이어 게임과 같이 고성능과 짧은 대기 시간이 필요한 시나리오에 적합합니다. Network Load Balancer 는 가용 영역당 단일 고정 IP 주소를 사용하면서 갑작스럽고 변동성이 큰 트래픽 패턴을 처리할 수도 있습니다.
시나리오의 요구 사항을 충족하려면 솔루션 설계자는 Auto Scaling 그룹의 EC2 인스턴스 간 트래픽 분산을 위해 Network Load Balancer 를 사용해야 합니다. Network Load Balancer 는 클라이언트에서 적절한 포트의 서버로 UDP 트래픽을 라우팅할 수 있습니다. Network Load Balancer 는 클라이언트와 서버 간의 보안 통신을 위해 TLS 오프로딩도 지원할 수 있습니다.
Amazon DynamoDB 는 일관된 성능과 짧은 지연 시간으로 모든 양의 데이터를 저장하고 검색할 수 있는 완전 관리형 NoSQL 데이터베이스 서비스입니다. Amazon DynamoDB 온디맨드는 용량 계획이 필요 없고 테이블에서 수행되는 읽기 및 쓰기 요청에 대해서만 요금을 부과하는 유연한 결제 옵션입니다 3. Amazon DynamoDB 온디맨드는 게임 애플리케이션과 같이 애플리케이션 트래픽을 예측할 수 없거나 산발적인 시나리오에 이상적입니다.
시나리오의 요구 사항을 충족하려면 솔루션 설계자는 데이터 스토리지에 Amazon DynamoDB 온디맨드를 사용해야 합니다. Amazon DynamoDB 온디맨드는 개발자의 개입 없이 게이머 점수 및 기타 비관계형 데이터를 저장할 수 있습니다. Amazon DynamoDB 온디맨드는 자동으로 확장하여 성능이나 가용성에 영향을 주지 않고 모든 수준의 요청 트래픽을 처리할 수 있습니다.

Q379
A company hosts a frontend application that uses an Amazon API Gateway API backend that is integrated with AWS Lambda. When the API receives requests, the Lambda function loads many libraries. Then the Lambda function connects to an Amazon RDS database, processes the data, and returns the data to the frontend application. The company wants to ensure that response latency is as low as possible for all its users with the fewest number of changes to the company's operations.
Which solution will meet these requirements?
A. Establish a connection between the frontend application and the database to make queries faster by bypassing the API.

B. Configure provisioned concurrency for the Lambda function that handles the requests.
C. Cache the results of the queries in Amazon S3 for faster retrieval of similar datasets.
D. Increase the size of the database to increase the number of connections Lambda can establish at one time.
Answer: B
https://www.examtopics.com/discussions/amazon/view/102144-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
요청을 처리하는 Lambda 함수에 대해 프로비저닝된 동시성을 구성합니다. 프로비저닝된 동시성을 사용하면 Lambda 함수에서 사용할 수 있는 컴퓨팅 리소스의 양을 설정할 수 있으므로 한 번에 더 많은 요청을 처리하고 지연 시간을 줄일 수 있습니다. 쿼리 결과를 Amazon S3 에 캐싱하면 대기 시간을 줄이는 데 도움이 되지만 프로비저닝된 동시성을 설정하는 것만큼 효과적이지는 않습니다. 데이터베이스 크기를 늘려도 지연 시간을 줄이는 데 도움이 되지 않습니다. 이는 Lambda 함수가 설정할 수 있는 연결 수를 늘리지 않고 프런트엔드 애플리케이션과 데이터베이스 사이에 직접 연결을 설정하면 API 를 우회하기 때문입니다. 최고의 솔루션 중 하나입니다.
https://docs.aws.amazon.com/lambda/latest/dg/services-apigateway.html
Using AWS Lambda with Amazon API Gateway - AWS Lambda
https://docs.aws.amazon.com/lambda/latest/dg/services-apigateway.html
https://aws.amazon.com/lambda/faqs/
AWS Lambda FAQs
https://aws.amazon.com/lambda/faqs/

Q380
A company is migrating its on-premises workload to the AWS Cloud. The company already uses several Amazon EC2 instances and Amazon RDS DB instances. The company wants a solution that automatically starts and stops the EC2 instances and DB instances outside of business hours. The solution must minimize cost and infrastructure maintenance.
Which solution will meet these requirements?
A. Scale the EC2 instances by using elastic resize. Scale the DB instances to zero outside of business hours.
B. Explore AWS Marketplace for partner solutions that will automatically start and stop the EC2 instances and DB instances on a schedule.
C. Launch another EC2 instance. Configure a crontab schedule to run shell scripts that will

start and stop the existing EC2 instances and DB instances on a schedule.
D. Create an AWS Lambda function that will start and stop the EC2 instances and DB instances. Configure Amazon EventBridge to invoke the Lambda function on a schedule.
Answer: D
https://www.examtopics.com/discussions/amazon/view/102145-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
비용 및 인프라 유지 관리를 최소화하면서 일정에 따라 EC2 인스턴스 및 DB 인스턴스를 자동으로 시작 및 중지하는 가장 효율적인 솔루션은 AWS Lambda 함수를 생성하고 일정에 따라 함수를 호출하도록 Amazon EventBridge 를 구성하는 것입니다.
옵션 A, 탄력적 크기 조정을 사용하여 EC2 인스턴스를 확장하고 업무 시간 외에 DB 인스턴스를 0 으로 확장하는 것은 DB 인스턴스를 0 으로 확장할 수 없기 때문에 실행 불가능합니다.
파트너 솔루션에 대한 AWS Marketplace 를 탐색하는 옵션 B 가 옵션일 수 있지만 가장 효율적인 솔루션이 아닐 수 있으며 잠재적으로 추가 비용이 추가될 수 있습니다.
다른 EC2 인스턴스를 시작하고 일정에 따라 기존 EC2 인스턴스 및 DB 인스턴스를 시작 및 중지하는 셸 스크립트를 실행하도록 crontab 일정을 구성하는 옵션 C 는 불필요한 인프라 및 유지 관리를 추가합니다.

Q381
A company hosts a three-tier web application that includes a PostgreSQL database. The database stores the metadata from documents. The company searches the metadata for key terms to retrieve documents that the company reviews in a report each month. The documents are stored in Amazon S3. The documents are usually written only once, but they are updated frequently.
The reporting process takes a few hours with the use of relational queries. The reporting process must not prevent any document modifications or the addition of new documents. A solutions architect needs to implement a solution to speed up the reporting process.
Which solution will meet these requirements with the LEAST amount of change to the application code?
A. Set up a new Amazon DocumentDB (with MongoDB compatibility) cluster that includes a read replica. Scale the read replica to generate the reports.
B. Set up a new Amazon Aurora PostgreSQL DB cluster that includes an Aurora Replica. Issue queries to the Aurora Replica to generate the reports.

C. Set up a new Amazon RDS for PostgreSQL Multi-AZ DB instance. Configure the reporting module to query the secondary RDS node so that the reporting module does not affect the primary node.
D. Set up a new Amazon DynamoDB table to store the documents. Use a fixed write capacity to support new document entries. Automatically scale the read capacity to support the reports.
Answer: B
https://www.examtopics.com/discussions/amazon/view/102147-exam-aws-certified-solutions-architect-associate-saa-c03/

Q382
A company has a three-tier application on AWS that ingests sensor data from its users' devices. The traffic flows through a Network Load Balancer (NLB), then to Amazon EC2 instances for the web tier, and finally to EC2 instances for the application tier. The application tier makes calls to a database.
What should a solutions architect do to improve the security of the data in transit?
A. Configure a TLS listener. Deploy the server certificate on the NLB.
B. Configure AWS Shield Advanced. Enable AWS WAF on the NLB.
C. Change the load balancer to an Application Load Balancer (ALB). Enable AWS WAF on the ALB.
D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances by using AWS Key Management Service (AWS KMS).
Answer: A
https://www.examtopics.com/discussions/amazon/view/102149-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
전송 중인 데이터의 보안을 개선하는 가장 좋은 옵션은 TLS 수신기를 구성하고 NLB 에서버 인증서를 배포하는 것입니다. 이렇게 하면 데이터가 네트워크를 통해 이동할 때 암호화되고 안전해집니다. 또한 AWS Shield Advanced 를 구성하고 NLB 에서 AWS WAF 를 활성화하여 악의적인 공격으로부터 네트워크를 추가로 보호할 수도 있습니다. 또는 로드 밸런서를 Application Load Balancer(ALB)로 변경하고 ALB 에서 AWS WAF 를 활성화할 수도 있습니다.
마지막으로 AWS Key Management Service(AWS KMS)를 사용하여 EC2 인스턴스에서 Amazon Elastic Block Store(Amazon EBS) 볼륨을 암호화할 수도 있습니다.

TLS 수신기에 대한 SSL 인증서를 지정해야 합니다. 로드 밸런서는 인증서를 사용하여 연결을 종료하고 대상으로 라우팅하기 전에 클라이언트의 요청을 해독합니다.
https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-listener.html

설명 2:
A: 전송 중인 데이터를 어떻게 보호합니까?
모범 사례:
보안 키 및 인증서 관리 구현: 암호화 키 및 인증서를 안전하게 저장하고 엄격한 액세스 제어를 적용하면서 적절한 시간 간격으로 교체합니다. 예를 들어 AWS Certificate Manager(ACM)와 같은 인증서 관리 서비스를 사용합니다.
전송 중 암호화 적용: 조직, 법률 및 규정 준수 요구 사항을 충족하는 데 도움이 되는 적절한 표준 및 권장 사항에 따라 정의된 암호화 요구 사항을 적용합니다.
의도하지 않은 데이터 액세스 탐지 자동화: GuardDuty 와 같은 도구를 사용하여 데이터 분류 수준에 따라 정의된 경계 외부로 데이터를 이동하려는 시도를 자동으로 탐지합니다. 예를 들어 DNS 프로토콜을 사용하여 알 수 없거나 신뢰할 수 없는 네트워크에 데이터를 복사하는 트로이 목마를 탐지합니다. .
네트워크 통신 인증: TLS(전송 계층 보안) 또는 IPsec 과 같은 인증을 지원하는 프로토콜을 사용하여 통신 ID 를 확인합니다.
https://wa.aws.amazon.com/wat.question.SEC_9.en.html

Q383
A company is planning to migrate a commercial off-the-shelf application from its on-premises data center to AWS. The software has a software licensing model using sockets and cores with predictable capacity and uptime requirements. The company wants to use its existing licenses, which were purchased earlier this year.
Which Amazon EC2 pricing option is the MOST cost-effective?
A. Dedicated Reserved Hosts
B. Dedicated On-Demand Hosts
C. Dedicated Reserved Instances
D. Dedicated On-Demand Instances
Answer: A
https://www.examtopics.com/discussions/amazon/view/102150-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

https://aws.amazon.com/ec2/dedicated-hosts/
Amazon EC2 전용 호스트를 사용하면 Amazon EC2 에서 Microsoft 및 Oracle 과 같은 공급업체의 적격 소프트웨어 라이선스를 사용할 수 있으므로 자체 라이선스 사용의 유연성과 비용 효율성을 얻으면서도 AWS 의 탄력성, 단순성 및 탄력성을 얻을 수 있습니다.

Q384
A company runs an application on Amazon EC2 Linux instances across multiple Availability Zones. The application needs a storage layer that is highly available and Portable Operating System Interface (POSIX)-compliant. The storage layer must provide maximum data durability and must be shareable across the EC2 instances. The data in the storage layer will be accessed frequently for the first 30 days and will be accessed infrequently after that time. Which solution will meet these requirements MOST cost-effectively?
A. Use the Amazon S3 Standard storage class. Create an S3 Lifecycle policy to move infrequently accessed data to S3 Glacier.
B. Use the Amazon S3 Standard storage class. Create an S3 Lifecycle policy to move infrequently accessed data to S3 Standard-Infrequent Access (S3 Standard-IA).
C. Use the Amazon Elastic File System (Amazon EFS) Standard storage class. Create a lifecycle management policy to move infrequently accessed data to EFS Standard-Infrequent Access (EFS Standard-IA).
D. Use the Amazon Elastic File System (Amazon EFS) One Zone storage class. Create a lifecycle management policy to move infrequently accessed data to EFS One Zone-Infrequent Access (EFS One Zone-IA).
Answer: C
https://www.examtopics.com/discussions/amazon/view/102152-exam-aws-certified-solutions-architect-associate-saa-c03/

참고:
https://aws.amazon.com/efs/features/infrequent-access/

Q385
A solutions architect is creating a new VPC design. There are two public subnets for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web servers use only HTTPS. The solutions architect has already created a security group for the load balancer allowing port 443 from 0.0.0.0/0. Company policy requires that each resource

has the least access required to still be able to perform its tasks.
Which additional configuration strategy should the solutions architect use to meet these requirements?
A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.
C. Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
D. Create a network ACL for the web servers and allow port 443 from the load balancer. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.
Answer: C
https://www.examtopics.com/discussions/amazon/view/102153-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 답변은 Windows IIS 웹 서버와 호환되는 온-프레미스 파일 공유에 대한 탄력적이고 내구성 있는 대체를 제공하기 때문에 정확합니다. Amazon FSx for Windows File Server 는 Windows Server 에 구축된 공유 파일 스토리지를 제공하는 완전관리형 서비스입니다. SMB 프로토콜을 지원하고 Windows 기반 애플리케이션에 대한 원활한 액세스 및 인증을 가능하게 하는 Microsoft Active Directory 와 통합됩니다. Amazon FSx for Windows File Server 는 또한 다음과 같은 이점을 제공합니다.
복원력: Amazon FSx for Windows File Server 는 고가용성 및 장애 조치 보호를 제공하는 여러 가용 영역에 배포할 수 있습니다. 또한 자동 백업 및 복원은 물론 문제를 감지하고 수정하는 자가 치유 기능을 지원합니다.
내구성: Windows File Server 용 Amazon FSx 는 가용 영역 내외에서 데이터를 복제하고 내구성이 뛰어난 스토리지 장치에 데이터를 저장합니다. 또한 유휴 및 전송 중 암호화는 물론 파일 액세스 감사 및 데이터 중복 제거를 지원합니다.
성능: Windows File Server 용 Amazon FSx 는 파일 작업을 위한 일관된 1 밀리초 미만의 지연 시간과 높은 처리량을 제공합니다. 또한 SSD 스토리지, 분산 파일 시스템(DFS) 네임스페이스 및 복제와 같은 기본 Windows 기능, 사용자 중심 성능 확장을 지원합니다.
AWS KMS CMK 를 사용하여 파일 공유의 이미지를 암호화하도록 Amazon FSx 파일 공유를 구성함으로써 회사는 무단 액세스로부터 이미지를 보호하고 회사 정책을 준수할 수

있습니다. 이미지에 대한 NTFS 권한 집합을 사용하여 회사는 이미지를 수정하거나 삭제할 수 있는 사람을 제한하여 실수로 이미지를 삭제하는 것을 방지할 수 있습니다.

Q386

An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers both run on Amazon EC2, and the database runs on Amazon RDS for MySQL. The backend tier communicates with the RDS instance. There are frequent calls to return identical datasets from the database that are causing performance slowdowns.

Which action should be taken to improve the performance of the backend?

A. Implement Amazon SNS to store the database calls.

B. Implement Amazon ElastiCache to cache the large datasets.

C. Implement an RDS for MySQL read replica to cache database calls.

D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

Answer: B

https://www.examtopics.com/discussions/amazon/view/102154-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

가장 좋은 솔루션은 Amazon ElastiCache 를 구현하여 대용량 데이터 세트를 캐시하는 것입니다. 이렇게 하면 자주 액세스하는 데이터를 메모리에 저장하여 검색 시간을 단축할 수 있습니다. 이는 데이터베이스에 대한 빈번한 호출을 완화하고 대기 시간을 줄이며 백엔드 계층의 전반적인 성능을 향상시키는 데 도움이 될 수 있습니다.

Q387

A new employee has joined a company as a deployment engineer. The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources. A solutions architect wants the deployment engineer to perform job activities while following the principle of least privilege.

Which combination of actions should the solutions architect take to accomplish this goal? (Choose two)

A. Have the deployment engineer use AWS account root user credentials for performing AWS CloudFormation stack operations.

B. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached.

C. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the AdministratorAccess IAM policy attached.
D. Create a new IAM user for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.
E. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using that IAM role.
Answer: D, E
https://www.examtopics.com/discussions/amazon/view/102155-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
배포 엔지니어가 CloudFormation 을 사용하여 필요한 작업을 전부 해결할 수 있으므로 관련 작업만 허용해주면 최소 권한의 원칙이 충족됨.
A(X) : 루트 사용자 자격 증명으로 최소 권한의 원칙에 어긋나서 제외.
B(X) : PowerUsers 는 PowerUser 사용자 그룹의 멤버는 사용자 관리 작업(예: IAM 및 Organizations)을 제공하는 일부 서비스를 제외한 모든 서비스에 대해 전체 권한을 갖으므로 최소 권한의 원칙에 어긋나서 제외
https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/getting-started_create-delegated-user.html
C(X) : 관리/액세스 권한을 굳이 줄 필요없음. CloudFormation 관련 권한만 부여하면 됨.
D(O) : CloudFormation 작업만 허용하도록 하여 최소 권한 부여 조건 충족.
E(O) : D 와 마찬가지 이유로 정답.

참고:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html

Q388
A company is deploying a two-tier web application in a VPC. The web tier is using an Amazon EC2 Auto Scaling group with public subnets that span multiple Availability Zones. The database tier consists of an Amazon RDS for MySQL DB instance in separate private subnets. The web tier requires access to the database to retrieve product information.
The web application is not working as intended. The web application reports that it cannot connect to the database. The database is confirmed to be up and running. All configurations for the network ACLs, security groups, and route tables are still in their default states.

What should a solutions architect recommend to fix the application?

A. Add an explicit rule to the private subnet's network ACL to allow traffic from the web tier's EC2 instances.

B. Add a route in the VPC route table to allow traffic between the web tier's EC2 instances and the database tier.

C. Deploy the web tier's EC2 instances and the database tier's RDS instance into two separate VPCs, and configure VPC peering.

D. Add an inbound rule to the security group of the database tier's RDS instance to allow traffic from the web tiers security group.

Answer: D

https://www.examtopics.com/discussions/amazon/view/102156-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

이 대답은 웹 계층이 보안 그룹을 소스로 사용하여 데이터베이스 계층에 액세스할 수 있도록 허용하기 때문에 정확합니다. 이는 VPC 연결에 권장되는 모범 사례입니다. 보안 그룹은 상태 저장이며 동일한 VPC 에 있는 다른 보안 그룹을 참조할 수 있으므로 방화벽 규칙의 구성 및 유지 관리가 간소화됩니다. 데이터베이스 계층의 보안 그룹에 인바운드 규칙을 추가하면 웹 계층의 EC2 인스턴스가 IP 주소나 서브넷에 관계없이 포트 3306 에서 RDS 인스턴스에 연결할 수 있습니다.

Q389

A company has a large dataset for its online advertising business stored in an Amazon RDS for MySQL DB instance in a single Availability Zone. The company wants business reporting queries to run without impacting the write operations to the production DB instance.

Which solution meets these requirements?

A. Deploy RDS read replicas to process the business reporting queries.

B. Scale out the DB instance horizontally by placing it behind an Elastic Load Balancer.

C. Scale up the DB instance to a larger instance type to handle write operations and queries.

D. Deploy the DB instance in multiple Availability Zones to process the business reporting queries.

Answer: A

https://www.examtopics.com/discussions/amazon/view/102157-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
읽기 전용 복제본 사용 사례 - 일반 로드를 수행하는 프로덕션 데이터베이스가 있고 일부 분석을 실행하기 위해 보고 애플리케이션을 실행하려고 합니다. * 읽기 전용 복제본을 생성하여 그곳에서 새 워크로드를 실행합니다. * 프로덕션 애플리케이션은 영향을 받지 않습니다. SELECT(=읽기) 종류의 문에만 사용됨(INSERT, UPDATE, DELETE 아님)

Q390
A company hosts a three-tier ecommerce application on a fleet of Amazon EC2 instances. The instances run in an Auto Scaling group behind an Application Load Balancer (ALB). All ecommerce data is stored in an Amazon RDS for MariaDB Multi-AZ DB instance.
The company wants to optimize customer session management during transactions. The application must store session data durably.
Which solutions will meet these requirements? (Choose two)
A. Turn on the sticky sessions feature (session affinity) on the ALB.
B. Use an Amazon DynamoDB table to store customer session information.
C. Deploy an Amazon Cognito user pool to manage user session information.
D. Deploy an Amazon ElastiCache for Redis cluster to store customer session information.
E. Use AWS Systems Manager Application Manager in the application to manage user session information.
Answer: A, D
https://www.examtopics.com/discussions/amazon/view/102213-exam-aws-certified-solutions-architect-associate-saa-c03/

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

Q391
A company needs a backup strategy for its three-tier stateless web application. The web application runs on Amazon EC2 instances in an Auto Scaling group with a dynamic scaling policy that is configured to respond to scaling events. The database tier runs on Amazon RDS for PostgreSQL. The web application does not require temporary local storage on the EC2 instances. The company's recovery point objective (RPO) is 2 hours.
The backup strategy must maximize scalability and optimize resource utilization for this environment.

Which solution will meet these requirements?
A. Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances and database every 2 hours to meet the RPO.
B. Configure a snapshot lifecycle policy to take Amazon Elastic Block Store (Amazon EBS) snapshots. Enable automated backups in Amazon RDS to meet the RPO.
C. Retain the latest Amazon Machine Images (AMIs) of the web and application tiers. Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO.
D. Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances every 2 hours. Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO.
Answer: C
https://www.examtopics.com/discussions/amazon/view/102212-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
애플리케이션에는 인스턴스에 대한 로컬 데이터가 없으므로 AMI 만으로는 최신 AMI 백업에서 인스턴스를 복원하여 RPO 를 충족할 수 있습니다. 데이터베이스에 대한 자동화된 RDS 백업과 결합하면 이 환경에 대한 완벽한 백업 솔루션을 제공합니다. EBS 스냅샷과 관련된 다른 옵션은 인스턴스의 상태 비저장 특성을 고려할 때 불필요합니다. AMI 는 앱 계층에 필요한 모든 백업을 제공합니다. 이는 최소한의 지속적인 관리가 필요한 기본 자동 AWS 백업 기능을 사용합니다. - AMI 자동 백업은 상태 비저장 앱 계층에 대한 특정 시점 복구를 제공합니다. - RDS 자동 백업은 데이터베이스에 대한 특정 시점 복구를 제공합니다.

Q392
A company wants to deploy a new public web application on AWS. The application includes a web server tier that uses Amazon EC2 instances. The application also includes a database tier that uses an Amazon RDS for MySQL DB instance.
The application must be secure and accessible for global customers that have dynamic IP addresses.
How should a solutions architect configure the security groups to meet these requirements?
A. Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers.
B. Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB instance to allow

inbound traffic on port 3306 from the security group of the web servers.
C. Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the IP addresses of the customers.
D. Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB instance to allow inbound traffic on port 3306 from 0.0.0.0/0.
Answer: A
https://www.examtopics.com/discussions/amazon/view/102160-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
A(O) : S3 에 넣으면 Lambda 를 통해 자동으로 처리가 되도록 하는 거라 OK. S3 는 저렴함.
B(X) : dynamodb 는 이미지 저장용으론…
C(X) : 저렴한 S3 가 있는데 굳이... 인스턴스 비용도 나감.
D(x) : C 와 마찬가지.

설명 2:
웹 서버에 대한 인바운드 액세스를 HTTPS 트래픽에 사용되는 포트 443 으로만 제한하고 애플리케이션이 공개되어 글로벌 고객이 액세스할 수 있으므로 모든 IP 주소(0.0.0.0/0)에서 액세스를 허용합니다.
DB 인스턴스에 대한 인바운드 액세스를 MySQL 트래픽에 사용되는 포트 3306 으로만 제한하고 웹 서버의 보안 그룹에서만 액세스를 허용하여 두 계층 간의 보안 연결을 생성하고 데이터베이스에 대한 무단 액세스를 방지합니다.
아웃바운드 액세스를 두 계층에 필요한 최소 수준으로 제한합니다. 이는 질문에 지정되지 않았지만 인바운드 규칙과 유사하다고 가정할 수 있습니다.

Q393
A payment processing company records all voice communication with its customers and stores the audio files in an Amazon S3 bucket. The company needs to capture the text from the audio files. The company must remove from the text any personally identifiable information (PII) that belongs to customers.
What should a solutions architect do to meet these requirements?
A. Process the audio files by using Amazon Kinesis Video Streams. Use an AWS Lambda function to scan for known PII patterns.

B. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start an Amazon Textract task to analyze the call recordings.
C. Configure an Amazon Transcribe transcription job with PII redaction turned on. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start the transcription job. Store the output in a separate S3 bucket.
D. Create an Amazon Connect contact flow that ingests the audio files with transcription turned on. Embed an AWS Lambda function to scan for known PII patterns. Use Amazon EventBridge to start the contact flow when an audio file is uploaded to the S3 bucket.
Answer: C
https://www.examtopics.com/discussions/amazon/view/102322-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
민감한 데이터 수정은 텍스트 스크립트와 오디오 파일의 개인 식별 가능 정보(PII)를 대체합니다. 수정된 내용은 원본 텍스트를 [PII]로 대체하고 수정된 오디오 파일은 음성 개인 정보를 침묵으로 대체합니다. 이 매개 변수는 고객 정보를 보호하는 데 유용합니다.
https://docs.aws.amazon.com/transcribe/latest/dg/call-analytics-insights.html#callanalytics-insights-redaction

Q394
A company is running a multi-tier ecommerce web application in the AWS Cloud. The application runs on Amazon EC2 instances with an Amazon RDS for MySQL Multi-AZ DB instance. Amazon RDS is configured with the latest generation DB instance with 2,000 GB of storage in a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. The database performance affects the application during periods of high demand.
A database administrator analyzes the logs in Amazon CloudWatch Logs and discovers that the application performance always degrades when the number of read and write IOPS is higher than 20,000.
What should a solutions architect do to improve the application performance?
A. Replace the volume with a magnetic volume.
B. Increase the number of IOPS on the gp3 volume.
C. Replace the volume with a Provisioned IOPS SSD (io2) volume.
D. Replace the 2,000 GB gp3 volume with two 1,000 GB gp3 volumes.
Answer: B
https://www.examtopics.com/discussions/amazon/view/102161-exam-aws-certified-sol

utions-architect-associate-saa-c03/

Q395

An IAM user made several configuration changes to AWS resources in their company's account during a production deployment last week. A solutions architect learned that a couple of security group rules are not configured as desired. The solutions architect wants to confirm which IAM user was responsible for making changes.

Which service should the solutions architect use to find the desired information?

A. Amazon GuardDuty

B. Amazon Inspector

C. AWS CloudTrail

D. AWS Config

Answer: C

https://www.examtopics.com/discussions/amazon/view/102162-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

가장 좋은 방법은 AWS CloudTrail 을 사용하여 원하는 정보를 찾는 것입니다. AWS CloudTrail 은 AWS 계정 활동의 거버넌스, 규정 준수, 운영 감사 및 위험 감사를 지원하는 서비스입니다. CloudTrail 은 IAM 사용자, EC2 인스턴스, AWS 관리 콘솔 및 기타 AWS 서비스에 의한 변경 사항을 포함하여 AWS 계정의 리소스에 대한 모든 변경 사항을 기록하는 데 사용할 수 있습니다. 솔루션 설계자는 CloudTrail 을 사용하여 보안 그룹 규칙의 구성을 변경한 IAM 사용자를 식별할 수 있습니다.

Q396

A company has implemented a self-managed DNS service on AWS. The solution consists of the following:

- Amazon EC2 instances in different AWS Regions
- Endpoints of a standard accelerator in AWS Global Accelerator

The company wants to protect the solution against DDoS attacks.

What should a solutions architect do to meet this requirement?

A. Subscribe to AWS Shield Advanced. Add the accelerator as a resource to protect.

B. Subscribe to AWS Shield Advanced. Add the EC2 instances as resources to protect.

C. Create an AWS WAF web ACL that includes a rate-based rule. Associate the web ACL

with the accelerator.
D. Create an AWS WAF web ACL that includes a rate-based rule. Associate the web ACL with the EC2 instances.
Answer: A
https://www.examtopics.com/discussions/amazon/view/102164-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
AWS Shield 는 AWS 에서 실행되는 애플리케이션에 대한 DDoS(Distributed Denial of Service) 공격으로부터 보호하는 관리형 서비스입니다. AWS Shield Standard 는 추가 비용 없이 모든 AWS 고객에게 자동으로 활성화됩니다. AWS Shield Advanced 는 선택적 유료 서비스입니다. AWS Shield Advanced 는 Amazon Elastic Compute Cloud(EC2), Elastic Load Balancing(ELB), Amazon CloudFront, AWS Global Accelerator 및 Route 53 에서 실행되는 애플리케이션에 대해 더 정교하고 더 큰 공격에 대한 추가 보호 기능을 제공합니다.
https://docs.aws.amazon.com/waf/latest/developerguide/ddos-event-mitigation-logic-gax.html

Q397
An ecommerce company needs to run a scheduled daily job to aggregate and filter sales records for analytics. The company stores the sales records in an Amazon S3 bucket. Each object can be up to 10 GB in size. Based on the number of sales events, the job can take up to an hour to complete. The CPU and memory usage of the job are constant and are known in advance.
A solutions architect needs to minimize the amount of operational effort that is needed for the job to run.
Which solution meets these requirements?
A. Create an AWS Lambda function that has an Amazon EventBridge notification. Schedule the EventBridge event to run once a day.
B. Create an AWS Lambda function. Create an Amazon API Gateway HTTP API, and integrate the API with the function. Create an Amazon EventBridge scheduled event that calls the API and invokes the function.
C. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.
D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2

launch type and an Auto Scaling group with at least one EC2 instance. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.
Answer: C
https://www.examtopics.com/discussions/amazon/view/102165-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
최소한의 운영 오버헤드로 요구 사항을 충족하는 솔루션은 속도 기반 규칙을 사용하여 리전 AWS WAF 웹 ACL 을 생성하고 웹 ACL 을 API 게이트웨이 단계와 연결하는 것입니다. 이 솔루션은 들어오는 요청을 모니터링하고 사전 정의된 속도를 초과하는 IP 주소의 요청을 차단하여 HTTP 플러드 공격으로부터 애플리케이션을 보호합니다. API Gateway 지역 API 엔드포인트 앞에 Lambda@Edge 가 있는 Amazon CloudFront 배포도 좋은 솔루션이지만 이전 솔루션보다 더 많은 운영 오버헤드가 필요합니다. Amazon CloudWatch 지표를 사용하여 개수 지표를 모니터링하고 미리 정의된 속도에 도달했을 때 보안 팀에 알리는 것은 HTTP 플러드 공격으로부터 보호할 수 있는 솔루션이 아닙니다. 최대 TTL 이 24 시간인 API Gateway 지역 API 엔드포인트 앞에 Amazon CloudFront 배포를 생성하는 것은 HTTP 플러드 공격으로부터 보호할 수 있는 솔루션이 아닙니다.

Q398
A company needs to transfer 600 TB of data from its on-premises network-attached storage (NAS) system to the AWS Cloud. The data transfer must be complete within 2 weeks. The data is sensitive and must be encrypted in transit. The company's internet connection can support an upload speed of 100 Mbps.
Which solution meets these requirements MOST cost-effectively?
A. Use Amazon S3 multi-part upload functionality to transfer the files over HTTPS.
B. Create a VPN connection between the on-premises NAS system and the nearest AWS Region. Transfer the data over the VPN connection.
C. Use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices. Use the devices to transfer the data to Amazon S3.
D. Set up a 10 Gbps AWS Direct Connect connection between the company location and the nearest AWS Region. Transfer the data over a VPN connection into the Region to store the data in Amazon S3.
Answer: C
https://www.examtopics.com/discussions/amazon/view/102166-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
가장 좋은 방법은 AWS Snow Family 콘솔을 사용하여 여러 AWS Snowball Edge Storage Optimized 디바이스를 주문하고 디바이스를 사용하여 데이터를 Amazon S3 로 전송하는 것입니다. Snowball Edge 는 많은 양의 데이터를 안전하고 빠르게 전송할 수 있는 페타바이트 규모의 데이터 전송 디바이스입니다.
Snowball Edge 를 사용하면 장거리에서 대량의 데이터를 전송하는 가장 비용 효율적인 솔루션이 될 수 있으며 2 주 이내에 600TB 의 데이터를 전송해야 하는 요구 사항을 충족할 수 있습니다.

Q399
A financial company hosts a web application on AWS. The application uses an Amazon API Gateway Regional API endpoint to give users the ability to retrieve current stock prices. The company's security team has noticed an increase in the number of API requests. The security team is concerned that HTTP flood attacks might take the application offline.
A solutions architect must design a solution to protect the application from this type of attack.
Which solution meets these requirements with the LEAST operational overhead?
A. Create an Amazon CloudFront distribution in front of the API Gateway Regional API endpoint with a maximum TTL of 24 hours.
B. Create a Regional AWS WAF web ACL with a rate-based rule. Associate the web ACL with the API Gateway stage.
C. Use Amazon CloudWatch metrics to monitor the Count metric and alert the security team when the predefined rate is reached.
D. Create an Amazon CloudFront distribution with Lambda@Edge in front of the API Gateway Regional API endpoint. Create an AWS Lambda function to block requests from IP addresses that exceed the predefined rate.
Answer: B
https://www.examtopics.com/discussions/amazon/view/102167-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
AWS WAF 의 속도 기반 규칙을 사용하면 보안 팀이 속도 기반 규칙을 트리거하는 임계값을 구성할 수 있습니다. 이를 통해 AWS WAF 는 지정된 기간 동안 요청 속도를 추적한 다음 임계값이 초과되면 자동으로 차단할 수 있습니다. 이는 최소한의 운영 오버헤드로 HTTP

플러드 공격을 방지하는 기능을 제공합니다.

참조:
https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html

Q400
A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store its data and wants to build a new service that sends an alert to the managers of four internal teams every time a new weather event is recorded. The company does not want this new service to affect the performance of the current application.
What should a solutions architect do to meet these requirements with the LEAST amount of operational overhead?
A. Use DynamoDB transactions to write new event data to the table. Configure the transactions to notify internal teams.
B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.
C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.
D. Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SQS) queue to which the teams can subscribe.
Answer: C
https://www.examtopics.com/discussions/amazon/view/102169-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 최상의 솔루션은 테이블에서 Amazon DynamoDB 스트림을 활성화하고 트리거를 사용하여 팀이 구독할 수 있는 단일 Amazon Simple Notification Service(Amazon SNS) 주제에 쓰는 것입니다. 이 솔루션에는 최소한의 구성 및 인프라 설정이 필요하며 Amazon DynamoDB Streams 는 DynamoDB 테이블에 대한 변경 사항을 캡처하는 지연 시간이 짧은 방법을 제공합니다. 트리거는 자동으로 변경 사항을 캡처하고 이를 내부 팀에 알리는 SNS 주제에 게시합니다.

Q401

A company wants to use the AWS Cloud to make an existing application highly available and resilient. The current version of the application resides in the company's data center. The application recently experienced data loss after a database server crashed because of an unexpected power outage.

The company needs a solution that avoids any single points of failure. The solution must give the application the ability to scale to meet user demand.

Which solution will meet these requirements?

A. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon RDS DB instance in a Multi-AZ configuration.

B. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group in a single Availability Zone. Deploy the database on an EC2 instance. Enable EC2 Auto Recovery.

C. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon RDS DB instance with a read replica in a single Availability Zone. Promote the read replica to replace the primary DB instance if the primary DB instance fails.

D. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Deploy the primary and secondary database servers on EC2 instances across multiple Availability Zones. Use Amazon Elastic Block Store (Amazon EBS) Multi-Attach to create shared storage between the instances.

Answer: A

https://www.examtopics.com/discussions/amazon/view/102170-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:

A(O) : Amazon RDS 다중 AZ 배포에서 Amazon RDS 는 자동으로 프라이머리 데이터베이스 DB 인스턴스를 생성하고 동시에 다른 AZ 의 인스턴스에 데이터를 복제합니다. 장애를 감지하면 Amazon RDS 는 수동 개입 없이 자동으로 대기 인스턴스로 장애 조치합니다.

https://aws.amazon.com/ko/rds/features/multi-az/

B(X) : Auto Scaling 을 단일 가용 영역에서 사용하므로 고가용성 조건 불충족.

C(X) : 단일 가용 영역에서 읽기 전용 복제본이 있는 DB 인스턴스를 사용한다고 했으므로 고가용성 조건 불충족.

D(X) : 공유 스토리지가 아니라 read replica 나 다중 AZ 가 더 합리적.

설명 2:
여러 가용 영역의 Auto Scaling 그룹에서 Amazon EC2 인스턴스를 사용하여 애플리케이션 서버를 배포합니다. 다중 AZ 구성에서 Amazon RDS DB 인스턴스를 사용합니다. 단일 장애 지점을 피하고 사용자 요구에 맞게 애플리케이션을 확장할 수 있는 기능을 제공하면서 기존 애플리케이션의 가용성과 탄력성을 높이려면 최상의 솔루션은 Auto Scaling 그룹의 Amazon EC2 인스턴스를 사용하여 애플리케이션 서버를 여러 그룹에 배포하는 것입니다. 가용 영역 및 다중 AZ 구성에서 Amazon RDS DB 인스턴스를 사용합니다. 다중 AZ 구성에서 Amazon RDS DB 인스턴스를 사용하면 데이터베이스가 여러 가용 영역에 걸쳐 자동으로 복제되므로 데이터베이스의 가용성이 높고 단일 가용 영역의 장애를 견딜 수 있습니다. 이는 내결함성을 제공하고 단일 실패 지점을 방지합니다.

Q402
A company needs to ingest and handle large amounts of streaming data that its application generates. The application runs on Amazon EC2 instances and sends data to Amazon Kinesis Data Streams, which is configured with default settings. Every other day, the application consumes the data and writes the data to an Amazon S3 bucket for business intelligence (BI) processing. The company observes that Amazon S3 is not receiving all the data that the application sends to Kinesis Data Streams.
What should a solutions architect do to resolve this issue?
A. Update the Kinesis Data Streams default settings by modifying the data retention period.
B. Update the application to use the Kinesis Producer Library (KPL) to send the data to Kinesis Data Streams.
C. Update the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams.
D. Turn on S3 Versioning within the S3 bucket to preserve every version of every object that is ingested in the S3 bucket.
Answer: A
https://www.examtopics.com/discussions/amazon/view/102175-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Kinesis 데이터 스트림의 데이터 보존 기간은 레코드가 추가된 시점부터 더 이상 액세스할 수 없는 시점까지의 기간입니다. Kinesis 데이터 스트림의 기본 보존 기간은 24 시간이며 최대 8760 시간(365 일)까지 연장할 수 있습니다. 데이터 보존 기간은 AWS Management Console, AWS CLI 또는 Kinesis Data Streams API 를 사용하여 업데이트할 수 있습니다.

시나리오의 요구 사항을 충족하려면 솔루션 설계자가 데이터 보존 기간을 수정하여 Kinesis Data Streams 기본 설정을 업데이트해야 합니다. 솔루션 설계자는 보존 기간을 데이터를 소비하고 S3 에 쓰는 빈도보다 크거나 같은 값으로 늘려야 합니다. 이렇게 하면 회사는 애플리케이션이 Kinesis Data Streams 로 보내는 모든 데이터를 S3 가 수신하도록 할 수 있습니다.

Q403

A developer has an application that uses an AWS Lambda function to upload files to Amazon S3 and needs the required permissions to perform the task. The developer already has an IAM user with valid IAM credentials required for Amazon S3.

What should a solutions architect do to grant the permissions?

A. Add required IAM permissions in the resource policy of the Lambda function.

B. Create a signed request using the existing IAM credentials in the Lambda function.

C. Create a new IAM user and use the existing IAM credentials in the Lambda function.

D. Create an IAM execution role with the required permissions and attach the IAM role to the Lambda function.

Answer: D

https://www.examtopics.com/discussions/amazon/view/102178-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪

Amazon S3 에 파일을 업로드하기 위해 AWS Lambda 함수에 필요한 권한을 부여하려면 솔루션 설계자는 필요한 권한이 있는 IAM 실행 역할을 생성하고 IAM 역할을 Lambda 함수에 연결해야 합니다. 이 접근 방식은 최소 권한 원칙을 따르며 Lambda 함수가 특정 작업을 수행하는 데 필요한 리소스에만 액세스할 수 있도록 합니다.

Q404

A company has deployed a serverless application that invokes an AWS Lambda function when new documents are uploaded to an Amazon S3 bucket. The application uses the Lambda function to process the documents. After a recent marketing campaign, the company noticed that the application did not process many of the documents.

What should a solutions architect do to improve the architecture of this application?

A. Set the Lambda function's runtime timeout value to 15 minutes.

B. Configure an S3 bucket replication policy. Stage the documents in the S3 bucket for later

processing.
C. Deploy an additional Lambda function. Load balance the processing of the documents across the two Lambda functions.
D. Create an Amazon Simple Queue Service (Amazon SQS) queue. Send the requests to the queue. Configure the queue as an event source for Lambda.
Answer: D
https://www.examtopics.com/discussions/amazon/view/102180-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
이 애플리케이션의 아키텍처를 개선하기 위한 최상의 솔루션은 Amazon Simple Queue Service(Amazon SQS)를 사용하여 요청을 버퍼링하고 Lambda 함수에서 S3 버킷을 분리하는 것입니다. 이렇게 하면 문서가 손실되지 않고 Lambda 함수를 사용할 수 없는 경우 나중에 처리할 수 있습니다. 이렇게 하면 문서가 손실되지 않고 Lambda 함수를 사용할 수 없는 경우 나중에 처리할 수 있습니다. Amazon SQS 를 사용하면 아키텍처가 분리되고 Lambda 함수가 확장 가능하고 내결함성 있는 방식으로 문서를 처리할 수 있습니다.

Q405
A solutions architect is designing the architecture for a software demonstration environment. The environment will run on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). The system will experience significant increases in traffic during working hours but is not required to operate on weekends.
Which combination of actions should the solutions architect take to ensure that the system can scale to meet demand? (Choose two)
A. Use AWS Auto Scaling to adjust the ALB capacity based on request rate.
B. Use AWS Auto Scaling to scale the capacity of the VPC internet gateway.
C. Launch the EC2 instances in multiple AWS Regions to distribute the load across Regions.
D. Use a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization.
E. Use scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends. Revert to the default values at the start of the week.
Answer: D, E
https://www.examtopics.com/discussions/amazon/view/102181-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
https://docs.aws.amazon.com/ko_kr/autoscaling/ec2/userguide/as-scaling-target-tracking.html#target-tracking-choose-metrics
대상 추적 조정 정책은 지정된 메트릭과 대상 값을 기반으로 Auto Scaling 그룹의 용량을 조정하는 일종의 동적 조정 정책입니다. 대상 추적 조정 정책은 Auto Scaling 그룹에서 자동으로 확장 또는 축소하여 실제 지표 값을 대상 값 또는 그 근처에 유지할 수 있습니다. 대상 추적 조정 정책은 근무 시간과 같이 애플리케이션에 대한 로드가 예측할 수 없이 자주 변경되는 시나리오에 적합합니다.
시나리오의 요구 사항을 충족하기 위해 솔루션 설계자는 대상 추적 조정 정책을 사용하여 인스턴스 CPU 사용률에 따라 Auto Scaling 그룹을 조정해야 합니다. 인스턴스 CPU 사용률은 애플리케이션에 대한 수요를 반영하는 일반적인 메트릭입니다. 솔루션 설계자는 애플리케이션의 이상적인 평균 CPU 사용률 수준(예: 50%)을 나타내는 목표 값을 지정해야 합니다. 그러면 Auto Scaling 그룹이 해당 수준의 CPU 사용률을 유지하기 위해 확장 또는 축소됩니다.
예약된 조정은 날짜와 시간을 기준으로 조정 작업을 수행하는 일종의 조정 정책입니다.
예약된 조정은 주말과 같이 애플리케이션의 부하가 주기적으로 예측 가능하게 변경되는 시나리오에 적합합니다.
시나리오의 요구 사항을 충족하기 위해 솔루션 설계자는 예약된 조정을 사용하여 Auto Scaling 그룹의 최소, 최대 및 원하는 용량을 주말 동안 0 으로 변경해야 합니다.
이렇게 하면 Auto Scaling 그룹은 작동이 필요하지 않은 주말에 모든 인스턴스를 종료합니다. 솔루션 설계자는 Auto Scaling 그룹이 정상 작동을 재개할 수 있도록 주의 시작 시 기본값으로 되돌려야 합니다.

Q406
A solutions architect is designing a two-tiered architecture that includes a public subnet and a database subnet. The web servers in the public subnet must be open to the internet on port 443. The Amazon RDS for MySQL DB instance in the database subnet must be accessible only to the web servers on port 3306.
Which combination of steps should the solutions architect take to meet these requirements? (Choose two)
A. Create a network ACL for the public subnet. Add a rule to deny outbound traffic to 0.0.0.0/0 on port 3306.
B. Create a security group for the DB instance. Add a rule to allow traffic from the public subnet CIDR block on port 3306.

C. Create a security group for the web servers in the public subnet. Add a rule to allow traffic from 0.0.0.0/0 on port 443.
D. Create a security group for the DB instance. Add a rule to allow traffic from the web servers' security group on port 3306.
E. Create a security group for the DB instance. Add a rule to deny all traffic except traffic from the web servers' security group on port 3306.
Answer: C, D
https://www.examtopics.com/discussions/amazon/view/102183-exam-aws-certified-solutions-architect-associate-saa-c03/

Q407
A company is implementing a shared storage solution for a gaming application that is hosted in the AWS Cloud. The company needs the ability to use Lustre clients to access data. The solution must be fully managed.
Which solution meets these requirements?
A. Create an AWS DataSync task that shares the data as a mountable file system. Mount the file system to the application server.
B. Create an AWS Storage Gateway file gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
C. Create an Amazon Elastic File System (Amazon EFS) file system, and configure it to support Lustre. Attach the file system to the origin server. Connect the application server to the file system.
D. Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.
Answer: D
https://www.examtopics.com/discussions/amazon/view/102184-exam-aws-certified-solutions-architect-associate-saa-c03/

Q408
A company runs an application that receives data from thousands of geographically dispersed remote devices that use UDP. The application processes the data immediately and sends a message back to the device if necessary. No data is stored.
The company needs a solution that minimizes latency for the data transmission from the devices. The solution also must provide rapid failover to another AWS Region.

Which solution will meet these requirements?

A. Configure an Amazon Route 53 failover routing policy. Create a Network Load Balancer (NLB) in each of the two Regions. Configure the NLB to invoke an AWS Lambda function to process the data.

B. Use AWS Global Accelerator. Create a Network Load Balancer (NLB) in each of the two Regions as an endpoint. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the NLProcess the data in Amazon ECS.

C. Use AWS Global Accelerator. Create an Application Load Balancer (ALB) in each of the two Regions as an endpoint. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the ALB. Process the data in Amazon ECS.

D. Configure an Amazon Route 53 failover routing policy. Create an Application Load Balancer (ALB) in each of the two Regions. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the ALB. Process the data in Amazon ECS.

Answer: B

https://www.examtopics.com/discussions/amazon/view/102185-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪

장치에서 데이터를 전송하는 지연 시간을 최소화하고 다른 AWS 영역으로 신속하게 페일오버해야 하는 요구 사항을 충족하기 위해 가장 좋은 솔루션은 네트워크 로드 밸런서(NLB) 및 Amazon Elastic Container Service(Amazon ECS)와 함께 AWS Global Accelerator 를 사용하는 것입니다.

AWS Global Accelerator 는 정적 IP 주소(Anycast)를 사용하여 트래픽을 최적의 AWS 끝점으로 라우팅하여 애플리케이션의 가용성과 성능을 향상시키는 서비스입니다. Global Accelerator 를 사용하면 트래픽을 여러 지역 및 끝점으로 유도하고 다른 AWS 지역으로 자동 페일오버를 제공할 수 있습니다.

Q409

A solutions architect must migrate a Windows Internet Information Services (IIS) web application to AWS. The application currently relies on a file share hosted in the user's on-premises network-attached storage (NAS). The solutions architect has proposed migrating the IIS web servers to Amazon EC2 instances in multiple Availability Zones that are

connected to the storage solution, and configuring an Elastic Load Balancer attached to the instances.

Which replacement to the on-premises file share is MOST resilient and durable?

A. Migrate the file share to Amazon RDS.

B. Migrate the file share to AWS Storage Gateway.

C. Migrate the file share to Amazon FSx for Windows File Server.

D. Migrate the file share to Amazon Elastic File System (Amazon EFS).

Answer: C

https://www.examtopics.com/discussions/amazon/view/102186-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪

이 대답은 Windows IIS 웹 서버와 호환되는 온-프레미스 파일 공유에 대한 탄력적이고 내구성 있는 대체를 제공하기 때문에 정확합니다. Amazon FSx for Windows File Server 는 Windows Server 에 구축된 공유 파일 스토리지를 제공하는 완전 관리형 서비스입니다. SMB 프로토콜을 지원하고 Windows 기반 애플리케이션에 대한 원활한 액세스 및 인증을 가능하게 하는 Microsoft Active Directory 와 통합됩니다. Amazon FSx for Windows File Server 는 또한 다음과 같은 이점을 제공합니다.

복원력: Amazon FSx for Windows File Server 는 고가용성 및 장애 조치 보호를 제공하는 여러 가용 영역에 배포할 수 있습니다. 또한 자동 백업 및 복원은 물론 문제를 감지하고 수정하는 자가 치유 기능도 지원합니다.

내구성: Windows File Server 용 Amazon FSx 는 가용 영역 내외에서 데이터를 복제하고 내구성이 뛰어난 스토리지 장치에 데이터를 저장합니다. 또한 유휴 및 전송 중 암호화는 물론 파일 액세스 감사 및 데이터 중복 제거를 지원합니다.

성능: Windows File Server 용 Amazon FSx 는 파일 작업을 위한 일관된 1 밀리초 미만의 지연 시간과 높은 처리량을 제공합니다. 또한 SSD 스토리지, 분산 파일 시스템(DFS) 네임스페이스 및 복제와 같은 기본 Windows 기능, 사용자 중심 성능 확장을 지원합니다.

Q410

A company is deploying a new application on Amazon EC2 instances. The application writes data to Amazon Elastic Block Store (Amazon EBS) volumes. The company needs to ensure that all data that is written to the EBS volumes is encrypted at rest.

Which solution will meet this requirement?

A. Create an IAM role that specifies EBS encryption. Attach the role to the EC2 instances.

B. Create the EBS volumes as encrypted volumes. Attach the EBS volumes to the EC2

instances.
C. Create an EC2 instance tag that has a key of Encrypt and a value of True. Tag all instances that require encryption at the EBS level.
D. Create an AWS Key Management Service (AWS KMS) key policy that enforces EBS encryption in the account. Ensure that the key policy is active.
Answer: B
https://www.examtopics.com/discussions/amazon/view/102187-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
EBS 볼륨에 기록되는 모든 데이터가 유휴 상태에서 암호화되도록 보장하는 요구 사항을 충족하는 솔루션은 B 입니다. EBS 볼륨을 암호화된 볼륨으로 생성하고 암호화된 EBS 볼륨을 EC2 인스턴스에 연결합니다. EBS 볼륨을 생성할 때 볼륨 암호화 여부를 지정할 수 있습니다. 볼륨을 암호화하도록 선택한 경우 볼륨에 기록된 모든 데이터는 AWS 관리형 키를 사용하여 유휴 상태에서 자동으로 암호화됩니다. 또한 AWS KMS 에 저장된 고객 관리형 키(CMK)를 사용하여 EBS 볼륨을 암호화하고 보호할 수 있습니다. 암호화된 EBS 볼륨을 생성하고 EC2 인스턴스에 연결하여 볼륨에 기록된 모든 데이터가 유휴 상태에서 암호화되도록 할 수 있습니다.

Q411
A company has a web application with sporadic usage patterns. There is heavy usage at the beginning of each month, moderate usage at the start of each week, and unpredictable usage during the week. The application consists of a web server and a MySQL database server running inside the data center. The company would like to move the application to the AWS Cloud, and needs to select a cost-effective database platform that will not require database modifications.
Which solution will meet these requirements?
A. Amazon DynamoDB
B. Amazon RDS for MySQL
C. MySQL-compatible Amazon Aurora Serverless
D. MySQL deployed on Amazon EC2 in an Auto Scaling group
Answer: C
https://www.examtopics.com/discussions/amazon/view/102188-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
Amazon RDS for MySQL 은 클라우드에서 MySQL 배포를 쉽게 설정, 운영 및 확장할 수 있는 완전관리형 관계형 데이터베이스 서비스입니다. Amazon Aurora Serverless 는 Amazon Aurora(MySQL 호환 버전)에 대한 온디맨드 자동 확장 구성으로, 데이터베이스가 애플리케이션의 요구 사항에 따라 자동으로 시작, 종료 및 용량 확장 또는 축소됩니다.
간헐적이거나 예측할 수 없는 워크로드를 위한 간단하고 비용 효율적인 옵션입니다.

Q412
An image-hosting company stores its objects in Amazon S3 buckets. The company wants to avoid accidental exposure of the objects in the S3 buckets to the public. All S3 objects in the entire AWS account need to remain private.
Which solution will meet these requirements?
A. Use Amazon GuardDuty to monitor S3 bucket policies. Create an automatic remediation action rule that uses an AWS Lambda function to remediate any change that makes the objects public.
B. Use AWS Trusted Advisor to find publicly accessible S3 buckets. Configure email notifications in Trusted Advisor when a change is detected. Manually change the S3 bucket policy if it allows public access.
C. Use AWS Resource Access Manager to find publicly accessible S3 buckets. Use Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function when a change is detected. Deploy a Lambda function that programmatically remediates the change.
D. Use the S3 Block Public Access feature on the account level. Use AWS Organizations to create a service control policy (SCP) that prevents IAM users from changing the setting. Apply the SCP to the account.
Answer: D
https://www.examtopics.com/discussions/amazon/view/102189-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
S3 퍼블릭 액세스 차단 기능을 사용하면 계정 내의 S3 버킷 및 객체에 대한 퍼블릭 액세스를 제한할 수 있습니다. 버킷 정책 설정에 관계없이 계정 수준에서 이 기능을 활성화하여 S3 버킷이 공개되지 않도록 할 수 있습니다. AWS Organizations 를 사용하여 IAM 사용자가 이 설정을 변경하지 못하도록 SCP(서비스 제어 정책)를 계정에 적용하여 모든 S3 객체가 비공개로 유지되도록 할 수 있습니다. 이는 최소한의 운영 오버헤드가

필요한 간단하고 효과적인 솔루션입니다.

Q413

An ecommerce company is experiencing an increase in user traffic. The company's store is deployed on Amazon EC2 instances as a two-tier web application consisting of a web tier and a separate database tier. As traffic increases, the company notices that the architecture is causing significant delays in sending timely marketing and order confirmation email to users. The company wants to reduce the time it spends resolving complex email delivery issues and minimize operational overhead.

What should a solutions architect do to meet these requirements?

A. Create a separate application tier using EC2 instances dedicated to email processing.

B. Configure the web instance to send email through Amazon Simple Email Service (Amazon SES).

C. Configure the web instance to send email through Amazon Simple Notification Service (Amazon SNS).

D. Create a separate application tier using EC2 instances dedicated to email processing. Place the instances in an Auto Scaling group.

Answer: B

https://www.examtopics.com/discussions/amazon/view/102190-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪

Amazon SES 는 기업이 자체 이메일 주소와 도메인을 사용하여 이메일을 보내고 받을 수 있도록 하는 비용 효율적이고 확장 가능한 이메일 서비스입니다. Amazon SES 를 통해 이메일을 보내도록 웹 인스턴스를 구성하는 것은 복잡한 이메일 전송 문제를 해결하는 데 소요되는 시간을 줄이고 운영 오버헤드를 최소화할 수 있는 간단하고 효과적인 솔루션입니다.

Q414

A company has a business system that generates hundreds of reports each day. The business system saves the reports to a network share in CSV format. The company needs to store this data in the AWS Cloud in near-real time for analysis.

Which solution will meet these requirements with the LEAST administrative overhead?

A. Use AWS DataSync to transfer the files to Amazon S3. Create a scheduled task that runs

at the end of each day.
B. Create an Amazon S3 File Gateway. Update the business system to use a new network share from the S3 File Gateway.
C. Use AWS DataSync to transfer the files to Amazon S3. Create an application that uses the DataSync API in the automation workflow.
D. Deploy an AWS Transfer for SFTP endpoint. Create a script that checks for new files on the network share and uploads the new files by using SFTP.
Answer: B
https://www.examtopics.com/discussions/amazon/view/103452-exam-aws-certified-solutions-architect-associate-saa-c03/

Q415
A company is storing petabytes of data in Amazon S3 Standard. The data is stored in multiple S3 buckets and is accessed with varying frequency. The company does not know access patterns for all the data. The company needs to implement a solution for each S3 bucket to optimize the cost of S3 usage.
Which solution will meet these requirements with the MOST operational efficiency?
A. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering.
B. Use the S3 storage class analysis tool to determine the correct tier for each object in the S3 bucket. Move each object to the identified storage tier.
C. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Glacier Instant Retrieval.
D. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 One Zone-Infrequent Access (S3 One Zone-IA).
Answer: A
https://www.examtopics.com/discussions/amazon/view/103404-exam-aws-certified-solutions-architect-associate-saa-c03/

Q416
A rapidly growing global ecommerce company is hosting its web application on AWS. The web application includes static content and dynamic content. The website stores online transaction processing (OLTP) data in an Amazon RDS database The website's users are experiencing slow page loads.

Which combination of actions should a solutions architect take to resolve this issue? (Choose two)

A. Configure an Amazon Redshift cluster.

B. Set up an Amazon CloudFront distribution.

C. Host the dynamic web content in Amazon S3.

D. Create a read replica for the RDS DB instance.

E. Configure a Multi-AZ deployment for the RDS DB instance.

Answer: B, D

https://www.examtopics.com/discussions/amazon/view/103423-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

AWS 에서 호스팅되는 빠르게 성장하는 전자 상거래 웹 사이트의 느린 페이지 로드 문제를 해결하기 위해 솔루션 설계자는 다음 두 가지 조치를 취할 수 있습니다.

1. Amazon CloudFront 배포 설정

2. RDS DB 인스턴스에 대한 읽기 전용 복제본 생성

Amazon Redshift 클러스터 구성은 Redshift 가 데이터 웨어하우징 서비스이고 일반적으로 대량 데이터의 분석 처리에 사용되기 때문에 이 문제와 관련이 없습니다.

S3 는 웹 애플리케이션 서버가 아니라 객체 스토리지 서비스이기 때문에 Amazon S3 에서 동적 웹 콘텐츠를 호스팅해도 성능이 반드시 향상되는 것은 아닙니다. S3 는 정적 웹 콘텐츠를 호스팅하는 데 사용할 수 있지만 S3 는 서버 측 스크립팅 또는 처리를 지원하지 않기 때문에 동적 웹 콘텐츠를 호스팅하는 데 적합하지 않을 수 있습니다.

RDS DB 인스턴스에 대해 다중 AZ 배포를 구성하면 고가용성이 향상되지만 반드시 성능이 향상되는 것은 아닙니다.

Q417

A company uses Amazon EC2 instances and AWS Lambda functions to run its application. The company has VPCs with public subnets and private subnets in its AWS account. The EC2 instances run in a private subnet in one of the VPCs. The Lambda functions need direct network access to the EC2 instances for the application to work.

The application will run for at least 1 year. The company expects the number of Lambda functions that the application uses to increase during that time. The company wants to maximize its savings on all application resources and to keep network latency between the services low.

Which solution will meet these requirements?

A. Purchase an EC2 Instance Savings Plan Optimize the Lambda functions' duration and memory usage and the number of invocations. Connect the Lambda functions to the private subnet that contains the EC2 instances.
B. Purchase an EC2 Instance Savings Plan Optimize the Lambda functions' duration and memory usage, the number of invocations, and the amount of data that is transferred. Connect the Lambda functions to a public subnet in the same VPC where the EC2 instances run.
C. Purchase a Compute Savings Plan. Optimize the Lambda functions' duration and memory usage, the number of invocations, and the amount of data that is transferred. Connect the Lambda functions to the private subnet that contains the EC2 instances.
D. Purchase a Compute Savings Plan. Optimize the Lambda functions' duration and memory usage, the number of invocations, and the amount of data that is transferred. Keep the Lambda functions in the Lambda service VPC.
Answer: C
https://www.examtopics.com/discussions/amazon/view/103598-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Compute Savings Plan 을 구매함으로써 회사는 EC2 인스턴스와 Lambda 기능을 모두 실행하는 비용을 절약할 수 있습니다. Lambda 함수는 AWS 서비스용 VPC 엔드포인트 또는 VPC 피어링 연결을 통해 EC2 인스턴스가 포함된 프라이빗 서브넷에 연결할 수 있습니다. 이렇게 하면 사설 네트워크 내에서 트래픽을 유지하면서 EC2 인스턴스에 대한 직접 네트워크 액세스를 제공하여 네트워크 대기 시간을 최소화하는 데 도움이 됩니다. Lambda 함수의 지속 시간, 메모리 사용량, 호출 수 및 전송된 데이터 양을 최적화하면 비용을 추가로 최소화하고 성능을 개선하는 데 도움이 될 수 있습니다. 또한 프라이빗 서브넷을 사용하면 보안 모범 사례인 퍼블릭 인터넷에서 EC2 인스턴스에 직접 액세스할 수 없도록 하는 데 도움이 됩니다.

Q418
A solutions architect needs to allow team members to access Amazon S3 buckets in two different AWS accounts: a development account and a production account. The team currently has access to S3 buckets in the development account by using unique IAM users that are assigned to an IAM group that has appropriate permissions in the account.
The solutions architect has created an IAM role in the production account. The role has a policy that grants access to an S3 bucket in the production account.

Which solution will meet these requirements while complying with the principle of least privilege?

A. Attach the Administrator Access policy to the development account users.

B. Add the development account as a principal in the trust policy of the role in the production account.

C. Turn off the S3 Block Public Access feature on the S3 bucket in the production account.

D. Create a user in the production account with unique credentials for each team member.

Answer: B

https://www.examtopics.com/discussions/amazon/view/103585-exam-aws-certified-solutions-architect-associate-saa-c03/

Q419

A company uses AWS Organizations with all features enabled and runs multiple Amazon EC2 workloads in the ap-southeast-2 Region. The company has a service control policy (SCP) that prevents any resources from being created in any other Region. A security policy requires the company to encrypt all data at rest.

An audit discovers that employees have created Amazon Elastic Block Store (Amazon EBS) volumes for EC2 instances without encrypting the volumes. The company wants any new EC2 instances that any IAM user or root user launches in ap-southeast-2 to use encrypted EBS volumes. The company wants a solution that will have minimal effect on employees who create EBS volumes.

Which combination of steps will meet these requirements? (Choose two)

A. In the Amazon EC2 console, select the EBS encryption account attribute and define a default encryption key.

B. Create an IAM permission boundary. Attach the permission boundary to the root organizational unit (OU). Define the boundary to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false.

C. Create an SCP. Attach the SCP to the root organizational unit (OU). Define the SCP to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false.

D. Update the IAM policies for each account to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false.

E. In the Organizations management account, specify the Default EBS volume encryption setting.

Answer: C, E

https://www.examtopics.com/discussions/amazon/view/109268-exam-aws-certified-sol

utions-architect-associate-saa-c03/

설명:
서비스 제어 정책(SCP)은 조직에서 권한을 관리하는 데 사용할 수 있는 정책 유형입니다. SCP 는 조직의 모든 계정에 대해 사용 가능한 최대 권한에 대한 중앙 제어를 제공하므로 계정이 조직의 액세스 제어 지침을 준수하도록 할 수 있습니다.
ec2:Encrypted 조건이 false 일 때 SCP 를 사용하여 ec2:CreateVolume 작업을 거부할 수 있습니다. 즉, 루트 OU 아래 계정의 모든 사용자 또는 역할은 암호화되지 않은 EBS 볼륨을 생성할 수 없습니다. 이 솔루션은 필요에 따라 암호화된 볼륨을 계속 생성할 수 있으므로 EBS 볼륨을 생성하는 직원에게 최소한의 영향을 미칩니다.
참조:
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

Q420
A company wants to use an Amazon RDS for PostgreSQL DB cluster to simplify time-consuming database administrative tasks for production database workloads. The company wants to ensure that its database is highly available and will provide automatic failover support in most scenarios in less than 40 seconds. The company wants to offload reads off of the primary instance and keep costs as low as possible.
Which solution will meet these requirements?
A. Use an Amazon RDS Multi-AZ DB instance deployment. Create one read replica and point the read workload to the read replica.
B. Use an Amazon RDS Multi-AZ DB duster deployment Create two read replicas and point the read workload to the read replicas.
C. Use an Amazon RDS Multi-AZ DB instance deployment. Point the read workload to the secondary instances in the Multi-AZ pair.
D. Use an Amazon RDS Multi-AZ DB cluster deployment Point the read workload to the reader endpoint.
Answer: D
https://www.examtopics.com/discussions/amazon/view/109269-exam-aws-certified-solutions-architect-associate-saa-c03/

Q421

A company runs a highly available SFTP service. The SFTP service uses two Amazon EC2 Linux instances that run with elastic IP addresses to accept traffic from trusted IP sources on the internet. The SFTP service is backed by shared storage that is attached to the instances. User accounts are created and managed as Linux users in the SFTP servers.

The company wants a serverless option that provides high IOPS performance and highly configurable security. The company also wants to maintain control over user permissions.

Which solution will meet these requirements?

A. Create an encrypted Amazon Elastic Block Store (Amazon EBS) volume. Create an AWS Transfer Family SFTP service with a public endpoint that allows only trusted IP addresses. Attach the EBS volume to the SFTP service endpoint. Grant users access to the SFTP service.

B. Create an encrypted Amazon Elastic File System (Amazon EFS) volume. Create an AWS Transfer Family SFTP service with elastic IP addresses and a VPC endpoint that has internet-facing access. Attach a security group to the endpoint that allows only trusted IP addresses. Attach the EFS volume to the SFTP service endpoint. Grant users access to the SFTP service.

C. Create an Amazon S3 bucket with default encryption enabled. Create an AWS Transfer Family SFTP service with a public endpoint that allows only trusted IP addresses. Attach the S3 bucket to the SFTP service endpoint. Grant users access to the SFTP service.

D. Create an Amazon S3 bucket with default encryption enabled. Create an AWS Transfer Family SFTP service with a VPC endpoint that has internal access in a private subnet. Attach a security group that allows only trusted IP addresses. Attach the S3 bucket to the SFTP service endpoint. Grant users access to the SFTP service.

Answer: B

https://www.examtopics.com/discussions/amazon/view/109270-exam-aws-certified-solutions-architect-associate-saa-c03/

Q422

A company is developing a new machine learning (ML) model solution on AWS. The models are developed as independent microservices that fetch approximately 1 GB of model data from Amazon S3 at startup and load the data into memory. Users access the models through an asynchronous API. Users can send a request or a batch of requests and specify where the results should be sent.

The company provides models to hundreds of users. The usage patterns for the models are irregular. Some models could be unused for days or weeks. Other models could receive

batches of thousands of requests at a time.
Which design should a solutions architect recommend to meet these requirements?
A. Direct the requests from the API to a Network Load Balancer (NLB). Deploy the models as AWS Lambda functions that are invoked by the NLB.
B. Direct the requests from the API to an Application Load Balancer (ALB). Deploy the models as Amazon Elastic Container Service (Amazon ECS) services that read from an Amazon Simple Queue Service (Amazon SQS) queue. Use AWS App Mesh to scale the instances of the ECS cluster based on the SQS queue size.
C. Direct the requests from the API into an Amazon Simple Queue Service (Amazon SQS) queue. Deploy the models as AWS Lambda functions that are invoked by SQS events. Use AWS Auto Scaling to increase the number of vCPUs for the Lambda functions based on the SQS queue size.
D. Direct the requests from the API into an Amazon Simple Queue Service (Amazon SQS) queue. Deploy the models as Amazon Elastic Container Service (Amazon ECS) services that read from the queue. Enable AWS Auto Scaling on Amazon ECS for both the cluster and copies of the service based on the queue size.
Answer: D
https://www.examtopics.com/discussions/amazon/view/109280-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
이 대답은 불규칙하고 예측할 수 없는 사용 패턴을 처리할 수 있는 독립적인 마이크로 서비스로 ML 모델을 실행하기 위한 요구 사항을 충족하기 때문에 정확합니다. API 의 요청을 Amazon SQS 대기열로 보내면 회사는 모델 실행에서 요청 처리를 분리하고 수요 급증으로 인해 요청이 손실되지 않도록 할 수 있습니다. 대기열에서 읽는 Amazon ECS 서비스로 모델을 배포함으로써 회사는 컨테이너를 활용하여 각 모델을 마이크로 서비스로 격리 및 패키징하고 시작 시 S3 에서 모델 데이터를 가져올 수 있습니다. 대기열 크기에 따라 서비스의 클러스터와 복사본 모두에 대해 Amazon ECS 에서 AWS Auto Scaling 을 활성화함으로써 회사는 클러스터의 EC2 인스턴스 수와 각 서비스의 작업 수를 성능을 요구하고 최적화합니다.

참조:
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html
https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html
https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-ecs.html

Q423

A solutions architect wants to use the following JSON text as an identity-based policy to grant specific permissions:

```
{    "Statement": [
        {
            "Action": [
                "ssm:ListDocuments",
                "ssm:GetDocument"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Sid": ""
        }
    ],
    "Version": "2012-10-17"
}
```

Which IAM principals can the solutions architect attach this policy to? (Choose two)

A. Role

B. Group

C. Organization

D. Amazon Elastic Container Service (Amazon ECS) resource

E. Amazon EC2 resource

Answer: A, B

https://www.examtopics.com/discussions/amazon/view/109281-exam-aws-certified-solutions-architect-associate-saa-c03/

Q424

A company is running a custom application on Amazon EC2 On-Demand Instances. The application has frontend nodes that need to run 24 hours a day, 7 days a week and backend nodes that need to run only for a short time based on workload. The number of backend nodes varies during the day.

The company needs to scale out and scale in more instances based on workload.

Which solution will meet these requirements MOST cost-effectively?

A. Use Reserved Instances for the frontend nodes. Use AWS Fargate for the backend nodes.

B. Use Reserved Instances for the frontend nodes. Use Spot Instances for the backend nodes.

C. Use Spot Instances for the frontend nodes. Use Reserved Instances for the backend nodes.
D. Use Spot Instances for the frontend nodes. Use AWS Fargate for the backend nodes.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109283-exam-aws-certified-solutions-architect-associate-saa-c03/

Q425
A company uses high block storage capacity to runs its workloads on premises. The company's daily peak input and output transactions per second are not more than 15,000 IOPS. The company wants to migrate the workloads to Amazon EC2 and to provision disk performance independent of storage capacity.
Which Amazon Elastic Block Store (Amazon EBS) volume type will meet these requirements MOST cost-effectively?
A. GP2 volume type
B. io2 volume type
C. GP3 volume type
D. io1 volume type
Answer: C
https://www.examtopics.com/discussions/amazon/view/109282-exam-aws-certified-solutions-architect-associate-saa-c03/

Q426
A company needs to store data from its healthcare application. The application's data frequently changes. A new regulation requires audit access at all levels of the stored data. The company hosts the application on an on-premises infrastructure that is running out of storage capacity. A solutions architect must securely migrate the existing data to AWS while satisfying the new regulation.
Which solution will meet these requirements?
A. Use AWS DataSync to move the existing data to Amazon S3. Use AWS CloudTrail to log data events.
B. Use AWS Snowcone to move the existing data to Amazon S3. Use AWS CloudTrail to log management events.
C. Use Amazon S3 Transfer Acceleration to move the existing data to Amazon S3. Use AWS

CloudTrail to log data events.
D. Use AWS Storage Gateway to move the existing data to Amazon S3. Use AWS CloudTrail to log management events.
Answer: A
https://www.examtopics.com/discussions/amazon/view/109278-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 답변은 기존 데이터를 AWS 로 안전하게 마이그레이션하는 요구 사항을 충족하고 새로운 규정을 충족하기 때문에 정답입니다. AWS DataSync 는 온프레미스 스토리지와 Amazon S3 간에 대량의 데이터를 온라인으로 쉽게 이동할 수 있게 해주는 서비스입니다. DataSync 는 전송 중인 데이터를 자동으로 암호화하고 전송 중에 데이터 무결성을 확인합니다. AWS CloudTrail 은 계정에 대한 AWS API 호출을 기록하고 로그 파일을 Amazon S3 에 전달하는 서비스입니다. CloudTrail 은 S3 객체 수준 API 활동과 같이 AWS 계정의 리소스에서 또는 리소스 내에서 수행된 리소스 작업을 보여주는 데이터 이벤트를 기록할 수 있습니다. CloudTrail 을 사용하여 데이터 이벤트를 기록하면 저장된 데이터의 모든 수준에서 액세스를 감사할 수 있습니다.

참조:
https://docs.aws.amazon.com/datasync/latest/userguide/what-is-datasync.html
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-data-events-withcloudtrail.html

Q427
A solutions architect is implementing a complex Java application with a MySQL database. The Java application must be deployed on Apache Tomcat and must be highly available.
What should the solutions architect do to meet these requirements?
A. Deploy the application in AWS Lambda. Configure an Amazon API Gateway API to connect with the Lambda functions.
B. Deploy the application by using AWS Elastic Beanstalk. Configure a load-balanced environment and a rolling deployment policy.
C. Migrate the database to Amazon ElastiCache. Configure the ElastiCache security group to allow access from the application.
D. Launch an Amazon EC2 instance. Install a MySQL server on the EC2 instance. Configure the application on the server. Create an AMI. Use the AMI to create a launch template with an

Auto Scaling group.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109279-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
AWS Elastic Beanstalk 는 애플리케이션을 쉽고 빠르게 배포, 관리 및 확장할 수 있는 방법을 제공합니다. Java 및 Apache Tomcat 을 포함한 다양한 플랫폼을 지원합니다. 솔루션 설계자는 Elastic Beanstalk 를 사용하여 Java 애플리케이션을 업로드하고 Apache Tomcat 을 실행하도록 환경을 구성할 수 있습니다.

Q428
A serverless application uses Amazon API Gateway, AWS Lambda, and Amazon DynamoDB. The Lambda function needs permissions to read and write to the DynamoDB table.
Which solution will give the Lambda function access to the DynamoDB table MOST securely?
A. Create an IAM user with programmatic access to the Lambda function. Attach a policy to the user that allows read and write access to the DynamoDB table. Store the access_key_id and secret_access_key parameters as part of the Lambda environment variables. Ensure that other AWS users do not have read and write access to the Lambda function configuration.
B. Create an IAM role that includes Lambda as a trusted service. Attach a policy to the role that allows read and write access to the DynamoDB table. Update the configuration of the Lambda function to use the new role as the execution role.
C. Create an IAM user with programmatic access to the Lambda function. Attach a policy to the user that allows read and write access to the DynamoDB table. Store the access_key_id and secret_access_key parameters in AWS Systems Manager Parameter Store as secure string parameters. Update the Lambda function code to retrieve the secure string parameters before connecting to the DynamoDB table.
D. Create an IAM role that includes DynamoDB as a trusted service. Attach a policy to the role that allows read and write access from the Lambda function. Update the code of the Lambda function to attach to the new role as an execution role.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109285-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪

옵션 B 는 Lambda 를 신뢰할 수 있는 서비스로 포함하는 IAM 역할을 생성할 것을 제안합니다. 즉, 이 역할은 Lambda 함수용으로 특별히 설계되었습니다. 역할에는 DynamoDB 테이블에 대한 필수 읽기 및 쓰기 액세스 권한을 부여하는 정책이 연결되어 있어야 합니다.

Q429

The following IAM policy is attached to an IAM group. This is the only policy applied to the group.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-1"
                }
            }
        },
        {
            "Sid": "2",
            "Effect": "Deny",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {"aws:MultiFactorAuthPresent": false}
            }
        }
    ]
}
```

What are the effective IAM permissions of this policy for group members?

A. Group members are permitted any Amazon EC2 action within the us-east-1 Region. Statements after the Allow permission are not applied.

B. Group members are denied any Amazon EC2 permissions in the us-east-1 Region unless they are logged in with multi-factor authentication (MFA).
C. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for all Regions when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action.
D. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action within the us-east-1 Region.
Answer: D
https://www.examtopics.com/discussions/amazon/view/109286-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
이 답변은 그룹 구성원에 대한 IAM 정책의 영향을 반영하기 때문에 정확합니다. 정책에는 두 개의 문이 있습니다. 하나는 허용 효과가 있고 다른 하나는 거부 효과가 있습니다. Allow 문은 us-east-1 지역 내의 모든 리소스에 대해 EC2 작업을 수행할 수 있는 권한을 부여합니다. Deny 문은 Allow 문을 재정의하고 그룹 구성원이 MFA 로 로그인하지 않는 한 us-east-1 리전 내의 모든 리소스에 대해 ec2:StopInstances 및 ec2:TerminateInstances 작업을 수행할 수 있는 권한을 거부합니다. 따라서 그룹 구성원은 모든 작업을 수행할 수 있습니다. MFA 를 사용하지 않는 한 us-east-1 리전에서 인스턴스 중지 또는 종료를 제외한 EC2 작업.

Q430
A manufacturing company has machine sensors that upload .csv files to an Amazon S3 bucket. These .csv files must be converted into images and must be made available as soon as possible for the automatic generation of graphical reports.
The images become irrelevant after 1 month, but the .csv files must be kept to train machine learning (ML) models twice a year. The ML trainings and audits are planned weeks in advance.
Which combination of steps will meet these requirements MOST cost-effectively? (Choose two)
A. Launch an Amazon EC2 Spot Instance that downloads the .csv files every hour, generates the image files, and uploads the images to the S3 bucket.
B. Design an AWS Lambda function that converts the .csv files into images and stores the

images in the S3 bucket. Invoke the Lambda function when a .csv file is uploaded.
C. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 Glacier 1 day after they are uploaded. Expire the image files after 30 days.
D. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) 1 day after they are uploaded. Expire the image files after 30 days.
E. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 1 day after they are uploaded. Keep the image files in Reduced Redundancy Storage (RRS).
Answer: B, C
https://www.examtopics.com/discussions/amazon/view/109288-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
이러한 답변은 .csv 파일을 이미지로 변환하고 가능한 한 빨리 사용 가능하게 하며 스토리지 비용을 최소화하기 위한 요구 사항을 충족하므로 정확합니다. AWS Lambda 는 서버를 프로비저닝하거나 관리하지 않고 코드를 실행할 수 있는 서비스입니다. AWS Lambda 를 사용하여 .csv 파일을 이미지로 변환하고 이미지를 S3 버킷에 저장하는 함수를 설계할 수 있습니다.
S3 이벤트 알림을 사용하여 .csv 파일이 S3 버킷에 업로드될 때 Lambda 함수를 호출할 수 있습니다. 이렇게 하면 이미지가 생성되어 그래픽 보고서에 가능한 한 빨리 사용할 수 있습니다. S3 수명 주기는 개체가 수명 주기 동안 비용 효율적으로 저장되도록 개체를 관리할 수 있게 해주는 기능입니다. S3 버킷의 .csv 파일 및 이미지 파일에 대한 S3 수명 주기 규칙을 생성하여 비즈니스 요구 사항에 따라 다른 스토리지 클래스로 전환하거나 만료할 수 있습니다. .csv 파일은 몇 주 전에 계획된 ML 교육 및 감사에 1 년에 두 번만 필요하므로 업로드한 지 1 일 후에 S3 Standard 에서 S3 Glacier 로 전환할 수 있습니다. S3 Glacier 는 검색 시간이 몇 분에서 몇 시간에 이르는 안전하고 내구성이 있으며 매우 저렴한 스토리지를 제공하는 데이터 아카이빙용 스토리지 클래스입니다.
이미지 파일은 1 개월이 지나면 관련성이 없어지므로 30 일 후에 만료될 수 있습니다.

참조:
https://docs.aws.amazon.com/lambda/latest/dg/welcome.html
https://docs.aws.amazon.com/AmazonS3/latest/userguide/NotificationHowTo.html
https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html
https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html#sc-

glacier

Q431

A company has developed a new video game as a web application. The application is in a three-tier architecture in a VPC with Amazon RDS for MySQL in the database layer. Several players will compete concurrently online. The game's developers want to display a top-10 scoreboard in near-real time and offer the ability to stop and restore the game while preserving the current scores.

What should a solutions architect do to meet these requirements?

A. Set up an Amazon ElastiCache for Memcached cluster to cache the scores for the web application to display.

B. Set up an Amazon ElastiCache for Redis cluster to compute and cache the scores for the web application to display.

C. Place an Amazon CloudFront distribution in front of the web application to cache the scoreboard in a section of the application.

D. Create a read replica on Amazon RDS for MySQL to run queries to compute the scoreboard and serve the read traffic to the web application.

Answer: B

https://www.examtopics.com/discussions/amazon/view/109274-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪

이 답변은 거의 실시간으로 상위 10 개 점수판을 표시하고 현재 점수를 유지하면서 게임을 중지하고 복원할 수 있는 기능을 제공하는 요구 사항을 충족하므로 정확합니다. Redis 용 Amazon ElastiCache 는 인터넷 규모의 실시간 애플리케이션을 지원하기 위해 1 밀리초 미만의 지연 시간을 제공하는 초고속 인 메모리 데이터 스토어입니다. Redis 용 Amazon ElastiCache 를 사용하여 Redis 용 ElastiCache 클러스터를 설정하여 웹 애플리케이션이 표시할 점수를 계산하고 캐시할 수 있습니다. 정렬된 세트 및 해시와 같은 Redis 데이터 구조를 사용하여 플레이어의 점수를 저장하고 순위를 매길 수 있으며 ZRANGE 및 ZADD 와 같은 Redis 명령을 사용하여 점수를 효율적으로 검색 및 업데이트할 수 있습니다. 또한 스냅샷 및 추가 전용 파일(AOF)과 같은 Redis 지속성 기능을 사용하여 데이터의 특정 시점 복구를 활성화할 수 있으므로 현재 점수를 유지하면서 게임을 중지하고 복원할 수 있습니다.

참조:

https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/WhatIs.html
https://redis.io/topics/data-types
https://redis.io/topics/persistence

Q432

An ecommerce company wants to use machine learning (ML) algorithms to build and train models. The company will use the models to visualize complex scenarios and to detect trends in customer data. The architecture team wants to integrate its ML models with a reporting platform to analyze the augmented data and use the data directly in its business intelligence dashboards.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS Glue to create an ML transform to build and train models. Use Amazon OpenSearch Service to visualize the data.

B. Use Amazon SageMaker to build and train models. Use Amazon QuickSight to visualize the data.

C. Use a pre-built ML Amazon Machine Image (AMI) from the AWS Marketplace to build and train models. Use Amazon OpenSearch Service to visualize the data.

D. Use Amazon QuickSight to build and train models by using calculated fields. Use Amazon QuickSight to visualize the data.

Answer: B

https://www.examtopics.com/discussions/amazon/view/109291-exam-aws-certified-solutions-architect-associate-saa-c03/

Q433

A company is running its production and nonproduction environment workloads in multiple AWS accounts. The accounts are in an organization in AWS Organizations. The company needs to design a solution that will prevent the modification of cost usage tags.

Which solution will meet these requirements?

A. Create a custom AWS Config rule to prevent tag modification except by authorized principals.

B. Create a custom trail in AWS CloudTrail to prevent tag modification.

C. Create a service control policy (SCP) to prevent tag modification except by authorized principals.

D. Create custom Amazon CloudWatch logs to prevent tag modification.

Answer: C
https://www.examtopics.com/discussions/amazon/view/109384-exam-aws-certified-solutions-architect-associate-saa-c03/

Q434
A company hosts its application in the AWS Cloud. The application runs on Amazon EC2 instances behind an Elastic Load Balancer in an Auto Scaling group and with an Amazon DynamoDB table. The company wants to ensure the application can be made available in anotherAWS Region with minimal downtime.
What should a solutions architect do to meet these requirements with the LEAST amount of downtime?
A. Create an Auto Scaling group and a load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.
B. Create an AWS CloudFormation template to create EC2 instances, load balancers, and DynamoDB tables to be launched when needed Configure DNS failover to point to the new disaster recovery Region's load balancer.
C. Create an AWS CloudFormation template to create EC2 instances and a load balancer to be launched when needed. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.
D. Create an Auto Scaling group and load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Create an Amazon CloudWatch alarm to trigger an AWS Lambda function that updates Amazon Route 53 pointing to the disaster recovery load balancer.
Answer: A
https://www.examtopics.com/discussions/amazon/view/109294-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 답변은 기존 데이터를 AWS 로 안전하게 마이그레이션하는 요구 사항을 충족하고 새로운 규정을 충족하기 때문에 정답입니다. AWS DataSync 는 온프레미스 스토리지와 Amazon S3 간에 대량의 데이터를 온라인으로 쉽게 이동할 수 있게 해주는 서비스입니다. DataSync 는 전송 중인 데이터를 자동으로 암호화하고 전송 중에 데이터 무결성을 확인합니다. AWS CloudTrail 은 계정에 대한 AWS API 호출을 기록하고 로그 파일을 Amazon S3 에 전달하는 서비스입니다. CloudTrail 은 S3 객체 수준 API 활동과 같이 AWS 계정의 리소스에서 또는

리소스 내에서 수행된 리소스 작업을 보여주는 데이터 이벤트를 기록할 수 있습니다. CloudTrail 을 사용하여 데이터 이벤트를 기록하면 저장된 데이터의 모든 수준에서 액세스를 감사할 수 있습니다.

참조:
https://docs.aws.amazon.com/datasync/latest/userguide/what-is-datasync.html
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-data-events-withcloudtrail.html

Q435
A company needs to migrate a MySQL database from its on-premises data center to AWS within 2 weeks. The database is 20 TB in size. The company wants to complete the migration with minimal downtime.
Which solution will migrate the database MOST cost-effectively?
A. Order an AWS Snowball Edge Storage Optimized device. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with replication of ongoing changes. Send the Snowball Edge device to AWS to finish the migration and continue the ongoing replication.
B. Order an AWS Snowmobile vehicle. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with ongoing changes. Send the Snowmobile vehicle back to AWS to finish the migration and continue the ongoing replication.
C. Order an AWS Snowball Edge Compute Optimized with GPU device. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with ongoing changes. Send the Snowball device to AWS to finish the migration and continue the ongoing replication.
D. Order a 1 GB dedicated AWS Direct Connect connection to establish a connection with the data center. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with replication of ongoing changes.
Answer: A
https://www.examtopics.com/discussions/amazon/view/109377-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 대답은 가동 중지 시간을 최소화하고 비용 효율적으로 2 주 이내에 20TB MySQL

데이터베이스를 마이그레이션해야 하는 요구 사항을 충족하기 때문에 정답입니다. AWS Snowball Edge Storage Optimized 디바이스에는 최대 80TB 의 사용 가능한 스토리지 공간이 있으며 이는 데이터베이스에 적합합니다. AWS Database Migration Service(AWS DMS)는 소스에서 대상으로 변경 사항을 지속적으로 복제하여 다운타임을 최소화하면서 MySQL 에서 Amazon Aurora, Amazon RDS for MySQL 또는 Amazon EC2 의 MySQL 로 데이터를 마이그레이션할 수 있습니다. AWS Schema Conversion Tool(AWS SCT)은 소스 스키마와 코드를 대상 데이터베이스와 호환되는 형식으로 변환할 수 있습니다. 이러한 서비스를 함께 사용함으로써 회사는 가동 중지 시간과 비용을 최소화하면서 데이터베이스를 AWS 로 마이그레이션할 수 있습니다.
Snowball Edge 디바이스를 다시 AWS 로 배송하여 마이그레이션을 완료하고 데이터베이스가 완전히 마이그레이션될 때까지 지속적인 복제를 계속할 수 있습니다.

참조:
https://docs.aws.amazon.com/snowball/latest/developer-guide/device-differences.html
https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Source.MySQL.html
https://docs.aws.amazon.com/SchemaConversionTool/latest/userguide/CHAP_Source.MySQL.htm

Q436
A company moved its on-premises PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. The company successfully launched a new product. The workload on the database has increased. The company wants to accommodate the larger workload without adding infrastructure.
Which solution will meet these requirements MOST cost-effectively?
A. Buy reserved DB instances for the total workload. Make the Amazon RDS for PostgreSQL DB instance larger.
B. Make the Amazon RDS for PostgreSQL DB instance a Multi-AZ DB instance.
C. Buy reserved DB instances for the total workload. Add another Amazon RDS for PostgreSQL DB instance.
D. Make the Amazon RDS for PostgreSQL DB instance an on-demand DB instance.
Answer: A
https://www.examtopics.com/discussions/amazon/view/109277-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪

이 대답은 인프라를 추가하지 않고 비용을 최소화하지 않고 더 큰 워크로드를 수용하는 요구 사항을 충족하기 때문에 맞습니다. 예약 DB 인스턴스는 계정에서 특정 온디맨드 DB 인스턴스 사용에 적용되는 청구 할인입니다. 예약 DB 인스턴스는 온디맨드 DB 인스턴스 요금에 비해 상당한 할인을 제공합니다. 총 워크로드에 대해 예약된 DB 인스턴스를 구입하고 선결제 없음, 부분 선결제 또는 전체 선결제의 세 가지 결제 옵션 중에서 선택할 수 있습니다. 인스턴스 유형을 더 높은 성능 클래스로 수정하여 Amazon RDS for PostgreSQL DB 인스턴스를 더 크게 만들 수 있습니다. 이렇게 하면 DB 인스턴스의 CPU, 메모리 및 네트워크 용량을 늘리고 늘어난 워크로드를 처리할 수 있습니다.

참조:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithReservedDBInstances.html
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.DBInstanceClass.html

Q437
A company operates an ecommerce website on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. The site is experiencing performance issues related to a high request rate from illegitimate external systems with changing IP addresses. The security team is worried about potential DDoS attacks against the website. The company must block the illegitimate incoming requests in a way that has a minimal impact on legitimate users.
What should a solutions architect recommend?
A. Deploy Amazon Inspector and associate it with the ALB.
B. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.
C. Deploy rules to the network ACLs associated with the ALB to block the incomingtraffic.
D. Deploy Amazon GuardDuty and enable rate-limiting protection when configuring GuardDuty.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109378-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
이 답변은 합법적인 사용자에게 최소한의 영향을 미치는 방식으로 불법적으로 들어오는 요청을 차단하는 요구 사항을 충족하기 때문에 정확합니다. AWS WAF 는 가용성에 영향을

미치거나 보안을 손상시키거나 과도한 리소스를 소비할 수 있는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API 를 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. AWS WAF 는 SQL 삽입 또는 사이트 간 스크립팅과 같은 일반적인 공격 패턴을 차단하는 보안 규칙과 정의한 특정 트래픽 패턴을 필터링하는 규칙을 생성할 수 있도록 하여 트래픽이 애플리케이션에 도달하는 방식을 제어할 수 있습니다. AWS WAF 를 ALB 와 연결하여 악의적인 요청으로부터 웹 애플리케이션을 보호할 수 있습니다. 각 발신 IP 주소에 대한 요청 속도를 추적하고 5 분 이내에 특정 제한을 초과하는 IP 주소의 요청을 차단하도록 AWS WAF 에서 속도 제한 규칙을 구성할 수 있습니다. 이렇게 하면 잠재적인 DDoS 공격을 완화하고 웹 사이트의 성능을 향상시킬 수 있습니다.

참조:
https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html
https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-rate-based.html

Q438
A company wants to share accounting data with an external auditor. The data is stored in an Amazon RDS DB instance that resides in a private subnet. The auditor has its own AWS account and requires its own copy of the database.
What is the MOST secure way for the company to share the database with the auditor?
A. Create a read replica of the database. Configure IAM standard database authentication to grant the auditor access.
B. Export the database contents to text files. Store the files in an Amazon S3 bucket. Create a new IAM user for the auditor. Grant the user access to the S3 bucket.
C. Copy a snapshot of the database to an Amazon S3 bucket. Create an IAM user. Share the user's keys with the auditor to grant access to the object in the S3 bucket.
D. Create an encrypted snapshot of the database. Share the snapshot with the auditor. Allow access to the AWS Key Management Service (AWS KMS) encryption key.
Answer: D
https://www.examtopics.com/discussions/amazon/view/109398-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
이 대답은 안전한 방식으로 감사자와 데이터베이스를 공유하는 요구 사항을 충족하기 때문에 정확합니다. AWS Key Management Service(AWS KMS)를 사용하여 데이터베이스의

암호화된 스냅샷을 생성하여 고객 관리형 키로 스냅샷을 암호화할 수 있습니다. 스냅샷의 권한을 수정하고 감사자의 AWS 계정 ID 를 지정하여 감사자와 스냅샷을 공유할 수 있습니다. 감사자의 계정에 권한을 부여하는 키 정책 설명을 추가하여 AWS KMS 암호화 키에 대한 액세스를 허용할 수도 있습니다. 이렇게 하면 감사자만 자신의 AWS 계정에서 스냅샷에 액세스하고 복원할 수 있습니다.

참조:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ShareSnapshot.html
https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html#key-policy-defaultallow-root-enable-iam

Q439
A solutions architect configured a VPC that has a small range of IP addresses. The number of Amazon EC2 instances that are in the VPC is increasing, and there is an insufficient number of IP addresses for future workloads.
Which solution resolves this issue with the LEAST operational overhead?
A. Add an additional IPv4 CIDR block to increase the number of IP addresses and create additional subnets in the VPC. Create new resources in the new subnets by using the new CIDR.
B. Create a second VPC with additional subnets. Use a peering connection to connect the second VPC with the first VPC Update the routes and create new resources in the subnets of the second VPC.
C. Use AWS Transit Gateway to add a transit gateway and connect a second VPC with the first VPUpdate the routes of the transit gateway and VPCs. Create new resources in the subnets of the second VPC.
D. Create a second VPC. Create a Site-to-Site VPN connection between the first VPC and the second VPC by using a VPN-hosted solution on Amazon EC2 and a virtual private gateway. Update the route between VPCs to the traffic through the VPN. Create new resources in the subnets of the second VPC.
Answer: A
https://www.examtopics.com/discussions/amazon/view/109400-exam-aws-certified-solutions-architect-associate-saa-c03/

Q440

A company used an Amazon RDS for MySQL DB instance during application testing. Before terminating the DB instance at the end of the test cycle, a solutions architect created two backups. The solutions architect created the first backup by using the mysqldump utility to create a database dump. The solutions architect created the second backup by enabling the final DB snapshot option on RDS termination.

The company is now planning for a new test cycle and wants to create a new DB instance from the most recent backup. The company has chosen a MySQL-compatible edition of Amazon Aurora to host the DB instance.

Which solutions will create the new DB instance? (Choose two)

A. Import the RDS snapshot directly into Aurora.

B. Upload the RDS snapshot to Amazon S3. Then import the RDS snapshot into Aurora.

C. Upload the database dump to Amazon S3. Then import the database dump into Aurora.

D. Use AWS Database Migration Service (AWS DMS) to import the RDS snapshot into Aurora.

E. Upload the database dump to Amazon S3. Then use AWS Database Migration Service (AWS DMS) to import the database dump into Aurora.

Answer: A, C

https://www.examtopics.com/discussions/amazon/view/109297-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪

이러한 답변은 최신 백업에서 새 DB 인스턴스를 생성하고 Amazon Aurora 의 MySQL 호환 에디션을 사용하여 DB 인스턴스를 호스팅해야 하는 요구 사항을 충족하기 때문에 정확합니다. MySQL DB 인스턴스와 Aurora DB 클러스터가 동일한 버전의 MySQL 을 실행 중인 경우 RDS 스냅샷을 Aurora 로 직접 가져올 수 있습니다. 예를 들어 MySQL 버전 5.6 스냅샷을 Aurora MySQL 버전 5.6 으로 직접 복원할 수 있지만 MySQL 버전 5.6 스냅샷을 Aurora MySQL 버전 5.7 로 직접 복원할 수는 없습니다. 이 방법은 간단하고 가장 적은 수의 단계가 필요합니다. MySQL DB 인스턴스와 Aurora DB 클러스터가 다른 버전의 MySQL 을 실행 중인 경우 데이터베이스 덤프를 Amazon S3 에 업로드한 다음 Aurora 로 데이터베이스 덤프를 가져올 수 있습니다. 예를 들어 MySQL 버전 5.6 데이터베이스 덤프를 Aurora MySQL 버전 5.7 로 가져올 수 있지만 MySQL 버전 5.6 스냅샷을 Aurora MySQL 버전 5.7 로 직접 복원할 수는 없습니다.

이 방법은 더 유연하며 다른 버전의 MySQL 간에 마이그레이션할 수 있습니다.

참조:

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Migrating.RDSMySQL.Import.html

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Migrating.RDSMySQL.Dump.html

Q441

A company hosts a multi-tier web application on Amazon Linux Amazon EC2 instances behind an Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The company observes that the Auto Scaling group launches more On-Demand Instances when the application's end users access high volumes of static web content. The company wants to optimize cost.

What should a solutions architect do to redesign the application MOST cost-effectively?

A. Update the Auto Scaling group to use Reserved Instances instead of On-Demand Instances.

B. Update the Auto Scaling group to scale by launching Spot Instances instead of On-Demand Instances.

C. Create an Amazon CloudFront distribution to host the static web contents from an Amazon S3 bucket.

D. Create an AWS Lambda function behind an Amazon API Gateway API to host the static website contents.

Answer: C

https://www.examtopics.com/discussions/amazon/view/109423-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪

이 대답은 비용을 최적화하고 데이터베이스의 작업 부하를 줄이는 요구 사항을 충족하므로 정확합니다. Amazon CloudFront 는 .html, .css, .js 및 이미지 파일과 같은 정적 및 동적 웹 콘텐츠를 사용자에게 빠르게 배포하는 콘텐츠 전송 네트워크(CDN) 서비스입니다. CloudFront 는 엣지 로케이션이라고 하는 전 세계 데이터 센터 네트워크를 통해 콘텐츠를 제공합니다. CloudFront 에서 제공하는 콘텐츠를 사용자가 요청하면 지연 시간(시간 지연)이 가장 짧은 엣지 로케이션으로 요청이 라우팅되므로 콘텐츠가 가능한 최상의 성능으로 제공됩니다. Amazon CloudFront 배포를 생성하여 CloudFront 에 대해 정의하는 오리진인 Amazon S3 버킷에서 정적 웹 콘텐츠를 호스팅할 수 있습니다.

이렇게 하면 정적 웹 콘텐츠에 대한 요청을 EC2 인스턴스에서 CloudFront 로 오프로드할 수 있으므로 웹 사이트의 성능과 가용성을 개선하고 EC2 인스턴스 실행 비용을 줄일 수 있습니다.

참조:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html
https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html

Q442
A company stores several petabytes of data across multiple AWS accounts. The company uses AWS Lake Formation to manage its data lake. The company's data science team wants to securely share selective data from its accounts with the company's engineering team for analytical purposes.
Which solution will meet these requirements with the LEAST operational overhead?
A. Copy the required data to a common account. Create an IAM access role in that account. Grant access by specifying a permission policy that includes users from the engineering team accounts as trusted entities.
B. Use the Lake Formation permissions Grant command in each account where the data is stored to allow the required engineering team users to access the data.
C. Use AWS Data Exchange to privately publish the required data to the required engineering team accounts.
D. Use Lake Formation tag-based access control to authorize and grant cross-account permissions for the required data to the engineering team accounts.
Answer: D
https://www.examtopics.com/discussions/amazon/view/109647-exam-aws-certified-solutions-architect-associate-saa-c03/

Q443
A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world. Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.
What should a solutions architect do to accomplish this?
A. Use Amazon S3 with Transfer Acceleration to host the application.
B. Use Amazon S3 with CacheControl headers to host the application.
C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.

D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.
Answer: A
https://www.examtopics.com/discussions/amazon/view/109424-exam-aws-certified-solutions-architect-associate-saa-c03/

Q444
A company has hired a solutions architect to design a reliable architecture for its application. The application consists of one Amazon RDS DB instance and two manually provisioned Amazon EC2 instances that run web servers. The EC2 instances are located in a single Availability Zone.
An employee recently deleted the DB instance, and the application was unavailable for 24 hours as a result. The company is concerned with the overall reliability of its environment.
What should the solutions architect do to maximize reliability of the application's infrastructure?
A. Delete one EC2 instance and enable termination protection on the other EC2 instance. Update the DB instance to be Multi-AZ, and enable deletion protection.
B. Update the DB instance to be Multi-AZ, and enable deletion protection. Place the EC2 instances behind an Application Load Balancer, and run them in an EC2 Auto Scaling group across multiple Availability Zones.
C. Create an additional DB instance along with an Amazon API Gateway and an AWS Lambda function. Configure the application to invoke the Lambda function through API Gateway. Have the Lambda function write the data to the two DB instances.
D. Place the EC2 instances in an EC2 Auto Scaling group that has multiple subnets located in multiple Availability Zones. Use Spot Instances instead of On-Demand Instances. Set up Amazon CloudWatch alarms to monitor the health of the instances Update the DB instance to be Multi-AZ, and enable deletion protection.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109426-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
이 대답은 응용 프로그램 인프라의 안정성을 최대화하기 위한 요구 사항을 충족하기 때문에 정확합니다. DB 인스턴스를 다중 AZ 로 업데이트할 수 있습니다. 즉, Amazon RDS 가 다른 가용 영역에서 동기식 대기 복제본을 자동으로 프로비저닝하고 유지합니다. 기본 DB 인스턴스는 가용 영역 전체에서 대기 복제본으로 동기식으로 복제되어 데이터 중복성을

제공하고 시스템 백업 중에 지연 시간 급증을 최소화합니다.
고가용성으로 DB 인스턴스를 실행하면 계획된 시스템 유지 관리 중에 가용성을 높일 수 있습니다. 또한 DB 인스턴스 장애 및 가용 영역 중단으로부터 데이터베이스를 보호하는 데 도움이 될 수 있습니다. 또한 DB 인스턴스에서 삭제 보호를 활성화하여 어떤 사용자도 DB 인스턴스를 삭제하지 못하도록 할 수 있습니다. 여러 가용 영역에서 EC2 인스턴스와 같은 여러 대상에 수신 애플리케이션 트래픽을 분산하는 Application Load Balancer 뒤에 EC2 인스턴스를 배치할 수 있습니다. 이렇게 하면 애플리케이션의 가용성과 내결함성이 향상됩니다.
여러 가용 영역의 EC2 Auto Scaling 그룹에서 EC2 인스턴스를 실행할 수 있으므로 애플리케이션 로드를 처리하는 데 사용할 수 있는 정확한 수의 EC2 인스턴스를 확보할 수 있습니다. 조정 정책을 사용하여 수요 변화에 따라 Auto Scaling 그룹의 인스턴스 수를 조정할 수 있습니다.

참조:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZSingleStandby.html
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_DeleteInstance.html#USER_DeleteInstance.DeletionProtection
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html
https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html

Q445
A company is storing 700 terabytes of data on a large network-attached storage (NAS) system in its corporate data center. The company has a hybrid environment with a 10 Gbps AWS Direct Connect connection.
After an audit from a regulator, the company has 90 days to move the data to the cloud. The company needs to move the data efficiently and without disruption. The company still needs to be able to access and update the data during the transfer window.
Which solution will meet these requirements?
A. Create an AWS DataSync agent in the corporate data center. Create a data transfer task Start the transfer to an Amazon S3 bucket.
B. Back up the data to AWS Snowball Edge Storage Optimized devices. Ship the devices to an AWS data center. Mount a target Amazon S3 bucket on the on-premises file system.
C. Use DataSync to copy the data directly from local storage to a designated Amazon S3 bucket over the Direct Connect connection.

D. Back up the data on tapes. Ship the tapes to an AWS data center. Mount a target Amazon S3 bucket on the on-premises file system.
Answer: A
https://www.examtopics.com/discussions/amazon/view/109403-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
이 답변은 중단 없이 데이터를 효율적으로 이동하고 전송 기간 동안 데이터에 계속 액세스하고 업데이트할 수 있어야 한다는 요구 사항을 충족하기 때문에 정답입니다. AWS DataSync 는 AWS 로의 데이터 마이그레이션을 간소화 및 가속화하고 온프레미스 스토리지, 엣지 로케이션, 기타 클라우드 및 AWS 스토리지 간에 데이터를 빠르고 안전하게 이동할 수 있도록 지원하는 온라인 데이터 이동 및 검색 서비스입니다. 회사 데이터 센터에서 AWS DataSync 에이전트를 생성하여 Direct Connect 연결을 통해 NAS 시스템을 AWS 에 연결할 수 있습니다. 데이터 전송 작업을 생성하여 소스 위치, 대상 위치 및 데이터 전송 옵션을 지정할 수 있습니다. Amazon S3 버킷으로 전송을 시작하고 작업 진행 상황을 모니터링할 수 있습니다.
DataSync 는 전송 중인 데이터를 자동으로 암호화하고 전송 중에 데이터 무결성을 확인합니다. DataSync 는 증분 전송도 지원합니다. 즉, 마지막 전송 이후 변경된 파일만 복사됩니다. 이렇게 하면 NAS 시스템과 S3 버킷 간에 데이터가 동기화되었는지 확인할 수 있으며 전송 기간 동안 데이터에 액세스하고 데이터를 업데이트할 수 있습니다.

참조:
https://docs.aws.amazon.com/datasync/latest/userguide/what-is-datasync.html
https://docs.aws.amazon.com/datasync/latest/userguide/how-datasync-works.html

Q446
A company stores data in PDF format in an Amazon S3 bucket. The company must follow a legal requirement to retain all new and existing data in Amazon S3 for 7 years.
Which solution will meet these requirements with the LEAST operational overhead?
A. Turn on the S3 Versioning feature for the S3 bucket. Configure S3 Lifecycle to delete the data after 7 years. Configure multi-factor authentication (MFA) delete for all S3 objects.
B. Turn on S3 Object Lock with governance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Recopy all existing objects to bring the existing data into compliance.
C. Turn on S3 Object Lock with compliance retention mode for the S3 bucket. Set the

retention period to expire after 7 years. Recopy all existing objects to bring the existing data into compliance.

D. Turn on S3 Object Lock with compliance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Use S3 Batch Operations to bring the existing data into compliance.

Answer: D

https://www.examtopics.com/discussions/amazon/view/109404-exam-aws-certified-solutions-architect-associate-saa-c03/

Q447

A company has a stateless web application that runs on AWS Lambda functions that are invoked by Amazon API Gateway. The company wants to deploy the application across multiple AWS Regions to provide Regional failover capabilities.

What should a solutions architect do to route traffic to multiple Regions?

A. Create Amazon Route 53 health checks for each Region. Use an active-active failover configuration.

B. Create an Amazon CloudFront distribution with an origin for each Region. Use CloudFront health checks to route traffic.

C. Create a transit gateway. Attach the transit gateway to the API Gateway endpoint in each Region. Configure the transit gateway to route requests.

D. Create an Application Load Balancer in the primary Region. Set the target group to point to the API Gateway endpoint hostnames in each Region.

Answer: A

https://www.examtopics.com/discussions/amazon/view/109405-exam-aws-certified-solutions-architect-associate-saa-c03/

Q448

A company has two VPCs named Management and Production. The Management VPC uses VPNs through a customer gateway to connect to a single device in the data center. The Production VPC uses a virtual private gateway with two attached AWS Direct Connect connections. The Management and Production VPCs both use a single VPC peering connection to allow communication between the applications.

What should a solutions architect do to mitigate any single point of failure in this architecture?

A. Add a set of VPNs between the Management and Production VPCs.
B. Add a second virtual private gateway and attach it to the Management VPC.
C. Add a second set of VPNs to the Management VPC from a second customer gateway device.
D. Add a second VPC peering connection between the Management VPC and the Production VPC.
Answer: C
https://www.examtopics.com/discussions/amazon/view/109499-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
이 답변은 관리 VPC 와 데이터 센터 간의 VPN 연결에 중복성을 제공하기 때문에 정답입니다. 하나의 고객 게이트웨이 디바이스 또는 하나의 VPN 터널을 사용할 수 없게 되더라도 트래픽은 여전히 두 번째 고객 게이트웨이 디바이스와 두 번째 VPN 터널을 통해 흐를 수 있습니다. 이렇게 하면 VPN 연결의 단일 실패 지점이 완화됩니다.

참조:
https://docs.aws.amazon.com/vpn/latest/s2svpn/vpn-redundant-connection.html
https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/VPC/vpn-tunnelredundancy.html

Q449
A company runs its application on an Oracle database. The company plans to quickly migrate to AWS because of limited resources for the database, backup administration, and data center maintenance. The application uses third-party database features that require privileged access.
Which solution will help the company migrate the database to AWS MOST cost-effectively?
A. Migrate the database to Amazon RDS for Oracle. Replace third-party features with cloud services.
B. Migrate the database to Amazon RDS Custom for Oracle. Customize the database settings to support third-party features.
C. Migrate the database to an Amazon EC2 Amazon Machine Image (AMI) for Oracle. Customize the database settings to support third-party features.
D. Migrate the database to Amazon RDS for PostgreSQL by rewriting the application code to remove dependency on Oracle APEX.

Answer: B
https://www.examtopics.com/discussions/amazon/view/109432-exam-aws-certified-solutions-architect-associate-saa-c03/

Q450
A company has a three-tier web application that is in a single server. The company wants to migrate the application to the AWS Cloud. The company also wants the application to align with the AWS Well-Architected Framework and to be consistent with AWS recommended best practices for security, scalability, and resiliency.
Which combination of solutions will meet these requirements? (Choose three)
A. Create a VPC across two Availability Zones with the application's existing architecture. Host the application with existing architecture on an Amazon EC2 instance in a private subnet in each Availability Zone with EC2 Auto Scaling groups. Secure the EC2 instance with security groups and network access control lists (network ACLs).
B. Set up security groups and network access control lists (network ACLs) to control access to the database layer. Set up a single Amazon RDS database in a private subnet.
C. Create a VPC across two Availability Zones. Refactor the application to host the web tier, application tier, and database tier. Host each tier on its own private subnet with Auto Scaling groups for the web tier and application tier.
D. Use a single Amazon RDS database. Allow database access only from the application tier security group.
E. Use Elastic Load Balancers in front of the web tier. Control access by using security groups containing references to each layer's security groups.
F. Use an Amazon RDS database Multi-AZ cluster deployment in private subnets. Allow database access only from application tier security groups.
Answer: C, E, F
https://www.examtopics.com/discussions/amazon/view/109406-exam-aws-certified-solutions-architect-associate-saa-c03/

Q451
A company is migrating its applications and databases to the AWS Cloud. The company will use Amazon Elastic Container Service (Amazon ECS), AWS Direct Connect, and Amazon RDS.
Which activities will be managed by the company's operational team? (Choose three)

A. Management of the Amazon RDS infrastructure layer, operating system, and platforms
B. Creation of an Amazon RDS DB instance and configuring the scheduled maintenance window
C. Configuration of additional software components on Amazon ECS for monitoring, patch management, log management, and host intrusion detection
D. Installation of patches for all minor and major database versions for Amazon RDS
E. Ensure the physical security of the Amazon RDS infrastructure in the data center
F. Encryption of the data that moves in transit through Direct Connect
Answer: B, C, F
https://www.examtopics.com/discussions/amazon/view/109408-exam-aws-certified-solutions-architect-associate-saa-c03/

Q452
A company runs a Java-based job on an Amazon EC2 instance. The job runs every hour and takes 10 seconds to run. The job runs on a scheduled interval and consumes 1 GB of memory. The CPU utilization of the instance is low except for short surges during which the job uses the maximum CPU available. The company wants to optimize the costs to run the job.
Which solution will meet these requirements?
A. Use AWS App2Container (A2C) to containerize the job. Run the job as an Amazon Elastic Container Service (Amazon ECS) task on AWS Fargate with 0.5 virtual CPU (vCPU) and 1 GB of memory.
B. Copy the code into an AWS Lambda function that has 1 GB of memory. Create an Amazon EventBridge scheduled rule to run the code each hour.
C. Use AWS App2Container (A2C) to containerize the job. Install the container in the existing Amazon Machine Image (AMI). Ensure that the schedule stops the container when the task finishes.
D. Configure the existing schedule to stop the EC2 instance at the completion of the job and restart the EC2 instance when the next job starts.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109521-exam-aws-certified-solutions-architect-associate-saa-c03/

Q453

A company wants to implement a backup strategy for Amazon EC2 data and multiple Amazon S3 buckets. Because of regulatory requirements, the company must retain backup files for a specific time period. The company must not alter the files for the duration of the retention period.

Which solution will meet these requirements?

A. Use AWS Backup to create a backup vault that has a vault lock in governance mode. Create the required backup plan.

B. Use Amazon Data Lifecycle Manager to create the required automated snapshot policy.

C. Use Amazon S3 File Gateway to create the backup. Configure the appropriate S3 Lifecycle management.

D. Use AWS Backup to create a backup vault that has a vault lock in compliance mode. Create the required backup plan.

Answer: D

https://www.examtopics.com/discussions/amazon/view/109410-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

AWS Backup 은 컴퓨팅, 스토리지 및 데이터베이스 전반에서 AWS 서비스의 데이터 보호를 중앙 집중화하고 자동화할 수 있는 완전 관리형 서비스입니다. AWS Backup Vault Lock 은 백업 볼트에 대한 보안 및 제어를 강화하는 데 도움이 되는 백업 볼트의 선택적 기능입니다. 규정 준수 모드에서 잠금이 활성화되고 유예 시간이 끝나면 고객, 계정/데이터 소유자 또는 AWS 가 볼트 구성을 변경하거나 삭제할 수 없습니다. 이렇게 하면 보존 기간이 만료되고 규정 요구 사항을 충족할 때까지 백업을 사용할 수 있습니다.

참조:

https://docs.aws.amazon.com/aws-backup/latest/devguide/vaultlock.html

Q454

A company has resources across multiple AWS Regions and accounts. A newly hired solutions architect discovers a previous employee did not provide details about the resources inventory. The solutions architect needs to build and map the relationship details of the various workloads across all accounts.

Which solution will meet these requirements in the MOST operationally efficient way?

A. Use AWS Systems Manager Inventory to generate a map view from the detailed view report.

B. Use AWS Step Functions to collect workload details. Build architecture diagrams of the workloads manually.
C. Use Workload Discovery on AWS to generate architecture diagrams of the workloads.
D. Use AWS X-Ray to view the workload details. Build architecture diagrams with relationships.
Answer: C
https://www.examtopics.com/discussions/amazon/view/109433-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
Workload Discovery on AWS(이전에는 AWS Perspective 라고 함)는 AWS 클라우드 워크로드를 시각화하는 도구입니다. 계정과 리전 전체에서 AWS 리소스의 인벤토리를 유지하고 이들 간의 관계를 매핑하고 웹 UI 에 표시합니다. 또한 AWS 비용 및 사용 보고서 쿼리, 리소스 검색, 아키텍처 다이어그램 저장 및 내보내기 등을 수행할 수 있습니다. 솔루션은 AWS 에서 Workload Discovery 를 사용하여 최소한의 운영 노력으로 모든 계정에서 다양한 워크로드의 관계 세부 정보를 구축하고 매핑할 수 있습니다.
1. AWS Systems Manager Inventory 를 사용하여 상세 보기 보고서에서 지도 보기를 생성합니다. AWS Systems Manager Inventory 는 관리형 인스턴스에서 메타데이터를 수집하여 중앙 Amazon S3 버킷에 저장하는 기능이므로 이 솔루션은 모든 계정에서 다양한 워크로드의 관계 세부 정보를 구축하고 매핑해야 하는 요구 사항을 충족하지 않습니다. 워크로드의 맵 보기 또는 아키텍처 다이어그램을 제공하지 않습니다.
2. AWS Step Functions 를 사용하여 워크로드 세부 정보를 수집합니다. 워크로드의 아키텍처 다이어그램을 수동으로 구축합니다. 이 솔루션은 워크로드 세부 정보 수집을 오케스트레이션하고 아키텍처 다이어그램을 수동으로 구축하기 위해 상태 시스템을 생성 및 관리해야 하므로 최소한의 운영 노력 요구 사항을 충족하지 않습니다.
3. AWS X-Ray 를 사용하여 워크로드 세부 정보 보기 관계가 있는 아키텍처 다이어그램을 구축합니다. 이 솔루션은 워크로드 세부 정보를 수집하고 아키텍처 다이어그램을 수동으로 구축하기 위해 X-Ray SDK 로 애플리케이션을 구성해야 하므로 최소한의 운영 노력 요구 사항을 충족하지 않습니다.

참조:
https://aws.amazon.com/solutions/implementations/workload-discovery-on-aws/

Q455
A company uses AWS Organizations. The company wants to operate some of its AWS

accounts with different budgets. The company wants to receive alerts and automatically prevent provisioning of additional resources on AWS accounts when the allocated budget threshold is met during a specific period.

Which combination of solutions will meet these requirements? (Choose three)

A. Use AWS Budgets to create a budget. Set the budget amount under the Cost and Usage Reports section of the required AWS accounts.

B. Use AWS Budgets to create a budget. Set the budget amount under the Billing dashboards of the required AWS accounts.

C. Create an IAM user for AWS Budgets to run budget actions with the required permissions.

D. Create an IAM role for AWS Budgets to run budget actions with the required permissions.

E. Add an alert to notify the company when each account meets its budget threshold. Add a budget action that selects the IAM identity created with the appropriate config rule to prevent provisioning of additional resources.

F. Add an alert to notify the company when each account meets its budget threshold. Add a budget action that selects the IAM identity created with the appropriate service control policy (SCP) to prevent provisioning of additional resources.

Answer: B, D, F

https://www.examtopics.com/discussions/amazon/view/109522-exam-aws-certified-solutions-architect-associate-saa-c03/

Q456

A company runs applications on Amazon EC2 instances in one AWS Region. The company wants to back up the EC2 instances to a second Region. The company also wants to provision EC2 resources in the second Region and manage the EC2 instances centrally from one AWS account.

Which solution will meet these requirements MOST cost-effectively?

A. Create a disaster recovery (DR) plan that has a similar number of EC2 instances in the second Region. Configure data replication.

B. Create point-in-time Amazon Elastic Block Store (Amazon EBS) snapshots of the EC2 instances. Copy the snapshots to the second Region periodically.

C. Create a backup plan by using AWS Backup. Configure cross-Region backup to the second Region for the EC2 instances.

D. Deploy a similar number of EC2 instances in the second Region. Use AWS DataSync to transfer the data from the source Region to the second Region.

Answer: C

https://www.examtopics.com/discussions/amazon/view/109523-exam-aws-certified-solutions-architect-associate-saa-c03/

Q457

A company that uses AWS is building an application to transfer data to a product manufacturer. The company has its own identity provider (IdP). The company wants the IdP to authenticate application users while the users use the application to transfer data. The company must use Applicability Statement 2 (AS2) protocol.

Which solution will meet these requirements?

A. Use AWS DataSync to transfer the data. Create an AWS Lambda function for IdP authentication.

B. Use Amazon AppFlow flows to transfer the data. Create an Amazon Elastic Container Service (Amazon ECS) task for IdP authentication.

C. Use AWS Transfer Family to transfer the data. Create an AWS Lambda function for IdP authentication.

D. Use AWS Storage Gateway to transfer the data. Create an Amazon Cognito identity pool for IdP authentication.

Answer: C

https://www.examtopics.com/discussions/amazon/view/109524-exam-aws-certified-solutions-architect-associate-saa-c03/

Q458

A solutions architect is designing a RESTAPI in Amazon API Gateway for a cash payback service. The application requires 1 GB of memory and 2 GB of storage for its computation resources. The application will require that the data is in a relational format.

Which additional combination of AWS services will meet these requirements with the LEAST administrative effort? (Choose two)

A. Amazon EC2

B. AWS Lambda

C. Amazon RDS

D. Amazon DynamoDB

E. Amazon Elastic Kubernetes Services (Amazon EKS)

Answer: B, C

https://www.examtopics.com/discussions/amazon/view/109435-exam-aws-certified-sol

utions-architect-associate-saa-c03/

Q459

A company uses AWS Organizations to run workloads within multiple AWS accounts. A tagging policy adds department tags to AWS resources when the company creates tags. An accounting team needs to determine spending on Amazon EC2 consumption. The accounting team must determine which departments are responsible for the costs regardless of AWS account. The accounting team has access to AWS Cost Explorer for all AWS accounts within the organization and needs to access all reports from Cost Explorer. Which solution meets these requirements in the MOST operationally efficient way?

A. From the Organizations management account billing console, activate a user-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name, and filter by EC2.

B. From the Organizations management account billing console, activate an AWS-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name, and filter by EC2.

C. From the Organizations member account billing console, activate a user-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by the tag name, and filter by EC2.

D. From the Organizations member account billing console, activate an AWS-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name, and filter by EC2.

Answer: A

https://www.examtopics.com/discussions/amazon/view/109440-exam-aws-certified-solutions-architect-associate-saa-c03/

Q460

A company wants to securely exchange data between its software as a service (SaaS) application Salesforce account and Amazon S3. The company must encrypt the data at rest by using AWS Key Management Service (AWS KMS) customer managed keys (CMKs). The company must also encrypt the data in transit. The company has enabled API access for the Salesforce account.

A. Create AWS Lambda functions to transfer the data securely from Salesforce to Amazon S3.

B. Create an AWS Step Functions workflow. Define the task to transfer the data securely from Salesforce to Amazon S3.
C. Create Amazon AppFlow flows to transfer the data securely from Salesforce to Amazon S3.
D. Create a custom connector for Salesforce to transfer the data securely from Salesforce to Amazon S3.
Answer: C
https://www.examtopics.com/discussions/amazon/view/109525-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
Amazon AppFlow 는 사용자가 SaaS 애플리케이션과 AWS 서비스 간에 안전하게 데이터를 전송할 수 있도록 하는 완전관리형 통합 서비스입니다. Salesforce 를 소스로, Amazon S3 를 대상으로 지원합니다. 또한 AWS KMS CMK 를 사용하여 유휴 데이터 암호화 및 SSL/TLS1 을 사용하여 전송 중인 데이터 암호화를 지원합니다. Amazon AppFlow 를 사용하면 솔루션이 최소한의 개발 노력으로 요구 사항을 충족할 수 있습니다.
1. 데이터를 Salesforce 에서 Amazon S3 로 안전하게 전송하는 AWS Lambda 함수를 생성합니다. 이 솔루션은 Salesforce 및 Amazon S3 API 와 상호 작용하고 인증, 암호화, 오류 처리 및 모니터링을 처리하기 위한 사용자 지정 코드 작성을 포함하므로 최소한의 개발 노력 요구 사항을 충족하지 않습니다.
2. AWS Step Functions 워크플로 생성 Salesforce 에서 Amazon S3 로 데이터를 안전하게 전송하는 작업을 정의합니다. 이 솔루션은 데이터 전송 작업을 오케스트레이션하기 위한 상태 시스템 정의를 생성하고 실제 데이터 전송을 수행하기 위해 Lambda 함수 또는 기타 서비스를 호출하기 때문에 최소한의 개발 노력 요구 사항을 충족하지 않습니다.
3. Salesforce 용 사용자 지정 커넥터를 생성하여 Salesforce 에서 Amazon S3 로 데이터를 안전하게 전송합니다. 이 솔루션은 Amazon AppFlow 사용자 지정 커넥터 SDK 를 사용하여 Salesforce 용 사용자 지정 커넥터를 구축하고 배포하므로 추가 구성 및 관리가 필요하므로 최소한의 개발 노력 요구 사항을 충족하지 않습니다.

참조 URL: https://aws.amazon.com/appflow/

Q461
A company is developing a mobile gaming app in a single AWS Region. The app runs on multiple Amazon EC2 instances in an Auto Scaling group. The company stores the app data in Amazon DynamoDB. The app communicates by using TCP traffic and UDP traffic between

the users and the servers. The application will be used globally. The company wants to ensure the lowest possible latency for all users.
Which solution will meet these requirements?
A. Use AWS Global Accelerator to create an accelerator. Create an Application Load Balancer (ALB) behind an accelerator endpoint that uses Global Accelerator integration and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the ALB.
B. Use AWS Global Accelerator to create an accelerator. Create a Network Load Balancer (NLB) behind an accelerator endpoint that uses Global Accelerator integration and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the NLB.
C. Create an Amazon CloudFront content delivery network (CDN) endpoint. Create a Network Load Balancer (NLB) behind the endpoint and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the NLB. Update CloudFront to use the NLB as the origin.
D. Create an Amazon CloudFront content delivery network (CDN) endpoint. Create an Application Load Balancer (ALB) behind the endpoint and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the ALB. Update CloudFront to use the ALB as the origin.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109446-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
AWS Global Accelerator 는 글로벌 사용자를 위해 애플리케이션의 성능과 가용성을 향상시키는 네트워킹 서비스입니다. AWS 글로벌 네트워크를 사용하여 사용자 트래픽을 성능 및 상태에 따라 최적의 엔드포인트로 라우팅합니다. 또한 애플리케이션에 대한 고정 진입점 역할을 하고 TCP 및 UDP 프로토콜을 모두 지원하는 고정 IP 주소를 제공합니다. 솔루션은 AWS Global Accelerator 를 사용하여 모든 사용자에게 가능한 최저 지연 시간을 보장할 수 있습니다.
1. AWS Global Accelerator 를 사용하여 가속기를 생성합니다. Global Accelerator 통합을 사용하고 TCP 및 UDP 포트에서 수신 대기하는 가속기 엔드포인트 뒤에 Application Load Balancer(ALB)를 생성합니다. Auto Scaling 그룹을 업데이트하여 ALB 에 인스턴스를 등록합니다. ALB 는 UDP 프로토콜을 지원하지 않으므로 이 솔루션은 작동하지 않습니다.
2. Amazon CloudFront 콘텐츠 전송 네트워크(CDN) 엔드포인트를 생성합니다. 엔드포인트 뒤에 NLB(Network Load Balancer)를 생성하고 TCP 및 UDP 포트에서 수신 대기합니다. Auto Scaling 그룹을 업데이트하여 NLB 에 인스턴스를 등록합니다. NLB 를 오리진으로

사용하도록 CloudFront 를 업데이트합니다. CloudFront 는 UDP 프로토콜을 지원하지 않으므로 이 솔루션은 작동하지 않습니다.
3. Amazon CloudFront 콘텐츠 전송 네트워크(CDN) 엔드포인트를 생성합니다. 엔드포인트 뒤에 Application Load Balancer(ALB)를 생성하고 TCP 및 UDP 포트에서 수신 대기합니다. Auto Scaling 그룹을 업데이트하여 ALB 에 인스턴스를 등록합니다. ALB 를 오리진으로 사용하도록 CloudFront 를 업데이트합니다. CloudFront 및 ALB 는 UDP 프로토콜을 지원하지 않으므로 이 솔루션은 작동하지 않습니다.

참조: https://aws.amazon.com/global-accelerator/

Q462
A company has an application that processes customer orders. The company hosts the application on an Amazon EC2 instance that saves the orders to an Amazon Aurora database. Occasionally when traffic is high the workload does not process orders fast enough.
What should a solutions architect do to write the orders reliably to the database as quickly as possible?
A. Increase the instance size of the EC2 instance when traffic is high. Write orders to Amazon Simple Notification Service (Amazon SNS). Subscribe the database endpoint to the SNS topic.
B. Write orders to an Amazon Simple Queue Service (Amazon SQS) queue. Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database.
C. Write orders to Amazon Simple Notification Service (Amazon SNS). Subscribe the database endpoint to the SNS topic. Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SNS topic.
D. Write orders to an Amazon Simple Queue Service (Amazon SQS) queue when the EC2 instance reaches CPU threshold limits. Use scheduled scaling of EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109653-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪

Amazon SQS는 마이크로서비스, 분산 시스템 및 서버리스 애플리케이션을 분리하고 확장할 수 있는 완전관리형 메시지 대기열 서비스입니다. 애플리케이션은 SQS 대기열에 주문을 기록함으로써 주문 손실 없이 트래픽 급증을 처리할 수 있습니다. Auto Scaling 그룹의 EC2 인스턴스는 SQS 대기열에서 읽고 꾸준한 속도로 데이터베이스로 주문을 처리할 수 있습니다. Application Load Balancer 는 EC2 인스턴스에 부하를 분산하고 상태 확인을 제공할 수 있습니다. 이 솔루션은 질문의 모든 요구 사항을 충족하지만 다른 옵션은 그렇지 않습니다.

참조:
https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/welcome.html
https://aws.amazon.com/architecture/serverless/
https://aws.amazon.com/sqs/

Q463
An IoT company is releasing a mattress that has sensors to collect data about a user's sleep. The sensors will send data to an Amazon S3 bucket. The sensors collect approximately 2 MB of data every night for each mattress. The company must process and summarize the data for each mattress. The results need to be available as soon as possible. Data processing will require 1 GB of memory and will finish within 30 seconds.
Which solution will meet these requirements MOST cost-effectively?
A. Use AWS Glue with a Scala job
B. Use Amazon EMR with an Apache Spark script
C. Use AWS Lambda with a Python script
D. Use AWS Glue with a PySpark job
Answer: C
https://www.examtopics.com/discussions/amazon/view/109501-exam-aws-certified-solutions-architect-associate-saa-c03/

Q464
A company hosts an online shopping application that stores all orders in an Amazon RDS for PostgreSQL Single-AZ DB instance. Management wants to eliminate single points of failure and has asked a solutions architect to recommend an approach to minimize database downtime without requiring any changes to the application code.
Which solution meets these requirements?

A. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance and specifying the Multi-AZ option.
B. Create a new RDS Multi-AZ deployment. Take a snapshot of the current RDS instance and restore the new Multi-AZ deployment with the snapshot.
C. Create a read-only replica of the PostgreSQL database in another Availability Zone. Use Amazon Route 53 weighted record sets to distribute requests across the databases.
D. Place the RDS for PostgreSQL database in an Amazon EC2 Auto Scaling group with a minimum group size of two. Use Amazon Route 53 weighted record sets to distribute requests across instances.
Answer: A
https://www.examtopics.com/discussions/amazon/view/109449-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
기존 단일 AZ DB 인스턴스를 다중 AZ 배포로 변환하려면 AWS Management Console 에서 DB 인스턴스에 해당하는 "수정" 옵션을 사용하십시오.

참고:
https://aws.amazon.com/rds/features/multi-az/

Q465
A company is developing an application to support customer demands. The company wants to deploy the application on multiple Amazon EC2 Nitro-based instances within the same Availability Zone. The company also wants to give the application the ability to write to multiple block storage volumes in multiple EC2 Nitro-based instances simultaneously to achieve higher application availability.
Which solution will meet these requirements?
A. Use General Purpose SSD (gp3) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
B. Use Throughput Optimized HDD (st1) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
C. Use Provisioned IOPS SSD (io2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
D. Use General Purpose SSD (gp2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach

Answer: C
https://www.examtopics.com/discussions/amazon/view/109655-exam-aws-certified-solutions-architect-associate-saa-c03/

Q466
A company designed a stateless two-tier application that uses Amazon EC2 in a single Availability Zone and an Amazon RDS Multi-AZ DB instance. New company management wants to ensure the application is highly available.
What should a solutions architect do to meet this requirement?
A. Configure the application to use Multi-AZ EC2 Auto Scaling and create an Application Load Balancer.
B. Configure the application to take snapshots of the EC2 instances and send them to a different AWS Region.
C. Configure the application to use Amazon Route 53 latency-based routing to feed requests to the application.
D. Configure Amazon Route 53 rules to handle incoming requests and create a Multi-AZ Application Load Balancer.
Answer: A
https://www.examtopics.com/discussions/amazon/view/109450-exam-aws-certified-solutions-architect-associate-saa-c03/

참고:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-availability-zone.html

Q467
A company uses AWS Organizations. A member account has purchased a Compute Savings Plan. Because of changes in the workloads inside the member account, the account no longer receives the full benefit of the Compute Savings Plan commitment. The company uses less than 50% of its purchased compute power.
A. Turn on discount sharing from the Billing Preferences section of the account console in the member account that purchased the Compute Savings Plan.
B. Turn on discount sharing from the Billing Preferences section of the account console in the company's Organizations management account.
C. Migrate additional compute workloads from another AWS account to the account that has

the Compute Savings Plan.
D. Sell the excess Savings Plan commitment in the Reserved Instance Marketplace.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109485-exam-aws-certified-solutions-architect-associate-saa-c03/

Q468
A company is developing a microservices application that will provide a search catalog for customers. The company must use REST APIs to present the frontend of the application to users. The REST APIs must access the backend services that the company hosts in containers in private VPC subnets.
Which solution will meet these requirements?
A. Design a WebSocket API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a private VPC link for API Gateway to access Amazon ECS.
B. Design a REST API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a private VPC link for API Gateway to access Amazon ECS.
C. Design a WebSocket API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a security group for API Gateway to access Amazon ECS.
D. Design a REST API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a security group for API Gateway to access Amazon ECS.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109451-exam-aws-certified-solutions-architect-associate-saa-c03/

Q469
A company stores raw collected data in an Amazon S3 bucket. The data is used for several types of analytics on behalf of the company's customers. The type of analytics requested determines the access pattern on the S3 objects.
The company cannot predict or control the access pattern. The company wants to reduce its S3 costs.

Which solution will meet these requirements?

A. Use S3 replication to transition infrequently accessed objects to S3 Standard-Infrequent Access (S3 Standard-IA)

B. Use S3 Lifecycle rules to transition objects from S3 Standard to Standard-Infrequent Access (S3 Standard-IA)

C. Use S3 Lifecycle rules to transition objects from S3 Standard to S3 Intelligent-Tiering

D. Use S3 Inventory to identify and transition objects that have not been accessed from S3 Standard to S3 Intelligent-Tiering

Answer: C

https://www.examtopics.com/discussions/amazon/view/109452-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪

S3 Intelligent-Tiering 은 액세스 빈도에 따라 가장 비용 효율적인 액세스 계층으로 데이터를 이동하여 스토리지 비용을 자동으로 줄이는 스토리지 클래스입니다. 여기에는 빈번한 액세스와 드문 액세스의 두 가지 액세스 계층이 있습니다. 데이터는 기본적으로 빈번한 액세스 계층에 저장되며 연속 30 일 동안 액세스가 없으면 빈번하지 않은 액세스 계층으로 이동됩니다. 데이터에 다시 액세스하면 자주 액세스하는 tier1 로 다시 이동됩니다. S3 수명 주기 규칙을 사용하여 개체를 S3 Standard 에서 S3 Intelligent-Tiering 으로 전환함으로써 솔루션은 액세스 패턴을 알 수 없거나 변경하는 데이터에 대한 S3 비용을 줄일 수 있습니다.

1. S3 복제를 사용하여 자주 액세스하지 않는 객체를 S3 Standard-Infrequent Access(S3 Standard-IA)로 전환합니다. 이 솔루션은 액세스 패턴을 알 수 없거나 변경하는 데이터에 대한 S3 비용 절감 요구 사항을 충족하지 않습니다. S3 복제는 중복성 또는 규정 준수를 위해 버킷 또는 리전 간에 개체를 복사하는 기능이기 때문입니다. 액세스 빈도에 따라 개체를 다른 스토리지 클래스로 자동으로 이동하지 않습니다.

2. S3 수명 주기 규칙을 사용하여 객체를 S3 Standard 에서 Standard-Infrequent Access(S3 Standard-IA)로 전환합니다. 이 솔루션은 액세스 패턴을 알 수 없거나 변경하는 데이터에 대한 S3 비용 절감 요구 사항을 충족하지 않습니다. S3 Standard-IA 는 S3 Standard 보다 낮은 스토리지 비용을 제공하지만 데이터 액세스에 대한 검색 요금을 부과하는 스토리지 클래스이기 때문입니다. 액세스 패턴이 변화하는 데이터가 아니라 수명이 길고 자주 액세스하지 않는 데이터에 적합합니다.

3. S3 Inventory 를 사용하여 S3 Standard 에서 S3 Intelligent-Tiering 으로 액세스하지 않은 객체를 식별하고 전환합니다. 이 솔루션은 액세스 패턴을 알 수 없거나 변경하는 데이터에 대한 S3 비용 절감 요구 사항을 충족하지 않습니다. S3 Inventory 는 버킷의 객체 및 해당 메타데이터에 대한 보고서를 매일 또는 매주 제공하는 기능이기 때문입니다. 액세스 빈도에

따라 개체를 다른 스토리지 클래스로 자동으로 이동하지 않습니다.
참조 URL: https://aws.amazon.com/s3/storage-classes/intelligent-tiering/
S3 지능형 계층화
액세스 패턴을 예측할 수 없거나 변경될 때 S3 비용을 줄이기 위한 최상의 솔루션입니다. S3 Intelligent-Tiering 은 성능에 미치는 영향이나 검색 비용 없이 액세스 빈도를 기준으로 두 액세스 계층(빈번함 및 비빈번함) 간에 객체를 자동으로 이동합니다. S3 Intelligent-Tiering 에는 거의 액세스하지 않는 개체에 대한 선택적 아카이브 계층도 있습니다. S3 수명 주기 규칙을 사용하여 객체를 S3 Standard 에서 S3 Intelligent-Tiering 으로 전환할 수 있습니다.

참조 URL:
1 https://aws.amazon.com/s3/storage-classes/intelligent-tiering/
2 https://docs.aws.amazon.com/AmazonS3/latest/userguide/using-intelligent-tiering.html
3 https://docs.aws.amazon.com/AmazonS3/latest/userguide/intelligent-tiering-overview.html

Q470
A company has applications hosted on Amazon EC2 instances with IPv6 addresses. The applications must initiate communications with other external applications using the internet. However the company's security policy states that any external service cannot initiate a connection to the EC2 instances.
What should a solutions architect recommend to resolve this issue?
A. Create a NAT gateway and make it the destination of the subnet's route table.
B. Create an internet gateway and make it the destination of the subnet's route table.
C. Create a virtual private gateway and make it the destination of the subnet's route table.
D. Create an egress-only internet gateway and make it the destination of the subnet's route table.
Answer: D
https://www.examtopics.com/discussions/amazon/view/109334-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
외부 전용 인터넷 게이트웨이는 VPC 의 인스턴스에서 인터넷으로 IPv6 을 통한 아웃바운드 통신을 허용하고 인터넷이 인스턴스와의 IPv6 연결을 시작하지 못하도록 하는 VPC 구성

요소입니다. 이것은 회사의 보안 정책 및 요구 사항을 충족합니다. 외부 전용 인터넷 게이트웨이를 사용하려면 IPv6 인터넷 트래픽(::/0)을 외부 전용 인터넷 게이트웨이로 라우팅하는 경로를 서브넷의 라우팅 테이블에 추가해야 합니다.

참조 URL:
1 https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html
2 https://dev.to/aws-builders/what-is-an-egress-only-internet-gateways-in-aws-7gp
3 https://docs.aws.amazon.com/vpc/latest/userguide/route-table-options.html

Q471
A company is creating an application that runs on containers in a VPC. The application stores and accesses data in an Amazon S3 bucket. During the development phase, the application will store and access 1 TB of data in Amazon S3 each day. The company wants to minimize costs and wants to prevent traffic from traversing the internet whenever possible.
Which solution will meet these requirements?
A. Enable S3 Intelligent-Tiering for the S3 bucket.
B. Enable S3 Transfer Acceleration for the S3 bucket.
C. Create a gateway VPC endpoint for Amazon S3. Associate this endpoint with all route tables in the VPC.
D. Create an interface endpoint for Amazon S3 in the VPC. Associate this endpoint with all route tables in the VPC.
Answer: C
https://www.examtopics.com/discussions/amazon/view/109453-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
Amazon S3 용 게이트웨이 VPC 엔드포인트는 인터넷 게이트웨이나 NAT 디바이스가 필요하지 않은 VPC 와 Amazon S3 간의 프라이빗 연결을 가능하게 합니다. 이렇게 하면 비용이 최소화되고 트래픽이 인터넷을 통과하는 것을 방지할 수 있습니다. 게이트웨이 VPC 엔드포인트는 트래픽을 비공개로 Amazon S31 로 라우팅하기 위해 접두사 목록을 VPC 라우팅 테이블의 라우팅 대상으로 사용합니다. 엔드포인트를 VPC 의 모든 라우팅 테이블과 연결하면 모든 서브넷이 엔드포인트를 통해 Amazon S3 에 액세스할 수 있습니다.

옵션 A 는 S3 Intelligent-Tiering 이 변화하는 액세스 패턴을 기반으로 두 액세스 계층 간에

객체를 자동으로 이동하여 스토리지 비용을 최적화하는 스토리지 클래스이기 때문에 올바르지 않습니다. VPC 와 Amazon S3 간의 네트워크 트래픽에는 영향을 미치지 않습니다.

옵션 B 는 올바르지 않습니다. S3 Transfer Acceleration 은 클라이언트와 S3 버킷 간에 장거리에서 파일을 빠르고 쉽고 안전하게 전송할 수 있는 기능이기 때문입니다. 트래픽이 인터넷을 통과하는 것을 막지는 않습니다.

옵션 D 는 Amazon S3 용 인터페이스 VPC 엔드포인트는 각 서브넷에 프라이빗 IP 주소가 있는 탄력적 네트워크 인터페이스(ENI)가 필요한 AWS PrivateLink 에 의해 구동되기 때문에 올바르지 않습니다. 이것은 솔루션에 복잡성과 비용을 추가합니다. 또한 인터페이스 VPC 엔드포인트는 Amazon S3 에 대한 교차 리전 액세스를 지원하지 않습니다.

참조 URL:
https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html
https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html#sc-dynamicdata-access
https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration.html
https://aws.amazon.com/blogs/architecture/choosing-your-vpc-endpoint-strategy-for-amazon-s3/

Q472
A company has a mobile chat application with a data store based in Amazon DynamoDB. Users would like new messages to be read with as little latency as possible. A solutions architect needs to design an optimal solution that requires minimal application changes. Which method should the solutions architect select?
A. Configure Amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use the DAX endpoint.
B. Add DynamoDB read replicas to handle the increased read load. Update the application to point to the read endpoint for the read replicas.
C. Double the number of read capacity units for the new messages table in DynamoDB. Continue to use the existing DynamoDB endpoint.
D. Add an Amazon ElastiCache for Redis cache to the application stack. Update the application to point to the Redis cache endpoint instead of DynamoDB.
Answer: A
https://www.examtopics.com/discussions/amazon/view/109454-exam-aws-certified-sol

utions-architect-associate-saa-c03/

설명: ▪
https://aws.amazon.com/premiumsupport/knowledge-center/dynamodb-high-latency/
Amazon DynamoDB Accelerator(DAX)는 DynamoDB 를 위한 완전 관리형 인 메모리 캐시로, DynamoDB 테이블의 성능을 최대 10 배까지 향상시키고 모든 규모에서 마이크로초 수준의 응답 시간을 제공합니다. DynamoDB API 작업과 호환되며 use1 에 대한 최소한의 코드 변경이 필요합니다. 새 메시지 테이블에 대해 DAX 를 구성함으로써 솔루션은 최소한의 애플리케이션 변경으로 새 메시지를 읽는 대기 시간을 줄일 수 있습니다.
1. 증가된 읽기 로드를 처리하기 위해 DynamoDB 읽기 replicas 를 추가합니다. 읽기 전용 복제본의 읽기 엔드포인트를 가리키도록 애플리케이션을 업데이트합니다. DynamoDB 는 읽기 전용 복제본을 기능으로 지원하지 않으므로 이 솔루션은 작동하지 않습니다. 읽기 전용 복제본은 DynamoDB 가 아닌 Amazon RDS 에서 사용할 수 있습니다.
2. DynamoDB 의 새 메시지 테이블에 대한 읽기 용량 단위 수를 두 배로 늘립니다. 기존 DynamoDB 엔드포인트를 계속 사용합니다. 읽기 용량 단위를 늘리면 성능이나 지연 시간이 아니라 DynamoDB 의 처리량만 증가하므로 이 솔루션은 가능한 한 적은 지연 시간으로 새 메시지를 읽어야 한다는 요구 사항을 충족하지 않습니다.
3. Redis 용 Amazon ElastiCache 캐시를 애플리케이션 스택에 추가합니다. DynamoDB 대신 Redis 캐시 엔드포인트를 가리키도록 애플리케이션을 업데이트합니다. Redis 용 ElastiCache 를 추가하려면 먼저 캐시 쿼리, DynamoDB 에 쓴 후 캐시 업데이트, 필요할 때 캐시 무효화와 같은 캐싱 로직을 구현하기 위해 상당한 코드 변경이 필요하므로 이 솔루션은 최소한의 애플리케이션 변경 요구 사항을 충족하지 않습니다.

참조: https://aws.amazon.com/dynamodb/dax/

Q473
A company hosts a website on Amazon EC2 instances behind an Application Load Balancer (ALB). The website serves static content. Website traffic is increasing, and the company is concerned about a potential increase in cost.
A. Create an Amazon CloudFront distribution to cache state files at edge locations.
B. Create an Amazon ElastiCache cluster. Connect the ALB to the ElastiCache cluster to serve cached files.
C. Create an AWS WAF web ACL and associate it with the ALB. Add a rule to the web ACL to cache static files.
D. Create a second ALB in an alternative AWS Region. Route user traffic to the closest

Region to minimize data transfer costs.
Answer: A
https://www.examtopics.com/discussions/amazon/view/109455-exam-aws-certified-solutions-architect-associate-saa-c03/

Q474
A company has multiple VPCs across AWS Regions to support and run workloads that are isolated from workloads in other Regions. Because of a recent application launch requirement, the company's VPCs must communicate with all other VPCs across all Regions.
Which solution will meet these requirements with the LEAST amount of administrative effort?
A. Use VPC peering to manage VPC communication in a single Region. Use VPC peering across Regions to manage VPC communications.
B. Use AWS Direct Connect gateways across all Regions to connect VPCs across regions and manage VPC communications.
C. Use AWS Transit Gateway to manage VPC communication in a single Region and Transit Gateway peering across Regions to manage VPC communications.
D. Use AWS PrivateLink across all Regions to connect VPCs across Regions and manage VPC communications.
Answer: C
https://www.examtopics.com/discussions/amazon/view/109659-exam-aws-certified-solutions-architect-associate-saa-c03/

Q475
A company is designing a containerized application that will use Amazon Elastic Container Service (Amazon ECS). The application needs to access a shared file system that is highly durable and can recover data to another AWS Region with a recovery point objective (RPO) of 8 hours. The file system needs to provide a mount target m each Availability Zone within a Region.
A solutions architect wants to use AWS Backup to manage the replication to another Region.
Which solution will meet these requirements?
A. Amazon FSx for Windows File Server with a Multi-AZ deployment
B. Amazon FSx for NetApp ONTAP with a Multi-AZ deployment
C. Amazon Elastic File System (Amazon EFS) with the Standard storage class

D. Amazon FSx for OpenZFS
Answer: C
https://www.examtopics.com/discussions/amazon/view/109456-exam-aws-certified-solutions-architect-associate-saa-c03/

Q476
A company is expecting rapid growth in the near future. A solutions architect needs to configure existing users and grant permissions to new users on AWS. The solutions architect has decided to create IAM groups. The solutions architect will add the new users to IAM groups based on department.
Which additional action is the MOST secure way to grant permissions to the new users?
A. Apply service control policies (SCPs) to manage access permissions.
B. Create IAM roles that have least privilege permission. Attach the roles to the IAM groups.
C. Create an IAM policy that grants least privilege permission. Attach the policy to the IAM groups.
D. Create IAM roles. Associate the roles with a permissions boundary that defines the maximum permissions.
Answer: C
https://www.examtopics.com/discussions/amazon/view/109458-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
IAM 정책은 IAM 자격 증명(예: 사용자, 그룹 또는 역할)에 대한 권한을 정의하는 문서입니다. IAM 정책을 사용하여 부서에 따라 기존 사용자 및 그룹에 권한을 부여할 수 있습니다. 최소 권한 권한을 부여하는 IAM 정책을 생성할 수 있습니다. 즉, 사용자가 작업을 수행하는 데 필요한 최소한의 권한만 부여한다는 의미입니다. 그런 다음 정책을 IAM 그룹에 연결하면 해당 그룹의 모든 사용자에게 정책이 적용됩니다. 이 솔루션은 운영 비용을 줄이고 권한 구성 및 관리를 단순화합니다.

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

Q477
A group requires permissions to list an Amazon S3 bucket and delete objects from that

bucket. An administrator has created the following IAM policy to provide access to the bucket and applied that policy to the group. The group is not able to delete objects in the bucket. The company follows least-privilege access rules.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Which statement should a solutions architect add to the policy to correct bucket access?

A.

```
"Action": [
    "s3:*Object"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

B.

```
"Action": [
    "s3:*"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

```
"Action": [
    "s3:DeleteObject"
],
"Resource": [
    "arn:aws:s3:::bucket-name*"
],
"Effect": "Allow"
```

C.

```
"Action": [
    "s3:DeleteObject"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

D.

Answer: D

https://www.examtopics.com/discussions/amazon/view/109459-exam-aws-certified-solutions-architect-associate-saa-c03/

Q478

A law firm needs to share information with the public. The information includes hundreds of files that must be publicly readable. Modifications or deletions of the files by anyone before a designated future date are prohibited.

Which solution will meet these requirements in the MOST secure way?

A. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Grant read-only IAM permissions to any AWS principals that access the S3 bucket until the designated date.

B. Create a new Amazon S3 bucket with S3 Versioning enabled. Use S3 Object Lock with a retention period in accordance with the designated date. Configure the S3 bucket for static website hosting. Set an S3 bucket policy to allow read-only access to the objects.

C. Create a new Amazon S3 bucket with S3 Versioning enabled. Configure an event trigger to run an AWS Lambda function in case of object modification or deletion. Configure the Lambda function to replace the objects with the original versions from a private S3 bucket.

D. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Select the folder that contains the files. Use S3 Object Lock with a retention period in accordance with the designated date. Grant read-only IAM permissions to any AWS

principals that access the S3 bucket.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109725-exam-aws-certified-solutions-architect-associate-saa-c03/

Q479
A company is making a prototype of the infrastructure for its new website by manually provisioning the necessary infrastructure. This infrastructure includes an Auto Scaling group, an Application Load Balancer and an Amazon RDS database. After the configuration has been thoroughly validated, the company wants the capability to immediately deploy the infrastructure for development and production use in two Availability Zones in an automated fashion.
What should a solutions architect recommend to meet these requirements?
A. Use AWS Systems Manager to replicate and provision the prototype infrastructure in two Availability Zones
B. Define the infrastructure as a template by using the prototype infrastructure as a guide. Deploy the infrastructure with AWS CloudFormation.
C. Use AWS Config to record the inventory of resources that are used in the prototype infrastructure. Use AWS Config to deploy the prototype infrastructure into two Availability Zones.
D. Use AWS Elastic Beanstalk and configure it to use an automated reference to the prototype infrastructure to automatically deploy new environments in two Availability Zones.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109461-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
AWS CloudFormation 은 Auto Scaling 그룹, 로드 밸런서, 데이터베이스 등 원하는 모든 리소스를 설명하는 템플릿을 사용하여 AWS 리소스를 모델링하고 설정할 수 있도록 도와주는 서비스입니다. AWS CloudFormation 을 사용하여 여러 환경과 리전에서 자동화되고 일관된 방식으로 인프라를 배포할 수 있습니다. 또한 AWS CloudFormation 을 사용하여 인프라를 단일 단위로 업데이트하거나 삭제할 수 있습니다.

참조 URL:
1 https://aws.amazon.com/cloudformation/

2 https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html
3
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-whatis-concepts.html

Q480
A business application is hosted on Amazon EC2 and uses Amazon S3 for encrypted object storage. The chief information security officer has directed that no application traffic between the two services should traverse the public internet.
Which capability should the solutions architect use to meet the compliance requirements?
A. AWS Key Management Service (AWS KMS)
B. VPC endpoint
C. Private subnet
D. Virtual private gateway
Answer: B
https://www.examtopics.com/discussions/amazon/view/109663-exam-aws-certified-solutions-architect-associate-saa-c03/

참고:
https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints.html

Q481
A company hosts a three-tier web application in the AWS Cloud. A Multi-AZAmazon RDS for MySQL server forms the database layer Amazon ElastiCache forms the cache layer. The company wants a caching strategy that adds or updates data in the cache when a customer adds an item to the database. The data in the cache must always match the data in the database.
Which solution will meet these requirements?
A. Implement the lazy loading caching strategy
B. Implement the write-through caching strategy
C. Implement the adding TTL caching strategy
D. Implement the AWS AppConfig caching strategy
Answer: B
https://www.examtopics.com/discussions/amazon/view/109462-exam-aws-certified-sol

utions-architect-associate-saa-c03/

Q482

A company wants to migrate 100 GB of historical data from an on-premises location to an Amazon S3 bucket. The company has a 100 megabits per second (Mbps) internet connection on premises. The company needs to encrypt the data in transit to the S3 bucket. The company will store new data directly in Amazon S3.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use the s3 sync command in the AWS CLI to move the data directly to an S3 bucket.

B. Use AWS DataSync to migrate the data from the on-premises location to an S3 bucket.

C. Use AWS Snowball to move the data to an S3 bucket.

D. Set up an IPsec VPN from the on-premises location to AWS. Use the s3 cp command in the AWS CLI to move the data directly to an S3 bucket.

Answer: B

https://www.examtopics.com/discussions/amazon/view/109490-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

AWS DataSync 는 인터넷 또는 AWS Direct Connect 를 통해 온프레미스 스토리지와 AWS 스토리지 서비스 간에 대량의 데이터를 온라인으로 쉽게 이동할 수 있게 해주는 데이터 전송 서비스입니다. DataSync 는 TLS 암호화를 사용하여 전송 중인 데이터를 자동으로 암호화하고 체크섬을 사용하여 전송하는 동안 데이터 무결성을 확인합니다. DataSync 는 오픈 소스 도구보다 최대 10 배 빠르게 데이터를 전송할 수 있으며 전송 예약, 모니터링 및 재개와 같은 작업을 단순화하고 자동화하여 운영 오버헤드를 줄입니다.

참조:

https://aws.amazon.com/datasync/

Q483

A company containerized a Windows job that runs on .NET 6 Framework under a Windows container. The company wants to run this job in the AWS Cloud. The job runs every 10 minutes. The job's runtime varies between 1 minute and 3 minutes.

Which solution will meet these requirements MOST cost-effectively?

A. Create an AWS Lambda function based on the container image of the job. Configure

Amazon EventBridge to invoke the function every 10 minutes.
B. Use AWS Batch to create a job that uses AWS Fargate resources. Configure the job scheduling to run every 10 minutes.
C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate to run the job. Create a scheduled task based on the container image of the job to run every 10 minutes.
D. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate to run the job. Create a standalone task based on the container image of the job. Use Windows task scheduler to run the job every 10 minutes.
Answer: C
https://www.examtopics.com/discussions/amazon/view/109463-exam-aws-certified-solutions-architect-associate-saa-c03/

Q484
A company wants to move from many standalone AWS accounts to a consolidated, multi-account architecture. The company plans to create many new AWS accounts for different business units. The company needs to authenticate access to these AWS accounts by using a centralized corporate directory service.
Which combination of actions should a solutions architect recommend to meet these requirements? (Choose two)
A. Create a new organization in AWS Organizations with all features turned on. Create the new AWS accounts in the organization.
B. Set up an Amazon Cognito identity pool. Configure AWS IAM Identity Center (AWS Single Sign-On) to accept Amazon Cognito authentication.
C. Configure a service control policy (SCP) to manage the AWS accounts. Add AWS IAM Identity Center (AWS Single Sign-On) to AWS Directory Service.
D. Create a new organization in AWS Organizations. Configure the organization's authentication mechanism to use AWS Directory Service directly.
E. Set up AWS IAM Identity Center (AWS Single Sign-On) in the organization. Configure IAM Identity Center, and integrate it with the company's corporate directory service.
Answer: A, E
https://www.examtopics.com/discussions/amazon/view/109467-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
AWS Organizations 는 사용자가 여러 AWS 계정을 중앙에서 관리하고 제어할 수 있도록

도와주는 서비스입니다. 이를 통해 사용자는 비즈니스 요구 사항 또는 기타 기준에 따라 계정을 그룹화하는 조직 단위(OU)를 만들 수 있습니다. 또한 사용자는 서비스 제어 정책(SCP)을 정의하고 OU 또는 계정에 연결하여 계정에서 수행할 수 있는 작업을 제한할 수 있습니다. 모든 기능을 켠 상태에서 AWS Organizations 에 새 조직을 생성하면 이 솔루션은 서로 다른 비즈니스 단위의 새 AWS 계정을 통합하고 관리할 수 있습니다. AWS IAM Identity Center(이전에는 AWS Single Sign-On 이라고 함)는 모든 AWS 계정 및 클라우드 애플리케이션에 대한 Single Sign-On 액세스를 제공하는 서비스입니다. AWS Directory Service 를 통해 Microsoft Active Directory 와 연결하여 해당 디렉터리의 사용자가 기존 Active Directory 사용자 이름과 암호를 사용하여 맞춤형 AWS 액세스 포털에 로그인할 수 있도록 합니다. AWS 액세스 포털에서 사용자는 권한이 있는 모든 AWS 계정 및 클라우드 애플리케이션에 액세스할 수 있습니다 2. 조직에 IAM Identity Center 를 설정하고 회사의 회사 디렉터리 서비스와 통합함으로써 솔루션은 중앙 집중식 회사 디렉터리 서비스를 사용하여 이러한 AWS 계정에 대한 액세스를 인증할 수 있습니다.

1. Amazon Cognito 자격 증명 풀을 설정합니다. Amazon Cognito 인증을 수락하도록 AWS IAM Identity Center(AWS Single Sign-On)를 구성합니다. 이 솔루션은 중앙 집중식 기업 디렉터리 서비스를 사용하여 이러한 AWS 계정에 대한 액세스 인증 요구 사항을 충족하지 않습니다. Amazon Cognito 는 웹 및 모바일 애플리케이션에 대한 사용자 가입, 로그인 및 액세스 제어를 제공하는 서비스이기 때문입니다. 기업 디렉토리 서비스.

2. 서비스 제어 정책(SCP)을 구성하여 AWS 계정을 관리합니다. AWS IAM Identity Center(AWS Single Sign-On)를 AWS Directory Service 에 추가합니다. SCP 는 계정 자체를 관리하는 것이 아니라 조직의 계정이 수행할 수 있는 작업을 제한하는 데 사용되기 때문에 이 솔루션은 작동하지 않습니다 1. 또한 IAM Identity Center 는 AWS Directory Service 를 통해 Microsoft Active Directory 와 연결하는 별도의 서비스이므로 AWS Directory Service 에 추가할 수 없습니다.

3. AWS Organizations 에서 새 조직을 생성합니다. AWS Directory Service 를 직접 사용하도록 조직의 인증 메커니즘을 구성합니다. AWS Organizations 에는 AWS Directory Service 를 직접 사용할 수 있는 인증 메커니즘이 없기 때문에 이 솔루션은 작동하지 않습니다. AWS Organizations 는 IAM Identity Center 를 사용하여 조직의 계정에 대한 Single Sign-On 액세스를 제공합니다.

참조:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_integrate_services.html

Q485

A company is looking for a solution that can store video archives in AWS from old news footage. The company needs to minimize costs and will rarely need to restore these files. When the files are needed, they must be available in a maximum of five minutes.
What is the MOST cost-effective solution?
A. Store the video archives in Amazon S3 Glacier and use Expedited retrievals.
B. Store the video archives in Amazon S3 Glacier and use Standard retrievals.
C. Store the video archives in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).
D. Store the video archives in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).
Answer: A
https://www.examtopics.com/discussions/amazon/view/109470-exam-aws-certified-solutions-architect-associate-saa-c03/

Q486
A company is building a three-tier application on AWS. The presentation tier will serve a static website The logic tier is a containerized application. This application will store data in a relational database. The company wants to simplify deployment and to reduce operational costs.
Which solution will meet these requirements?
A. Use Amazon S3 to host static content. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute power. Use a managed Amazon RDS cluster for the database.
B. Use Amazon CloudFront to host static content. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 for compute power. Use a managed Amazon RDS cluster for the database.
C. Use Amazon S3 to host static content. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute power. Use a managed Amazon RDS cluster for the database.
D. Use Amazon EC2 Reserved Instances to host static content. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 for compute power. Use a managed Amazon RDS cluster for the database.
Answer: A
https://www.examtopics.com/discussions/amazon/view/109664-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

Amazon S3는 업계 최고의 확장성, 데이터 가용성, 보안 및 성능을 제공하는 객체 스토리지 서비스입니다. Amazon S3 를 사용하여 HTML 파일, 이미지, 비디오 등과 같은 웹 사이트용 정적 콘텐츠를 호스팅할 수 있습니다. Amazon Elastic Container Service(Amazon ECS)는 AWS 에서 컨테이너화된 애플리케이션을 실행하고 확장할 수 있는 완전 관리형 컨테이너 오케스트레이션 서비스입니다. .
AWS Fargate 는 Amazon ECS 및 Amazon EKS 모두에서 작동하는 컨테이너용 서버리스 컴퓨팅 엔진입니다. Fargate 를 사용하면 서버를 프로비저닝하고 관리할 필요가 없으므로 애플리케이션 구축에 쉽게 집중할 수 있습니다. 컨테이너화된 애플리케이션 논리 계층의 컴퓨팅 성능을 위해 AWS Fargate 와 함께 Amazon ECS 를 사용할 수 있습니다. Amazon RDS 는 클라우드에서 관계형 데이터베이스를 쉽게 설정, 운영 및 확장할 수 있게 해주는 관리형 관계형 데이터베이스 서비스입니다. 애플리케이션의 데이터베이스 계층에 대해 관리형 Amazon RDS 클러스터를 사용할 수 있습니다. 이 솔루션은 배포를 단순화하고 3 계층 애플리케이션의 운영 비용을 줄여줍니다.

참조:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html
https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

Q487
A company seeks a storage solution for its application. The solution must be highly available and scalable. The solution also must function as a file system be mountable by multiple Linux instances in AWS and on premises through native protocols, and have no minimum size requirements. The company has set up a Site-to-Site VPN for access from its on-premises network to its VPC.
Which storage solution meets these requirements?
A. Amazon FSx Multi-AZ deployments
B. Amazon Elastic Block Store (Amazon EBS) Multi-Attach volumes
C. Amazon Elastic File System (Amazon EFS) with multiple mount targets
D. Amazon Elastic File System (Amazon EFS) with a single mount target and multiple access points
Answer: C
https://www.examtopics.com/discussions/amazon/view/109665-exam-aws-certified-solutions-architect-associate-saa-c03/

Q488

A 4-year-old media company is using the AWS Organizations all features feature set to organize its AWS accounts. According to the company's finance team, the billing information on the member accounts must not be accessible to anyone, including the root user of the member accounts.

Which solution will meet these requirements?

A. Add all finance team users to an IAM group. Attach an AWS managed policy named Billing to the group.

B. Attach an identity-based policy to deny access to the billing information to all users, including the root user.

C. Create a service control policy (SCP) to deny access to the billing information. Attach the SCP to the root organizational unit (OU).

D. Convert from the Organizations all features feature set to the Organizations consolidated billing feature set.

Answer: C

https://www.examtopics.com/discussions/amazon/view/109509-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪

서비스 제어 정책(SCP): SCP 는 AWS Organizations 의 필수적인 부분이며 이를 통해 AWS Organization 내 조직 단위(OU)에 대한 세분화된 권한을 설정할 수 있습니다. SCP 는 루트 사용자를 포함하여 멤버 계정에 부여할 수 있는 최대 권한에 대한 중앙 제어를 제공합니다. 청구 정보에 대한 액세스 거부: SCP 를 만들어 루트 OU 에 연결하면 조직 내 모든 계정의 청구 정보에 대한 액세스를 명시적으로 거부할 수 있습니다. SCP 는 청구 관련 서비스를 포함하여 다양한 AWS 서비스 및 작업에 대한 액세스를 제한하는 데 사용할 수 있습니다. 세분화된 제어: SCP 를 사용하면 조직 단위 수준에서 특정 권한 및 제한을 정의할 수 있습니다. 루트 OU 에서 청구 정보에 대한 액세스를 거부하면 루트 사용자를 포함한 어떤 멤버 계정도 청구 정보에 액세스할 수 없습니다.

Q489

An ecommerce company runs an application in the AWS Cloud that is integrated with an on-premises warehouse solution. The company uses Amazon Simple Notification Service (Amazon SNS) to send order messages to an on-premises HTTPS endpoint so the warehouse application can process the orders. The local data center team has detected that

some of the order messages were not received.
A solutions architect needs to retain messages that are not delivered and analyze the messages for up to 14 days.
Which solution will meet these requirements with the LEAST development effort?
A. Configure an Amazon SNS dead letter queue that has an Amazon Kinesis Data Stream target with a retention period of 14 days.
B. Add an Amazon Simple Queue Service (Amazon SQS) queue with a retention period of 14 days between the application and Amazon SNS.
C. Configure an Amazon SNS dead letter queue that has an Amazon Simple Queue Service (Amazon SQS) target with a retention period of 14 days.
D. Configure an Amazon SNS dead letter queue that has an Amazon DynamoDB target with a TTL attribute set for a retention period of 14 days.
Answer: C
https://www.examtopics.com/discussions/amazon/view/109637-exam-aws-certified-solutions-architect-associate-saa-c03/

Q490
A gaming company uses Amazon DynamoDB to store user information such as geographic location, player data, and leaderboards. The company needs to configure continuous backups to an Amazon S3 bucket with a minimal amount of coding. The backups must not affect availability of the application and must not affect the read capacity units (RCUs) that are defined for the table.
Which solution meets these requirements?
A. Use an Amazon EMR cluster. Create an Apache Hive job to back up the data to Amazon S3.
B. Export the data directly from DynamoDB to Amazon S3 with continuous backups. Turn on point-in-time recovery for the table.
C. Configure Amazon DynamoDB Streams. Create an AWS Lambda function to consume the stream and export the data to an Amazon S3 bucket.
D. Create an AWS Lambda function to export the data from the database tables to Amazon S3 on a regular basis. Turn on point-in-time recovery for the table.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109577-exam-aws-certified-solutions-architect-associate-saa-c03/

참고:
https://aws.amazon.com/ko/blogs/database/dynamodb-streams-use-cases-and-design-patterns/
https://repost.aws/ko/knowledge-center/back-up-dynamodb-s3

Q491
A solutions architect is designing an asynchronous application to process credit card data validation requests for a bank. The application must be secure and be able to process each request at least once.
Which solution will meet these requirements MOST cost-effectively?
A. Use AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) standard queues as the event source. Use AWS Key Management Service (SSE-KMS) for encryption. Add the kms:Decrypt permission for the Lambda execution role.
B. Use AWS Lambda event source mapping. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues as the event source. Use SQS managed encryption keys (SSE-SQS) for encryption. Add the encryption key invocation permission for the Lambda function.
C. Use the AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) FIFO queues as the event source. Use AWS KMS keys (SSE-KMS). Add the kms:Decrypt permission for the Lambda execution role.
D. Use the AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) standard queues as the event source. Use AWS KMS keys (SSE-KMS) for encryption. Add the encryption key invocation permission for the Lambda function.
Answer: A
https://www.examtopics.com/discussions/amazon/view/109513-exam-aws-certified-solutions-architect-associate-saa-c03/

Q492
A company has multiple AWS accounts for development work. Some staff consistently use oversized Amazon EC2 instances, which causes the company to exceed the yearly budget for the development accounts. The company wants to centrally restrict the creation of AWS resources in these accounts.
Which solution will meet these requirements with the LEAST development effort?
A. Develop AWS Systems Manager templates that use an approved EC2 creation process. Use the approved Systems Manager templates to provision EC2 instances.

B. Use AWS Organizations to organize the accounts into organizational units (OUs). Define and attach a service control policy (SCP) to control the usage of EC2 instance types.
C. Configure an Amazon EventBridge rule that invokes an AWS Lambda function when an EC2 instance is created. Stop disallowed EC2 instance types.
D. Set up AWS Service Catalog products for the staff to create the allowed EC2 instance types. Ensure that staff can deploy EC2 instances only by using the Service Catalog products.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109638-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
동적 조정은 수요 또는 부하에 따라 Auto Scaling 그룹의 EC2 인스턴스 수를 자동으로 조정하는 일종의 자동 조정입니다. 지정된 지표가 임계값을 초과하면 CloudWatch 경보를 사용하여 조정 작업을 트리거합니다. 필요에 따라 확장(인스턴스 추가) 또는 축소(인스턴스 제거)할 수 있습니다 1. 솔루션은 동적 확장을 사용하여 갑작스러운 트래픽 증가 중에 가장 비용 효율적으로 애플리케이션 성능을 유지할 수 있습니다.
1. 수동 조정을 사용하여 Auto Scaling 그룹의 크기를 변경합니다. 수동 확장은 사용자가 CLI 또는 콘솔을 통해 인스턴스 수를 수동으로 늘리거나 줄여야 하므로 이 솔루션은 트래픽이 갑자기 증가하는 동안 애플리케이션 성능을 유지해야 하는 요구 사항을 충족하지 않습니다. 수요나 부하의 변화에 자동으로 반응하지 않습니다.
2. 예측 조정을 사용하여 Auto Scaling 그룹의 크기를 변경합니다. 이 솔루션은 예측 확장이 기계 학습 및 인공 지능 도구를 사용하여 트래픽 부하를 평가하고 더 많거나 적은 리소스가 필요할 때를 예상하므로 대부분의 비용 효율성 요구 사항을 충족하지 않습니다. 주어진 시간에 실제 수요 또는 로드와 일치하지 않을 수 있는 예측을 기반으로 예약된 조정 작업을 수행합니다. 예측 조정은 예측 가능한 트래픽 패턴이 있거나 트래픽 부하의 알려진 변경 사항이 있는 시나리오에 더 적합합니다.
3. 일정 조정을 사용하여 Auto Scaling 그룹의 크기를 변경합니다. 일정 조정은 사용자가 예약한 특정 시간에 조정 작업을 수행하므로 이 솔루션은 트래픽이 갑자기 증가하는 동안 애플리케이션 성능을 유지해야 하는 요구 사항을 충족하지 않습니다. 수요나 부하의 변화에 자동으로 반응하지 않습니다. 일정 조정은 하루 중 특정 시간에 예측 가능한 트래픽 감소 또는 급증이 있는 시나리오에 더 적합합니다.

참조:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-ondemand.html

Q493

A company wants to use artificial intelligence (AI) to determine the quality of its customer service calls. The company currently manages calls in four different languages, including English. The company will offer new languages in the future. The company does not have the resources to regularly maintain machine learning (ML) models.

The company needs to create written sentiment analysis reports from the customer service call recordings. The customer service call recording text must be translated into English.

Which combination of steps will meet these requirements? (Choose three)

A. Use Amazon Comprehend to translate the audio recordings into English.

B. Use Amazon Lex to create the written sentiment analysis reports.

C. Use Amazon Polly to convert the audio recordings into text.

D. Use Amazon Transcribe to convert the audio recordings in any language into text.

E. Use Amazon Translate to translate text in any language to English.

F. Use Amazon Comprehend to create the sentiment analysis reports.

Answer: D, E, F

https://www.examtopics.com/discussions/amazon/view/109639-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪

이러한 답변은 모든 언어로 된 고객 서비스 통화 녹음에서 서면 감정 분석 보고서를 작성하고 이를 영어로 번역하는 요구 사항을 충족하므로 정확합니다. Amazon Transcribe 는 고급 기계 학습 기술을 사용하여 오디오 파일의 음성을 인식하고 텍스트로 변환하는 서비스입니다. Amazon Transcribe 를 사용하여 모든 언어의 오디오 녹음을 텍스트로 변환하고 소스 오디오의 언어 코드를 지정할 수 있습니다. Amazon Translate 는 빠르고 고품질의 저렴한 언어 번역을 제공하는 신경망 기계 번역 서비스입니다. Amazon Translate 를 사용하여 모든 언어의 텍스트를 영어로 번역하고 소스 및 대상 언어 코드를 지정할 수 있습니다. Amazon Comprehend 는 기계 학습을 사용하여 텍스트에서 통찰력과 관계를 찾는 자연어 처리(NLP) 서비스입니다. Amazon Comprehend 를 사용하여 텍스트가 긍정적인지, 부정적인지, 중립적인지 또는 혼합되어 있는지 판단하는 감정 분석 보고서를 생성할 수 있습니다.

참조:

https://docs.aws.amazon.com/transcribe/latest/dg/what-is-transcribe.html

https://docs.aws.amazon.com/translate/latest/dg/what-is.html
https://docs.aws.amazon.com/comprehend/latest/dg/how-sentiment.html

Q494

A company uses Amazon EC2 instances to host its internal systems. As part of a deployment operation, an administrator tries to use the AWS CLI to terminate an EC2 instance. However, the administrator receives a 403 (Access Denied) error message.

The administrator is using an IAM role that has the following IAM policy attached:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["ec2:TerminateInstances"],
            "Resource": ["*"]
        },
        {
            "Effect": "Deny",
            "Action": ["ec2:TerminateInstances"],
            "Condition": {
                "NotIpAddress": {
                    "aws:SourceIp": [
                        "192.0.2.0/24",
                        "203.0.113.0/24"
                    ]
                }
            },
            "Resource": ["*"]
        }
    ]
}
```

What is the cause of the unsuccessful request?

A. The EC2 instance has a resource-based policy with a Deny statement.

B. The principal has not been specified in the policy statement.

C. The "Action" field does not grant the actions that are required to terminate the EC2 instance.

D. The request to terminate the EC2 instance does not originate from the CIDR blocks 192.0.2.0/24 or 203.0.113.0/24.
Answer: D
https://www.examtopics.com/discussions/amazon/view/109727-exam-aws-certified-solutions-architect-associate-saa-c03/

Q495
A company is conducting an internal audit. The company wants to ensure that the data in an Amazon S3 bucket that is associated with the company's AWS Lake Formation data lake does not contain sensitive customer or employee data. The company wants to discover personally identifiable information (PII) or financial information, including passport numbers and credit card numbers.
Which solution will meet these requirements?
A. Configure AWS Audit Manager on the account. Select the Payment Card Industry Data Security Standards (PCI DSS) for auditing.
B. Configure Amazon S3 Inventory on the S3 bucket Configure Amazon Athena to query the inventory.
C. Configure Amazon Macie to run a data discovery job that uses managed identifiers for the required data types.
D. Use Amazon S3 Select to run a report across the S3 bucket.
Answer: C
https://www.examtopics.com/discussions/amazon/view/109666-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Amazon Macie 는 기계 학습 및 패턴 일치를 사용하여 AWS 에서 중요한 데이터를 검색하고 보호하는 완전 관리형 데이터 보안 및 데이터 개인 정보 보호 서비스입니다. Macie 는 다양한 유형의 PII 또는 금융 정보(예: 여권 번호 및 신용 카드 번호)에 대해 관리형 식별자를 사용하는 데이터 검색 작업을 실행할 수 있습니다. Macie 는 또한 데이터의 잠재적인 문제나 위험을 경고하는 결과를 생성할 수 있습니다.
참조:
https://docs.aws.amazon.com/macie/latest/userguide/macie-identifiers.html

Q496

A company uses on-premises servers to host its applications. The company is running out of storage capacity. The applications use both block storage and NFS storage. The company needs a high-performing solution that supports local caching without re-architecting its existing applications.
Which combination of actions should a solutions architect take to meet these requirements? (Choose two)
A. Mount Amazon S3 as a file system to the on-premises servers.
B. Deploy an AWS Storage Gateway file gateway to replace NFS storage.
C. Deploy AWS Snowball Edge to provision NFS mounts to on-premises servers.
D. Deploy an AWS Storage Gateway volume gateway to replace the block storage.
E. Deploy Amazon Elastic File System (Amazon EFS) volumes and mount them to on-premises servers.
Answer: B, D
https://www.examtopics.com/discussions/amazon/view/109552-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
https://aws.amazon.com/storagegateway/file/
파일 게이트웨이는 애플리케이션 데이터 파일과 백업 이미지를 Amazon S3 클라우드 스토리지에 내구성 있는 개체로 저장하기 위해 클라우드에 원활하게 연결할 수 있는 방법을 제공합니다. 파일 게이트웨이는 로컬 캐싱을 통해 Amazon S3 의 데이터에 대한 SMB 또는 NFS 기반 액세스를 제공합니다. 온프레미스 애플리케이션과 S3 객체 스토리지에 대한 파일 프로토콜 액세스가 필요한 Amazon EC2 기반 애플리케이션에 사용할 수 있습니다.
https://aws.amazon.com/storagegateway/volume/
볼륨 게이트웨이는 온프레미스 애플리케이션에 클라우드 지원 iSCSI 블록 스토리지 볼륨을 제공합니다.
볼륨 게이트웨이는 사용자를 대신하여 Amazon S3 에 온프레미스 데이터를 저장하고 관리하며 캐시 모드 또는 저장 모드에서 작동합니다. 캐싱된 볼륨 게이트웨이 모드에서 기본 데이터는 Amazon S3 에 저장되는 반면 자주 액세스하는 데이터는 짧은 지연 시간 액세스를 위해 캐시에 로컬로 유지됩니다.

Q497
A company has a service that reads and writes large amounts of data from an Amazon S3 bucket in the same AWS Region. The service is deployed on Amazon EC2 instances within the private subnet of a VPC. The service communicates with Amazon S3 over a NAT gateway

in the public subnet. However, the company wants a solution that will reduce the data output costs.
Which solution will meet these requirements MOST cost-effectively?
A. Provision a dedicated EC2 NAT instance in the public subnet. Configure the route table for the private subnet to use the elastic network interface of this instance as the destination for all S3 traffic.
B. Provision a dedicated EC2 NAT instance in the private subnet. Configure the route table for the public subnet to use the elastic network interface of this instance as the destination for all S3 traffic.
C. Provision a VPC gateway endpoint. Configure the route table for the private subnet to use the gateway endpoint as the route for all S3 traffic.
D. Provision a second NAT gateway. Configure the route table for the private subnet to use this NAT gateway as the destination for all S3 traffic.
Answer: C
https://www.examtopics.com/discussions/amazon/view/109667-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이를 통해 회사는 VPC 의 Amazon EC2 인스턴스에서 Amazon S3 에 액세스하기 위한 데이터 출력 비용을 줄일 수 있습니다. 회사는 VPC 게이트웨이 엔드포인트를 프로비저닝함으로써 VPC 와 S3 간의 프라이빗 연결을 활성화할 수 있습니다. 게이트웨이 엔드포인트를 모든 S3 트래픽의 경로로 사용하도록 프라이빗 서브넷의 라우팅 테이블을 구성함으로써 회사는 데이터 처리 및 데이터 전송 비용을 청구하는 NAT 게이트웨이 사용을 피할 수 있습니다.

Q498
A company uses Amazon S3 to store high-resolution pictures in an S3 bucket. To minimize application changes, the company stores the pictures as the latest version of an S3 object. The company needs to retain only the two most recent versions of the pictures.
The company wants to reduce costs. The company has identified the S3 bucket as a large expense.
Which solution will reduce the S3 costs with the LEAST operational overhead?
A. Use S3 Lifecycle to delete expired object versions and retain the two most recent versions.
B. Use an AWS Lambda function to check for older versions and delete all but the two most

recent versions.

C. Use S3 Batch Operations to delete noncurrent object versions and retain only the two most recent versions.

D. Deactivate versioning on the S3 bucket and retain the two most recent versions.

Answer: A

https://www.examtopics.com/discussions/amazon/view/109668-exam-aws-certified-solutions-architect-associate-saa-c03/

▪

Q499

A company needs to minimize the cost of its 1 Gbps AWS Direct Connect connection. The company's average connection utilization is less than 10%. A solutions architect must recommend a solution that will reduce the cost without compromising security.

Which solution will meet these requirements?

A. Set up a new 1 Gbps Direct Connect connection. Share the connection with another AWS account.

B. Set up a new 200 Mbps Direct Connect connection in the AWS Management Console.

C. Contact an AWS Direct Connect Partner to order a 1 Gbps connection. Share the connection with another AWS account.

D. Contact an AWS Direct Connect Partner to order a 200 Mbps hosted connection for an existing AWS account.

Answer: D

https://www.examtopics.com/discussions/amazon/view/109515-exam-aws-certified-solutions-architect-associate-saa-c03/

설명

회사는 더 저렴한 연결(200M)을 설정해야 하지만 호스트 연결로 더 많은 유연성을 위해 1, 10 또는 100Gbps 의 포트 속도만 주문할 수 있기 때문에 B 는 올바르지 않습니다. 50Mbps 에서 10Gbps 사이의 포트 속도를 주문할 수 있습니다.

https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-directconnect.html

Q500

A company has multiple Windows file servers on premises. The company wants to migrate

and consolidate its files into an Amazon FSx for Windows File Server file system. File permissions must be preserved to ensure that access rights do not change.
Which solutions will meet these requirements? (Choose two)
A. Deploy AWS DataSync agents on premises. Schedule DataSync tasks to transfer the data to the FSx for Windows File Server file system.
B. Copy the shares on each file server into Amazon S3 buckets by using the AWS CLI. Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system.
C. Remove the drives from each file server. Ship the drives to AWS for import into Amazon S3. Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system.
D. Order an AWS Snowcone device. Connect the device to the on-premises network. Launch AWS DataSync agents on the device. Schedule DataSync tasks to transfer the data to the FSx for Windows File Server file system.
E. Order an AWS Snowball Edge Storage Optimized device. Connect the device to the on-premises network. Copy data to the device by using the AWS CLI. Ship the device back to AWS for import into Amazon S3. Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system.
Answer: A, D
https://www.examtopics.com/discussions/amazon/view/109689-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
A 이 옵션에는 온프레미스 파일 서버에 DataSync 에이전트를 배포하고 DataSync 를 사용하여 데이터를 FSx for Windows File Server 로 직접 전송하는 작업이 포함됩니다. DataSync 는 마이그레이션 프로세스 중에 파일 권한이 보존되도록 합니다.
D 이 옵션에는 휴대용 데이터 전송 장치인 AWS Snowcone 장치 사용이 포함됩니다. Snowcone 디바이스를 온프레미스 네트워크에 연결하고 디바이스에서 DataSync 에이전트를 시작하고 DataSync 작업을 예약하여 데이터를 FSx for Windows File Server 로 전송합니다.
DataSync 는 파일 권한을 유지하면서 마이그레이션 프로세스를 처리합니다.

Q501
A company wants to ingest customer payment data into the company's data lake in Amazon S3. The company receives payment data every minute on average. The company wants to

analyze the payment data in real time. Then the company wants to ingest the data into the data lake.

Which solution will meet these requirements with the MOST operational efficiency?

A. Use Amazon Kinesis Data Streams to ingest data. Use AWS Lambda to analyze the data in real time.

B. Use AWS Glue to ingest data. Use Amazon Kinesis Data Analytics to analyze the data in real time.

C. Use Amazon Kinesis Data Firehose to ingest data. Use Amazon Kinesis Data Analytics to analyze the data in real time.

D. Use Amazon API Gateway to ingest data. Use AWS Lambda to analyze the data in real time.

Answer: C

https://www.examtopics.com/discussions/amazon/view/109421-exam-aws-certified-solutions-architect-associate-saa-c03/

▪

Q502

A company runs a website that uses a content management system (CMS) on Amazon EC2. The CMS runs on a single EC2 instance and uses an Amazon Aurora MySQL Multi-AZ DB instance for the data tier. Website images are stored on an Amazon Elastic Block Store (Amazon EBS) volume that is mounted inside the EC2 instance.

Which combination of actions should a solutions architect take to improve the performance and resilience of the website? (Choose two)

A. Move the website images into an Amazon S3 bucket that is mounted on every EC2 instance.

B. Share the website images by using an NFS share from the primary EC2 instance. Mount this share on the other EC2 instances.

C. Move the website images onto an Amazon Elastic File System (Amazon EFS) file system that is mounted on every EC2 instance.

D. Create an Amazon Machine Image (AMI) from the existing EC2 instance. Use the AMI to provision new instances behind an Application Load Balancer as part of an Auto Scaling group. Configure the Auto Scaling group to maintain a minimum of two instances. Configure an accelerator in AWS Global Accelerator for the website.

E. Create an Amazon Machine Image (AMI) from the existing EC2 instance. Use the AMI to provision new instances behind an Application Load Balancer as part of an Auto Scaling

group. Configure the Auto Scaling group to maintain a minimum of two instances. Configure an Amazon CloudFront distribution for the website.
Answer: C, E
https://www.examtopics.com/discussions/amazon/view/109420-exam-aws-certified-solutions-architect-associate-saa-c03/

설명
옵션 C 는 웹 사이트 이미지를 모든 EC2 인스턴스에 탑재된 Amazon EFS 파일 시스템으로 이동하는 기능을 제공합니다. Amazon EFS 는 여러 EC2 인스턴스에서 동시에 액세스할 수 있는 확장 가능하고 완벽하게 관리되는 파일 스토리지 솔루션을 제공합니다. 이렇게 하면 모든 인스턴스에서 웹 사이트 이미지에 효율적이고 일관되게 액세스할 수 있으므로 옵션 E 에서 성능이 향상됩니다. Auto Scaling 그룹은 최소 2 개의 인스턴스를 유지 관리하여 비정상 인스턴스를 자동으로 교체하여 복원력을 보장합니다.
또한 웹 사이트에 대해 Amazon CloudFront 배포를 구성하면 최종 사용자에게 더 가까운 엣지 위치에서 콘텐츠를 캐싱하여 지연 시간을 줄이고 콘텐츠 전송을 개선하여 성능을 더욱 향상시킵니다.
따라서 이러한 작업을 결합하면 효율적인 이미지 저장 및 콘텐츠 전달을 통해 웹 사이트의 성능이 향상됩니다.

Q503
A company runs an infrastructure monitoring service. The company is building a new feature that will enable the service to monitor data in customer AWS accounts. The new feature will call AWS APIs in customer accounts to describe Amazon EC2 instances and read Amazon CloudWatch metrics.
What should the company do to obtain access to customer accounts in the MOST secure way?
A. Ensure that the customers create an IAM role in their account with read-only EC2 and CloudWatch permissions and a trust policy to the company's account.
B. Create a serverless API that implements a token vending machine to provide temporary AWS credentials for a role with read-only EC2 and CloudWatch permissions.
C. Ensure that the customers create an IAM user in their account with read-only EC2 and CloudWatch permissions. Encrypt and store customer access and secret keys in a secrets management system.
D. Ensure that the customers create an Amazon Cognito user in their account to use an IAM role with read-only EC2 and CloudWatch permissions. Encrypt and store the Amazon

Cognito user and password in a secrets management system.
Answer: A
https://www.examtopics.com/discussions/amazon/view/109595-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 ·
고객이 자신의 계정에서 필요한 권한이 있는 IAM 역할을 생성하도록 함으로써 회사는 AWS Identity and Access Management(IAM)를 사용하여 교차 계정 액세스를 설정할 수 있습니다. 신뢰 정책은 회사의 AWS 계정이 일시적으로 고객의 IAM 역할을 맡도록 허용하여 고객 계정 내의 지정된 리소스(EC2 인스턴스 및 CloudWatch 지표)에 대한 액세스 권한을 부여합니다. 이 접근 방식은 회사가 필요한 권한만 요청하고 고객의 장기 액세스 키나 사용자 자격 증명을 요구하지 않기 때문에 최소 권한 원칙을 따릅니다.

Q504
A company needs to connect several VPCs in the us-east-1 Region that span hundreds of AWS accounts. The company's networking team has its own AWS account to manage the cloud network.
What is the MOST operationally efficient solution to connect the VPCs?
A. Set up VPC peering connections between each VPC. Update each associated subnet's route table.
B. Configure a NAT gateway and an internet gateway in each VPC to connect each VPC through the internet.
C. Create an AWS Transit Gateway in the networking team's AWS account. Configure static routes from each VPC.
D. Deploy VPN gateways in each VPC. Create a transit VPC in the networking team's AWS account to connect to each VPC.
Answer: C
https://www.examtopics.com/discussions/amazon/view/109690-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 ·
AWS Transit Gateway 는 여러 VPC, 온프레미스 네트워크 및 원격 네트워크를 연결하기 위한 확장성이 뛰어난 중앙 집중식 허브입니다. 단일 진입점을 제공하고 필요한 연결 수를 줄임으로써 네트워크 연결을 단순화합니다. 이 시나리오에서 네트워킹 팀의 AWS 계정에 AWS Transit Gateway 를 배포하면 여러 VPC 에서 네트워크 연결을 효율적으로 관리하고

제어할 수 있습니다.

Q505

A company has Amazon EC2 instances that run nightly batch jobs to process data. The EC2 instances run in an Auto Scaling group that uses On-Demand billing. If a job fails on one instance, another instance will reprocess the job. The batch jobs run between 12:00 AM and 06:00 AM local time every day.

Which solution will provide EC2 instances to meet these requirements MOST cost-effectively?

A. Purchase a 1-year Savings Plan for Amazon EC2 that covers the instance family of the Auto Scaling group that the batch job uses.

B. Purchase a 1-year Reserved Instance for the specific instance type and operating system of the instances in the Auto Scaling group that the batch job uses.

C. Create a new launch template for the Auto Scaling group. Set the instances to Spot Instances. Set a policy to scale out based on CPU usage.

D. Create a new launch template for the Auto Scaling group. Increase the instance size. Set a policy to scale out based on CPU usage.

Answer: C

https://www.examtopics.com/discussions/amazon/view/109691-exam-aws-certified-solutions-architect-associate-saa-c03/

▪

Q506

A social media company is building a feature for its website. The feature will give users the ability to upload photos. The company expects significant increases in demand during large events and must ensure that the website can handle the upload traffic from users.

Which solution meets these requirements with the MOST scalability?

A. Upload files from the user's browser to the application servers. Transfer the files to an Amazon S3 bucket.

B. Provision an AWS Storage Gateway file gateway. Upload files directly from the user's browser to the file gateway.

C. Generate Amazon S3 presigned URLs in the application. Upload files directly from the user's browser into an S3 bucket.

D. Provision an Amazon Elastic File System (Amazon EFS) file system. Upload files directly

from the user's browser to the file system.

Answer: C

https://www.examtopics.com/discussions/amazon/view/109692-exam-aws-certified-solutions-architect-associate-saa-c03/

▪

Q507

A company has a web application for travel ticketing. The application is based on a database that runs in a single data center in North America. The company wants to expand the application to serve a global user base. The company needs to deploy the application to multiple AWS Regions. Average latency must be less than 1 second on updates to the reservation database.

The company wants to have separate deployments of its web platform across multiple Regions. However, the company must maintain a single primary reservation database that is globally consistent.

Which solution should a solutions architect recommend to meet these requirements?

A. Convert the application to use Amazon DynamoDB. Use a global table for the center reservation table. Use the correct Regional endpoint in each Regional deployment.

B. Migrate the database to an Amazon Aurora MySQL database. Deploy Aurora Read Replicas in each Region. Use the correct Regional endpoint in each Regional deployment for access to the database.

C. Migrate the database to an Amazon RDS for MySQL database. Deploy MySQL read replicas in each Region. Use the correct Regional endpoint in each Regional deployment for access to the database.

D. Migrate the application to an Amazon Aurora Serverless database. Deploy instances of the database to each Region. Use the correct Regional endpoint in each Regional deployment to access the database. Use AWS Lambda functions to process event streams in each Region to synchronize the databases.

Answer: A

https://www.examtopics.com/discussions/amazon/view/109608-exam-aws-certified-solutions-architect-associate-saa-c03/

Q508

A company has migrated multiple Microsoft Windows Server workloads to Amazon EC2

instances that run in the us-west-1 Region. The company manually backs up the workloads to create an image as needed.
In the event of a natural disaster in the us-west-1 Region, the company wants to recover workloads quickly in the us-west-2 Region. The company wants no more than 24 hours of data loss on the EC2 instances. The company also wants to automate any backups of the EC2 instances.
Which solutions will meet these requirements with the LEAST administrative effort? (Choose two)
A. Create an Amazon EC2-backed Amazon Machine Image (AMI) lifecycle policy to create a backup based on tags. Schedule the backup to run twice daily. Copy the image on demand.
B. Create an Amazon EC2-backed Amazon Machine Image (AMI) lifecycle policy to create a backup based on tags. Schedule the backup to run twice daily. Configure the copy to the us-west-2 Region.
C. Create backup vaults in us-west-1 and in us-west-2 by using AWS Backup. Create a backup plan for the EC2 instances based on tag values. Create an AWS Lambda function to run as a scheduled job to copy the backup data to us-west-2.
D. Create a backup vault by using AWS Backup. Use AWS Backup to create a backup plan for the EC2 instances based on tag values. Define the destination for the copy as us-west-2. Specify the backup schedule to run twice daily.
E. Create a backup vault by using AWS Backup. Use AWS Backup to create a backup plan for the EC2 instances based on tag values. Specify the backup schedule to run twice daily. Copy on demand to us-west-2.
Answer: B, D
https://www.examtopics.com/discussions/amazon/view/109530-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
옵션 B 는 EC2 지원 Amazon 머신 이미지(AMI) 수명 주기 정책을 사용하여 백업 프로세스를 자동화할 것을 제안합니다. 하루에 두 번 실행되도록 정책을 구성하고 uswest-2 리전에 대한 복사본을 지정함으로써 회사는 정기적인 백업이 생성되고 대체 리전에 복사되도록 할 수 있습니다.
옵션 D 는 중앙 집중식 백업 관리 솔루션을 제공하는 AWS Backup 사용을 제안합니다. 태그 값을 기반으로 백업 볼트 및 백업 계획을 생성함으로써 회사는 EC2 인스턴스에 대한 백업 프로세스를 자동화할 수 있습니다.
백업 일정은 하루에 두 번 실행되도록 설정할 수 있으며 복사 대상은 us-west-2 리전으로 정의할 수 있습니다.

두 옵션 모두 백업 프로세스를 자동화하고 백업을 us-west-2 리전에 복사하는 것을 포함하여 재해 발생 시 데이터 복원력을 보장합니다. 이러한 솔루션은 AWS 서비스에서 제공하는 자동화된 백업 및 복사 메커니즘을 활용하여 관리 작업을 최소화합니다.

Q509

A company operates a two-tier application for image processing. The application uses two Availability Zones, each with one public subnet and one private subnet. An Application Load Balancer (ALB) for the web tier uses the public subnets. Amazon EC2 instances for the application tier use the private subnets.

Users report that the application is running more slowly than expected. A security audit of the web server log files shows that the application is receiving millions of illegitimate requests from a small number of IP addresses. A solutions architect needs to resolve the immediate performance problem while the company investigates a more permanent solution.

What should the solutions architect recommend to meet this requirement?

A. Modify the inbound security group for the web tier. Add a deny rule for the IP addresses that are consuming resources.

B. Modify the network ACL for the web tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.

C. Modify the inbound security group for the application tier. Add a deny rule for the IP addresses that are consuming resources.

D. Modify the network ACL for the application tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.

Answer: B

https://www.examtopics.com/discussions/amazon/view/109531-exam-aws-certified-solutions-architect-associate-saa-c03/

설명

퍼블릭 서브넷의 첫 번째 항목에서 요청을 거부하고 프라이빗 서브넷에 도달하는 것을 허용하지 마십시오.

이 시나리오에서 보안 감사는 애플리케이션이 소수의 IP 주소로부터 수백만 건의 불법 요청을 수신하고 있음을 보여줍니다. 이 문제를 해결하려면 웹 계층 서브넷에 대한 네트워크 ACL(액세스 제어 목록)을 수정하는 것이 좋습니다. 리소스를 소비하는 IP 주소를 특별히 대상으로 하는 인바운드 거부 규칙을 추가함으로써 네트워크 ACL 은 불법 트래픽이 웹 서버에 도달하기 전에 서브넷 수준에서 차단할 수 있습니다. 이는 웹 계층의 과도한

로드를 완화하고 애플리케이션의 성능을 향상시키는 데 도움이 됩니다.

Q510

A global marketing company has applications that run in the ap-southeast-2 Region and the eu-west-1 Region. Applications that run in a VPC in eu-west-1 need to communicate securely with databases that run in a VPC in ap-southeast-2.

Which network design will meet these requirements?

A. Create a VPC peering connection between the eu-west-1 VPC and the ap-southeast-2 VPC. Create an inbound rule in the eu-west-1 application security group that allows traffic from the database server IP addresses in the ap-southeast-2 security group.

B. Configure a VPC peering connection between the ap-southeast-2 VPC and the eu-west-1 VPC. Update the subnet route tables. Create an inbound rule in the ap-southeast-2 database security group that references the security group ID of the application servers in eu-west-1.

C. Configure a VPC peering connection between the ap-southeast-2 VPC and the eu-west-1 VPUpdate the subnet route tables. Create an inbound rule in the ap-southeast-2 database security group that allows traffic from the eu-west-1 application server IP addresses.

D. Create a transit gateway with a peering attachment between the eu-west-1 VPC and the ap-southeast-2 VPC. After the transit gateways are properly peered and routing is configured, create an inbound rule in the database security group that references the security group ID of the application servers in eu-west-1.

Answer: C

https://www.examtopics.com/discussions/amazon/view/109708-exam-aws-certified-solutions-architect-associate-saa-c03/

설명

다른 리전에 있는 피어 VPC 의 보안 그룹을 참조할 수 없습니다. 대신 피어 VPC 의 CIDR 블록을 사용하십시오.

https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-securitygroups.html

Q511

A company is developing software that uses a PostgreSQL database schema. The company needs to configure multiple development environments and databases for the company's

developers. On average, each development environment is used for half of the 8-hour workday.

Which solution will meet these requirements MOST cost-effectively?

A. Configure each development environment with its own Amazon Aurora PostgreSQL database

B. Configure each development environment with its own Amazon RDS for PostgreSQL Single-AZ DB instances

C. Configure each development environment with its own Amazon Aurora On-Demand PostgreSQL-Compatible database

D. Configure each development environment with its own Amazon S3 bucket by using Amazon S3 Object Select

Answer: C

https://www.examtopics.com/discussions/amazon/view/109532-exam-aws-certified-solutions-architect-associate-saa-c03/

Q512

A company uses AWS Organizations with resources tagged by account. The company also uses AWS Backup to back up its AWS infrastructure resources. The company needs to back up all AWS resources.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS Config to identify all untagged resources. Tag the identified resources programmatically. Use tags in the backup plan.

B. Use AWS Config to identify all resources that are not running. Add those resources to the backup vault.

C. Require all AWS account owners to review their resources to identify the resources that need to be backed up.

D. Use Amazon Inspector to identify all noncompliant resources.

Answer: A

https://www.examtopics.com/discussions/amazon/view/109709-exam-aws-certified-solutions-architect-associate-saa-c03/

Q513

A social media company wants to allow its users to upload images in an application that is

hosted in the AWS Cloud. The company needs a solution that automatically resizes the images so that the images can be displayed on multiple device types. The application experiences unpredictable traffic patterns throughout the day. The company is seeking a highly available solution that maximizes scalability.

What should a solutions architect do to meet these requirements?

A. Create a static website hosted in Amazon S3 that invokes AWS Lambda functions to resize the images and store the images in an Amazon S3 bucket.

B. Create a static website hosted in Amazon CloudFront that invokes AWS Step Functions to resize the images and store the images in an Amazon RDS database.

C. Create a dynamic website hosted on a web server that runs on an Amazon EC2 instance. Configure a process that runs on the EC2 instance to resize the images and store the images in an Amazon S3 bucket.

D. Create a dynamic website hosted on an automatically scaling Amazon Elastic Container Service (Amazon ECS) cluster that creates a resize job in Amazon Simple Queue Service (Amazon SQS). Set up an image-resizing program that runs on an Amazon EC2 instance to process the resize jobs.

Answer: A

https://www.examtopics.com/discussions/amazon/view/109713-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 :

Amazon S3 와 AWS Lambda 를 함께 사용하면 확장성과 가용성이 뛰어난 이미지 크기 조정 기능을 제공하는 서버리스 아키텍처를 생성할 수 있습니다.

솔루션이 작동하는 방식은 다음과 같습니다.

사용자가 업로드한 원본 이미지를 저장하도록 Amazon S3 버킷을 설정합니다.

새 이미지가 업로드될 때마다 AWS Lambda 함수를 호출하도록 S3 버킷에서 이벤트 트리거를 구성합니다.

Lambda 함수는 업로드된 이미지를 검색하고, 장치 요구 사항에 따라 필요한 크기 조정 작업을 수행하고, 크기 조정된 이미지를 S3 버킷 또는 크기 조정된 이미지용으로 지정된 다른 버킷에 다시 저장하도록 설계할 수 있습니다.

사용자에게 제공하기 위해 크기 조정된 이미지에 공개적으로 액세스할 수 있도록 Amazon S3 버킷을 구성합니다.

Q514

A company is running a microservices application on Amazon EC2 instances. The company

wants to migrate the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for scalability. The company must configure the Amazon EKS control plane with endpoint private access set to true and endpoint public access set to false to maintain security compliance. The company must also put the data plane in private subnets. However, the company has received error notifications because the node cannot join the cluster.
Which solution will allow the node to join the cluster?
A. Grant the required permission in AWS Identity and Access Management (IAM) to the AmazonEKSNodeRole IAM role.
B. Create interface VPC endpoints to allow nodes to access the control plane.
C. Recreate nodes in the public subnet. Restrict security groups for EC2 nodes.
D. Allow outbound traffic in the security group of the nodes.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109534-exam-aws-certified-solutions-architect-associate-saa-c03/

설명
클러스터의 VPC 내 Kubernetes API 요청(예: 노드와 컨트롤 플레인 통신)은 프라이빗 VPC 엔드포인트를 사용합니다.
https://docs.aws.amazon.com/eks/latest/userguide/cluster-endpoint.html

Q515
A company is migrating an on-premises application to AWS. The company wants to use Amazon Redshift as a solution.
Which use cases are suitable for Amazon Redshift in this scenario? (Choose three)
A. Supporting data APIs to access data with traditional, containerized, and event-driven applications
B. Supporting client-side and server-side encryption
C. Building analytics workloads during specified hours and when the application is not active
D. Caching data to reduce the pressure on the backend database
E. Scaling globally to support petabytes of data and tens of millions of requests per minute
F. Creating a secondary replica of the cluster by using the AWS Management Console
Answer: B, C, E
https://www.examtopics.com/discussions/amazon/view/109535-exam-aws-certified-solutions-architect-associate-saa-c03/

Q516

A company provides an API interface to customers so the customers can retrieve their financial information. The company expects a larger number of requests during peak usage times of the year.

The company requires the API to respond consistently with low latency to ensure customer satisfaction. The company needs to provide a compute host for the API.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use an Application Load Balancer and Amazon Elastic Container Service (Amazon ECS).

B. Use Amazon API Gateway and AWS Lambda functions with provisioned concurrency.

C. Use an Application Load Balancer and an Amazon Elastic Kubernetes Service (Amazon EKS) cluster.

D. Use Amazon API Gateway and AWS Lambda functions with reserved concurrency.

Answer: B

https://www.examtopics.com/discussions/amazon/view/109719-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪

Amazon API Gateway 는 개발자가 모든 규모에서 API 를 쉽게 생성, 게시, 유지 관리, 모니터링 및 보호할 수 있게 해주는 완전관리형 서비스입니다. AWS Lambda 는 서버를 프로비저닝하거나 관리하지 않고도 코드를 실행할 수 있는 서버리스 컴퓨팅 서비스입니다. Lambda 는 들어오는 요청에 따라 자동으로 확장되지만 수요가 갑자기 증가하면 함수의 새 인스턴스를 초기화하는 데 시간이 걸릴 수 있습니다. 이로 인해 API 에 대한 긴 대기 시간 또는 콜드 스타트가 발생할 수 있습니다. 이를 방지하기 위해 함수가 초기화되고 언제든지 응답할 준비가 되도록 프로비저닝된 동시성을 사용할 수 있습니다. 프로비저닝된 동시성은 또한 확장이 성능에 미치는 영향을 줄임으로써 API 의 지연 시간을 일관되게 줄이는 데 도움이 됩니다.

참조:

https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-develop-integrationslambda.html

https://docs.aws.amazon.com/lambda/latest/dg/configuration-concurrency.html

Q517

A company wants to send all AWS Systems Manager Session Manager logs to an Amazon S3

bucket for archival purposes.

Which solution will meet this requirement with the MOST operational efficiency?

A. Enable S3 logging in the Systems Manager console. Choose an S3 bucket to send the session data to.

B. Install the Amazon CloudWatch agent. Push all logs to a CloudWatch log group. Export the logs to an S3 bucket from the group for archival purposes.

C. Create a Systems Manager document to upload all server logs to a central S3 bucket. Use Amazon EventBridge to run the Systems Manager document against all servers that are in the account daily.

D. Install an Amazon CloudWatch agent. Push all logs to a CloudWatch log group. Create a CloudWatch logs subscription that pushes any incoming log events to an Amazon Kinesis Data Firehose delivery stream. Set Amazon S3 as the destination.

Answer: A

https://www.examtopics.com/discussions/amazon/view/109536-exam-aws-certified-solutions-architect-associate-saa-c03/

Q518

An application uses an Amazon RDS MySQL DB instance. The RDS database is becoming low on disk space. A solutions architect wants to increase the disk space without downtime. Which solution meets these requirements with the LEAST amount of effort?

A. Enable storage autoscaling in RDS

B. Increase the RDS database instance size

C. Change the RDS database instance storage type to Provisioned IOPS

D. Back up the RDS database, increase the storage capacity, restore the database, and stop the previous instance

Answer: A

https://www.examtopics.com/discussions/amazon/view/109721-exam-aws-certified-solutions-architect-associate-saa-c03/

▪

Q519

A consulting company provides professional services to customers worldwide. The company provides solutions and tools for customers to expedite gathering and analyzing data on AWS. The company needs to centrally manage and deploy a common set of

solutions and tools for customers to use for self-service purposes.
Which solution will meet these requirements?
A. Create AWS CloudFormation templates for the customers.
B. Create AWS Service Catalog products for the customers.
C. Create AWS Systems Manager templates for the customers.
D. Create AWS Config items for the customers.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109722-exam-aws-certified-solutions-architect-associate-saa-c03/

Q520
A company is designing a new web application that will run on Amazon EC2 Instances. The application will use Amazon DynamoDB for backend data storage. The application traffic will be unpredictable. The company expects that the application read and write throughput to the database will be moderate to high. The company needs to scale in response to application traffic.
Which DynamoDB table configuration will meet these requirements MOST cost-effectively?
A. Configure DynamoDB with provisioned read and write by using the DynamoDB Standard table class. Set DynamoDB auto scaling to a maximum defined capacity.
B. Configure DynamoDB in on-demand mode by using the DynamoDB Standard table class.
C. Configure DynamoDB with provisioned read and write by using the DynamoDB Standard Infrequent Access (DynamoDB Standard-IA) table class. Set DynamoDB auto scaling to a maximum defined capacity.
D. Configure DynamoDB in on-demand mode by using the DynamoDB Standard Infrequent Access (DynamoDB Standard-IA) table class.
Answer: B
https://www.examtopics.com/discussions/amazon/view/109539-exam-aws-certified-solutions-architect-associate-saa-c03/

Q521
A retail company has several businesses. The IT team for each business manages its own AWS account. Each team account is part of an organization in AWS Organizations. Each team monitors its product inventory levels in an Amazon DynamoDB table in the team's own AWS account.

The company is deploying a central inventory reporting application into a shared AWS account. The application must be able to read items from all the teams' DynamoDB tables. Which authentication option will meet these requirements MOST securely?

A. Integrate DynamoDB with AWS Secrets Manager in the inventory application account. Configure the application to use the correct secret from Secrets Manager to authenticate and read the DynamoDB table. Schedule secret rotation for every 30 days.

B. In every business account, create an IAM user that has programmatic access. Configure the application to use the correct IAM user access key ID and secret access key to authenticate and read the DynamoDB table. Manually rotate IAM access keys every 30 days.

C. In every business account, create an IAM role named BU_ROLE with a policy that gives the role access to the DynamoDB table and a trust policy to trust a specific role in the inventory application account. In the inventory account, create a role named APP_ROLE that allows access to the STS AssumeRole API operation. Configure the application to use APP_ROLE and assume the crossaccount role BU_ROLE to read the DynamoDB table.

D. Integrate DynamoDB with AWS Certificate Manager (ACM). Generate identity certificates to authenticate DynamoDB. Configure the application to use the correct certificate to authenticate and read the DynamoDB table.

Answer: C

https://www.examtopics.com/discussions/amazon/view/109703-exam-aws-certified-solutions-architect-associate-saa-c03/

▪

Q522

A company runs container applications by using Amazon Elastic Kubernetes Service (Amazon EKS). The company's workload is not consistent throughout the day. The company wants Amazon EKS to scale in and out according to the workload.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two)

A. Use an AWS Lambda function to resize the EKS cluster.

B. Use the Kubernetes Metrics Server to activate horizontal pod autoscaling.

C. Use the Kubernetes Cluster Autoscaler to manage the number of nodes in the cluster.

D. Use Amazon API Gateway and connect it to Amazon EKS.

E. Use AWS App Mesh to observe network activity.

Answer: B, C

https://www.examtopics.com/discussions/amazon/view/109702-exam-aws-certified-sol

utions-architect-associate-saa-c03/

설명:
https://docs.aws.amazon.com/eks/latest/userguide/horizontal-pod-autoscaler.html
https://docs.aws.amazon.com/eks/latest/userguide/autoscaling.html
수평적 포드 자동 확장은 해당 리소스의 CPU 사용률을 기반으로 배포, 복제 컨트롤러 또는 복제 세트의 포드 수를 자동으로 확장하는 Kubernetes 의 기능입니다. CPU 사용량 데이터를 제공하려면 Kubernetes Metrics Server 와 같은 메트릭 소스가 필요합니다. 클러스터 자동 크기 조정은 Pod 가 실패하거나 다른 노드로 다시 예약될 때 클러스터의 노드 수를 자동으로 조정하는 Kubernetes 의 기능입니다. 클러스터 2 에 가입하는 EC2 인스턴스를 관리하려면 AWS Auto Scaling 그룹과의 통합이 필요합니다. 이 솔루션은 수평적 포드 자동 확장과 클러스터 자동 확장을 모두 사용하여 Amazon EKS 가 워크로드에 따라 확장 및 축소되도록 할 수 있습니다.

Q523
A company runs a microservice-based serverless web application. The application must be able to retrieve data from multiple Amazon DynamoDB tables A solutions architect needs to give the application the ability to retrieve the data with no impact on the baseline performance of the application.
Which solution will meet these requirements in the MOST operationally efficient way?
A. AWS AppSync pipeline resolvers
B. Amazon CloudFront with Lambda@Edge functions
C. Edge-optimized Amazon API Gateway with AWS Lambda functions
D. Amazon Athena Federated Query with a DynamoDB connector
Answer: D
https://www.examtopics.com/discussions/amazon/view/109701-exam-aws-certified-solutions-architect-associate-saa-c03/
B??

Q524
A company wants to analyze and troubleshoot Access Denied errors and Unauthorized errors that are related to IAM permissions. The company has AWS CloudTrail turned on.
Which solution will meet these requirements with the LEAST effort?
A. Use AWS Glue and write custom scripts to query CloudTrail logs for the errors.

B. Use AWS Batch and write custom scripts to query CloudTrail logs for the errors.
C. Search CloudTrail logs with Amazon Athena queries to identify the errors.
D. Search CloudTrail logs with Amazon QuickSight. Create a dashboard to identify the errors.
Answer: C
https://www.examtopics.com/discussions/amazon/view/111425-exam-aws-certified-solutions-architect-associate-saa-c03/
D??

Q525
A company wants to add its existing AWS usage cost to its operation cost dashboard. A solutions architect needs to recommend a solution that will give the company access to its usage cost programmatically. The company must be able to access cost data for the current year and forecast costs for the next 12 months.
Which solution will meet these requirements with the LEAST operational overhead?
A. Access usage cost-related data by using the AWS Cost Explorer API with pagination.
B. Access usage cost-related data by using downloadable AWS Cost Explorer report .csv files.
C. Configure AWS Budgets actions to send usage cost data to the company through FTP.
D. Create AWS Budgets reports for usage cost data. Send the data to the company through SMTP.
Answer: A
https://www.examtopics.com/discussions/amazon/view/111278-exam-aws-certified-solutions-architect-associate-saa-c03/
▪

Q526
A solutions architect is reviewing the resilience of an application. The solutions architect notices that a database administrator recently failed over the application's Amazon Aurora PostgreSQL database writer instance as part of a scaling exercise. The failover resulted in 3 minutes of downtime for the application.
Which solution will reduce the downtime for scaling exercises with the LEAST operational overhead?
A. Create more Aurora PostgreSQL read replicas in the cluster to handle the load during

failover.
B. Set up a secondary Aurora PostgreSQL cluster in the same AWS Region. During failover, update the application to use the secondary cluster's writer endpoint.
C. Create an Amazon ElastiCache for Memcached cluster to handle the load during failover.
D. Set up an Amazon RDS proxy for the database. Update the application to use the proxy endpoint.
Answer: D
https://www.examtopics.com/discussions/amazon/view/111245-exam-aws-certified-solutions-architect-associate-saa-c03/
▪

Q527
A company has a regional subscription-based streaming service that runs in a single AWS Region. The architecture consists of web servers and application servers on Amazon EC2 instances. The EC2 instances are in Auto Scaling groups behind Elastic Load Balancers. The architecture includes an Amazon Aurora global database cluster that extends across multiple Availability Zones.
The company wants to expand globally and to ensure that its application has minimal downtime.
Which solution will provide the MOST fault tolerance?
A. Extend the Auto Scaling groups for the web tier and the application tier to deploy instances in Availability Zones in a second Region. Use an Aurora global database to deploy the database in the primary Region and the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region.
B. Deploy the web tier and the application tier to a second Region. Add an Aurora PostgreSQL cross-Region Aurora Replica in the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region. Promote the secondary to primary as needed.
C. Deploy the web tier and the application tier to a second Region. Create an Aurora PostgreSQL database in the second Region. Use AWS Database Migration Service (AWS DMS) to replicate the primary database to the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region.
D. Deploy the web tier and the application tier to a second Region. Use an Amazon Aurora global database to deploy the database in the primary Region and the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region. Promote

the secondary to primary as needed.
Answer: D
https://www.examtopics.com/discussions/amazon/view/111428-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 옵션은 애플리케이션에 고가용성과 중복성을 제공하는 두 번째 리전에 웹 계층과 애플리케이션 계층을 배포하기 때문에 가장 효율적입니다. 또한 단일 Aurora 데이터베이스가 여러 AWS 지역에 걸쳐 있을 수 있도록 하는 기능인 Amazon Aurora 글로벌 데이터베이스를 사용합니다. 또한 기본 지역과 두 번째 지역에 데이터베이스를 배포하여 지연 시간이 짧은 글로벌 읽기 및 지역 중단 시 빠른 복구를 제공합니다. 또한 두 번째 리전에 대한 장애 조치 라우팅 정책과 함께 Amazon Route 53 상태 확인을 사용하여 다른 리전의 정상적인 엔드포인트로 트래픽을 라우팅하여 데이터 보호를 제공합니다. 또한 필요에 따라 보조를 기본으로 승격하여 한 번에 리전 중 하나에서 쓰기 작업을 허용하여 데이터 일관성을 제공합니다. 이 솔루션은 전 세계적으로 확장하고 해당 애플리케이션의 다운타임을 최소화해야 한다는 요구 사항을 충족합니다.

옵션 A 는 웹 계층 및 애플리케이션 계층에 대한 Auto Scaling 그룹을 확장하여 두 번째 리전의 가용 영역에 인스턴스를 배포하기 때문에 효율성이 떨어집니다. 이렇게 하면 별도로 배포하는 것보다 더 높은 비용과 복잡성이 발생할 수 있습니다. 또한 Aurora 글로벌 데이터베이스를 사용하여 기본 리전과 두 번째 리전에 데이터베이스를 배포합니다. 이는 맞습니다. 그러나 두 번째 리전에 대한 장애 조치 라우팅 정책과 함께 Amazon Route 53 상태 확인을 사용하지 않으므로 트래픽이 비정상 엔드포인트로 라우팅될 수 있습니다.

옵션 B 는 웹 계층과 애플리케이션 계층을 올바른 두 번째 리전에 배포하기 때문에 효율성이 떨어집니다. 또한 두 번째 리전에 Aurora PostgreSQL 교차 리전 Aurora 복제본을 추가하여 리전 간 읽기 확장성을 제공합니다. 그러나 리전 간 복제본보다 더 빠른 복제 및 복구를 제공하는 Aurora 글로벌 데이터베이스를 사용하지 않습니다. 또한 올바른 두 번째 리전에 대한 장애 조치 라우팅 정책과 함께 Amazon Route 53 상태 확인을 사용합니다. 그러나 필요에 따라 보조를 기본으로 승격하지 않으므로 데이터 불일치 또는 손실이 발생할 수 있습니다.

옵션 C 는 웹 계층과 애플리케이션 계층을 올바른 두 번째 리전에 배포하기 때문에 효율성이 떨어집니다.
또한 두 번째 리전에 Aurora PostgreSQL 데이터베이스를 생성하여 리전 간 데이터 중복성을 제공합니다. 그러나 별도의 데이터베이스를 생성하는 것보다 더 빠른 복제 및

복구를 제공하는 Aurora 글로벌 데이터베이스 또는 리전 간 복제본을 사용하지 않습니다. 또한 AWS DMS(AWS Database Migration Service)를 사용하여 기본 데이터베이스를 두 번째 리전에 복제하여 서로 다른 소스와 대상 간에 데이터 마이그레이션을 제공합니다. 그러나 AWS DMS 를 사용하는 것보다 더 빠른 복제 및 복구를 제공하는 Aurora 글로벌 데이터베이스 또는 리전 간 복제본을 사용하지 않습니다. 또한 올바른 두 번째 리전에 대한 장애 조치 라우팅 정책과 함께 Amazon Route 53 상태 확인을 사용합니다.

Q528

A data analytics company wants to migrate its batch processing system to AWS. The company receives thousands of small data files periodically during the day through FTP. An on-premises batch job processes the data files overnight. However, the batch job takes hours to finish running.

The company wants the AWS solution to process incoming data files as soon as possible with minimal changes to the FTP clients that send the files. The solution must delete the incoming data files after the files have been processed successfully. Processing for each file needs to take 3-8 minutes.

Which solution will meet these requirements in the MOST operationally efficient way?

A. Use an Amazon EC2 instance that runs an FTP server to store incoming files as objects in Amazon S3 Glacier Flexible Retrieval. Configure a job queue in AWS Batch. Use Amazon EventBridge rules to invoke the job to process the objects nightly from S3 Glacier Flexible Retrieval. Delete the objects after the job has processed the objects.

B. Use an Amazon EC2 instance that runs an FTP server to store incoming files on an Amazon Elastic Block Store (Amazon EBS) volume. Configure a job queue in AWS Batch. Use Amazon EventBridge rules to invoke the job to process the files nightly from the EBS volume. Delete the files after the job has processed the files.

C. Use AWS Transfer Family to create an FTP server to store incoming files on an Amazon Elastic Block Store (Amazon EBS) volume. Configure a job queue in AWS Batch. Use an Amazon S3 event notification when each file arrives to invoke the job in AWS Batch. Delete the files after the job has processed the files.

D. Use AWS Transfer Family to create an FTP server to store incoming files in Amazon S3 Standard. Create an AWS Lambda function to process the files and to delete the files after they are processed. Use an S3 event notification to invoke the Lambda function when the files arrive.

Answer: D

https://www.examtopics.com/discussions/amazon/view/111317-exam-aws-certified-sol

utions-architect-associate-saa-c03/

설명: ▪
이 옵션은 AWS Transfer Family 를 사용하여 저비용 고가용성 스토리지 서비스인 Amazon S3 Standard 에 수신 파일을 저장할 수 있는 FTP 서버를 생성하기 때문에 운영상 가장 효율적입니다. 또한 AWS Lambda 를 사용하여 파일을 처리하고 처리 후 삭제합니다. 이는 배치 스케줄링이나 인프라 관리가 필요하지 않은 확장 가능한 서버리스 솔루션입니다. 또한 S3 이벤트 알림을 사용하여 파일이 도착하면 Lambda 함수를 호출하여 수신 데이터 파일을 거의 실시간으로 처리할 수 있습니다.

옵션 A 는 Amazon S3 Standard 보다 검색 비용이 높고 검색 시간이 긴 콜드 스토리지 클래스인 Amazon S3 Glacier Flexible Retrieval 을 사용하기 때문에 효율성이 떨어집니다. 또한 EventBridge 규칙을 사용하여 야간에 작업을 호출하므로 들어오는 데이터 파일을 가능한 한 빨리 처리해야 한다는 요구 사항을 충족하지 않습니다.

옵션 B 는 EBS 볼륨을 사용하여 수신 파일을 저장하기 때문에 효율성이 떨어집니다. 이는 Amazon S3 보다 비용이 높고 내구성이 낮은 블록 스토리지 서비스입니다. 또한 EventBridge 규칙을 사용하여 야간에 작업을 호출하므로 들어오는 데이터 파일을 가능한 한 빨리 처리해야 한다는 요구 사항을 충족하지 않습니다.

옵션 C 는 EBS 볼륨을 사용하여 수신 파일을 저장하기 때문에 효율성이 떨어집니다. 이는 Amazon S3 보다 비용이 높고 내구성이 낮은 블록 스토리지 서비스입니다. 또한 AWS Batch 를 사용하여 파일을 처리하므로 컴퓨팅 리소스와 작업 대기열을 관리해야 합니다.

Q529
A company is migrating its workloads to AWS. The company has transactional and sensitive data in its databases. The company wants to use AWS Cloud solutions to increase security and reduce operational overhead for the databases.
Which solution will meet these requirements?
A. Migrate the databases to Amazon EC2. Use an AWS Key Management Service (AWS KMS) AWS managed key for encryption.
B. Migrate the databases to Amazon RDS Configure encryption at rest.
C. Migrate the data to Amazon S3 Use Amazon Macie for data security and protection.
D. Migrate the database to Amazon RDS. Use Amazon CloudWatch Logs for data security and protection.

Answer: B

https://www.examtopics.com/discussions/amazon/view/111246-exam-aws-certified-solutions-architect-associate-saa-c03/

▪

Q530

A company has an online gaming application that has TCP and UDP multiplayer gaming capabilities. The company uses Amazon Route 53 to point the application traffic to multiple Network Load Balancers (NLBs) in different AWS Regions. The company needs to improve application performance and decrease latency for the online game in preparation for user growth.

Which solution will meet these requirements?

A. Add an Amazon CloudFront distribution in front of the NLBs. Increase the Cache-Control max-age parameter.

B. Replace the NLBs with Application Load Balancers (ALBs). Configure Route 53 to use latency-based routing.

C. Add AWS Global Accelerator in front of the NLBs. Configure a Global Accelerator endpoint to use the correct listener ports.

D. Add an Amazon API Gateway endpoint behind the NLBs. Enable API caching. Override method caching for the different stages.

Answer: C

https://www.examtopics.com/discussions/amazon/view/111271-exam-aws-certified-solutions-architect-associate-saa-c03/

▪

Q531

A company needs to integrate with a third-party data feed. The data feed sends a webhook to notify an external service when new data is ready for consumption. A developer wrote an AWS Lambda function to retrieve data when the company receives a webhook callback. The developer must make the Lambda function available for the third party to call.

Which solution will meet these requirements with the MOST operational efficiency?

A. Create a function URL for the Lambda function. Provide the Lambda function URL to the third party for the webhook.

B. Deploy an Application Load Balancer (ALB) in front of the Lambda function. Provide the

ALB URL to the third party for the webhook.
C. Create an Amazon Simple Notification Service (Amazon SNS) topic. Attach the topic to the Lambda function. Provide the public hostname of the SNS topic to the third party for the webhook.
D. Create an Amazon Simple Queue Service (Amazon SQS) queue. Attach the queue to the Lambda function. Provide the public hostname of the SQS queue to the third party for the webhook.
Answer: A
https://www.examtopics.com/discussions/amazon/view/111430-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
함수 URL 은 HTTPS 를 통해 함수를 호출하는 데 사용할 수 있는 Lambda 함수의 고유 식별자입니다. 함수가 배포된 AWS 리전의 API 엔드포인트와 function1 의 이름 또는 ARN 으로 구성됩니다. Lambda 함수에 대한 함수 URL 을 생성함으로써 솔루션은 제 3 자가 Lambda 함수를 가장 효율적으로 호출할 수 있도록 할 수 있습니다.
1. Lambda 함수 앞에 Application Load Balancer(ALB)를 배포합니다. Webhook 에 대한 ALB URL 을 타사에 제공합니다. 이 솔루션은 HTTPS 를 통해 Lambda 함수를 호출하는 데 필요하지 않은 추가 리소스(ALB)를 생성하고 관리하기 때문에 최고의 운영 효율성 요구 사항을 충족하지 않습니다.
2. Amazon Simple Notification Service(Amazon SNS) 주제를 생성합니다. Lambda 함수에 주제를 연결합니다. Webhook 에 대한 제 3 자에게 SNS 주제의 공개 호스트 이름을 제공합니다. Amazon SNS 주제에는 웹훅으로 사용할 수 있는 공개 호스트 이름이 없기 때문에 이 솔루션은 작동하지 않습니다. SNS 주제는 외부 소스로부터 메시지를 받는 것이 아니라 구독자에게 메시지를 게시하는 데 사용됩니다.
3. Amazon Simple Queue Service(Amazon SQS) 대기열을 생성합니다. 대기열을 Lambda 함수에 연결합니다. Webhook 에 대해 타사에 SQS 대기열의 공개 호스트 이름을 제공합니다. Amazon SQS 대기열에는 웹훅으로 사용할 수 있는 공개 호스트 이름이 없기 때문에 이 솔루션은 작동하지 않습니다. SQS 대기열은 외부 소스에서 메시지를 수신하는 것이 아니라 AWS 서비스 간에 메시지를 전송, 저장 및 수신하는 데 사용됩니다.
참조 URL:
https://docs.aws.amazon.com/lambda/latest/dg/lambda-api-permissions-ref.html

Q532
A company has a workload in an AWS Region. Customers connect to and access the

workload by using an Amazon API Gateway REST API. The company uses Amazon Route 53 as its DNS provider. The company wants to provide individual and secure URLs for all customers.

Which combination of steps will meet these requirements with the MOST operational efficiency? (Choose three)

A. Register the required domain in a registrar. Create a wildcard custom domain name in a Route 53 hosted zone and record in the zone that points to the API Gateway endpoint.

B. Request a wildcard certificate that matches the domains in AWS Certificate Manager (ACM) in a different Region.

C. Create hosted zones for each customer as required in Route 53. Create zone records that point to the API Gateway endpoint.

D. Request a wildcard certificate that matches the custom domain name in AWS Certificate Manager (ACM) in the same Region.

E. Create multiple API endpoints for each customer in API Gateway.

F. Create a custom domain name in API Gateway for the REST API. Import the certificate from AWS Certificate Manager (ACM).

Answer: A, D, F

https://www.examtopics.com/discussions/amazon/view/111382-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪

API Gateway REST API 를 사용하는 모든 고객에게 개별 보안 URL 을 제공하려면 다음 단계를 수행해야 합니다.

a) 등록 기관에 필요한 도메인을 등록합니다. Route 53 호스팅 영역에서 와일드카드 사용자 지정 도메인 이름을 생성하고 API 게이트웨이 엔드포인트를 가리키는 영역에 기록합니다. 이 단계를 통해 API Gateway 에서 생성한 기본 도메인 이름 대신 API 에 대한 사용자 지정 도메인 이름을 사용할 수 있습니다. 와일드카드 사용자 지정 도메인 이름은 도메인 이름 아래의 모든 하위 도메인(예: customer1.example.com 또는 customer2.example.com)을 사용하여 API 에 액세스할 수 있음을 의미합니다. 도메인 이름을 등록 대행자(예: Route 53 또는 타사 등록 대행자)에 등록하고 도메인 이름에 대해 Route 53 에 호스팅 영역을 생성해야 합니다. 또한 별칭 레코드를 사용하여 API Gateway 엔드포인트를 가리키는 호스팅 영역에 레코드를 생성해야 합니다.

d) 동일한 리전의 AWS Certificate Manager(ACM)에서 사용자 지정 도메인 이름과 일치하는 와일드카드 인증서를 요청합니다. 이 단계에서는 ACM 에서 발급한 인증서를 사용하여

HTTPS 로 API 를 보호할 수 있습니다. 와일드카드 인증서는 도메인 이름 아래의 모든 하위 도메인(예: *.example.com)과 일치할 수 있음을 의미합니다. 사용자 지정 도메인 이름과 일치하는 ACM 에서 인증서를 요청하거나 가져와 도메인 이름을 소유하고 있는지 확인해야 합니다. 또한 API 와 동일한 리전에서 인증서를 요청해야 합니다.

f) API Gateway 에서 REST API 용 사용자 지정 도메인 이름을 생성합니다. AWS Certificate Manager(ACM)에서 인증서를 가져옵니다. 이 단계에서는 사용자 지정 도메인 이름을 API 와 연결하고 ACM 의 인증서를 사용하여 HTTPS 를 활성화할 수 있습니다. API Gateway 에서 REST API 용 사용자 지정 도메인 이름을 생성하고 ACM 에서 인증서 ARN 을 지정해야 합니다. 또한 사용자 지정 도메인 이름에서 API 단계로 경로를 매핑하는 기본 경로 매핑을 생성해야 합니다.

Q533

A company stores data in Amazon S3. According to regulations, the data must not contain personally identifiable information (PII). The company recently discovered that S3 buckets have some objects that contain PII. The company needs to automatically detect PII in S3 buckets and to notify the company's security team.

Which solution will meet these requirements?

A. Use Amazon Macie. Create an Amazon EventBridge rule to filter the SensitiveData event type from Macie findings and to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.

B. Use Amazon GuardDuty. Create an Amazon EventBridge rule to filter the CRITICAL event type from GuardDuty findings and to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.

C. Use Amazon Macie. Create an Amazon EventBridge rule to filter the SensitiveData:S3Object/Personal event type from Macie findings and to send an Amazon Simple Queue Service (Amazon SQS) notification to the security team.

D. Use Amazon GuardDuty. Create an Amazon EventBridge rule to filter the CRITICAL event type from GuardDuty findings and to send an Amazon Simple Queue Service (Amazon SQS) notification to the security team.

Answer: A

https://www.examtopics.com/discussions/amazon/view/111432-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

Amazon Macie 는 또한 다양한 소스의 데이터를 사용하여 애플리케이션을 쉽게 연결할 수 있게 해주는 서버리스 이벤트 버스인 Amazon EventBridge 로 결과를 보낼 수 있습니다. Macie 결과에서 SensitiveData 이벤트 유형을 필터링하고 보안 팀에 Amazon SNS 알림을 보내는 EventBridge 규칙을 생성할 수 있습니다. Amazon SNS 는 구독자 또는 다른 애플리케이션에 메시지를 보낼 수 있는 완전 관리형 메시징 서비스입니다.
참조:
https://docs.aws.amazon.com/macie/latest/userguide/macie-findings.html#macie-findingseventbridge

Q534
A company wants to build a logging solution for its multiple AWS accounts. The company currently stores the logs from all accounts in a centralized account. The company has created an Amazon S3 bucket in the centralized account to store the VPC flow logs and AWS CloudTrail logs. All logs must be highly available for 30 days for frequent analysis, retained for an additional 60 days for backup purposes, and deleted 90 days after creation.
Which solution will meet these requirements MOST cost-effectively?
A. Transition objects to the S3 Standard storage class 30 days after creation. Write an expiration action that directs Amazon S3 to delete objects after 90 days.
B. Transition objects to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class 30 days after creation. Move all objects to the S3 Glacier Flexible Retrieval storage class after 90 days. Write an expiration action that directs Amazon S3 to delete objects after 90 days.
C. Transition objects to the S3 Glacier Flexible Retrieval storage class 30 days after creation. Write an expiration action that directs Amazon S3 to delete objects after 90 days.
D. Transition objects to the S3 One Zone-Infrequent Access (S3 One Zone-IA) storage class 30 days after creation. Move all objects to the S3 Glacier Flexible Retrieval storage class after 90 days. Write an expiration action that directs Amazon S3 to delete objects after 90 days.
Answer: C
https://www.examtopics.com/discussions/amazon/view/111434-exam-aws-certified-solutions-architect-associate-saa-c03/

Q535
A company is building an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for its

workloads. All secrets that are stored in Amazon EKS must be encrypted in the Kubernetes etcd key-value store.

Which solution will meet these requirements?

A. Create a new AWS Key Management Service (AWS KMS) key. Use AWS Secrets Manager to manage, rotate, and store all secrets in Amazon EKS.

B. Create a new AWS Key Management Service (AWS KMS) key. Enable Amazon EKS KMS secrets encryption on the Amazon EKS cluster.

C. Create the Amazon EKS cluster with default options. Use the Amazon Elastic Block Store (Amazon EBS) Container Storage Interface (CSI) driver as an add-on.

D. Create a new AWS Key Management Service (AWS KMS) key with the alias/aws/ebs alias. Enable default Amazon Elastic Block Store (Amazon EBS) volume encryption for the account.

Answer: B

https://www.examtopics.com/discussions/amazon/view/111385-exam-aws-certified-solutions-architect-associate-saa-c03/

Q536

A company wants to provide data scientists with near real-time read-only access to the company's production Amazon RDS for PostgreSQL database. The database is currently configured as a Single-AZ database. The data scientists use complex queries that will not affect the production database. The company needs a solution that is highly available.

Which solution will meet these requirements MOST cost-effectively?

A. Scale the existing production database in a maintenance window to provide enough power for the data scientists.

B. Change the setup from a Single-AZ to a Multi-AZ instance deployment with a larger secondary standby instance. Provide the data scientists access to the secondary instance.

C. Change the setup from a Single-AZ to a Multi-AZ instance deployment. Provide two additional read replicas for the data scientists.

D. Change the setup from a Single-AZ to a Multi-AZ cluster deployment with two readable standby instances. Provide read endpoints to the data scientists.

Answer: D

https://www.examtopics.com/discussions/amazon/view/111435-exam-aws-certified-solutions-architect-associate-saa-c03/

Q537

A company runs a three-tier web application in the AWS Cloud that operates across three Availability Zones. The application architecture has an Application Load Balancer, an Amazon EC2 web server that hosts user session states, and a MySQL database that runs on an EC2 instance. The company expects sudden increases in application traffic. The company wants to be able to scale to meet future application capacity demands and to ensure high availability across all three Availability Zones.

Which solution will meet these requirements?

A. Migrate the MySQL database to Amazon RDS for MySQL with a Multi-AZ DB cluster deployment. Use Amazon ElastiCache for Redis with high availability to store session data and to cache reads. Migrate the web server to an Auto Scaling group that is in three Availability Zones.

B. Migrate the MySQL database to Amazon RDS for MySQL with a Multi-AZ DB cluster deployment. Use Amazon ElastiCache for Memcached with high availability to store session data and to cache reads. Migrate the web server to an Auto Scaling group that is in three Availability Zones.

C. Migrate the MySQL database to Amazon DynamoDB Use DynamoDB Accelerator (DAX) to cache reads. Store the session data in DynamoDB. Migrate the web server to an Auto Scaling group that is in three Availability Zones.

D. Migrate the MySQL database to Amazon RDS for MySQL in a single Availability Zone. Use Amazon ElastiCache for Redis with high availability to store session data and to cache reads. Migrate the web server to an Auto Scaling group that is in three Availability Zones.

Answer: A

https://www.examtopics.com/discussions/amazon/view/111386-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

이 답변은 향후 애플리케이션 용량 요구 사항을 충족하기 위한 확장 요구 사항을 충족하고 세 가용 영역 모두에서 고가용성을 보장하기 때문에 정답입니다. 다중 AZ DB 클러스터 배포를 사용하여 MySQL 데이터베이스를 MySQL 용 Amazon RDS 로 마이그레이션함으로써 회사는 여러 가용 영역에서 데이터베이스의 자동 장애 조치, 백업 및 패치 적용의 이점을 누릴 수 있습니다. 고가용성 Redis 용 Amazon ElastiCache 를 사용하여 회사는 가용 영역 전체에서 장애 조치할 수 있는 빠른 인 메모리 데이터 저장소에 세션 데이터 및 캐시 읽기를 저장할 수 있습니다. 3 개의 가용 영역에 있는 Auto Scaling 그룹으로 웹 서버를 마이그레이션함으로써 회사는 수요 및 트래픽 패턴에 따라 웹 서버 용량을 자동으로 확장할 수 있습니다.

참조:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html
https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/AutoFailover.html
https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html

Q538
A global video streaming company uses Amazon CloudFront as a content distribution network (CDN). The company wants to roll out content in a phased manner across multiple countries. The company needs to ensure that viewers who are outside the countries to which the company rolls out content are not able to view the content.
Which solution will meet these requirements?
A. Add geographic restrictions to the content in CloudFront by using an allow list. Set up a custom error message.
B. Set up a new URL tor restricted content. Authorize access by using a signed URL and cookies. Set up a custom error message.
C. Encrypt the data for the content that the company distributes. Set up a custom error message.
D. Create a new URL for restricted content. Set up a time-restricted access policy for signed URLs.
Answer: A
https://www.examtopics.com/discussions/amazon/view/111387-exam-aws-certified-solutions-architect-associate-saa-c03/
▪

Q539
A company wants to use the AWS Cloud to improve its on-premises disaster recovery (DR) configuration. The company's core production business application uses Microsoft SQL Server Standard, which runs on a virtual machine (VM). The application has a recovery point objective (RPO) of 30 seconds or fewer and a recovery time objective (RTO) of 60 minutes. The DR solution needs to minimize costs wherever possible.
Which solution will meet these requirements?
A. Configure a multi-site active/active setup between the on-premises server and AWS by

using Microsoft SQL Server Enterprise with Always On availability groups.
B. Configure a warm standby Amazon RDS for SQL Server database on AWS. Configure AWS Database Migration Service (AWS DMS) to use change data capture (CDC).
C. Use AWS Elastic Disaster Recovery configured to replicate disk changes to AWS as a pilot light.
D. Use third-party backup software to capture backups every night. Store a secondary set of backups in Amazon S3.
Answer: B
https://www.examtopics.com/discussions/amazon/view/111301-exam-aws-certified-solutions-architect-associate-saa-c03/

Q540
A company has an on-premises server that uses an Oracle database to process and store customer information. The company wants to use an AWS database service to achieve higher availability and to improve application performance. The company also wants to offload reporting from its primary database system.
Which solution will meet these requirements in the MOST operationally efficient way?
A. Use AWS Database Migration Service (AWS DMS) to create an Amazon RDS DB instance in multiple AWS Regions. Point the reporting functions toward a separate DB instance from the primary DB instance.
B. Use Amazon RDS in a Single-AZ deployment to create an Oracle database. Create a read replica in the same zone as the primary DB instance. Direct the reporting functions to the read replica.
C. Use Amazon RDS deployed in a Multi-AZ cluster deployment to create an Oracle database. Direct the reporting functions to use the reader instance in the cluster deployment.
D. Use Amazon RDS deployed in a Multi-AZ instance deployment to create an Amazon Aurora database. Direct the reporting functions to the reader instances.
Answer: D
https://www.examtopics.com/discussions/amazon/view/111439-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Amazon Aurora 는 MySQL 및 PostgreSQL 과 호환되는 완전관리형 관계형 데이터베이스입니다. MySQL 보다 최대 5 배, PostgreSQL 보다 최대 3 배 뛰어난 성능을

제공합니다. 또한 여러 가용 영역에 걸쳐 데이터를 복제하고 데이터를 Amazon S31 에 지속적으로 백업하여 고가용성과 내구성을 제공합니다. 다중 AZ 인스턴스 배포에 배포된 Amazon RDS 를 사용하여 Amazon Aurora 데이터베이스를 생성함으로써 솔루션은 더 높은 가용성을 달성하고 애플리케이션 성능을 개선할 수 있습니다.
Amazon Aurora 는 기본 인스턴스와 동일한 기본 스토리지를 공유하는 별도의 인스턴스인 읽기 전용 복제본을 지원합니다. 읽기 전용 복제본을 사용하여 기본 인스턴스에서 읽기 전용 쿼리를 오프로드하고 성능을 향상할 수 있습니다. 읽기 전용 복제본은 보고 기능에도 사용할 수 있습니다.
보고 기능을 판독기 인스턴스로 지정함으로써 솔루션은 기본 데이터베이스 시스템에서 보고를 오프로드할 수 있습니다.
1. AWS Database Migration Service(AWS DMS)를 사용하여 여러 AWS 리전에서 Amazon RDS DB 인스턴스 생성 보고 기능이 기본 DB 인스턴스와 별도의 DB 인스턴스를 가리키도록 합니다. 이 솔루션은 AWS 데이터베이스 서비스 사용 요구 사항을 충족하지 않습니다. AWS DMS 는 데이터베이스 서비스 자체가 아니라 사용자가 데이터베이스를 AWS 로 마이그레이션하는 데 도움을 주는 서비스이기 때문입니다. 또한 서로 다른 리전에서 여러 DB 인스턴스를 생성해야 하므로 복잡성과 비용이 증가할 수 있습니다.
2. 단일 AZ 배포에서 Amazon RDS 를 사용하여 Oracle 데이터베이스 생성 기본 DB 인스턴스와 동일한 영역에 읽기 전용 복제본을 생성합니다. 보고 기능을 읽기 전용 복제본으로 지정합니다. 단일 AZ 배포는 가용 영역 중단 시 장애 조치 보호를 제공하지 않으므로 이 솔루션은 고가용성 달성 요구 사항을 충족하지 않습니다. 또한 Oracle 을 데이터베이스 엔진으로 사용하므로 Aurora보다 더 나은 성능을 제공하지 못할 수 있습니다.
3. 다중 AZ 클러스터 배포에 배포된 Amazon RDS 를 사용하여 Oracle 데이터베이스 생성 클러스터 배포에서 리더 인스턴스를 사용하도록 보고 기능에 지시합니다. Oracle 이 Aurora 보다 더 나은 성능을 제공하지 않을 수 있으므로 이 솔루션은 애플리케이션 성능 향상 요구 사항을 충족하지 않습니다. 또한 Oracle 이 아닌 Aurora 에서만 지원되는 클러스터 배포를 사용합니다.

참조:
https://aws.amazon.com/rds/aurora/

Q541
A company wants to build a web application on AWS. Client access requests to the website are not predictable and can be idle for a long time. Only customers who have paid a subscription fee can have the ability to sign in and use the web application.
Which combination of steps will meet these requirements MOST cost-effectively? (Choose

three)

A. Create an AWS Lambda function to retrieve user information from Amazon DynamoDB. Create an Amazon API Gateway endpoint to accept RESTful APIs. Send the API calls to the Lambda function.

B. Create an Amazon Elastic Container Service (Amazon ECS) service behind an Application Load Balancer to retrieve user information from Amazon RDS. Create an Amazon API Gateway endpoint to accept RESTful APIs. Send the API calls to the Lambda function.

C. Create an Amazon Cognito user pool to authenticate users.

D. Create an Amazon Cognito identity pool to authenticate users.

E. Use AWS Amplify to serve the frontend web content with HTML, CSS, and JS. Use an integrated Amazon CloudFront configuration.

F. Use Amazon S3 static web hosting with PHP, CSS, and JS. Use Amazon CloudFront to serve the frontend web content.

Answer: A, C, E

https://www.examtopics.com/discussions/amazon/view/111440-exam-aws-certified-solutions-architect-associate-saa-c03/

참고

https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html

Q542

A media company uses an Amazon CloudFront distribution to deliver content over the internet. The company wants only premium customers to have access to the media streams and file content. The company stores all content in an Amazon S3 bucket. The company also delivers content on demand to customers for a specific purpose, such as movie rentals or music downloads.

Which solution will meet these requirements?

A. Generate and provide S3 signed cookies to premium customers.

B. Generate and provide CloudFront signed URLs to premium customers.

C. Use origin access control (OAC) to limit the access of non-premium customers.

D. Generate and activate field-level encryption to block non-premium customers.

Answer: B

https://www.examtopics.com/discussions/amazon/view/111441-exam-aws-certified-solutions-architect-associate-saa-c03/

▪

Q543

A company runs Amazon EC2 instances in multiple AWS accounts that are individually bled. The company recently purchased a Savings Pian. Because of changes in the company's business requirements, the company has decommissioned a large number of EC2 instances. The company wants to use its Savings Plan discounts on its other AWS accounts.

Which combination of steps will meet these requirements? (Choose two)

A. From the AWS Account Management Console of the management account, turn on discount sharing from the billing preferences section.

B. From the AWS Account Management Console of the account that purchased the existing Savings Plan, turn on discount sharing from the billing preferences section. Include all accounts.

C. From the AWS Organizations management account, use AWS Resource Access Manager (AWS RAM) to share the Savings Plan with other accounts.

D. Create an organization in AWS Organizations in a new payer account. Invite the other AWS accounts to join the organization from the management account.

E. Create an organization in AWS Organizations in the existing AWS account with the existing EC2 instances and Savings Plan. Invite the other AWS accounts to join the organization from the management account.

Answer: A, E

https://www.examtopics.com/discussions/amazon/view/111442-exam-aws-certified-solutions-architect-associate-saa-c03/

Q544

A retail company uses a regional Amazon API Gateway API for its public REST APIs. The API Gateway endpoint is a custom domain name that points to an Amazon Route 53 alias record. A solutions architect needs to create a solution that has minimal effects on customers and minimal data loss to release the new version of APIs.

Which solution will meet these requirements?

A. Create a canary release deployment stage for API Gateway. Deploy the latest API version. Point an appropriate percentage of traffic to the canary stage. After API verification, promote the canary stage to the production stage.

B. Create a new API Gateway endpoint with a new version of the API in OpenAPI YAML file format. Use the import-to-update operation in merge mode into the API in API Gateway.

Deploy the new version of the API to the production stage.
C. Create a new API Gateway endpoint with a new version of the API in OpenAPI JSON file format. Use the import-to-update operation in overwrite mode into the API in API Gateway. Deploy the new version of the API to the production stage.
D. Create a new API Gateway endpoint with new versions of the API definitions. Create a custom domain name for the new API Gateway API. Point the Route 53 alias record to the new API Gateway API custom domain name.
Answer: A
https://www.examtopics.com/discussions/amazon/view/111450-exam-aws-certified-solutions-architect-associate-saa-c03/

설명: ▪
이 답변은 고객에게 미치는 영향을 최소화하고 데이터 손실을 최소화하면서 API 의 새 버전을 릴리스하기 위한 요구 사항을 충족하므로 정확합니다. 카나리아 릴리스 배포는 테스트 목적으로 API 의 새 버전을 배포하고 기본 버전은 동일한 단계에서 일반 작업을 위해 프로덕션 릴리스로 배포된 상태로 유지하는 소프트웨어 개발 전략입니다. 카나리아 릴리스 배포에서 총 API 트래픽은 미리 구성된 비율로 프로덕션 릴리스와 카나리아 릴리스로 무작위로 분리됩니다. 일반적으로 카나리아 릴리스는 API 트래픽의 작은 비율을 수신하고 프로덕션 릴리스가 나머지를 차지합니다. 업데이트된 API 기능은 카나리아를 통한 API 트래픽에만 표시됩니다. 카나리아 트래픽 비율을 조정하여 테스트 범위 또는 성능을 최적화할 수 있습니다. 카나리아 트래픽을 작게 유지하고 선택을 무작위로 유지함으로써 대부분의 사용자는 새 버전의 잠재적인 버그로 인해 언제든지 악영향을 받지 않으며 단일 사용자도 항상 악영향을 받지 않습니다. 테스트 메트릭이 요구 사항을 통과한 후 canary 릴리스를 프로덕션 릴리스로 승격하고 배포에서 canary 를 비활성화할 수 있습니다. 이렇게 하면 생산 단계에서 새로운 기능을 사용할 수 있습니다.

참조:
https://docs.aws.amazon.com/apigateway/latest/developerguide/canary-release.html

Q545
A company wants to direct its users to a backup static error page if the company's primary website is unavailable. The primary website's DNS records are hosted in Amazon Route 53. The domain is pointing to an Application Load Balancer (ALB). The company needs a solution that minimizes changes and infrastructure overhead.
Which solution will meet these requirements?

A. Update the Route 53 records to use a latency routing policy. Add a static error page that is hosted in an Amazon S3 bucket to the records so that the traffic is sent to the most responsive endpoints.
B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page that is hosted in an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
C. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance that hosts a static error page as endpoints. Configure Route 53 to send requests to the instance only if the health checks fail for the ALB.
D. Update the Route 53 records to use a multivalue answer routing policy. Create a health check. Direct traffic to the website if the health check passes. Direct traffic to a static error page that is hosted in Amazon S3 if the health check does not pass.
Answer: B
https://www.examtopics.com/discussions/amazon/view/116974-exam-aws-certified-solutions-architect-associate-saa-c03/

설명 1:
Route 53 상태 확인을 사용하여 활성-활성 및 활성-수동 장애 조치 구성을 구성할 수 있습니다. 능동-수동 장애 조치 : 기본 리소스 또는 리소스 그룹을 대부분의 시간 동안 사용할 수 있도록 하고 모든 기본 리소스를 사용할 수 없는 경우에 대비하여 보조 리소스 또는 리소스 그룹을 대기 상태로 유지하려는 경우 활성-수동 장애 조치 구성을 사용합니다. 쿼리에 응답할 때 Route 53 에는 정상적인 기본 리소스만 포함됩니다. 모든 기본 리소스가 비정상인 경우 Route 53 은 DNS 쿼리에 대한 응답으로 정상적인 보조 리소스만 포함하기 시작합니다.
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html

설명 2:
이 솔루션은 기본 웹 사이트를 사용할 수 없는 경우 사용자를 백업 정적 오류 페이지로 안내하여 변경 및 인프라 오버헤드를 최소화하는 요구 사항을 충족합니다. Route 53 활성-수동 장애 조치 구성은 정상인 경우 기본 리소스로, 기본 리소스가 비정상인 경우 보조 리소스로 트래픽을 라우팅할 수 있습니다. Route 53 상태 확인은 ALB 엔드포인트의 상태를 모니터링하고 필요할 때 장애 조치를 트리거할 수 있습니다. 정적 오류 페이지는 웹사이트로 구성된 S3 버킷에서 호스팅할 수 있으며 이는 정적 콘텐츠를 제공하는 간단하고 비용 효율적인 방법입니다.
대기 시간 라우팅 정책을 사용하면 사용자에 대한 가장 낮은 네트워크 대기 시간을 기반으로 트래픽을 라우팅할 수 있지만 장애 조치 기능을 제공하지 않기 때문에 옵션 A 는

올바르지 않습니다.
ALB 및 EC2 인스턴스와 함께 활성-활성 구성을 사용하면 인프라 오버헤드와 복잡성이 증가할 수 있고 EC2 인스턴스가 항상 정상 상태임을 보장하지 않기 때문에 옵션 C 는 올바르지 않습니다.
다중값 응답 라우팅 정책을 사용하면 쿼리에 대해 여러 값을 반환할 수 있지만 장애 조치 기능을 제공하지 않기 때문에 옵션 D 는 올바르지 않습니다.

참조:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy-failover.html
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html
https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html

Q546
A recent analysis of a company's IT expenses highlights the need to reduce backup costs. The company's chief information officer wants to simplify the on-premises backup infrastructure and reduce costs by eliminating the use of physical backup tapes. The company must preserve the existing investment in the on-premises backup applications and workflows.
What should a solutions architect recommend?
A. Set up AWS Storage Gateway to connect with the backup applications using the NFS interface.
B. Set up an Amazon EFS file system that connects with the backup applications using the NFS interface.
C. Set up an Amazon EFS file system that connects with the backup applications using the iSCSI interface.
D. Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface.
Answer: D
https://www.examtopics.com/discussions/amazon/view/116975-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이를 통해 회사는 온프레미스 백업 인프라를 단순화하고 물리적 백업 테이프의 사용을 제거하여 비용을 절감할 수 있습니다. iSCSI-가상 테이프 라이브러리(VTL) 인터페이스를

사용하여 백업 애플리케이션과 연결하도록 AWS Storage Gateway 를 설정함으로써 회사는 S3 또는 Glacier 의 가상 테이프에 백업 데이터를 저장할 수 있습니다. 이를 통해 AWS 스토리지 서비스를 활용하는 동시에 온프레미스 백업 애플리케이션 및 워크플로에 대한 기존 투자를 보존합니다.

Q547

A company has data collection sensors at different locations. The data collection sensors stream a high volume of data to the company. The company wants to design a platform on AWS to ingest and process high-volume streaming data. The solution must be scalable and support data collection in near real time. The company must store the data in Amazon S3 for future reporting.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use Amazon Kinesis Data Firehose to deliver streaming data to Amazon S3.

B. Use AWS Glue to deliver streaming data to Amazon S3.

C. Use AWS Lambda to deliver streaming data and store the data to Amazon S3.

D. Use AWS Database Migration Service (AWS DMS) to deliver streaming data to Amazon S3.

Answer: A

https://www.examtopics.com/discussions/amazon/view/116976-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

최소한의 운영 오버헤드로 대용량 스트리밍 데이터를 수집하고 처리하려면 Amazon Kinesis Data Firehose 가 적합한 솔루션입니다. Amazon Kinesis Data Firehose 는 스트리밍 데이터를 캡처, 변환하여 Amazon S3 또는 기타 대상으로 전달할 수 있습니다. Amazon Kinesis Data Firehose 는 데이터 처리량에 맞춰 자동으로 확장하고 모든 양의 데이터를 처리할 수 있습니다. Amazon Kinesis Data Firehose 는 프로비저닝이나 관리를 위해 서버가 필요하지 않은 완전관리형 서비스이기도 합니다.

Q548

A company has separate AWS accounts for its finance, data analytics, and development departments. Because of costs and security concerns, the company wants to control which services each AWS account can use.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS Systems Manager templates to control which AWS services each department can use.
B. Create organization units (OUs) for each department in AWS Organizations. Attach service control policies (SCPs) to the OUs.
C. Use AWS CloudFormation to automatically provision only the AWS services that each department can use.
D. Set up a list of products in AWS Service Catalog in the AWS accounts to manage and control the usage of specific AWS services.
Answer: B
https://www.examtopics.com/discussions/amazon/view/116977-exam-aws-certified-solutions-architect-associate-saa-c03/

Q549
A company has created a multi-tier application for its ecommerce website. The website uses an Application Load Balancer that resides in the public subnets, a web tier in the public subnets, and a MySQL cluster hosted on Amazon EC2 instances in the private subnets. The MySQL database needs to retrieve product catalog and pricing information that is hosted on the internet by a third-party provider. A solutions architect must devise a strategy that maximizes security without increasing operational overhead.
What should the solutions architect do to meet these requirements?
A. Deploy a NAT instance in the VPC. Route all the internet-based traffic through the NAT instance.
B. Deploy a NAT gateway in the public subnets. Modify the private subnet route table to direct all internet-bound traffic to the NAT gateway.
C. Configure an internet gateway and attach it to the VPModify the private subnet route table to direct internet-bound traffic to the internet gateway.
D. Configure a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the virtual private gateway.
Answer: B
https://www.examtopics.com/discussions/amazon/view/116978-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
프라이빗 서브넷의 MySQL 데이터베이스가 공개적으로 노출되지 않고 인터넷에 액세스할 수 있도록 하려면 NAT 게이트웨이가 적합한 솔루션입니다. NAT 게이트웨이를 사용하면

프라이빗 서브넷의 인스턴스가 인터넷이나 다른 AWS 서비스에 연결할 수 있지만 인터넷이 해당 인스턴스와 연결을 시작하는 것은 방지됩니다. NAT 게이트웨이는 퍼블릭 서브넷에 상주하며 짧은 대기 시간으로 높은 트래픽 처리량을 처리할 수 있습니다. NAT 게이트웨이는 운영 오버헤드가 필요하지 않은 관리형 서비스이기도 합니다.

Q550

A company is using AWS Key Management Service (AWS KMS) keys to encrypt AWS Lambda environment variables. A solutions architect needs to ensure that the required permissions are in place to decrypt and use the environment variables.

Which steps must the solutions architect take to implement the correct permissions? (Choose two)

A. Add AWS KMS permissions in the Lambda resource policy.

B. Add AWS KMS permissions in the Lambda execution role.

C. Add AWS KMS permissions in the Lambda function policy.

D. Allow the Lambda execution role in the AWS KMS key policy.

E. Allow the Lambda resource policy in the AWS KMS key policy.

Answer: B, D

https://www.examtopics.com/discussions/amazon/view/116979-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

B 와 D 는 정답입니다. Lambda 실행 역할에 환경 변수를 해독하고 사용할 수 있는 권한이 있고 AWS KMS 키 정책에 따라 Lambda 실행 역할이 키를 사용할 수 있도록 허용하기 때문입니다. Lambda 실행 역할은 AWS KMS 와 같은 AWS 리소스에 액세스할 수 있는 권한을 Lambda 함수에 부여하는 IAM 역할입니다. AWS KMS 키 정책은 키에 대한 액세스를 제어하는 리소스 기반 정책입니다. Lambda 실행 역할에 AWS KMS 권한을 추가하고 AWS KMS 키 정책에서 Lambda 실행 역할을 허용함으로써 솔루션 아키텍트는 환경 변수를 암호화하고 해독하기 위한 올바른 권한을 구현할 수 있습니다.

Q551

A company has a financial application that produces reports. The reports average 50 KB in size and are stored in Amazon S3. The reports are frequently accessed during the first week after production and must be stored for several years. The reports must be retrievable within 6 hours.

Which solution meets these requirements MOST cost-effectively?

A. Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Glacier after 7 days.

B. Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days.

C. Use S3 Intelligent-Tiering. Configure S3 Intelligent-Tiering to transition the reports to S3 Standard-Infrequent Access (S3 Standard-IA) and S3 Glacier.

D. Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Glacier Deep Archive after 7 days.

Answer: A

https://www.examtopics.com/discussions/amazon/view/116896-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

첫 주 동안 자주 액세스하고 수년간 보관해야 하는 보고서를 저장하고 검색하려면 S3 Standard 와 S3 Glacier 가 적합한 솔루션입니다. S3 Standard 는 자주 액세스하는 데이터에 대해 높은 내구성, 가용성 및 성능을 제공합니다. S3 Glacier 는 저렴한 비용으로 장기 데이터 보관을 위한 안전하고 내구성 있는 스토리지를 제공합니다. S3 수명 주기 규칙을 사용하면 7 일 후에 보고서를 S3 Standard 에서 S3 Glacier 로 전환할 수 있으므로 스토리지 비용을 줄일 수 있습니다. S3 Glacier 는 6 시간 이내 검색도 지원합니다.

Q552

A company needs to optimize the cost of its Amazon EC2 instances. The company also needs to change the type and family of its EC2 instances every 2-3 months.

What should the company do to meet these requirements?

A. Purchase Partial Upfront Reserved Instances for a 3-year term.

B. Purchase a No Upfront Compute Savings Plan for a 1-year term.

C. Purchase All Upfront Reserved Instances for a 1-year term.

D. Purchase an All Upfront EC2 Instance Savings Plan for a 1-year term.

Answer: B

https://www.examtopics.com/discussions/amazon/view/116897-exam-aws-certified-solutions-architect-associate-saa-c03/

Q553

A solutions architect needs to review a company's Amazon S3 buckets to discover personally identifiable information (PII). The company stores the PII data in the us-east-1 Region and us-west-2 Region.

Which solution will meet these requirements with the LEAST operational overhead?

A. Configure Amazon Macie in each Region. Create a job to analyze the data that is in Amazon S3.

B. Configure AWS Security Hub for all Regions. Create an AWS Config rule to analyze the data that is in Amazon S3.

C. Configure Amazon Inspector to analyze the data that is in Amazon S3.

D. Configure Amazon GuardDuty to analyze the data that is in Amazon S3.

Answer: A

https://www.examtopics.com/discussions/amazon/view/117206-exam-aws-certified-solutions-architect-associate-saa-c03/

Q554

A company's SAP application has a backend SQL Server database in an on-premises environment. The company wants to migrate its on-premises application and database server to AWS. The company needs an instance type that meets the high demands of its SAP database. On-premises performance data shows that both the SAP application and the database have high memory utilization.

Which solution will meet these requirements?

A. Use the compute optimized instance family for the application. Use the memory optimized instance family for the database.

B. Use the storage optimized instance family for both the application and the database.

C. Use the memory optimized instance family for both the application and the database.

D. Use the high performance computing (HPC) optimized instance family for the application. Use the memory optimized instance family for the database.

Answer: C

https://www.examtopics.com/discussions/amazon/view/117442-exam-aws-certified-solutions-architect-associate-saa-c03/

Q555

A company runs an application in a VPC with public and private subnets. The VPC extends across multiple Availability Zones. The application runs on Amazon EC2 instances in private

subnets. The application uses an Amazon Simple Queue Service (Amazon SQS) queue.
A solutions architect needs to design a secure solution to establish a connection between the EC2 instances and the SQS queue.
Which solution will meet these requirements?
A. Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the private subnets. Add to the endpoint a security group that has an inbound access rule that allows traffic from the EC2 instances that are in the private subnets.
B. Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the public subnets. Attach to the interface endpoint a VPC endpoint policy that allows access from the EC2 instances that are in the private subnets.
C. Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the public subnets. Attach an Amazon SQS access policy to the interface VPC endpoint that allows requests from only a specified VPC endpoint.
D. Implement a gateway endpoint for Amazon SQS. Add a NAT gateway to the private subnets. Attach an IAM role to the EC2 instances that allows access to the SQS queue.
Answer: A
https://www.examtopics.com/discussions/amazon/view/116983-exam-aws-certified-solutions-architect-associate-saa-c03/

Q556
A solutions architect is using an AWS CloudFormation template to deploy a three-tier web application. The web application consists of a web tier and an application tier that stores and retrieves user data in Amazon DynamoDB tables. The web and application tiers are hosted on Amazon EC2 instances, and the database tier is not publicly accessible. The application EC2 instances need to access the DynamoDB tables without exposing API credentials in the template.
What should the solutions architect do to meet these requirements?
A. Create an IAM role to read the DynamoDB tables. Associate the role with the application instances by referencing an instance profile.
B. Create an IAM role that has the required permissions to read and write from the DynamoDB tables. Add the role to the EC2 instance profile, and associate the instance profile with the application instances.
C. Use the parameter section in the AWS CloudFormation template to have the user input access and secret keys from an already-created IAM user that has the required permissions to read and write from the DynamoDB tables.

D. Create an IAM user in the AWS CloudFormation template that has the required permissions to read and write from the DynamoDB tables. Use the GetAtt function to retrieve the access and secret keys, and pass them to the application instances through the user data.

Answer: B

https://www.examtopics.com/discussions/amazon/view/117434-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

이를 통해 애플리케이션 EC2 인스턴스는 템플릿에 API 자격 증명을 노출하지 않고도 DynamoDB 테이블에 액세스할 수 있습니다. DynamoDB 테이블에서 읽고 쓰는 데 필요한 권한이 있는 IAM 역할을 생성하고 이를 EC2 인스턴스 프로필에 추가하면 애플리케이션 인스턴스는 AWS 에서 자동으로 교체하는 임시 보안 자격 증명을 사용할 수 있습니다. 이는 EC2 인스턴스에서 AWS 리소스에 대한 액세스 권한을 부여하는 안전한 모범 사례 방법입니다.

Q557

A solutions architect manages an analytics application. The application stores large amounts of semistructured data in an Amazon S3 bucket. The solutions architect wants to use parallel data processing to process the data more quickly. The solutions architect also wants to use information that is stored in an Amazon Redshift database to enrich the data. Which solution will meet these requirements?

A. Use Amazon Athena to process the S3 data. Use AWS Glue with the Amazon Redshift data to enrich the S3 data.

B. Use Amazon EMR to process the S3 data. Use Amazon EMR with the Amazon Redshift data to enrich the S3 data.

C. Use Amazon EMR to process the S3 data. Use Amazon Kinesis Data Streams to move the S3 data into Amazon Redshift so that the data can be enriched.

D. Use AWS Glue to process the S3 data. Use AWS Lake Formation with the Amazon Redshift data to enrich the S3 data.

Answer: B

https://www.examtopics.com/discussions/amazon/view/117344-exam-aws-certified-solutions-architect-associate-saa-c03/

Q558

A company has two VPCs that are located in the us-west-2 Region within the same AWS account. The company needs to allow network traffic between these VPCs. Approximately 500 GB of data transfer will occur between the VPCs each month.

What is the MOST cost-effective solution to connect these VPCs?

A. Implement AWS Transit Gateway to connect the VPCs. Update the route tables of each VPC to use the transit gateway for inter-VPC communication.

B. Implement an AWS Site-to-Site VPN tunnel between the VPCs. Update the route tables of each VPC to use the VPN tunnel for inter-VPC communication.

C. Set up a VPC peering connection between the VPCs. Update the route tables of each VPC to use the VPC peering connection for inter-VPC communication.

D. Set up a 1 GB AWS Direct Connect connection between the VPCs. Update the route tables of each VPC to use the Direct Connect connection for inter-VPC communication.

Answer: C

https://www.examtopics.com/discussions/amazon/view/117053-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

동일한 AWS 계정 내 동일한 리전에 있는 두 개의 VPC 를 연결하려면 VPC 피어링이 가장 비용 효과적인 솔루션입니다. VPC 피어링을 사용하면 게이트웨이, VPN 연결 또는 AWS Transit Gateway 없이도 VPC 간의 직접 네트워크 트래픽을 허용할 수 있습니다. 또한 VPC 피어링은 VPC 간 데이터 전송에 대한 추가 요금을 발생시키지 않습니다.

Q559

A company hosts multiple applications on AWS for different product lines. The applications use different compute resources, including Amazon EC2 instances and Application Load Balancers. The applications run in different AWS accounts under the same organization in AWS Organizations across multiple AWS Regions. Teams for each product line have tagged each compute resource in the individual accounts.

The company wants more details about the cost for each product line from the consolidated billing feature in Organizations.

Which combination of steps will meet these requirements? (Choose two)

A. Select a specific AWS generated tag in the AWS Billing console.

B. Select a specific user-defined tag in the AWS Billing console.

C. Select a specific user-defined tag in the AWS Resource Groups console.

D. Activate the selected tag from each AWS account.
E. Activate the selected tag from the Organizations management account.
Answer: B, E
https://www.examtopics.com/discussions/amazon/view/117403-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
사용자 정의 태그는 AWS 리소스에 적용하여 분류하고 추적할 수 있는 키-값 쌍입니다. 사용자 정의 태그를 사용하여 비용을 할당하고 AWS 결제 콘솔에서 세부 결제 보고서를 생성할 수도 있습니다. 비용 할당을 위해 사용자 정의 태그를 사용하려면 조직의 모든 회원 계정에 대한 모든 권한을 갖는 루트 계정인 조직 마스터 계정에서 태그를 활성화해야 합니다. 활성화되면 사용자 정의 태그가 비용 할당 보고서의 열로 표시되며 제품 라인별로 비용을 필터링하고 그룹화하는 데 사용할 수 있습니다. 이 솔루션은 기존 태깅 전략을 활용하고 코드 개발이나 수동 개입이 필요하지 않으므로 최소한의 운영 오버헤드로 요구 사항을 충족합니다.

Q560
A company's solutions architect is designing an AWS multi-account solution that uses AWS Organizations. The solutions architect has organized the company's accounts into organizational units (OUs).
The solutions architect needs a solution that will identify any changes to the OU hierarchy. The solution also needs to notify the company's operations team of any changes.
Which solution will meet these requirements with the LEAST operational overhead?
A. Provision the AWS accounts by using AWS Control Tower. Use account drift notifications to identify the changes to the OU hierarchy.
B. Provision the AWS accounts by using AWS Control Tower. Use AWS Config aggregated rules to identify the changes to the OU hierarchy.
C. Use AWS Service Catalog to create accounts in Organizations. Use an AWS CloudTrail organization trail to identify the changes to the OU hierarchy.
D. Use AWS CloudFormation templates to create accounts in Organizations. Use the drift detection operation on a stack to identify the changes to the OU hierarchy.
Answer: A
https://www.examtopics.com/discussions/amazon/view/117021-exam-aws-certified-solutions-architect-associate-saa-c03/

Q561

A company's website handles millions of requests each day, and the number of requests continues to increase. A solutions architect needs to improve the response time of the web application. The solutions architect determines that the application needs to decrease latency when retrieving product details from the Amazon DynamoDB table.

Which solution will meet these requirements with the LEAST amount of operational overhead?

A. Set up a DynamoDB Accelerator (DAX) cluster. Route all read requests through DAX.

B. Set up Amazon ElastiCache for Redis between the DynamoDB table and the web application. Route all read requests through Redis.

C. Set up Amazon ElastiCache for Memcached between the DynamoDB table and the web application. Route all read requests through Memcached.

D. Set up Amazon DynamoDB Streams on the table, and have AWS Lambda read from the table and populate Amazon ElastiCache. Route all read requests through ElastiCache.

Answer: A

https://www.examtopics.com/discussions/amazon/view/117022-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

이를 통해 회사는 Amazon DynamoDB 테이블에서 제품 세부 정보를 검색할 때 웹 애플리케이션의 응답 시간을 개선하고 지연 시간을 줄일 수 있습니다. DynamoDB Accelerator(DAX) 클러스터를 설정함으로써 회사는 최대 10 배의 성능 향상을 제공하는 DynamoDB 용 완전 관리형 고가용성 인 메모리 캐시를 사용할 수 있습니다. 모든 읽기 요청을 DAX 를 통해 라우팅함으로써 회사는 DynamoDB 테이블에 대한 읽기 작업 수를 줄이고 사용자 경험을 향상시킬 수 있습니다.

Q562

A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not travel across the internet.

Which combination of steps should the solutions architect take to meet this requirement? (Choose two)

A. Create a route table entry for the endpoint.

B. Create a gateway endpoint for DynamoDB.

C. Create an interface endpoint for Amazon EC2.

D. Create an elastic network interface for the endpoint in each of the subnets of the VPC.
E. Create a security group entry in the endpoint's security group to provide access.
Answer: A, B
https://www.examtopics.com/discussions/amazon/view/117251-exam-aws-certified-solutions-architect-associate-saa-c03/

Q563
A company runs its applications on both Amazon Elastic Kubernetes Service (Amazon EKS) clusters and on-premises Kubernetes clusters. The company wants to view all clusters and workloads from a central location.
Which solution will meet these requirements with the LEAST operational overhead?
A. Use Amazon CloudWatch Container Insights to collect and group the cluster information.
B. Use Amazon EKS Connector to register and connect all Kubernetes clusters.
C. Use AWS Systems Manager to collect and view the cluster information.
D. Use Amazon EKS Anywhere as the primary cluster to view the other clusters with native Kubernetes commands.
Answer: B
https://www.examtopics.com/discussions/amazon/view/117023-exam-aws-certified-solutions-architect-associate-saa-c03/

Q564
A company is building an ecommerce application and needs to store sensitive customer information. The company needs to give customers the ability to complete purchase transactions on the website. The company also needs to ensure that sensitive customer data is protected, even from database administrators.
Which solution meets these requirements?
A. Store sensitive data in an Amazon Elastic Block Store (Amazon EBS) volume. Use EBS encryption to encrypt the data. Use an IAM instance role to restrict access.
B. Store sensitive data in Amazon RDS for MySQL. Use AWS Key Management Service (AWS KMS) client-side encryption to encrypt the data.
C. Store sensitive data in Amazon S3. Use AWS Key Management Service (AWS KMS) server-side encryption to encrypt the data. Use S3 bucket policies to restrict access.
D. Store sensitive data in Amazon FSx for Windows Server. Mount the file share on application servers. Use Windows file permissions to restrict access.

Answer: B
https://www.examtopics.com/discussions/amazon/view/117024-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이를 통해 회사는 중요한 고객 정보를 관리형 AWS 서비스에 저장하고 고객이 웹 사이트에서 구매 거래를 완료할 수 있는 기능을 제공할 수 있습니다. AWS Key Management Service(AWS KMS) 클라이언트 측 암호화를 사용하여 회사는 데이터를 MySQL 용 Amazon RDS 로 보내기 전에 암호화할 수 있습니다. 애플리케이션만이 암호화 키에 액세스할 수 있으므로 이를 통해 데이터베이스 관리자로부터도 민감한 고객 데이터가 보호됩니다.

Q565
A company has an on-premises MySQL database that handles transactional data. The company is migrating the database to the AWS Cloud. The migrated database must maintain compatibility with the company's applications that use the database. The migrated database also must scale automatically during periods of increased demand.
Which migration solution will meet these requirements?
A. Use native MySQL tools to migrate the database to Amazon RDS for MySQL. Configure elastic storage scaling.
B. Migrate the database to Amazon Redshift by using the mysqldump utility. Turn on Auto Scaling for the Amazon Redshift cluster.
C. Use AWS Database Migration Service (AWS DMS) to migrate the database to Amazon Aurora. Turn on Aurora Auto Scaling.
D. Use AWS Database Migration Service (AWS DMS) to migrate the database to Amazon DynamoDB. Configure an Auto Scaling policy.
Answer: C
https://www.examtopics.com/discussions/amazon/view/117025-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
호환성과 확장성을 갖춘 MySQL 데이터베이스를 AWS 로 마이그레이션하려면 Amazon Aurora 가 적합한 옵션입니다. Aurora 는 MySQL 과 호환되며 Aurora Auto Scaling 을 통해 자동으로 확장할 수 있습니다. AWS Database Migration Service(AWS DMS)를 사용하면 가동 중지 시간을 최소화하면서 온프레미스에서 Aurora 로 데이터베이스를 마이그레이션할 수 있습니다.

Q566

A company runs multiple Amazon EC2 Linux instances in a VPC across two Availability Zones. The instances host applications that use a hierarchical directory structure. The applications need to read and write rapidly and concurrently to shared storage.

What should a solutions architect do to meet these requirements?

A. Create an Amazon S3 bucket. Allow access from all the EC2 instances in the VPC.

B. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system from each EC2 instance.

C. Create a file system on a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume. Attach the EBS volume to all the EC2 instances.

D. Create file systems on Amazon Elastic Block Store (Amazon EBS) volumes that are attached to each EC2 instance. Synchronize the EBS volumes across the different EC2 instances.

Answer: B

https://www.examtopics.com/discussions/amazon/view/116902-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

이를 통해 EC2 인스턴스는 두 가용 영역에 걸쳐 공유 스토리지에 동시에 빠르게 읽고 쓸 수 있습니다. Amazon EFS 는 여러 EC2 인스턴스에서 탑재할 수 있는 확장 가능하고 탄력적이며 가용성이 높은 파일 시스템을 제공합니다. Amazon EFS 는 높은 수준의 처리량과 IOPS, 일관되게 낮은 지연 시간을 지원합니다. Amazon EFS 는 또한 높은 수준의 동시성을 지원하는 NFSv4 잠금 업그레이드 및 다운그레이드를 지원합니다.

Q567

A solutions architect is designing a workload that will store hourly energy consumption by business tenants in a building. The sensors will feed a database through HTTP requests that will add up usage for each tenant. The solutions architect must use managed services when possible. The workload will receive more features in the future as the solutions architect adds independent components.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use Amazon API Gateway with AWS Lambda functions to receive the data from the sensors, process the data, and store the data in an Amazon DynamoDB table.

B. Use an Elastic Load Balancer that is supported by an Auto Scaling group of Amazon EC2 instances to receive and process the data from the sensors. Use an Amazon S3 bucket to store the processed data.
C. Use Amazon API Gateway with AWS Lambda functions to receive the data from the sensors, process the data, and store the data in a Microsoft SQL Server Express database on an Amazon EC2 instance.
D. Use an Elastic Load Balancer that is supported by an Auto Scaling group of Amazon EC2 instances to receive and process the data from the sensors. Use an Amazon Elastic File System (Amazon EFS) shared file system to store the processed data.
Answer: A
https://www.examtopics.com/discussions/amazon/view/117026-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
AWS Lambda 에서 이벤트 기반 프로그래밍 모델을 사용하고 운영 오버헤드를 줄이려면 Amazon API Gateway 와 Amazon DynamoDB 가 적합한 솔루션입니다. Amazon API Gateway 는 센서로부터 데이터를 수신하고 AWS Lambda 함수를 호출하여 데이터를 처리할 수 있습니다. AWS Lambda 는 서버를 프로비저닝하거나 관리하지 않고도 코드를 실행하고 수신 요청에 따라 자동으로 확장할 수 있습니다. Amazon DynamoDB 는 일관된 성능으로 모든 양의 데이터를 처리할 수 있는 빠르고 유연한 NoSQL 데이터베이스에 데이터를 저장할 수 있습니다.

Q568
A solutions architect is designing the storage architecture for a new web application used for storing and viewing engineering drawings. All application components will be deployed on the AWS infrastructure.
The application design must support caching to minimize the amount of time that users wait for the engineering drawings to load. The application must be able to store petabytes of data.
Which combination of storage and caching should the solutions architect use?
A. Amazon S3 with Amazon CloudFront
B. Amazon S3 Glacier with Amazon ElastiCache
C. Amazon Elastic Block Store (Amazon EBS) volumes with Amazon CloudFront
D. AWS Storage Gateway with Amazon ElastiCache
Answer: A

https://www.examtopics.com/discussions/amazon/view/117027-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
캐싱 지원을 통해 엔지니어링 도면을 저장하고 보려면 Amazon S3 및 Amazon CloudFront 가 적합한 솔루션입니다. Amazon S3 는 높은 내구성, 가용성 및 성능으로 모든 양의 데이터를 저장할 수 있습니다. Amazon CloudFront 는 엔지니어링 도면을 사용자에게 더 가까운 엣지 로케이션에 배포하여 지연 시간을 줄이고 사용자 경험을 향상시킬 수 있습니다. Amazon CloudFront 는 엔지니어링 도면을 엣지 로케이션에 캐시할 수도 있으므로 사용자가 도면이 로드될 때까지 기다리는 시간을 최소화할 수 있습니다.

Q569
An Amazon EventBridge rule targets a third-party API. The third-party API has not received any incoming traffic. A solutions architect needs to determine whether the rule conditions are being met and if the rule's target is being invoked.
Which solution will meet these requirements?
A. Check for metrics in Amazon CloudWatch in the namespace for AWS/Events.
B. Review events in the Amazon Simple Queue Service (Amazon SQS) dead-letter queue.
C. Check for the events in Amazon CloudWatch Logs.
D. Check the trails in AWS CloudTrail for the EventBridge events.
Answer: A
https://www.examtopics.com/discussions/amazon/view/117377-exam-aws-certified-solutions-architect-associate-saa-c03/

Q570
A company has a large workload that runs every Friday evening. The workload runs on Amazon EC2 instances that are in two Availability Zones in the us-east-1 Region. Normally, the company must run no more than two instances at all times. However, the company wants to scale up to six instances each Friday to handle a regularly repeating increased workload.
Which solution will meet these requirements with the LEAST operational overhead?
A. Create a reminder in Amazon EventBridge to scale the instances.
B. Create an Auto Scaling group that has a scheduled action.
C. Create an Auto Scaling group that uses manual scaling.

D. Create an Auto Scaling group that uses automatic scaling.
Answer: B
https://www.examtopics.com/discussions/amazon/view/116903-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Auto Scaling 그룹은 유사한 특성을 공유하고 수요에 따라 자동으로 확장 또는 축소될 수 있는 EC2 인스턴스 모음입니다. Auto Scaling 그룹에는 특정 시간에 특정 크기로 확장하도록 그룹에 지시하는 구성인 예약된 작업이 있을 수 있습니다. 이러한 방식으로 회사는 매주 금요일 저녁 최대 6 개의 인스턴스로 확장하여 증가된 워크로드를 처리하고, 다른 시간에는 2 개의 인스턴스로 축소하여 비용을 절감할 수 있습니다. 이 솔루션은 수동 개입이나 사용자 지정 스크립트가 필요하지 않으므로 최소한의 운영 오버헤드로 요구 사항을 충족합니다.

Q571
A company is creating a REST API. The company has strict requirements for the use of TLS. The company requires TLSv1.3 on the API endpoints. The company also requires a specific public third-party certificate authority (CA) to sign the TLS certificate.
Which solution will meet these requirements?
A. Use a local machine to create a certificate that is signed by the third-party CImport the certificate into AWS Certificate Manager (ACM). Create an HTTP API in Amazon API Gateway with a custom domain. Configure the custom domain to use the certificate.
B. Create a certificate in AWS Certificate Manager (ACM) that is signed by the third-party CA. Create an HTTP API in Amazon API Gateway with a custom domain. Configure the custom domain to use the certificate.
C. Use AWS Certificate Manager (ACM) to create a certificate that is signed by the third-party CA. Import the certificate into AWS Certificate Manager (ACM). Create an AWS Lambda function with a Lambda function URL. Configure the Lambda function URL to use the certificate.
D. Create a certificate in AWS Certificate Manager (ACM) that is signed by the third-party CA. Create an AWS Lambda function with a Lambda function URL. Configure the Lambda function URL to use the certificate.
Answer: B
https://www.examtopics.com/discussions/amazon/view/116904-exam-aws-certified-solutions-architect-associate-saa-c03/

Q572

A company runs an application on AWS. The application receives inconsistent amounts of usage. The application uses AWS Direct Connect to connect to an on-premises MySQL-compatible database. The on-premises database consistently uses a minimum of 2 GiB of memory.

The company wants to migrate the on-premises database to a managed AWS service. The company wants to use auto scaling capabilities to manage unexpected workload increases.

Which solution will meet these requirements with the LEAST administrative overhead?

A. Provision an Amazon DynamoDB database with default read and write capacity settings.

B. Provision an Amazon Aurora database with a minimum capacity of 1 Aurora capacity unit (ACU).

C. Provision an Amazon Aurora Serverless v2 database with a minimum capacity of 1 Aurora capacity unit (ACU).

D. Provision an Amazon RDS for MySQL database with 2 GiB of memory.

Answer: C

https://www.examtopics.com/discussions/amazon/view/117029-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

이를 통해 회사는 온프레미스 데이터베이스를 Auto Scaling 기능을 지원하고 관리 오버헤드가 가장 적은 관리형 AWS 서비스로 마이그레이션할 수 있습니다. Amazon Aurora Serverless v2 는 워크로드 수요에 따라 컴퓨팅 용량을 자동으로 확장하는 Amazon Aurora 의 구성입니다. 단 몇 초 만에 수백 건에서 수십만 건의 트랜잭션을 확장할 수 있습니다. Amazon Aurora Serverless v2 는 MySQL 호환 데이터베이스와 AWS Direct Connect 연결도 지원합니다.

Q573

A company wants to use an event-driven programming model with AWS Lambda. The company wants to reduce startup latency for Lambda functions that run on Java 11. The company does not have strict latency requirements for the applications. The company wants to reduce cold starts and outlier latencies when a function scales up.

Which solution will meet these requirements MOST cost-effectively?

A. Configure Lambda provisioned concurrency.

B. Increase the timeout of the Lambda functions.
C. Increase the memory of the Lambda functions.
D. Configure Lambda SnapStart.
Answer: D
https://www.examtopics.com/discussions/amazon/view/116925-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Java 11 에서 실행되는 Lambda 함수의 시작 지연 시간을 줄이기 위해 Lambda SnapStart 가 적합한 솔루션입니다. Lambda SnapStart 는 Java 11 기능에 대한 더 빠른 콜드 스타트와 더 낮은 이상치 지연 시간을 지원하는 기능입니다. Lambda SnapStart 는 사전 초기화된 JVM(Java Virtual Machine)을 사용하여 기능을 실행하므로 초기화 시간과 메모리 공간이 줄어듭니다. Lambda SnapStart 에는 추가 비용이 발생하지 않습니다.

Q574
A financial services company launched a new application that uses an Amazon RDS for MySQL database. The company uses the application to track stock market trends. The company needs to operate the application for only 2 hours at the end of each week. The company needs to optimize the cost of running the database.
Which solution will meet these requirements MOST cost-effectively?
A. Migrate the existing RDS for MySQL database to an Aurora Serverless v2 MySQL database cluster.
B. Migrate the existing RDS for MySQL database to an Aurora MySQL database cluster.
C. Migrate the existing RDS for MySQL database to an Amazon EC2 instance that runs MySQL. Purchase an instance reservation for the EC2 instance.
D. Migrate the existing RDS for MySQL database to an Amazon Elastic Container Service (Amazon ECS) cluster that uses MySQL container images to run tasks.
Answer: A
https://www.examtopics.com/discussions/amazon/view/117272-exam-aws-certified-solutions-architect-associate-saa-c03/

Q575
A company deploys its applications on Amazon Elastic Kubernetes Service (Amazon EKS) behind an Application Load Balancer in an AWS Region. The application needs to store data

in a PostgreSQL database engine. The company wants the data in the database to be highly available. The company also needs increased capacity for read workloads.
Which solution will meet these requirements with the MOST operational efficiency?
A. Create an Amazon DynamoDB database table configured with global tables.
B. Create an Amazon RDS database with Multi-AZ deployments.
C. Create an Amazon RDS database with Multi-AZ DB cluster deployment.
D. Create an Amazon RDS database configured with cross-Region read replicas.
Answer: C
https://www.examtopics.com/discussions/amazon/view/116969-exam-aws-certified-solutions-architect-associate-saa-c03/

Q576
A company is building a RESTful serverless web application on AWS by using Amazon API Gateway and AWS Lambda. The users of this web application will be geographically distributed, and the company wants to reduce the latency of API requests to these users.
Which type of endpoint should a solutions architect use to meet these requirements?
A. Private endpoint
B. Regional endpoint
C. Interface VPC endpoint
D. Edge-optimized endpoint
Answer: D
https://www.examtopics.com/discussions/amazon/view/116906-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
엣지 최적화 API 엔드포인트는 API 요청을 가장 가까운 CloudFront POP(Point of Presence)로 라우팅하므로 지리적으로 분산된 클라이언트에 가장 적합합니다. 이렇게 하면 대기 시간이 줄어들고 API 성능이 향상됩니다. 엣지 최적화 엔드포인트는 API Gateway REST API 의 기본 유형입니다.
지역 API 엔드포인트는 API 와 동일한 지역에 있는 클라이언트를 위한 것이며 CloudFront 를 사용하여 요청을 라우팅하지 않습니다. 프라이빗 API 엔드포인트는 인터페이스 VPC 엔드포인트를 사용하여 VPC 에서만 액세스할 수 있는 API 엔드포인트입니다. 지역 또는 개인 끝점은 지리적으로 분산된 사용자의 대기 시간을 줄이는 요구 사항을 충족하지 않습니다.

Q577

A company uses an Amazon CloudFront distribution to serve content pages for its website. The company needs to ensure that clients use a TLS certificate when accessing the company's website. The company wants to automate the creation and renewal of the TLS certificates.

Which solution will meet these requirements with the MOST operational efficiency?

A. Use a CloudFront security policy to create a certificate.

B. Use a CloudFront origin access control (OAC) to create a certificate.

C. Use AWS Certificate Manager (ACM) to create a certificate. Use DNS validation for the domain.

D. Use AWS Certificate Manager (ACM) to create a certificate. Use email validation for the domain.

Answer: C

https://www.examtopics.com/discussions/amazon/view/117037-exam-aws-certified-solutions-architect-associate-saa-c03/

Q578

A company deployed a serverless application that uses Amazon DynamoDB as a database layer. The application has experienced a large increase in users. The company wants to improve database response time from milliseconds to microseconds and to cache requests to the database.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use DynamoDB Accelerator (DAX).

B. Migrate the database to Amazon Redshift.

C. Migrate the database to Amazon RDS.

D. Use Amazon ElastiCache for Redis.

Answer: A

https://www.examtopics.com/discussions/amazon/view/117038-exam-aws-certified-solutions-architect-associate-saa-c03/

Q579

A company runs an application that uses Amazon RDS for PostgreSQL. The application receives traffic only on weekdays during business hours. The company wants to optimize

costs and reduce operational overhead based on this usage.
Which solution will meet these requirements?
A. Use the Instance Scheduler on AWS to configure start and stop schedules.
B. Turn off automatic backups. Create weekly manual snapshots of the database.
C. Create a custom AWS Lambda function to start and stop the database based on minimum CPU utilization.
D. Purchase All Upfront reserved DB instances.
Answer: A
https://www.examtopics.com/discussions/amazon/view/116924-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
AWS 솔루션의 인스턴스 스케줄러는 Amazon Elastic Compute Cloud(Amazon EC2) 및 Amazon Relational Database Service(Amazon RDS) 인스턴스의 시작 및 중지를 자동화합니다. 이 솔루션은 사용하지 않는 리소스를 중지하고 필요할 때 시작하여 운영 비용을 절감하는 데 도움이 됩니다 1. 이 솔루션을 사용하면 명령줄 인터페이스(CLI) 또는 SSM 유지 관리 기간을 사용하여 맞춤형 일정과 기간을 정의할 수 있습니다. 선결제 없음, 부분 선결제, 전체 선결제 등 예약 DB 인스턴스에 대한 다양한 결제 옵션 중에서 선택할 수도 있습니다.

참고:
https://aws.amazon.com/ko/solutions/implementations/instance-scheduler-on-aws/?nc1=h_ls

Q580
A company uses locally attached storage to run a latency-sensitive application on premises. The company is using a lift and shift method to move the application to the AWS Cloud. The company does not want to change the application architecture.
Which solution will meet these requirements MOST cost-effectively?
A. Configure an Auto Scaling group with an Amazon EC2 instance. Use an Amazon FSx for Lustre file system to run the application.
B. Host the application on an Amazon EC2 instance. Use an Amazon Elastic Block Store (Amazon EBS) GP2 volume to run the application.
C. Configure an Auto Scaling group with an Amazon EC2 instance. Use an Amazon FSx for OpenZFS file system to run the application.

D. Host the application on an Amazon EC2 instance. Use an Amazon Elastic Block Store (Amazon EBS) GP3 volume to run the application.
Answer: D
https://www.examtopics.com/discussions/amazon/view/117663-exam-aws-certified-solutions-architect-associate-saa-c03/

Q581
A company runs a stateful production application on Amazon EC2 instances. The application requires at least two EC2 instances to always be running.
A solutions architect needs to design a highly available and fault-tolerant architecture for the application. The solutions architect creates an Auto Scaling group of EC2 instances.
Which set of additional steps should the solutions architect take to meet these requirements?
A. Set the Auto Scaling group's minimum capacity to two. Deploy one On-Demand Instance in one Availability Zone and one On-Demand Instance in a second Availability Zone.
B. Set the Auto Scaling group's minimum capacity to four. Deploy two On-Demand Instances in one Availability Zone and two On-Demand Instances in a second Availability Zone.
C. Set the Auto Scaling group's minimum capacity to two. Deploy four Spot Instances in one Availability Zone.
D. Set the Auto Scaling group's minimum capacity to four. Deploy two On-Demand Instances in one Availability Zone and two Spot Instances in a second Availability Zone.
Answer: B
https://www.examtopics.com/discussions/amazon/view/116968-exam-aws-certified-solutions-architect-associate-saa-c03/

Q582
An ecommerce company uses Amazon Route 53 as its DNS provider. The company hosts its website on premises and in the AWS Cloud. The company's on-premises data center is near the us-west-1 Region. The company uses the eu-central-1 Region to host the website. The company wants to minimize load time for the website as much as possible.
Which solution will meet these requirements?
A. Set up a geolocation routing policy. Send the traffic that is near us-west-1 to the on-premises data center. Send the traffic that is near eu-central-1 to eu-central-1.

B. Set up a simple routing policy that routes all traffic that is near eu-central-1 to eu-central-1 and routes all traffic that is near the on-premises datacenter to the on-premises data center.
C. Set up a latency routing policy. Associate the policy with us-west-1.
D. Set up a weighted routing policy. Split the traffic evenly between eu-central-1 and the on-premises data center.
Answer: A
https://www.examtopics.com/discussions/amazon/view/118597-exam-aws-certified-solutions-architect-associate-saa-c03/

Q583
A company has 5 PB of archived data on physical tapes. The company needs to preserve the data on the tapes for another 10 years for compliance purposes. The company wants to migrate to AWS in the next 6 months. The data center that stores the tapes has a 1 Gbps uplink internet connectivity.
Which solution will meet these requirements MOST cost-effectively?
A. Read the data from the tapes on premises. Stage the data in a local NFS storage. Use AWS DataSync to migrate the data to Amazon S3 Glacier Flexible Retrieval.
B. Use an on-premises backup application to read the data from the tapes and to write directly to Amazon S3 Glacier Deep Archive.
C. Order multiple AWS Snowball devices that have Tape Gateway. Copy the physical tapes to virtual tapes in Snowball. Ship the Snowball devices to AWS. Create a lifecycle policy to move the tapes to Amazon S3 Glacier Deep Archive.
D. Configure an on-premises Tape Gateway. Create virtual tapes in the AWS Cloud. Use backup software to copy the physical tape to the virtual tape.
Answer: C
https://www.examtopics.com/discussions/amazon/view/117215-exam-aws-certified-solutions-architect-associate-saa-c03/

Q584
A company is deploying an application that processes large quantities of data in parallel. The company plans to use Amazon EC2 instances for the workload. The network architecture must be configurable to prevent groups of nodes from sharing the same underlying hardware.

Which networking solution meets these requirements?

A. Run the EC2 instances in a spread placement group.

B. Group the EC2 instances in separate accounts.

C. Configure the EC2 instances with dedicated tenancy.

D. Configure the EC2 instances with shared tenancy.

Answer: A

https://www.examtopics.com/discussions/amazon/view/119485-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

이를 통해 회사는 대량의 데이터를 병렬로 처리하고 노드 그룹이 동일한 기본 하드웨어를 공유하는 것을 방지하는 애플리케이션을 배포할 수 있습니다. 분산 배치 그룹에서 EC2 인스턴스를 실행함으로써 회사는 서로 다른 기본 하드웨어에서 소수의 인스턴스를 시작하여 상관 오류를 줄일 수 있습니다. 분산 배치 그룹은 각 인스턴스가 랙 수준에서 서로 격리되도록 보장합니다.

Q585

A solutions architect is designing a disaster recovery (DR) strategy to provide Amazon EC2 capacity in a failover AWS Region. Business requirements state that the DR strategy must meet capacity in the failover Region.

Which solution will meet these requirements?

A. Purchase On-Demand Instances in the failover Region.

B. Purchase an EC2 Savings Plan in the failover Region.

C. Purchase regional Reserved Instances in the failover Region.

D. Purchase a Capacity Reservation in the failover Region.

Answer: D

https://www.examtopics.com/discussions/amazon/view/119642-exam-aws-certified-solutions-architect-associate-saa-c03/

Q586

A company has five organizational units (OUs) as part of its organization in AWS Organizations. Each OU correlates to the five businesses that the company owns. The company's research and development (R&D) business is separating from the company and will need its own organization. A solutions architect creates a separate new management

account for this purpose.
What should the solutions architect do next in the new management account?
A. Have the R&D AWS account be part of both organizations during the transition.
B. Invite the R&D AWS account to be part of the new organization after the R&D AWS account has left the prior organization.
C. Create a new R&D AWS account in the new organization. Migrate resources from the prior R&D AWS account to the new R&D AWS account.
D. Have the R&D AWS account join the new organization. Make the new management account a member of the prior organization.
Answer: B
https://www.examtopics.com/discussions/amazon/view/119645-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이를 통해 솔루션 아키텍트는 연구 개발(R&D) 비즈니스를 위한 별도의 조직을 만들고 AWS 계정을 새 조직으로 이동할 수 있습니다. R&D AWS 계정이 이전 조직을 떠난 후 새 조직의 일부가 되도록 초대함으로써 솔루션 아키텍트는 두 조직 간에 중복이나 충돌이 없는지 확인할 수 있습니다. R&D AWS 계정은 새 조직에 가입하라는 초대를 수락하거나 거부할 수 있습니다. 일단 수락되면 새 조직에서 적용하는 모든 정책과 통제가 적용됩니다.

Q587
A company is designing a solution to capture customer activity in different web applications to process analytics and make predictions. Customer activity in the web applications is unpredictable and can increase suddenly. The company requires a solution that integrates with other web applications. The solution must include an authorization step for security purposes.
Which solution will meet these requirements?
A. Configure a Gateway Load Balancer (GWLB) in front of an Amazon Elastic Container Service (Amazon ECS) container instance that stores the information that the company receives in an Amazon Elastic File System (Amazon EFS) file system. Authorization is resolved at the GWLB.
B. Configure an Amazon API Gateway endpoint in front of an Amazon Kinesis data stream that stores the information that the company receives in an Amazon S3 bucket. Use an AWS Lambda function to resolve authorization.
C. Configure an Amazon API Gateway endpoint in front of an Amazon Kinesis Data Firehose

that stores the information that the company receives in an Amazon S3 bucket. Use an API Gateway Lambda authorizer to resolve authorization.
D. Configure a Gateway Load Balancer (GWLB) in front of an Amazon Elastic Container Service (Amazon ECS) container instance that stores the information that the company receives on an Amazon Elastic File System (Amazon EFS) file system. Use an AWS Lambda function to resolve authorization.
Answer: C
https://www.examtopics.com/discussions/amazon/view/119576-exam-aws-certified-solutions-architect-associate-saa-c03/

Q588
An ecommerce company wants a disaster recovery solution for its Amazon RDS DB instances that run Microsoft SQL Server Enterprise Edition. The company's current recovery point objective (RPO) and recovery time objective (RTO) are 24 hours.
Which solution will meet these requirements MOST cost-effectively?
A. Create a cross-Region read replica and promote the read replica to the primary instance.
B. Use AWS Database Migration Service (AWS DMS) to create RDS cross-Region replication.
C. Use cross-Region replication every 24 hours to copy native backups to an Amazon S3 bucket.
D. Copy automatic snapshots to another Region every 24 hours.
Answer: D
https://www.examtopics.com/discussions/amazon/view/119718-exam-aws-certified-solutions-architect-associate-saa-c03/

Q589
A company runs a web application on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer that has sticky sessions enabled. The web server currently hosts the user session state. The company wants to ensure high availability and avoid user session state loss in the event of a web server outage.
Which solution will meet these requirements?
A. Use an Amazon ElastiCache for Memcached instance to store the session data. Update the application to use ElastiCache for Memcached to store the session state.
B. Use Amazon ElastiCache for Redis to store the session state. Update the application to

use ElastiCache for Redis to store the session state.

C. Use an AWS Storage Gateway cached volume to store session data. Update the application to use AWS Storage Gateway cached volume to store the session state.

D. Use Amazon RDS to store the session state. Update the application to use Amazon RDS to store the session state.

Answer: B

https://www.examtopics.com/discussions/amazon/view/119487-exam-aws-certified-solutions-architect-associate-saa-c03/

Q590

A company migrated a MySQL database from the company's on-premises data center to an Amazon RDS for MySQL DB instance. The company sized the RDS DB instance to meet the company's average daily workload. Once a month, the database performs slowly when the company runs queries for a report. The company wants to have the ability to run reports and maintain the performance of the daily workloads.

Which solution will meet these requirements?

A. Create a read replica of the database. Direct the queries to the read replica.

B. Create a backup of the database. Restore the backup to another DB instance. Direct the queries to the new database.

C. Export the data to Amazon S3. Use Amazon Athena to query the S3 bucket.

D. Resize the DB instance to accommodate the additional workload.

Answer: A

https://www.examtopics.com/discussions/amazon/view/119719-exam-aws-certified-solutions-architect-associate-saa-c03/

Q591

A company runs a container application by using Amazon Elastic Kubernetes Service (Amazon EKS). The application includes microservices that manage customers and place orders. The company needs to route incoming requests to the appropriate microservices.

Which solution will meet this requirement MOST cost-effectively?

A. Use the AWS Load Balancer Controller to provision a Network Load Balancer.

B. Use the AWS Load Balancer Controller to provision an Application Load Balancer.

C. Use an AWS Lambda function to connect the requests to Amazon EKS.

D. Use Amazon API Gateway to connect the requests to Amazon EKS.

Answer: D
https://www.examtopics.com/discussions/amazon/view/119574-exam-aws-certified-solutions-architect-associate-saa-c03/]

Q592
A company uses AWS and sells access to copyrighted images. The company's global customer base needs to be able to access these images quickly. The company must deny access to users from specific countries. The company wants to minimize costs as much as possible.
Which solution will meet these requirements?
A. Use Amazon S3 to store the images. Turn on multi-factor authentication (MFA) and public bucket access. Provide customers with a link to the S3 bucket.
B. Use Amazon S3 to store the images. Create an IAM user for each customer. Add the users to a group that has permission to access the S3 bucket.
C. Use Amazon EC2 instances that are behind Application Load Balancers (ALBs) to store the images. Deploy the instances only in the countries the company services. Provide customers with links to the ALBs for their specific country's instances.
D. Use Amazon S3 to store the images. Use Amazon CloudFront to distribute the images with geographic restrictions. Provide a signed URL for each customer to access the data in CloudFront.
Answer: D
https://www.examtopics.com/discussions/amazon/view/119573-exam-aws-certified-solutions-architect-associate-saa-c03/

Q593
A solutions architect is designing a highly available Amazon ElastiCache for Redis based solution. The solutions architect needs to ensure that failures do not result in performance degradation or loss of data locally and within an AWS Region. The solution needs to provide high availability at the node level and at the Region level.
Which solution will meet these requirements?
A. Use Multi-AZ Redis replication groups with shards that contain multiple nodes.
B. Use Redis shards that contain multiple nodes with Redis append only files (AOF) turned on.
C. Use a Multi-AZ Redis cluster with more than one read replica in the replication group.

D. Use Redis shards that contain multiple nodes with Auto Scaling turned on.
Answer: B
https://www.examtopics.com/discussions/amazon/view/119572-exam-aws-certified-solutions-architect-associate-saa-c03/

Q594
A company plans to migrate to AWS and use Amazon EC2 On-Demand Instances for its application. During the migration testing phase, a technical team observes that the application takes a long time to launch and load memory to become fully productive.
Which solution will reduce the launch time of the application during the next testing phase?
A. Launch two or more EC2 On-Demand Instances. Turn on auto scaling features and make the EC2 On-Demand Instances available during the next testing phase.
B. Launch EC2 Spot Instances to support the application and to scale the application so it is available during the next testing phase.
C. Launch the EC2 On-Demand Instances with hibernation turned on. Configure EC2 Auto Scaling warm pools during the next testing phase.
D. Launch EC2 On-Demand Instances with Capacity Reservations. Start additional EC2 instances during the next testing phase.
Answer: C
https://www.examtopics.com/discussions/amazon/view/119570-exam-aws-certified-solutions-architect-associate-saa-c03/

Q595
A company's applications run on Amazon EC2 instances in Auto Scaling groups. The company notices that its applications experience sudden traffic increases on random days of the week. The company wants to maintain application performance during sudden traffic increases.
Which solution will meet these requirements MOST cost-effectively?
A. Use manual scaling to change the size of the Auto Scaling group.
B. Use predictive scaling to change the size of the Auto Scaling group.
C. Use dynamic scaling to change the size of the Auto Scaling group.
D. Use schedule scaling to change the size of the Auto Scaling group.
Answer: C
https://www.examtopics.com/discussions/amazon/view/119569-exam-aws-certified-sol

utions-architect-associate-saa-c03/

Q596

An ecommerce application uses a PostgreSQL database that runs on an Amazon EC2 instance. During a monthly sales event, database usage increases and causes database connection issues for the application. The traffic is unpredictable for subsequent monthly sales events, which impacts the sales forecast. The company needs to maintain performance when there is an unpredictable increase in traffic.

Which solution resolves this issue in the MOST cost-effective way?

A. Migrate the PostgreSQL database to Amazon Aurora Serverless v2.

B. Enable auto scaling for the PostgreSQL database on the EC2 instance to accommodate increased usage.

C. Migrate the PostgreSQL database to Amazon RDS for PostgreSQL with a larger instance type.

D. Migrate the PostgreSQL database to Amazon Redshift to accommodate increased usage.

Answer: A

https://www.examtopics.com/discussions/amazon/view/119590-exam-aws-certified-solutions-architect-associate-saa-c03/

Q597

A company hosts an internal serverless application on AWS by using Amazon API Gateway and AWS Lambda. The company's employees report issues with high latency when they begin using the application each day. The company wants to reduce latency.

Which solution will meet these requirements?

A. Increase the API Gateway throttling limit.

B. Set up a scheduled scaling to increase Lambda provisioned concurrency before employees begin to use the application each day.

C. Create an Amazon CloudWatch alarm to initiate a Lambda function as a target for the alarm at the beginning of each day.

D. Increase the Lambda function memory.

Answer: B

https://www.examtopics.com/discussions/amazon/view/119465-exam-aws-certified-solutions-architect-associate-saa-c03/

Q598

A research company uses on-premises devices to generate data for analysis. The company wants to use the AWS Cloud to analyze the data. The devices generate .csv files and support writing the data to an SMB file share. Company analysts must be able to use SQL commands to query the data. The analysts will run queries periodically throughout the day.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose three.)

A. Deploy an AWS Storage Gateway on premises in Amazon S3 File Gateway mode.

B. Deploy an AWS Storage Gateway on premises in Amazon FSx File Gateway made.

C. Set up an AWS Glue crawler to create a table based on the data that is in Amazon S3.

D. Set up an Amazon EMR cluster with EMR File System (EMRFS) to query the data that is in Amazon S3. Provide access to analysts.

E. Set up an Amazon Redshift cluster to query the data that is in Amazon S3. Provide access to analysts.

F. Setup Amazon Athena to query the data that is in Amazon S3. Provide access to analysts.

Answer: A, C, F

https://www.examtopics.com/discussions/amazon/view/119563-exam-aws-certified-solutions-architect-associate-saa-c03/

Q599

A company wants to use Amazon Elastic Container Service (Amazon ECS) clusters and Amazon RDS DB instances to build and run a payment processing application. The company will run the application in its on-premises data center for compliance purposes.

A solutions architect wants to use AWS Outposts as part of the solution. The solutions architect is working with the company's operational team to build the application.

Which activities are the responsibility of the company's operational team? (Choose three)

A. Providing resilient power and network connectivity to the Outposts racks.

B. Managing the virtualization hypervisor, storage systems, and the AWS services that run on Outposts.

C. Physical security and access controls of the data center environment.

D. Availability of the Outposts infrastructure including the power supplies, servers, and networking equipment within the Outposts racks.

E. Physical maintenance of Outposts components.

F. Providing extra capacity for Amazon ECS clusters to mitigate server failures and

maintenance events.
Answer: A, C, E
https://www.examtopics.com/discussions/amazon/view/119530-exam-aws-certified-solutions-architect-associate-saa-c03/
??

Q600
A company is planning to migrate a TCP-based application into the company's VPC. The application is publicly accessible on a nonstandard TCP port through a hardware appliance in the company's data center. This public endpoint can process up to 3 million requests per second with low latency. The company requires the same level of performance for the new public endpoint in AWS.
What should a solutions architect recommend to meet this requirement?
A. Deploy a Network Load Balancer (NLB). Configure the NLB to be publicly accessible over the TCP port that the application requires.
B. Deploy an Application Load Balancer (ALB). Configure the ALB to be publicly accessible over the TCP port that the application requires.
C. Deploy an Amazon CloudFront distribution that listens on the TCP port that the application requires. Use an Application Load Balancer as the origin.
D. Deploy an Amazon API Gateway API that is configured with the TCP port that the application requires. Configure AWS Lambda functions with provisioned concurrency to process the requests.
Answer: A
https://www.examtopics.com/discussions/amazon/view/121205-exam-aws-certified-solutions-architect-associate-saa-c03/

Q601
A company runs its critical database on an Amazon RDS for PostgreSQL DB instance. The company wants to migrate to Amazon Aurora PostgreSQL with minimal downtime and data loss.
Which solution will meet these requirements with the LEAST operational overhead?
A. Create a DB snapshot of the RDS for PostgreSQL DB instance to populate a new Aurora PostgreSQL DB cluster.
B. Create an Aurora read replica of the RDS for PostgreSQL DB instance. Promote the

Aurora read replicate to a new Aurora PostgreSQL DB cluster.
C. Use data import from Amazon S3 to migrate the database to an Aurora PostgreSQL DB cluster.
D. Use the pg_dump utility to back up the RDS for PostgreSQL database. Restore the backup to a new Aurora PostgreSQL DB cluster.
Answer: B
https://www.examtopics.com/discussions/amazon/view/121210-exam-aws-certified-solutions-architect-associate-saa-c03/

Q602
A company's infrastructure consists of hundreds of Amazon EC2 instances that use Amazon Elastic Block Store (Amazon EBS) storage. A solutions architect must ensure that every EC2 instance can be recovered after a disaster.
What should the solutions architect do to meet this requirement with the LEAST amount of effort?
A. Take a snapshot of the EBS storage that is attached to each EC2 instance. Create an AWS CloudFormation template to launch new EC2 instances from the EBS storage.
B. Take a snapshot of the EBS storage that is attached to each EC2 instance. Use AWS Elastic Beanstalk to set the environment based on the EC2 template and attach the EBS storage.
C. Use AWS Backup to set up a backup plan for the entire group of EC2 instances. Use the AWS Backup API or the AWS CLI to speed up the restore process for multiple EC2 instances.
D. Create an AWS Lambda function to take a snapshot of the EBS storage that is attached to each EC2 instance and copy the Amazon Machine Images (AMIs). Create another Lambda function to perform the restores with the copied AMIs and attach the EBS storage.
Answer: C
https://www.examtopics.com/discussions/amazon/view/121212-exam-aws-certified-solutions-architect-associate-saa-c03/

Q603
A company recently migrated to the AWS Cloud. The company wants a serverless solution for large-scale parallel on-demand processing of a semistructured dataset. The data consists of logs, media files, sales transactions, and IoT sensor data that is stored in Amazon S3. The company wants the solution to process thousands of items in the dataset in

parallel.

Which solution will meet these requirements with the MOST operational efficiency?

A. Use the AWS Step Functions Map state in Inline mode to process the data in parallel.

B. Use the AWS Step Functions Map state in Distributed mode to process the data in parallel.

C. Use AWS Glue to process the data in parallel.

D. Use several AWS Lambda functions to process the data in parallel.

Answer: B

https://www.examtopics.com/discussions/amazon/view/121211-exam-aws-certified-solutions-architect-associate-saa-c03/

Q604

A company will migrate 10 PB of data to Amazon S3 in 6 weeks. The current data center has a 500 Mbps uplink to the internet. Other on-premises applications share the uplink. The company can use 80% of the internet bandwidth for this one-time migration task.

Which solution will meet these requirements?

A. Configure AWS DataSync to migrate the data to Amazon S3 and to automatically verify the data.

B. Use rsync to transfer the data directly to Amazon S3.

C. Use the AWS CLI and multiple copy processes to send the data directly to Amazon S3.

D. Order multiple AWS Snowball devices. Copy the data to the devices. Send the devices to AWS to copy the data to Amazon S3.

Answer: D

https://www.examtopics.com/discussions/amazon/view/121186-exam-aws-certified-solutions-architect-associate-saa-c03/

Q605

A company has several on-premises Internet Small Computer Systems Interface (ISCSI) network storage servers. The company wants to reduce the number of these servers by moving to the AWS Cloud. A solutions architect must provide low-latency access to frequently used data and reduce the dependency on on-premises servers with a minimal number of infrastructure changes.

Which solution will meet these requirements?

A. Deploy an Amazon S3 File Gateway.

B. Deploy Amazon Elastic Block Store (Amazon EBS) storage with backups to Amazon S3.
C. Deploy an AWS Storage Gateway volume gateway that is configured with stored volumes.
D. Deploy an AWS Storage Gateway volume gateway that is configured with cached volumes.
Answer: D
https://www.examtopics.com/discussions/amazon/view/121170-exam-aws-certified-solutions-architect-associate-saa-c03/

Q606
A solutions architect is designing an application that will allow business users to upload objects to Amazon S3. The solution needs to maximize object durability. Objects also must be readily available at any time and for any length of time. Users will access objects frequently within the first 30 days after the objects are uploaded, but users are much less likely to access objects that are older than 30 days.
Which solution meets these requirements MOST cost-effectively?
A. Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 Glacier after 30 days.
B. Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
C. Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
D. Store all the objects in S3 Intelligent-Tiering with an S3 Lifecycle rule to transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
Answer: B
https://www.examtopics.com/discussions/amazon/view/121214-exam-aws-certified-solutions-architect-associate-saa-c03/

Q607
A company has migrated a two-tier application from its on-premises data center to the AWS Cloud. The data tier is a Multi-AZ deployment of Amazon RDS for Oracle with 12 TB of General Purpose SSD Amazon Elastic Block Store (Amazon EBS) storage. The application is designed to process and store documents in the database as binary large objects (blobs) with an average document size of 6 MB.
The database size has grown over time, reducing the performance and increasing the cost

of storage. The company must improve the database performance and needs a solution that is highly available and resilient.

Which solution will meet these requirements MOST cost-effectively?

A. Reduce the RDS DB instance size. Increase the storage capacity to 24 TiB. Change the storage type to Magnetic.

B. Increase the RDS DB instance size. Increase the storage capacity to 24 TiChange the storage type to Provisioned IOPS.

C. Create an Amazon S3 bucket. Update the application to store documents in the S3 bucket. Store the object metadata in the existing database.

D. Create an Amazon DynamoDB table. Update the application to use DynamoDB. Use AWS Database Migration Service (AWS DMS) to migrate data from the Oracle database to DynamoDB.

Answer: C

https://www.examtopics.com/discussions/amazon/view/121215-exam-aws-certified-solutions-architect-associate-saa-c03/

Q608

A company has an application that serves clients that are deployed in more than 20.000 retail storefront locations around the world. The application consists of backend web services that are exposed over HTTPS on port 443. The application is hosted on Amazon EC2 instances behind an Application Load Balancer (ALB). The retail locations communicate with the web application over the public internet. The company allows each retail location to register the IP address that the retail location has been allocated by its local ISP.

The company's security team recommends to increase the security of the application endpoint by restricting access to only the IP addresses registered by the retail locations.

What should a solutions architect do to meet these requirements?

A. Associate an AWS WAF web ACL with the ALB. Use IP rule sets on the ALB to filter traffic. Update the IP addresses in the rule to include the registered IP addresses.

B. Deploy AWS Firewall Manager to manage the ALConfigure firewall rules to restrict traffic to the ALModify the firewall rules to include the registered IP addresses.

C. Store the IP addresses in an Amazon DynamoDB table. Configure an AWS Lambda authorization function on the ALB to validate that incoming requests are from the registered IP addresses.

D. Configure the network ACL on the subnet that contains the public interface of the ALB. Update the ingress rules on the network ACL with entries for each of the registered IP

addresses.
Answer: A
https://www.examtopics.com/discussions/amazon/view/121216-exam-aws-certified-solutions-architect-associate-saa-c03/

Q609
A company is building a data analysis platform on AWS by using AWS Lake Formation. The platform will ingest data from different sources such as Amazon S3 and Amazon RDS. The company needs a secure solution to prevent access to portions of the data that contain sensitive information.
A. Create an IAM role that includes permissions to access Lake Formation tables.
B. Create data filters to implement row-level security and cell-level security.
C. Create an AWS Lambda function that removes sensitive information before Lake Formation ingests re data.
D. Create an AWS Lambda function that periodically Queries and removes sensitive information from Lake Formation tables.
Answer: B
https://www.examtopics.com/discussions/amazon/view/121162-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
이 옵션은 Lake Formation 과 통합된 엔진 및 쿼리 결과의 특정 데이터에 대한 액세스를 제한하는 사양인 데이터 필터를 사용하기 때문에 가장 효율적입니다. 데이터 필터는 중요한 정보가 포함된 데이터 부분에 대한 액세스를 방지하는 기술인 행 수준 보안 및 셀 수준 보안을 구현하는 데 사용할 수 있습니다. Data Catalog 테이블에 대한 Lake Formation 권한을 부여할 때 데이터 필터를 적용할 수 있으며 PartiQL 표현식을 사용하여 조건에 따라 데이터를 필터링할 수 있습니다. 이 솔루션은 중요한 정보가 포함된 데이터 부분에 대한 액세스를 방지하는 보안 솔루션을 제공해야 한다는 요구 사항을 충족합니다.

옵션 A 는 IAM 정책을 사용하여 Lake Formation 의 데이터에 대한 액세스 권한을 부여하는 방법인 Lake Formation 테이블에 대한 액세스 권한이 포함된 IAM 역할을 사용하기 때문에 효율성이 떨어집니다. 그러나 이것은 중요한 정보가 포함된 데이터 부분에 대한 액세스를 방지하는 방법을 제공하지 않습니다.

옵션 C 는 Lake Formation 이 데이터를 수집하기 전에 민감한 정보를 제거하는 AWS

Lambda 함수를 사용하기 때문에 효율성이 떨어집니다. 이는 서버리스 함수를 사용하여 데이터 정리 또는 변환을 수행하는 방법입니다. 그러나 여기에는 애플리케이션 코드 및 논리에 대한 상당한 변경이 포함될 수 있으며 데이터 손실 또는 불일치가 발생할 수도 있습니다.

옵션 D 는 서버리스 함수를 사용하여 데이터 정리 또는 변환을 수행하는 방법인 Lake Formation 테이블에서 민감한 정보를 주기적으로 쿼리하고 제거하는 AWS Lambda 함수를 사용하기 때문에 효율성이 떨어집니다. 그러나 여기에는 애플리케이션 코드 및 논리에 대한 상당한 변경이 포함될 수 있으며 데이터 손실 또는 불일치가 발생할 수도 있습니다.

Q610

A company deploys Amazon EC2 instances that run in a VPC. The EC2 instances load source data into Amazon S3 buckets so that the data can be processed in the future. According to compliance laws, the data must not be transmitted over the public internet. Servers in the company's on-premises data center will consume the output from an application that runs on the EC2 instances.

Which solution will meet these requirements?

A. Deploy an interface VPC endpoint for Amazon EC2. Create an AWS Site-to-Site VPN connection between the company and the VPC.

B. Deploy a gateway VPC endpoint for Amazon S3. Set up an AWS Direct Connect connection between the on-premises network and the VPC.

C. Set up an AWS Transit Gateway connection from the VPC to the S3 buckets. Create an AWS Site-to-Site VPN connection between the company and the VPC.

D. Set up proxy EC2 instances that have routes to NAT gateways. Configure the proxy EC2 instances to fetch S3 data and feed the application instances.

Answer: B

https://www.examtopics.com/discussions/amazon/view/121217-exam-aws-certified-solutions-architect-associate-saa-c03/

Q611

A company has an application with a REST-based interface that allows data to be received in near-real time from a third-party vendor. Once received, the application processes and stores the data for further analysis. The application is running on Amazon EC2 instances.

The third-party vendor has received many 503 Service Unavailable Errors when sending data

to the application. When the data volume spikes, the compute capacity reaches its maximum limit and the application is unable to process all requests.

Which design should a solutions architect recommend to provide a more scalable solution?

A. Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions.

B. Use Amazon API Gateway on top of the existing application. Create a usage plan with a quota limit for the third-party vendor.

C. Use Amazon Simple Notification Service (Amazon SNS) to ingest the data. Put the EC2 instances in an Auto Scaling group behind an Application Load Balancer.

D. Repackage the application as a container. Deploy the application using Amazon Elastic Container Service (Amazon ECS) using the EC2 launch type with an Auto Scaling group.

Answer: A

https://www.examtopics.com/discussions/amazon/view/121218-exam-aws-certified-solutions-architect-associate-saa-c03/

Q612

A company has an application that runs on Amazon EC2 instances in a private subnet. The application needs to process sensitive information from an Amazon S3 bucket. The application must not use the internet to connect to the S3 bucket.

Which solution will meet these requirements?

A. Configure an internet gateway. Update the S3 bucket policy to allow access from the internet gateway. Update the application to use the new internet gateway.

B. Configure a VPN connection. Update the S3 bucket policy to allow access from the VPN connection. Update the application to use the new VPN connection.

C. Configure a NAT gateway. Update the S3 bucket policy to allow access from the NAT gateway. Update the application to use the new NAT gateway.

D. Configure a VPC endpoint. Update the S3 bucket policy to allow access from the VPC endpoint. Update the application to use the new VPC endpoint.

Answer: D

https://www.examtopics.com/discussions/amazon/view/121159-exam-aws-certified-solutions-architect-associate-saa-c03/

Q613

A company uses Amazon Elastic Kubernetes Service (Amazon EKS) to run a container

application. The EKS cluster stores sensitive information in the Kubernetes secrets object. The company wants to ensure that the information is encrypted Which solution will meet these requirements with the LEAST operational overhead?

A. Use the container application to encrypt the information by using AWS Key Management Service (AWS KMS).

B. Enable secrets encryption in the EKS cluster by using AWS Key Management Service (AWS KMS).

C. Implement an AWS Lambda tuncuon to encrypt the information by using AWS Key Management Service (AWS KMS).

D. use AWS Systems Manager Parameter Store to encrypt the information by using AWS Key Management Service (AWS KMS).

Answer: B

https://www.examtopics.com/discussions/amazon/view/121158-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:

이를 통해 회사는 최소한의 운영 오버헤드로 EKS 클러스터의 Kubernetes 비밀 개체를 암호화할 수 있습니다. EKS 클러스터에서 비밀 암호화를 활성화함으로써 회사는 AWS Key Management Service(AWS KMS)를 사용하여 저장된 비밀을 암호화하고 해독하기 위한 암호화 키를 생성하고 관리할 수 있습니다. 이는 EKS 클러스터의 중요한 정보를 보호하는 간단하고 안전한 방법입니다.

Q614

A company is designing a new multi-tier web application that consists of the following components:

- Web and application servers that run on Amazon EC2 instances as part of Auto Scaling groups
- An Amazon RDS DB instance for data storage

A solutions architect needs to limit access to the application servers so that only the web servers can access them.

Which solution will meet these requirements?

A. Deploy AWS PrivateLink in front of the application servers. Configure the network ACL to allow only the web servers to access the application servers.

B. Deploy a VPC endpoint in front of the application servers. Configure the security group to allow only the web servers to access the application servers.
C. Deploy a Network Load Balancer with a target group that contains the application servers' Auto Scaling group. Configure the network ACL to allow only the web servers to access the application servers.
D. Deploy an Application Load Balancer with a target group that contains the application servers' Auto Scaling group. Configure the security group to allow only the web servers to access the application servers.
Answer: D
https://www.examtopics.com/discussions/amazon/view/121157-exam-aws-certified-solutions-architect-associate-saa-c03/

Q615
A company runs a critical, customer-facing application on Amazon Elastic Kubernetes Service (Amazon EKS). The application has a microservices architecture. The company needs to implement a solution that collects, aggregates, and summarizes metrics and logs from the application in a centralized location.
Which solution meets these requirements?
A. Run the Amazon CloudWatch agent in the existing EKS cluster. View the metrics and logs in the CloudWatch console.
B. Run AWS App Mesh in the existing EKS cluster. View the metrics and logs in the App Mesh console.
C. Configure AWS CloudTrail to capture data events. Query CloudTrail by using Amazon OpenSearch Service.
D. Configure Amazon CloudWatch Container Insights in the existing EKS cluster. View the metrics and logs in the CloudWatch console.
Answer: D
https://www.examtopics.com/discussions/amazon/view/121154-exam-aws-certified-solutions-architect-associate-saa-c03/

Q616
A company has deployed its newest product on AWS. The product runs in an Auto Scaling group behind a Network Load Balancer. The company stores the product's objects in an Amazon S3 bucket.

The company recently experienced malicious attacks against its systems. The company needs a solution that continuously monitors for malicious activity in the AWS account, workloads, and access patterns to the S3 bucket. The solution must also report suspicious activity and display the information on a dashboard.
Which solution will meet these requirements?
A. Configure Amazon Macie to monitor and report findings to AWS Config.
B. Configure Amazon Inspector to monitor and report findings to AWS CloudTrail.
C. Configure Amazon GuardDuty to monitor and report findings to AWS Security Hub.
D. Configure AWS Config to monitor and report findings to Amazon EventBridge.
Answer: C
https://www.examtopics.com/discussions/amazon/view/121177-exam-aws-certified-solutions-architect-associate-saa-c03/

설명:
Amazon GuardDuty 는 AWS 계정과 워크로드 전체에서 악의적인 활동과 무단 행동을 지속적으로 모니터링하는 위협 탐지 서비스입니다. GuardDuty 는 AWS CloudTrail 이벤트 로그, Amazon VPC 흐름 로그 및 DNS 로그와 같은 데이터 소스를 분석하여 손상된 인스턴스, 정찰, 포트 스캐닝 및 데이터 유출과 같은 잠재적인 위협을 식별합니다. GuardDuty 는 AWS 계정 및 워크로드의 보안 상태에 대한 포괄적인 보기를 제공하는 서비스인 AWS Security Hub 에 조사 결과를 보고할 수 있습니다. Security Hub 는 여러 AWS 서비스 및 파트너 솔루션의 보안 경고를 집계, 구성 및 우선순위를 지정하여 대시보드에 표시합니다. 이 솔루션은 AWS 계정의 악의적인 활동, 워크로드 및 S3 버킷에 대한 액세스 패턴을 지속적으로 모니터링, 보고 및 시각화할 수 있으므로 요구 사항을 충족합니다.

Q617
A company wants to migrate an on-premises data center to AWS. The data center hosts a storage server that stores data in an NFS-based file system. The storage server holds 200 GB of data. The company needs to migrate the data without interruption to existing services. Multiple resources in AWS must be able to access the data by using the NFS protocol.
Which combination of steps will meet these requirements MOST cost-effectively? (Choose two)
A. Create an Amazon FSx for Lustre file system.
B. Create an Amazon Elastic File System (Amazon EFS) file system.
C. Create an Amazon S3 bucket to receive the data.
D. Manually use an operating system copy command to push the data into the AWS

destination.

E. Install an AWS DataSync agent in the on-premises data center. Use a DataSync task between the on-premises location and AWS.

Answer: B, E

https://www.examtopics.com/discussions/amazon/view/121176-exam-aws-certified-solutions-architect-associate-saa-c03/

102 문제와 중복

Q618

A company wants to use Amazon FSx for Windows File Server for its Amazon EC2 instances that have an SMB file share mounted as a volume in the us-east-1 Region. The company has a recovery point objective (RPO) of 5 minutes for planned system maintenance or unplanned service disruptions. The company needs to replicate the file system to the us-west-2 Region. The replicated data must not be deleted by any user for 5 years.

Which solution will meet these requirements?

A. Create an FSx for Windows File Server file system in us-east-1 that has a Single-AZ 2 deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in compliance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.

B. Create an FSx for Windows File Server file system in us-east-1 that has a Multi-AZ deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in governance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.

C. Create an FSx for Windows File Server file system in us-east-1 that has a Multi-AZ deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in compliance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.

D. Create an FSx for Windows File Server file system in us-east-1 that has a Single-AZ 2 deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in governance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.

Answer: C

https://www.examtopics.com/discussions/amazon/view/121219-exam-aws-certified-solutions-architect-associate-saa-c03/

Q619

A solutions architect is designing a security solution for a company that wants to provide developers with individual AWS accounts through AWS Organizations, while also maintaining standard security controls. Because the individual developers will have AWS account root user-level access to their own accounts, the solutions architect wants to ensure that the mandatory AWS CloudTrail configuration that is applied to new developer accounts is not modified.

Which action meets these requirements?

A. Create an IAM policy that prohibits changes to CloudTrail. and attach it to the root user.

B. Create a new trail in CloudTrail from within the developer accounts with the organization trails option enabled.

C. Create a service control policy (SCP) that prohibits changes to CloudTrail, and attach it the developer accounts.

D. Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the management account.

Answer: C

https://www.examtopics.com/discussions/amazon/view/121220-exam-aws-certified-solutions-architect-associate-saa-c03/

Q620

A company is planning to deploy a business-critical application in the AWS Cloud. The application requires durable storage with consistent, low-latency performance.

Which type of storage should a solutions architect recommend to meet these requirements?

A. Instance store volume

B. Amazon ElastiCache for Memcached cluster

C. Provisioned IOPS SSD Amazon Elastic Block Store (Amazon EBS) volume

D. Throughput Optimized HDD Amazon Elastic Block Store (Amazon EBS) volume

Answer: C

https://www.examtopics.com/discussions/amazon/view/121221-exam-aws-certified-solutions-architect-associate-saa-c03/

Q621

An online photo-sharing company stores its photos in an Amazon S3 bucket that exists in

the us-west-1 Region. The company needs to store a copy of all new photos in the us-east-1 Region.

Which solution will meet this requirement with the LEAST operational effort?

A. Create a second S3 bucket in us-east-1. Use S3 Cross-Region Replication to copy photos from the existing S3 bucket to the second S3 bucket.

B. Create a cross-origin resource sharing (CORS) configuration of the existing S3 bucket. Specify us-east-1 in the CORS rule's AllowedOrigin element.

C. Create a second S3 bucket in us-east-1 across multiple Availability Zones. Create an S3 Lifecycle rule to save photos into the second S3 bucket.

D. Create a second S3 bucket in us-east-1. Configure S3 event notifications on object creation and update events to invoke an AWS Lambda function to copy photos from the existing S3 bucket to the second S3 bucket.

Answer: A

https://www.examtopics.com/discussions/amazon/view/121222-exam-aws-certified-solutions-architect-associate-saa-c03/

Q622

A company is creating a new web application for its subscribers. The application will consist of a static single page and a persistent database layer. The application will have millions of users for 4 hours in the morning, but the application will have only a few thousand users during the rest of the day. The company's data architects have requested the ability to rapidly evolve their schema.

Which solutions will meet these requirements and provide the MOST scalability? (Choose two)

A. Deploy Amazon DynamoDB as the database solution. Provision on-demand capacity.

B. Deploy Amazon Aurora as the database solution. Choose the serverless DB engine mode.

C. Deploy Amazon DynamoDB as the database solution. Ensure that DynamoDB auto scaling is enabled.

D. Deploy the static content into an Amazon S3 bucket. Provision an Amazon CloudFront distribution with the S3 bucket as the origin.

E. Deploy the web servers for static content across a fleet of Amazon EC2 instances in Auto Scaling groups. Configure the instances to periodically refresh the content from an Amazon Elastic File System (Amazon EFS) volume.

Answer: C, D

https://www.examtopics.com/discussions/amazon/view/121223-exam-aws-certified-sol

utions-architect-associate-saa-c03/

A, D ??

Q623

A company uses Amazon API Gateway to manage its REST APIs that third-party service providers access. The company must protect the REST APIs from SQL injection and cross-site scripting attacks.

What is the MOST operationally efficient solution that meets these requirements?

A. Configure AWS Shield.

B. Configure AWS WAF.

C. Set up API Gateway with an Amazon CloudFront distribution. Configure AWS Shield in CloudFront.

D. Set up API Gateway with an Amazon CloudFront distribution. Configure AWS WAF in CloudFront.

Answer: B

https://www.examtopics.com/discussions/amazon/view/121172-exam-aws-certified-solutions-architect-associate-saa-c03/

Q624

A company hosts an application on Amazon EC2 instances that run in a single Availability Zone. The application is accessible by using the transport layer of the Open Systems Interconnection (OSI) model. The company needs the application architecture to have high availability Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO)

A. Configure new EC2 instances in a different Availability Zone. Use Amazon Route 53 to route traffic to all instances.

B. Configure a Network Load Balancer in front of the EC2 instances.

C. Configure a Network Load Balancer tor TCP traffic to the instances. Configure an Application Load Balancer tor HTTP and HTTPS traffic to the instances.

D. Create an Auto Scaling group for the EC2 instances. Configure the Auto Scaling group to use multiple Availability Zones. Configure the Auto Scaling group to run application health checks on the instances.

E. Create an Amazon CloudWatch alarm. Configure the alarm to restart EC2 instances that transition to a stopped state.

Answer: A, D
설명:
EC2 인스턴스에서 실행되는 애플리케이션의 고가용성을 달성하려면 애플리케이션을 여러 가용 영역에 배포하고 로드 밸런서를 사용하여 트래픽을 분산해야 합니다. Auto Scaling 그룹을 사용하면 여러 가용 영역에서 EC2 인스턴스를 시작 및 관리하고 상태 확인을 수행할 수 있습니다. Network Load Balancer 를 사용하여 EC2 인스턴스에 대한 전송 계층 트래픽을 처리할 수 있습니다.

Q625
A company runs its applications on Amazon EC2 instances. The company performs periodic financial assessments of itsAWS costs. The company recently identified unusual spending. The company needs a solution to prevent unusual spending. The solution must monitor costs and notify responsible stakeholders in the event of unusual spending.
Which solution will meet these requirements?
A. Use an AWS Budgets template to create a zero spend budget.
B. Create an AWS Cost Anomaly Detection monitor in the AWS Billing and Cost Management console.
C. CreateAWS Pricing Calculator estimates for the current running workload pricing details.
D. Use Amazon CloudWatch to monitor costs and to identify unusual spending.
Answer: B
설명:
이를 통해 회사는 비용을 모니터링하고 비정상적인 지출이 발생할 경우 책임 있는 이해관계자에게 알릴 수 있습니다. AWS Billing and Cost Management 콘솔에서 AWS 비용 이상 탐지 모니터를 생성함으로써 회사는 비정상적인 지출을 자동으로 탐지하고 경고하는 기계 학습 서비스를 사용할 수 있습니다. 경고 임계값, 알림 기본 설정 및 근본 원인 분석을 구성함으로써 회사는 비정상적인 지출을 방지하고 그 출처를 식별할 수 있습니다.

Q626
A company runs a website that stores images of historical events. Website users need the ability to search and view images based on the year that the event in the image occurred. On average, users request each image only once or twice a year The company wants a highly available solution to store and deliver the images to users.
Which solution will meet these requirements MOST cost-effectively?
A. Store images in Amazon Elastic Block Store (Amazon EBS). Use a web server that runs on

Amazon EC2.
B. Store images in Amazon Elastic File System (Amazon EFS). Use a web server that runs on Amazon EC2.
C. Store images in Amazon S3 Standard. use S3 Standard to directly deliver images by using a static website.
D. Store images in Amazon S3 Standard-InfrequentAccess (S3 Standard-IA). use S3 Standard-IA to directly deliver images by using a static website.
Answer: C
설명:
이를 통해 회사는 가용성이 높고 비용 효율적인 방식으로 이미지를 저장하고 사용자에게 전달할 수 있습니다. Amazon S3 Standard 에 이미지를 저장함으로써 회사는 고가용성과 성능을 제공하는 내구성 있고 확장 가능하며 안전한 개체 스토리지 서비스를 사용할 수 있습니다. S3 Standard 를 사용하여 정적 웹 사이트를 통해 이미지를 직접 전달함으로써 회사는 웹 서버 실행을 방지하고 운영 오버헤드를 줄일 수 있습니다. S3 Standard 는 또한 AWS 리전 내에서 저렴한 스토리지 가격과 무료 데이터 전송을 제공합니다.

Q627
A company sends AWS CloudTrail logs from multiple AWS accounts to an Amazon S3 bucket in a centralized account. The company must keep the CloudTrail logs. The company must also be able to query the CloudTrail logs at any time Which solution will meet these requirements?
A. Use the CloudTrail event history in the centralized account to create an Amazon Athena table. Query the CloudTrail logs from Athena.
B. Configure an Amazon Neptune instance to manage the CloudTrail logs. Query the CloudTrail logs from Neptune.
C. Configure CloudTrail to send the logs to an Amazon DynamoDB table. Create a dashboard in Amazon QulCkSight to query the logs in the table.
D. use Amazon Athena to create an Athena notebook. Configure CloudTrail to send the logs to the notebook. Run queries from Athena.
Answer: A
설명:
이를 통해 회사는 CloudTrail 로그를 유지하고 언제든지 쿼리할 수 있습니다. 회사는 중앙 집중식 계정의 CloudTrail 이벤트 기록을 사용하여 여러 AWS 계정의 최근 API 활동을 보고, 필터링하고, 다운로드할 수 있습니다. CloudTrail 이벤트 기록에서 Amazon Athena 테이블을 생성함으로써 회사는 표준 SQL 을 사용하여 S3 의 데이터를 쉽게 분석할 수 있는 서버리스

대화형 쿼리 서비스를 사용할 수 있습니다. Athena 에서 CloudTrail 로그를 쿼리함으로써 회사는 사용자 활동 및 리소스 변경 사항에 대한 통찰력을 얻을 수 있습니다.

Q628

A company is moving its data and applications to AWS during a multiyear migration project. The company wants to securely access data on Amazon S3 from the company's AWS Region and from the company's on-premises location. The data must not traverse the internet. The company has established an AWS Direct Connect connection between its Region and its on-premises location Which solution will meet these requirements?

A. Create gateway endpoints for Amazon S3. Use the gateway endpoints to securely access the data from the Region and the on-premises location.

B. Create a gateway in AWS Transit Gateway to access Amazon S3 securely from the Region and the on-premises location.

C. Create interface endpoints for Amazon S3. Use the interface endpoints to securely access the data from the Region and the on-premises location.

D. Use an AWS Key Management Service (AWS KMS) key to access the data securely from the Region and the on-premises location.

Answer: B

설명:

게이트웨이 엔드포인트는 지원되는 AWS 서비스로 향하는 트래픽에 사용되는 라우팅 테이블의 지정된 경로에 대한 대상인 게이트웨이입니다. Amazon S3 는 게이트웨이 엔드포인트를 지원하지 않고 인터페이스 엔드포인트만 지원합니다. 따라서 선택지 A 는 올바르지 않습니다.

인터페이스 엔드포인트는 지원되는 서비스로 향하는 트래픽의 진입점 역할을 하는 개인 IP 주소가 있는 탄력적 네트워크 인터페이스입니다. 인터페이스 엔드포인트는 지역 내에서 Amazon S3 에 대한 보안 액세스를 제공할 수 있지만 온프레미스 위치에서는 제공할 수 없습니다. 따라서 선택지 C 는 올바르지 않습니다.

AWS Key Management Service(AWS KMS)는 데이터를 보호하기 위해 암호화 키를 생성하고 관리할 수 있는 서비스입니다. AWS KMS 는 인터넷을 통과하지 않고 Amazon S3 의 데이터에 액세스할 수 있는 방법을 제공하지 않습니다. 따라서 옵션 D 가 올바르지 않습니다.

AWS Transit Gateway 는 Amazon Virtual Private Cloud(VPC)와 온프레미스 네트워크를 단일

게이트웨이에 연결할 수 있게 해주는 서비스입니다. AWS Transit Gateway 에서 게이트웨이를 생성하면 AWS Direct Connect 를 사용하여 리전과 온프레미스 위치 모두에서 Amazon S3 에 안전하게 액세스할 수 있습니다. 따라서 선택 B 가 맞습니다.

Q629

A company stores its data on premises. The amount of data is growing beyond the company's available capacity. The company wants to migrate its data from the on-premises location to an Amazon S3 bucket. The company needs a solution that will automatically validate the integrity of the data after the transfer Which solution will meet these requirements?

A. Order an AWS Snowball Edge device Configure the Snowball Edge device to perform the online data transfer to an S3 bucket.

B. Deploy an AWS DataSync agent on premises. Configure the DataSync agent to perform the online data transfer to an S3 bucket.

C. Create an Amazon S3 File Gateway on premises. Configure the S3 File Gateway to perform the online data transfer to an S3 bucket.

D. Configure an accelerator in Amazon S3 Transfer Acceleration on premises. Configure the accelerator to perform the online data transfer to an S3 bucket.

Answer: B

설명:

이를 통해 회사는 온프레미스 위치에서 Amazon S3 버킷으로 데이터를 마이그레이션하고 전송 후 데이터 무결성을 자동으로 확인할 수 있습니다. AWS DataSync 에이전트를 온프레미스에 배포함으로써 회사는 AWS 에서 대량의 데이터를 쉽게 이동할 수 있는 완전 관리형 데이터 전송 서비스를 사용할 수 있습니다. S3 버킷으로의 온라인 데이터 전송을 수행하도록 DataSync 에이전트를 구성함으로써 회사는 암호화, 압축, 대역폭 조절, 데이터 검증과 같은 DataSync 의 기능을 활용할 수 있습니다. DataSync 는 각 전송 작업 후에 소스와 대상 모두에서 데이터 무결성을 자동으로 확인합니다.

Q630

A company runs a three-tier application in two AWS Regions. The web tier, the application tier, and the database tier run on Amazon EC2 instances. The company uses Amazon RDS for Microsoft SQL Server Enterprise for the database tier The database tier is experiencing high load when weekly and monthly reports are run. The company wants to reduce the load on the database tier.

Which solution will meet these requirements with the LEAST administrative effort?
A. Create read replicas. Configure the reports to use the new read replicas.
B. Convert the RDS database to Amazon DynamoDB_ Configure the reports to use DynamoDB.
C. Modify the existing RDS DB instances by selecting a larger instance size.
D. Modify the existing ROS DB instances and put the instances into an Auto Scaling group.
Answer: A
설명:
이를 통해 회사는 RDS 데이터베이스의 읽기 전용 복제본을 생성하고 데이터베이스 계층의 로드를 줄일 수 있습니다. 읽기 전용 복제본을 생성하면 회사는 기본 데이터베이스 인스턴스의 읽기 트래픽을 하나 이상의 복제본으로 오프로드할 수 있습니다. 새로운 읽기 전용 복제본을 사용하도록 보고서를 구성함으로써 회사는 데이터베이스 계층의 성능과 가용성을 향상시킬 수 있습니다.

Q631
A company runs applications on AWS that connect to the company's Amazon RDS database. The applications scale on weekends and at peak times of the year. The company wants to scale the database more effectively for its applications that connect to the database.
Which solution will meet these requirements with the LEAST operational overhead?
A. Use Amazon DynamoDB with connection pooling with a target group configuration for the database. Change the applications to use the DynamoDB endpoint.
B. Use Amazon RDS Proxy with a target group for the database. Change the applications to use the RDS Proxy endpoint.
C. Use a custom proxy that runs on Amazon EC2 as an intermediary to the database. Change the applications to use the custom proxy endpoint.
D. Use an AWS Lambda function to provide connection pooling with a target group configuration for the database. Change the applications to use the Lambda function.
Answer: B
설명:
Amazon RDS 프록시는 Amazon Relational Database Service(RDS)를 위한 완전 관리형 고가용성 데이터베이스 프록시로, 애플리케이션의 확장성과 데이터베이스 오류에 대한 복원력 및 보안을 더욱 강화합니다. RDS Proxy 를 사용하면 애플리케이션이 데이터베이스와 설정된 연결을 풀링하고 공유할 수 있어 데이터베이스 효율성과 애플리케이션 확장성이 향상됩니다. 또한 RDS Proxy 는 Aurora 및 RDS 데이터베이스의 장애 조치 시간을 최대 66%까지 줄이고 데이터베이스 액세스를 위한 IAM 인증 및 Secrets Manager 통합을

지원합니다. 코드 변경 없이 대부분의 애플리케이션에 대해 RDS Proxy 를 활성화할 수 있습니다.

Q632

A company runs its applications on Amazon EC2 instances that are backed by Amazon Elastic Block Store (Amazon EBS). The EC2 instances run the most recent Amazon Linux release. The applications are experiencing availability issues when the company's employees store and retrieve files that are 25 GB or larger. The company needs a solution that does not require the company to transfer files between EC2 instances. The files must be available across many EC2 instances and across multiple Availability Zones.

Which solution will meet these requirements?

A. Migrate all the files to an Amazon S3 bucket. Instruct the employees to access the files from the S3 bucket.

B. Take a snapshot of the existing EBS volume. Mount the snapshot as an EBS volume across the EC2 instances. Instruct the employees to access the files from the EC2 instances.

C. Mount an Amazon Elastic File System (Amazon EFS) file system across all the EC2 instances. Instruct the employees to access the files from the EC2 instances.

D. Create an Amazon Machine Image (AMI) from the EC2 instances. Configure new EC2 instances from the AMI that use an instance store volume. Instruct the employees to access the files from the EC2 instances.

Answer: C

설명:

여러 EC2 인스턴스와 여러 가용 영역에 걸쳐 25GB 이상의 파일을 저장하고 액세스하려면 Amazon Elastic File System(Amazon EFS)이 적합한 솔루션입니다. Amazon EFS 는 여러 EC2 인스턴스에 동시에 탑재할 수 있는 간단하고 확장 가능하며 탄력적인 파일 시스템을 제공합니다. Amazon EFS 는 한 지역 내의 여러 가용 영역에 데이터를 저장하여 고가용성과 내구성을 지원합니다.

Q633

A company wants to use an AWS CloudFormation stack for its application in a test environment. The company stores the CloudFormation template in an Amazon S3 bucket that blocks public access. The company wants to grant CloudFormation access to the template in the S3 bucket based on specific user requests to create the test environment

The solution must follow security best practices.
Which solution will meet these requirements?
A. Create a gateway VPC endpoint for Amazon S3. Configure the CloudFormation stack to use the S3 object URL.
B. Create an Amazon API Gateway REST API that has the S3 bucket as the target. Configure the CloudFormat10n stack to use the API Gateway URL.
C. Create a presigned URL for the template object_ Configure the CloudFormation stack to use the presigned URL.
D. Allow public access to the template object in the S3 bucket. Block the public access after the test environment is created.
Answer: C
설명:
이를 통해 CloudFormation 은 공개 액세스 권한을 부여하거나 추가 리소스를 생성하지 않고도 S3 버킷의 템플릿에 액세스할 수 있습니다. 미리 서명된 URL 은 객체에 액세스할 권한이 있는 IAM 사용자 또는 역할의 액세스 키로 서명된 URL 입니다. 미리 서명된 URL 은 이를 수신하는 누구나 사용할 수 있지만 지정된 시간이 지나면 만료됩니다. 템플릿 객체에 대해 미리 서명된 URL 을 생성하고 이를 사용하도록 CloudFormation 스택을 구성함으로써 회사는 특정 사용자 요청에 따라 템플릿에 대한 CloudFormation 액세스 권한을 부여하고 보안 모범 사례를 따를 수 있습니다.

Q634
A corporation has recruited a new cloud engineer who should not have access to the CompanyConfidential Amazon S3 bucket. The cloud engineer must have read and write permissions on an S3 bucket named AdminTools.
Which IAM policy will satisfy these criteria?
A.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::AdminTools"
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::CompanyConfidential"
            ]
        }
    ]
}
```

B.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::AdminTools",
                "arn:aws:s3:::CompanyConfidential/*"
                ]
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject", "s3:DeleteObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::CompanyConfidential"
        }
    ]
}
```

C.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*",
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::CompanyConfidential"
            ]
        }
    ]
}
```

D.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject", "s3:DeleteObject" ],
            "Resource": "arn:aws:s3:::AdminTools/"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential",
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::AdminTools/*"
            ]
        }
    ]
}
```

Answer: A

설명 1:

A(O) : arn:aws:s3:::AdminTools 는 버킷 자체를 의미. arn:aws:s3:::AdminTools/* 는 버킷 내 모든 객체를 의미

다음은 특정 Amazon S3 버킷 내에 포함된 모든 항목을 나타낸 예제입니다. 이하의 내용 참고.

https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/reference_policies_elements_resource.html
B(X) : CompanyConfidention 버킷에 권한이 없어야 하는데 s3:ListBucket 권한이 있으므로 오답.
C(X) : AdminTools 버킷에 s3:ListBucket 권한이 있어야 하는데 없으므로 오답. s3:ListBucket 권한이 없이 읽고 쓰는 권한만 가지는 것은 무의미. 아래 링크 참고.
https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/reference_policies_examples_s3_rw-bucket.html
D(X) : Allow, Deny 에 모두 AdminTools/*가 등록되어있으므로 오답. Deny 문은 Allow 문보다 우선시 되기 때문.
정책이 Allow 설명문과 Deny 설명문을 포함한 요청에 적용된다면 Deny 설명문은 Allow 설명문에 우선합니다. 이 요청은 명시적으로 거부됩니다.
https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

설명 2:
https://docs.amazonaws.cn/en_us/IAM/latest/UserGuide/reference_policies_examples_s3_rwbucket.html
ListBucket 작업에는 버킷에 대한 권한이 필요하고 다른 작업에는 버킷의 객체에 대한 권한이 필요하기 때문에 정책은 두 부분으로 구분됩니다.
버킷 수준 및 객체 수준 권한을 지정하려면 서로 다른 두 개의 ARN(Amazon 리소스 이름)을 사용해야 합니다.
첫 번째 Resource 요소는 애플리케이션이 AdminTools 버킷의 모든 객체를 나열할 수 있도록 ListBucket 작업에 대해 arn:aws:s3:::AdminTools 를 지정합니다.

Q635
A company collects temperature, humidity, and atmospheric pressure data in cities across multiple continents. The average volume of data collected per site each day is 500 GB. Each site has a high-speed internet connection. The company's weather forecasting applications are based in a single Region and analyze the data daily.
What is the FASTEST way to aggregate data from all of these global sites?
A. Enable Amazon S3 Transfer Acceleration on the destination bucket. Use multipart uploads to directly upload site data to the destination bucket.
B. Upload site data to an Amazon S3 bucket in the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.

C. Schedule AWS Snowball jobs daily to transfer data to the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.
D. Upload the data to an Amazon EC2 instance in the closest Region. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. Once a day take an EBS snapshot and copy it to the centralized Region. Restore the EBS volume in the centralized Region and run an analysis on the data daily.
Answer: A

설명
다음과 같은 다양한 이유로 버킷에서 Transfer Acceleration 을 사용할 수 있습니다.
전 세계에서 중앙 집중식 버킷에 업로드하는 고객이 있습니다.
대륙 간에 정기적으로 기가바이트에서 테라바이트의 데이터를 전송합니다.
Amazon S3 에 업로드할 때 인터넷을 통해 사용 가능한 모든 대역폭을 활용할 수 없습니다.
https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html
"Amazon S3 Transfer Acceleration 은 더 큰 객체의 장거리 전송을 위해 Amazon S3 와의 콘텐츠 전송 속도를 50~500%까지 높일 수 있습니다.
광범위한 사용자가 있는 웹 또는 모바일 애플리케이션이 있거나 S3 버킷에서 멀리 떨어진 애플리케이션을 호스팅하는 고객은 인터넷을 통해 길고 가변적인 업로드 및 다운로드 속도를 경험할 수 있습니다."
https://docs.aws.amazon.com/AmazonS3/latest/userguide/mpuoverview.html
"개선된 처리량 - 처리량을 개선하기 위해 부품을 병렬로 업로드할 수 있습니다."

여러 대륙의 도시에서 온도, 습도 및 대기압 데이터를 수집한다고 했으므로 여러 지역에서 업로드를 하는 상황. 즉 S3 Transfer Acceleration 을 사용하는 A 가 정답.

Q636
A company is planning to build a high performance computing (HPC) workload as a service solution that is hosted on AWS. A group of 16 Amazon EC2 Linux instances requires the lowest possible latency for node-to-node communication. The instances also need a shared block device volume for high-performing storage.
Which solution will meet these requirements?
A. Use a cluster placement group. Attach a single Provisioned IOPS SSD Amazon Elastic Block Store (Amazon EBS) volume to all the instances by using Amazon EBS Multi-Attach.
B. Use a cluster placement group. Create shared file systems across the instances by using Amazon Elastic File System (Amazon EFS).

C. Use a partition placement group. Create shared file systems across the instances by using Amazon Elastic File System (Amazon EFS).
D. Use a spread placement group. Attach a single Provisioned IOPS SSD Amazon Elastic Block Store (Amazon EBS) volume to all the instances by using Amazon EBS Multi-Attach.
Answer: A

설명
노드 간 통신에 가장 낮은 지연 시간 = 클러스터 배치 그룹. A,B 둘 중 하나가 정답.
A(O) : Amazon EBS 다중 연결을 사용하면 단일 프로비저닝된 IOPS SSD(io1 또는 io2) 볼륨을 동일한 가용 영역에 있는 여러 인스턴스에 연결할 수 있습니다. 여러 다중 연결 지원 볼륨을 인스턴스 또는 인스턴스 집합에 연결할 수 있습니다....다중 연결을 사용하면 동시 쓰기 작업을 관리하는 클러스터링된 Linux 애플리케이션에서 더 쉽게 더 높은 애플리케이션 가용성을 얻을 수 있습니다.....다중 연결 지원 볼륨은 동일한 가용 영역에 있는 최대 16 개의 Nitro 시스템 기반 Linux 인스턴스에 연결할 수 있습니다.....다중 연결은 프로비저닝된 IOPS SSD(io1 및 io2) 볼륨에만 지원됩니다
https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/ebs-volumes-multi.html
Provisioned IOPS SSD 볼륨의 크기는 4GiB 에서 16TiB 사이가 될 수 있고 볼륨당 100 IOPS 에서 최대 64,000 IOPS 가 프로비저닝될 수 있습니다. Nitro 시스템에 구축된 인스턴스에서만 최대 64,000 IOPS 를 달성할 수 있습니다. 다른 인스턴스 패밀리에서는 최대 32,000 IOPS 성능을 얻을 수 있습니다.
https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/provisioned-iops.html#EBSVolumeTypes_piops
B(X) : 공유 블록 장치 볼륨이라고 했으므로 오답. 블록 스토리지는 EBS. 그래도 IOPS 자체는 EBS 보다 더 높은 편.
Amazon EFS 범용 및 최대 I/O 라는 두 가지 성능 모드를 제공합니다.
◎범용 모드 : 최대 35,000 IOPS 를 지원하며 작업당 지연 시간이 가장 낮습니다. EFS One Zone 스토리지 클래스가 있는 파일 시스템은 항상 범용 성능 모드를 사용합니다. EFS Standard 스토리지 클래스가 있는 파일 시스템의 경우 기본 범용 성능 모드 또는 최대 I/O 성능 모드를 사용할 수 있습니다.
◎최대 I/O 모드 : 500,000+ IOPS 를 지원하며 범용 모드에 비해 작업당 지연 시간이 더 깁니다. https://docs.aws.amazon.com/ko_kr/efs/latest/ug/performance.html

Q637
A company has an event-driven application that invokes AWS Lambda functions up to 800 times each minute with varying runtimes. The Lambda functions access data that is stored in

an Amazon Aurora MySQL OB cluster. The company is noticing connection timeouts as user activity increases. The database shows no signs of being overloaded. CPU, memory, and disk access metrics are all low.
Which solution will resolve this issue with the LEAST operational overhead?
A. Adjust the size of the Aurora MySQL nodes to handle more connections. Configure retry logic in the Lambda functions for attempts to connect to the database.
B. Set up Amazon ElastiCache for reads to cache commonly read items from the database. Configure the Lambda functions to connect to ElastiCache for reads.
C. Add an Aurora Replica as a reader node. Configure the Lambda functions to connect to the reader endpoint of the OB cluster rather than lo the writer endpoint.
D. Use Amazon ROS Proxy to create a proxy. Set the DB cluster as the target database Configure the Lambda functions lo connect to the proxy rather than to the DB cluster.
Answer: D

설명 1:
A(X) : 노드 크기 조절은 아무 상관 없음.
B(X) : 데이터베이스 자체에 부하가 걸리는 것이 아니므로 읽기 부하를 분산하는 ElastiCache 는 솔루션으로 적합하지 않음.
C(X) : 데이터베이스 자체에 부하가 걸리는 것이 아니므로 읽기 부하를 분산하는 복제본은 솔루션으로 적합하지 않음.
D(O) : RDS 프록시를 사용하여 예기치 않은 데이터베이스 트래픽 급증을 처리할 수 있습니다. 급증을 처리하지 않으면 연결 초과 구독 또는 빠른 속도의 새 연결 생성으로 인한 문제가 발생할 수 있습니다. RDS 프록시는 데이터베이스 연결 풀을 설정하고 이 풀에서 연결을 재사용합니다.
https://docs.aws.amazon.com/ko_kr/AmazonRDS/latest/UserGuide/rds-proxy.html

설명 2:
1. 데이터베이스가 과부하의 징후를 보이지 않습니다. CPU, 메모리 및 디스크 액세스 메트릭은 모두 낮음==>A 및 C 출력입니다. 노드 인스턴스를 추가하거나 읽기 전용 복제본을 추가할 수는 없습니다.
2. "최소 운영 오버헤드"==>B 출력, b 는 람다를 구성해야 하기 때문입니다.
3. ROS 프록시: 자주 사용되지 않는 연결을 공유합니다. 장애 조치를 통한 고가용성.
효율성 향상==>프록시는 장애 조치를 활용하여 시간 초과 rds 인스턴스에서 정상 rds 인스턴스로 트래픽을 리디렉션할 수 있습니다. 그래서 D 가 맞습니다.

Q638

A company hosts a two-tier application on Amazon EC2 instances and Amazon RDS. The application's demand varies based on the time of day. The load is minimal after work hours and on weekends. The EC2 instances run in an EC2 Auto Scaling group that is configured with a minimum of two instances and a maximum of five instances. The application must be available at all times, but the company is concerned about overall cost.

Which solution meets the availability requirement MOST cost-effectively?

A. Use all EC2 Spot Instances. Stop the RDS database when it is not in use.

B. Purchase EC2 Instance Savings Plans to cover five EC2 instances. Purchase an RDS Reserved DB Instance.

C. Purchase two EC2 Reserved Instances. Use up to three additional EC2 Spot Instances as needed. Stop the RDS database when it is not in use.

D. Purchase EC2 Instance Savings Plans to cover two EC2 instances. Use up to three additional EC2 On-Demand Instances as needed. Purchase an RDS Reserved DB Instance.

Answer: C

설명:

이 솔루션은 하루 중 시간에 따라 수요가 가변적이며 전체 비용을 최소화하면서 항상 사용할 수 있어야 하는 2 계층 애플리케이션의 요구 사항을 충족합니다. EC2 예약 인스턴스는 기본 사용 수준에 대해 온디맨드 인스턴스에 비해 상당한 비용 절감을 제공할 수 있으며 필요할 때 용량 예약을 보장할 수 있습니다. EC2 스팟 인스턴스는 피크 시간 동안 애플리케이션에 필요한 추가 용량에 대해 온디맨드 인스턴스에 비해 최대 90% 절감 효과를 제공할 수 있습니다. 스팟 인스턴스는 중단을 허용하고 다른 인스턴스로 교체할 수 있는 상태 비저장 애플리케이션에 적합합니다. RDS 데이터베이스를 사용하지 않을 때 중지하면 데이터베이스 계층 실행 비용을 줄일 수 있습니다.

여분의 용량이 충분하지 않거나 스팟 가격이 최대 가격을 초과하는 경우 모든 EC2 스팟 인스턴스를 사용하면 애플리케이션의 가용성에 영향을 미칠 수 있으므로 옵션 A 는 올바르지 않습니다. RDS 데이터베이스를 사용하지 않을 때 중지하면 데이터베이스 계층 실행 비용을 줄일 수 있지만 애플리케이션의 가용성에도 영향을 미칠 수 있습니다.

5 개의 EC2 인스턴스에 적용되는 EC2 Instance Savings Plans 를 구매하면 시간당 컴퓨팅 사용량이 고정되어 애플리케이션의 실제 사용 패턴과 일치하지 않을 수 있으므로 옵션 B 는 올바르지 않습니다. RDS 예약 DB 인스턴스를 구매하면 데이터베이스 계층을 절약할 수 있지만 사용하지 않을 때 데이터베이스를 중지할 수는 없습니다.

두 개의 EC2 인스턴스에 적용되는 EC2 Instance Savings Plans 를 구매하면 시간당 컴퓨팅 사용량이 고정되어 애플리케이션의 실제 사용 패턴과 일치하지 않을 수 있으므로 옵션 D 는 올바르지 않습니다. 필요에 따라 최대 3 개의 추가 EC2 온디맨드 인스턴스를 사용하면 스팟

인스턴스를 사용하는 것보다 더 많은 비용이 발생할 수 있습니다.

참조:
https://aws.amazon.com/ec2/pricing/reserved-instances/
https://aws.amazon.com/ec2/spot/
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_StopInstance.html

Q639
A company's application runs on AWS. The application stores large documents in an Amazon S3 bucket that uses the S3 Standard-infrequent Access (S3 Standard-IA) storage class. The company will continue paying to store the data but wants to save on its total S3 costs. The company wants authorized external users to have the ability to access the documents in milliseconds. Which solution will meet these requirements MOST cost-effectively?
A. Configure the S3 bucket to be a Requester Pays bucket.
B. Change the storage tier to S3 Standard for all existing and future objects.
C. Turn on S3 Transfer Acceleration tor the S3 Docket.
D. Use Amazon CloudFront to handle all the requests to the S3 bucket.
Answer: D

설명:
이 옵션은 .html, .css, .js 및 이미지 파일과 같은 정적 및 동적 웹 콘텐츠를 사용자에게 빠르게 배포하는 웹 서비스인 Amazon CloudFront 를 사용하기 때문에 가장 효율적입니다. 또한 CloudFront 를 사용하여 S3 버킷에 대한 모든 요청을 처리하므로 에지 위치에서 콘텐츠를 캐싱하고 거기에서 콘텐츠를 제공하여 S3 비용을 줄입니다. 또한 CloudFront 가 지연 시간이 짧고 데이터 전송 속도가 빠른 콘텐츠를 제공하므로 인증된 외부 사용자가 밀리초 안에 문서에 액세스할 수 있습니다. 이 솔루션은 데이터 저장 비용을 계속 지불하면서 총 S3 비용을 절감해야 한다는 요구 사항을 충족합니다.
옵션 A 는 S3 버킷을 요청자 지불 버킷으로 구성하기 때문에 덜 효율적입니다. 이는 데이터 전송 및 요청 비용을 버킷 소유자에서 요청자에게 이전하는 방법입니다. 그러나 이것은 회사가 여전히 데이터 저장 및 자체 사용자의 요청에 대해 비용을 지불해야 하므로 총 S3 비용을 줄이지 않습니다.
옵션 B 는 높은 내구성과 가용성으로 자주 액세스하는 데이터를 저장하는 방법인 모든 기존 및 향후 객체에 대해 스토리지 계층을 S3 Standard 로 변경하기 때문에 효율성이 떨어집니다.

그러나 S3 Standard 는 S3 Standard-IA 보다 스토리지 비용이 높기 때문에 총 S3 비용은 줄어들지 않습니다.
옵션 C 는 CloudFront 엣지 로케이션을 통해 요청을 라우팅하여 S3 버킷 안팎으로 전송 속도를 높이는 방법인 S3 버킷에 대해 S3 Transfer Acceleration 을 활성화하기 때문에 효율성이 떨어집니다. 그러나 S3 Transfer Acceleration 에는 데이터 전송 및 요청에 대한 추가 요금이 있으므로 총 S3 비용은 줄어들지 않습니다.

Q640
A company wants to migrate its 1 PB on-premises image repository to AWS. The images will be used by a serverless web application images stored in the repository are rarely accessed, but they must be immediately available. Additionally, the images must be encrypted at rest and protected from accidental deletion.
Which solution meets these requirements?
A. Implement client-side encryption and store the images in an Amazon S3 Glacier vault. Set a vault lock to prevent accidental deletion.
B. Store the images in an Amazon S3 bucket in the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Enable versioning, default encryption, and MFA Delete on the S3 bucket.
C. Store the images in an Amazon FSx for Windows File Server file share. Configure the Amazon FSx file share to use an AWS Key Management Service (AWS KMS) customer master key (CMK) to encrypt the images in the file share. Use NTFS permission sets on the images to prevent accidental deletion.
D. Store the Images in an Amazon Elastic File System (Amazon EFS) file share in the Infrequent Access storage class. Configure the EFS file share to use an AWS Key Management Service (AWS KMS) customer master key (CMK) to encrypt the images in the file share. Use NFS permission sets on the images to prevent accidental deletion.
Answer: B
https://www.examtopics.com/discussions/amazon/view/68997-exam-aws-certified-solutions-architect-associate-saa-c02/

설명:
서버리스 웹 애플리케이션과 호환되는 온프레미스 파일 공유에 대한 탄력적이고 내구성 있는 대체를 제공하기 때문에 이 대답은 정확합니다. Amazon S3 는 모든 양의 데이터를 저장하고 인터넷을 통해 제공할 수 있는 완전관리형 객체 스토리지 서비스입니다. 다음 기능을 지원합니다.

복원력: Amazon S3 는 리전 내의 여러 가용 영역에 데이터를 저장하고 99.999999999%(11 9)의 내구성을 제공합니다. 또한 서로 다른 AWS 리전에 있는 버킷 간에 객체를 자동 및 비동기식으로 복사할 수 있는 교차 리전 복제를 지원합니다.
내구성: Amazon S3 는 Amazon S3 관리형 키(SSE-S3), AWS KMS 키(SSE-KMS) 또는 고객 제공 키(SSE-C)로 서버 측 암호화를 사용하여 유휴 데이터를 암호화합니다. 또한 SSL/TLS 를 사용하여 전송 중 암호화를 지원합니다. 또한 Amazon S3 는 동일한 버킷에 객체의 여러 버전을 유지하는 버전 관리 및 객체 버전을 삭제하거나 버킷의 버전 관리 상태를 변경하기 위해 추가 인증이 필요한 MFA 삭제와 같은 데이터 보호 기능을 제공합니다.
성능: Amazon S3 는 정적 및 동적 웹 콘텐츠를 제공하기 위한 고성능 및 확장성을 제공합니다. 또한 요청을 AWS 엣지 로케이션으로 라우팅하여 데이터 전송 속도를 높이는 S3 Transfer Acceleration 및 간단한 SQL 표현식을 사용하여 객체에서 데이터의 하위 집합만 검색할 수 있는 S3 Select 와 같은 기능을 지원합니다.
S3 Standard-Infrequent Access(S3 Standard-IA) 스토리지 클래스는 거의 액세스하지 않지만 필요할 때 즉시 사용할 수 있어야 하는 이미지를 저장하는 데 적합합니다. S3 Standard 와 동일한 높은 내구성, 처리량 및 짧은 대기 시간을 제공하지만 GB 당 스토리지 비용은 더 낮고 요청당 비용은 더 높습니다.

Q641
A company wants to run a gaming application on Amazon EC2 instances that are part of an Auto Scaling group in the AWS Cloud. The application will transmit data by using UDP packets. The company wants to ensure that the application can scale out and in as traffic increases and decreases.
What should a solutions architect do to meet these requirements?
A. Attach a Network Load Balancer to the Auto Scaling group
B. Attach an Application Load Balancer to the Auto Scaling group.
C. Deploy an Amazon Route 53 record set with a weighted policy to route traffic appropriately.
D. Deploy a NAT instance that is configured with port forwarding to the EC2 instances in the Auto Scaling group.
Answer: A

설명:
이 솔루션은 UDP 패킷을 사용하고 트래픽이 증가 및 감소함에 따라 확장 및 축소하여 데이터를 전송하는 게임 애플리케이션 실행 요구 사항을 충족합니다. Network Load

Balancer 는 매우 낮은 대기 시간으로 높은 처리량을 유지하면서 초당 수백만 건의 요청을 처리할 수 있으며 TCP 및 UDP 프로토콜을 모두 지원합니다. Auto Scaling 그룹은 수요 및 조정 정책에 따라 EC2 인스턴스 수를 자동으로 조정할 수 있습니다.

Application Load Balancer 가 UDP 프로토콜을 지원하지 않고 HTTP 및 HTTPS 만 지원하기 때문에 옵션 B 는 올바르지 않습니다.

Amazon Route 53 은 다양한 정책을 기반으로 트래픽을 라우팅할 수 있는 DNS 서비스이지만 로드 밸런싱 또는 확장 기능을 제공하지 않기 때문에 옵션 C 는 올바르지 않습니다.

옵션 D 는
NAT 인스턴스는 프라이빗 서브넷의 인스턴스를 인터넷 또는 다른 AWS 서비스에 연결하는데 사용되지만 로드 밸런싱 또는 확장 기능을 제공하지 않기 때문에 올바르지 않습니다.

참조:
https://aws.amazon.com/blogs/aws/new-udp-load-balancing-for-network-load-balancer/
https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html

A : UDP 패킷을 사용한다고 했으니 네트워크 계층 서비스인 NLB 가 적합.

Q642
A company wants to measure the effectiveness of its recent marketing campaigns. The company performs batch processing on csv files of sales data and stores the results in an Amazon S3 bucket once every hour. The S3 is petabytes of objects. The company runs onetime queries in Amazon Athena to determine which products are most popular on a particular date for a particular region Queries sometimes fail or take longer than expected to finish.
Which actions should a solutions architect take to improve the query performance and reliability? (Choose two)
A. Reduce the S3 object sizes to less than 128 MB.
B. Partition the data by date and region n Amazon S3.
C. Store the files as large, single objects in Amazon S3.
D. Use Amazon Kinesis Data Analytics to run the Queries as pan of the batch processing

operation.
E. Use an AWS Glue extract, transform, and load (ETL) process to convert the csv files into Apache Parquet format.
Answer: C, E
https://www.examtopics.com/discussions/amazon/view/86458-exam-aws-certified-solutions-architect-associate-saa-c02/

문제에서 보면 S3 2 페타바이트의 개체이고 쿼리 실행이 예상보다 오래 걸리는 상황입니다. 이를 위한 조치로는 먼저 파일을 Amazon S3 큰 단일 객체로 저장하여 AWS SDK, REST API 또는 AWS CLI 를 사용하여 객체를 부분적으로 업로드합니다.
다음으로 Apache Parquet 출력 형식으로 이용할 수 있습니다. Amazon S3 Inventory 는 객체의 플랫 파일 목록과 버킷 또는 공유된 접두사에 대해 선택한 메타데이터를 제공합니다. S3 Inventory 를 사용하여 객체 상태를 목록화, 감사 및 보고하거나 비즈니스 워크플로 및 빅 데이터 작업을 간소화하고 속도를 높일 수 있습니다.
따라서 답은 C, E 로 보입니다.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/upload-objects.html
https://aws.amazon.com/ko/about-aws/whats-new/2018/12/amazon-s3-announces-parquet-output-format-for-inventory/
객체의 크기가 100MB 를 넘는 경우, 멀티파트 업로드 기능을 사용하는 방법을 고려해야 합니다. https://aws.amazon.com/ko/s3/faqs/ 따라서 A 는 오답.

Q643
A company uses multiple vendors to distribute digital assets that are stored in Amazon S3 buckets. The company wants to ensure that its vendor AWS accounts have the minimum access that is needed to download objects in these S3 buckets.
Which solution will meet these requirements with the LEAST operational overhead?
A. Design a bucket policy that has anonymous read permissions and permissions to list ail buckets.
B. Design a bucket policy that gives read-only access to users. Specify IAM entities as principals.
C. Create a cross-account IAM role that has a read-only access policy specified for the IAM role.
D. Create a user policy and vendor user groups that give read-only access to vendor users.
Answer: C

설명:
교차 계정 IAM 역할은 한 AWS 계정의 사용자에게 다른 AWS 계정의 리소스에 대한 액세스 권한을 부여하는 방법입니다. 교차 계정 IAM 역할에는 읽기 전용 액세스 정책이 연결되어 있어 사용자가 객체를 수정하거나 삭제하지 않고도 S3 버킷에서 객체를 다운로드할 수 있습니다. 교차 계정 IAM 역할은 또한 각 계정에서 여러 IAM 사용자 및 정책을 관리하는 운영 오버헤드를 줄입니다. 교차 계정 IAM 역할은 질문의 모든 요구 사항을 충족하지만 다른 옵션은 그렇지 않습니다.

참조:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-walkthroughs-managing-accessexample2.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html

Q644
A solutions architect is designing a customer-facing application for a company. The application's database will have a clearly defined access pattern throughout the year and will have a variable number of reads and writes that depend on the time of year. The company must retain audit records for the database for 7 days. The recovery point objective (RPO) must be less than 5 hours.
Which solution meets these requirements?
A. Use Amazon DynamoDB with auto scaling. Use on-demand backups and Amazon DynamoDB Streams.
B. Use Amazon Redshift. Configure concurrency scaling. Activate audit logging. Perform database snapshots every 4 hours.
C. Use Amazon RDS with Provisioned IOPS. Activate the database auditing parameter Perform database snapshots every 5 hours.
D. Use Amazon Aurora MySQL with auto scaling. Activate the database auditing parameter.
Answer: D

설명 1:
A(X) : DynamoDB Streams 는 수정/변경 사항을 최대 24 시간까지밖에 로그에 저장할 수 없음. 이를 변경할 수도 없음.
DynamoDB Streams 의 모든 데이터는 24 시간 동안 유지됩니다. 특정 테이블에 대한 지난 24 시간 동안의 활동을 조회하고 분석할 수 있습니다. 그러나 24 시간이 지난 데이터는

언제든 트리밍(제거)될 수 있습니다....기존 스트림을 수동으로 삭제하기 위한 메커니즘은 없습니다. 보유 제한이 만료(24 시간)될 때까지 기다려야 하며, 모든 스트림 레코드가 삭제됩니다.
https://docs.aws.amazon.com/ko_kr/amazondynamodb/latest/developerguide/Streams.html
B(X) : Redshift 는 데이터베이스 서비스가 아니라 데이터 웨어하우스 서비스.
C(X) : 프로비저닝되었으므로 확장성이 떨어짐.
D(O) : Amazon Aurora MySQL 은 기본적으로 Auto Scaling 기능이 켜져있음. 복구 시간도 매우 짧음. 데이터베이스 감사 로그 또한 다운로드 가능
Aurora 는 단일 AWS 리전에서 다중 가용 영역에 걸쳐 DB 클러스터에 데이터 복사본을 저장합니다. DB 클러스터에 Aurora 복제본이 하나 이상인 경우에는 장애가 발생하더라도 Aurora 복제본이 기본 인스턴스로 승격됩니다. 이 실패 이벤트로 인해 예외적으로 실패하는 읽기 및 쓰기 작업 동안 짧은 중단이 발생합니다. 하지만, 일반적인 서비스 복구 시간은 120 초 미만이지만 대부분 60 초 미만에 복원됩니다.
https://docs.aws.amazon.com/ko_kr/AmazonRDS/latest/AuroraUserGuide/Concepts.AuroraHighAvailability.html#Concepts.AuroraHighAvailability.Data
Amazon Aurora MySQL 의 고성능 고급 감사 기능을 사용하여 데이터베이스 활동을 감사할 수 있습니다. 이를 위해 여러 DB 클러스터 파라미터를 설정하여 감사 로그 수집을 활성화합니다. 콘솔을 사용하여 감사 로그를 확인하고 다운로드할 수 있습니다.
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Auditing.html

Q645
A company's applications run on Amazon EC2 instances in Auto Scaling groups. The company notices that its applications experience sudden traffic increases on random days of the week. The company wants to maintain application performance during sudden traffic increases.
Which solution will meet these requirements MOST cost-effectively?
A. Use manual scaling to change the size of the Auto Scaling group.
B. Use predictive scaling to change the size of the Auto Scaling group.
C. Use dynamic scaling to change the size of the Auto Scaling group.
D. Use schedule scaling to change the size of the Auto Scaling group.
Answer: C

설명:

동적 조정은 수요 또는 부하에 따라 Auto Scaling 그룹의 EC2 인스턴스 수를 자동으로 조정하는 일종의 자동 조정입니다. 지정된 지표가 임계값을 초과하면 CloudWatch 경보를 사용하여 조정 작업을 트리거합니다. 필요에 따라 확장(인스턴스 추가) 또는 축소(인스턴스 제거)할 수 있습니다 1. 솔루션은 동적 확장을 사용하여 갑작스러운 트래픽 증가 중에 가장 비용 효율적으로 애플리케이션 성능을 유지할 수 있습니다.

1. 수동 조정을 사용하여 Auto Scaling 그룹의 크기를 변경합니다. 수동 확장은 사용자가 CLI 또는 콘솔을 통해 인스턴스 수를 수동으로 늘리거나 줄여야 하므로 이 솔루션은 트래픽이 갑자기 증가하는 동안 애플리케이션 성능을 유지해야 하는 요구 사항을 충족하지 않습니다. 수요나 부하의 변화에 자동으로 반응하지 않습니다.

2. 예측 조정을 사용하여 Auto Scaling 그룹의 크기를 변경합니다. 이 솔루션은 예측 확장이 기계 학습 및 인공 지능 도구를 사용하여 트래픽 부하를 평가하고 더 많거나 적은 리소스가 필요할 때를 예상하므로 대부분의 비용 효율성 요구 사항을 충족하지 않습니다. 주어진 시간에 실제 수요 또는 로드와 일치하지 않을 수 있는 예측을 기반으로 예약된 조정 작업을 수행합니다. 예측 조정은 예측 가능한 트래픽 패턴이 있거나 트래픽 부하의 알려진 변경 사항이 있는 시나리오에 더 적합합니다.

3. 일정 조정을 사용하여 Auto Scaling 그룹의 크기를 변경합니다. 일정 조정은 사용자가 예약한 특정 시간에 조정 작업을 수행하므로 이 솔루션은 트래픽이 갑자기 증가하는 동안 애플리케이션 성능을 유지해야 하는 요구 사항을 충족하지 않습니다. 수요나 부하의 변화에 자동으로 반응하지 않습니다. 일정 조정은 하루 중 특정 시간에 예측 가능한 트래픽 감소 또는 급증이 있는 시나리오에 더 적합합니다.

참조 URL:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-ondemand.html

Q646

A company has a serverless application on AWS that uses Amazon RDS as a backend database. The application sometimes experiences a sudden unpredictable increase in traffic. During traffic increases, the application frequently opens and closes connections to the database, which causes the application to receive errors from the database or run out of connections. The company needs to ensure that the application is always scalable and highly available.

Which solution will meet these requirements WITHOUT any code changes to the application?

A. Increase the maximum number of connections in the option group of the RDS database of the serverless application.

B. Increase the instance size of the RDS DB instance to meet the peak load traffic.
C. Deploy Amazon RDS Proxy between the serverless application and Amazon RDS.
D. Purchase Reserved Instances for Amazon RDS to ensure that the database is highly available during peak load traffic.
Answer: C

설명:
Amazon RDS Proxy 는 애플리케이션의 확장성, 데이터베이스 장애에 대한 복원력, 보안을 강화하는 완전 관리형 데이터베이스 프록시입니다. RDS Proxy 는 애플리케이션과 관계형 데이터베이스 사이에 위치하여 설정된 데이터베이스 연결을 풀링하고 공유하여 데이터베이스 효율성과 애플리케이션 확장성을 개선합니다. 또한 RDS Proxy 는 일시적인 오류에 대한 연결 관리 및 쿼리 재시도를 처리하여 데이터베이스의 부하를 줄입니다. 서버리스 애플리케이션과 Amazon RDS 사이에 RDS Proxy 를 배포하면 오류가 발생하거나 연결이 끊어질 수 있는 데이터베이스 연결을 자주 열고 닫는 것을 방지할 수 있습니다. 이 솔루션은 또한 운영 비용을 절감하고 애플리케이션의 가용성을 향상시킵니다.

참조:
https://aws.amazon.com/rds/proxy/

Q647
A solutions architect is developing a multiple-subnet VPC architecture. The solution will consist of six subnets in two Availability Zones. The subnets are defined as public, private and dedicated for databases. Only the Amazon EC2 instances running in the private subnets should be able to access a database.
Which solution meets these requirements?
A. Create a now route table that excludes the route to the public subnets' CIDR blocks. Associate the route table to the database subnets.
B. Create a security group that denies ingress from the security group used by instances in the public subnets. Attach the security group to an Amazon RDS DB instance.
C. Create a security group that allows ingress from the security group used by instances in the private subnets. Attach the security group to an Amazon RDS DB instance.
D. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.
Answer: C

설명 1:
전체적인 프로세스는 퍼블릭 서브넷 -> 프라이빗 서브넷(EC2 인스턴스가 있는 곳) -> 데이터베이스 전용 서브넷.
데이터베이스를 구동하는 인스턴스의 보안은 Security Group 이 담당. Security Group 은 허용 설정만 가능하고 차단 설정은 불가능하며, 기본적으로 모든 인바운드 트래픽을 차단. 따라서 허용할 곳만 등록시켜두면 나머지는 자동으로 다 차단하는 셈.
보안 그룹은 연결된 리소스에 도달하고 나갈 수 있는 트래픽을 제어합니다. 예를 들어 보안 그룹을 EC2 인스턴스와 연결하면 인스턴스에 대한 인바운드 및 아웃바운드 트래픽을 제어합니다. 허용 규칙을 지정할 수 있지만 거부 규칙은 지정할 수 없습니다. 보안 그룹을 처음 만들 때 인바운드 규칙이 없습니다. 따라서 보안 그룹에 인바운드 규칙을 추가하기 전에는 어떤 인바운드 트래픽도 허용되지 않습니다.
https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/VPC_SecurityGroups.html

설명 2:
보안 그룹은 상태 저장입니다. 모든 인바운드 트래픽은 기본적으로 차단됩니다. 트래픽 인바운드를 허용하는 인바운드 규칙을 생성하면 해당 트래픽이 자동으로 다시 백아웃됩니다.
보안 그룹을 사용하여 특정 IP 주소를 차단할 수 없습니다(대신 네트워크 액세스 제어 목록 사용).
허용 규칙은 지정할 수 있지만 거부 규칙은 지정할 수 없습니다. 보안 그룹을 처음 생성하면 인바운드 규칙이 없습니다. 따라서 인바운드 규칙을 보안 그룹에 추가할 때까지 다른 호스트에서 시작하여 인스턴스로 들어오는 인바운드 트래픽은 허용되지 않습니다.
https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/vpc-security-groups.html#VPCSecurityGroups

Q648
A company wants to configure its Amazon CloudFront distribution to use SSL/TLS certificates. The company does not want to use the default domain name for the distribution. Instead, the company wants to use a different domain name for the distribution.
Which solution will deploy the certificate with incurring any additional costs?
A. Request an Amazon issued private certificate from AWS Certificate Manager (ACM) in the useast-1 Region.
B. Request an Amazon issued private certificate from AWS Certificate Manager (ACM) in the uswest-1 Region.

C. Request an Amazon issued public certificate from AWS Certificate Manager (ACU) in the us-east-1 Region.
D. Request an Amazon issued public certificate from AWS Certificate Manager (ACU) in the us-west-1 Region.
Answer: C

설명:
이 옵션은 AWS 서비스와 함께 사용할 공개 및 비공개 SSL/TLS 인증서를 쉽게 프로비저닝, 관리 및 배포할 수 있는 서비스인 AWS Certificate Manager(ACM)에서 Amazon 에서 발급한 공개 인증서를 요청하기 때문에 가장 효율적입니다. 내부 연결 자원. 또한 CloudFront 에서 ACM 인증서를 사용하는 데 필요한 us-east-1 리전에서 인증서를 요청합니다. 또한 ACM 은 지원되는 AWS 서비스와 함께 사용되는 인증서에 대해 비용을 청구하지 않으므로 추가 비용 없이 인증서를 배포해야 한다는 요구 사항을 충족합니다. 이 솔루션은 SSL/TLS 인증서를 사용하고 배포에 다른 도메인 이름을 사용하도록 CloudFront 배포를 구성해야 하는 요구 사항을 충족합니다.

옵션 A 는 조직 또는 Virtual Private Cloud(VPC) 내에서만 사용할 수 있는 인증서 유형인 ACM 에서 Amazon 에서 발급한 사설 인증서를 요청하기 때문에 효율성이 떨어집니다. 그러나 CloudFront 에는 공개 인증서가 필요하므로 이는 SSL/TLS 인증서를 사용하도록 CloudFront 배포를 구성해야 하는 요구 사항을 충족하지 않습니다. 또한 올바른 us-east-1 리전에서 인증서를 요청합니다.

옵션 B 는 옵션 A 와 같은 이유로 올바르지 않은 ACM 에서 Amazon 에서 발급한 사설 인증서를 요청하기 때문에 효율성이 떨어집니다. 또한 us-west-1 리전에서 인증서를 요청합니다. us-east-1 지역.

옵션 D 는 ACM 에서 Amazon 이 발행한 공용 인증서를 요청하기 때문에 효율성이 떨어집니다. 이는 올바른 것입니다.
하지만 us-west-1 리전에서 인증서를 요청합니다. 이는 CloudFront 가 us-east-1 리전의 인증서를 요구하기 때문에 올바르지 않습니다.

Q649
A company runs a high performance computing (HPC) workload on AWS. The workload required low-latency network performance and high network throughput with tightly coupled node-to-node communication. The Amazon EC2 instances are properly sized for compute

and storage capacity, and are launched using default options.
What should a solutions architect propose to improve the performance of the workload?
A. Choose a cluster placement group while launching Amazon EC2 instances.
B. Choose dedicated instance tenancy while launching Amazon EC2 instances.
C. Choose an Elastic Inference accelerator while launching Amazon EC2 instances.
D. Choose the required capacity reservation while launching Amazon EC2 instances.
Answer: A

설명
https://docs.aws.amazon.com/ko_kr/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-placementgroup.html
"클러스터 배치 그룹은 네트워크 대기 시간이 짧고 네트워크 처리량이 높은 단일 가용 영역 내 인스턴스의 논리적 그룹입니다."
-> 긴밀하게 결합된 노드 = Cluster Deployment Group.

Q650
A company hosts an internal serverless application on AWS by using Amazon API Gateway and AWS Lambda. The company's employees report issues with high latency when they begin using the application each day. The company wants to reduce latency.
Which solution will meet these requirements?
A. Increase the API Gateway throttling limit.
B. Set up a scheduled scaling to increase Lambda provisioned concurrency before employees begin to use the application each day.
C. Create an Amazon CloudWatch alarm to initiate a Lambda function as a target for the alarm at the beginning of each day.
D. Increase the Lambda function memory.
Answer: B

설명:
AWS Lambda 는 서버를 프로비저닝하거나 관리하지 않고도 코드를 실행할 수 있는 서버리스 컴퓨팅 서비스입니다. Lambda 는 들어오는 요청에 따라 자동으로 확장되지만 수요가 갑자기 증가하면 함수의 새 인스턴스를 초기화하는 데 시간이 걸릴 수 있습니다. 이로 인해 애플리케이션의 대기 시간이 길어지거나 콜드 스타트가 발생할 수 있습니다. 이를 방지하기 위해 함수가 초기화되고 언제든지 응답할 준비가 되도록 프로비저닝된 동시성을 사용할 수 있습니다. 또한 직원이 매일 애플리케이션을 사용하기 전에

프로비저닝된 동시성을 늘리고 수요가 적을 때 줄이는 예약된 조정 정책을 설정할 수도 있습니다.

참조:
https://docs.aws.amazon.com/lambda/latest/dg/configuration-concurrency.html

Q651
A company wants to use Amazon Elastic Container Service (Amazon ECS) clusters and Amazon RDS DB instances to build and run a payment processing application. The company will run the application in its on-premises data center for compliance purposes.
A solutions architect wants to use AWS Outposts as part of the solution. The solutions architect is working with the company's operational team to build the application.
Which activities are the responsibility of the company's operational team? (Select THREE)
A. Providing resilient power and network connectivity to the Outposts racks.
B. Managing the virtualization hypervisor, storage systems, and the AWS services that run on Outposts.
C. Physical security and access controls of the data center environment.
D. Availability of the Outposts infrastructure including the power supplies, servers, and network-ing equipment within the Outposts racks.
E. Physical maintenance of Outposts components.
F. Providing extra capacity for Amazon ECS clusters to mitigate server failures and maintenance events.
Answer: A, C, F

설명:
이러한 답변은 솔루션의 일부로 AWS Outposts 를 사용하는 데 대한 고객의 책임을 반영하기 때문에 정확합니다. AWS 공유 책임 모델에 따르면 고객은 Outposts 랙에 탄력적인 전력 및 네트워크 연결을 제공하고, 데이터 센터 환경의 물리적 보안 및 액세스 제어를 보장하며, 서버 오류 및 유지 관리를 완화하기 위해 Amazon ECS 클러스터에 추가 용량을 제공할 책임이 있습니다. 이벤트. AWS 는 가상화 하이퍼바이저, 스토리지 시스템 및 Outposts 에서 실행되는 AWS 서비스를 관리할 뿐만 아니라 Outposts 랙 내 전원 공급 장치, 서버 및 네트워킹 장비를 포함한 Outposts 인프라의 가용성 및 물리적 유지 관리를 담당합니다. 전초기지 구성 요소.

참조:

https://docs.aws.amazon.com/outposts/latest/userguide/what-is-outposts.html
https://www.contino.io/insights/the-sandwich-responsibility-model-aws-outposts/

Q652

A solutions architect is designing a highly available Amazon ElastiCache for Redis based solution. The solutions architect needs to ensure that failures do not result in performance degradation or loss of data locally and within an AWS Region. The solution needs to provide high availability at the node level and at the Region level.

Which solution will meet these requirements?

A. Use Multi-AZ Redis replication groups with shards that contain multiple nodes.

B. Use Redis shards that contain multiple nodes with Redis append only files (AOF) tured on.

C. Use a Multi-AZ Redis cluster with more than one read replica in the replication group.

D. Use Redis shards that contain multiple nodes with Auto Scaling turned on.

Answer: A

설명:

Redis 솔루션용 ElastiCache 에 대해 노드 수준 및 리전 수준에서 고가용성을 제공하기 때문에 이 대답은 정확합니다. 다중 AZ Redis 복제 그룹은 각각 다른 가용 영역에 있는 기본 클러스터와 최대 5 개의 읽기 전용 복제본 클러스터로 구성됩니다. 기본 클러스터에 장애가 발생하면 읽기 전용 복제본 중 하나가 자동으로 새 기본 클러스터로 승격됩니다. 샤드가 있는 Redis 복제 그룹을 사용하면 여러 노드에 걸쳐 데이터를 분할할 수 있으므로 솔루션의 확장성과 성능이 향상됩니다. 각 샤드는 중복성과 읽기 확장성을 제공하기 위해 하나 이상의 복제본을 가질 수 있습니다.

참조:

https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/AutoFailover.html
https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/Shards.html

Q653

A company migrated a MySQL database from the company's on-premises data center to an Amazon RDS for MySQL DB instance. The company sized the RDS DB instance to meet the company's average daily workload. Once a month, the database performs slowly when the company runs queries for a report. The company wants to have the ability to run reports and maintain the performance of the daily workloads.

Which solution will meet these requirements?
A. Create a read replica of the database. Direct the queries to the read replica.
B. Create a backup of the database. Restore the backup to another DB instance. Direct the queries to the new database.
C. Export the data to Amazon S3. Use Amazon Athena to query the S3 bucket.
D. Resize the DB instance to accommodate the additional workload.
Answer: C

설명
Amazon Athena 는 Amazon S3 에 저장된 데이터에 대해 SQL 쿼리를 실행할 수 있는 서비스입니다. 서버리스이므로 인프라를 프로비저닝하거나 관리할 필요가 없습니다. 실행한 쿼리와 스캔한 데이터 양에 대해서만 비용을 지불하면 됩니다.
Amazon Athena 를 사용하여 Amazon S3 에서 데이터를 쿼리하면 다음과 같은 이점을 얻을 수 있습니다.
* Amazon RDS for MySQL DB 인스턴스의 성능에 영향을 주지 않고 보고서에 대한 쿼리를 실행할 수 있습니다. DB 인스턴스에서 S3 버킷으로 데이터를 내보내고 Athena 를 사용하여 버킷의 데이터를 쿼리할 수 있습니다. 이렇게 하면 DB 인스턴스에서 쿼리를 실행하는 오버헤드와 경합을 피할 수 있습니다.
* 보고서에 대한 쿼리를 실행하는 비용과 복잡성을 줄일 수 있습니다. 추가 요금이 발생하고 유지 관리가 필요한 읽기 전용 복제본이나 DB 인스턴스의 백업을 생성할 필요가 없습니다. 또한 운영 오버헤드를 증가시키는 추가 워크로드를 수용하기 위해 DB 인스턴스의 크기를 조정할 필요가 없습니다.
* Amazon S3 및 Athena 의 확장성과 유연성을 활용할 수 있습니다. 용량이나 성능 제한에 대한 걱정 없이 S3 에 대량의 데이터를 저장하고 Athena 로 쿼리할 수 있습니다. 또한 다양한 형식, 압축 방법 및 파티셔닝 체계를 사용하여 데이터 스토리지 및 쿼리 성능을 최적화할 수 있습니다.

Q654
A company's data platform uses an Amazon Aurora MySQL database. The database has multiple read replicas and multiple DB instances across different Availability Zones. Users have recently reported errors from the database that indicate that there are too many connections. The company wants to reduce the failover time by 20% when a read replica is promoted to primary writer.
Which solution will meet this requirement?
A. Switch from Aurora to Amazon RDS with Multi-AZ cluster deployment.

B. Use Amazon RDS Proxy in front of the Aurora database.
C. Switch to Amazon DynamoDB with DynamoDB Accelerator (DAX) for read connections.
D. Switch to Amazon Redshift with relocation capability.
Answer: B

설명
Amazon RDS Proxy 는 Amazon RDS 및 Aurora 데이터베이스를 위한 완전관리형 고가용성 데이터베이스 프록시를 제공하는 서비스입니다. 이를 통해 데이터베이스 연결 풀링 및 공유, 데이터베이스 로드 감소, 애플리케이션 확장성 및 가용성 향상이 가능합니다.
Aurora 데이터베이스 앞에서 Amazon RDS Proxy 를 사용하면 다음과 같은 이점을 얻을 수 있습니다.
* 데이터베이스에 대한 연결 수를 줄이고 너무 많은 연결이 있음을 나타내는 오류를 피할 수 있습니다. Amazon RDS Proxy 는 연결 관리 및 멀티플렉싱을 처리하므로 더 적은 수의 데이터베이스 연결 및 리소스를 사용할 수 있습니다.
* 읽기 복제본이 기본 작성자로 승격되면 장애 조치 시간을 20%까지 줄일 수 있습니다. Amazon RDS Proxy 는 애플리케이션 코드나 구성을 변경할 필요 없이 장애를 자동으로 감지하고 새로운 기본 인스턴스로 트래픽을 라우팅합니다. 벤치마크 테스트에 따르면 Amazon RDS Proxy 를 사용하면 장애 조치 시간이 66 초에서 53 초로 단축되어 20% 향상되었습니다.
* 데이터베이스 액세스의 보안 및 규정 준수를 향상시킬 수 있습니다. Amazon RDS Proxy 는 AWS Secrets Manager 및 AWS Identity and Access Management(IAM)와 통합되어 데이터베이스 연결에 대한 안전하고 세분화된 인증 및 권한 부여를 지원합니다.

Q655
An IoT company is releasing a mattress that has sensors to collect data about a user's sleep. The sensors will send data to an Amazon S3 bucket. The sensors collect approximately 2 MB of data every night for each mattress. The company must process and summarize the data for each mattress. The results need to be available as soon as possible Data processing will require 1 GB of memory and will finish within 30 seconds.
Which solution will meet these requirements MOST cost-effectively?
A. Use AWS Glue with a Scalajob.
B. Use Amazon EMR with an Apache Spark script.
C. Use AWS Lambda with a Python script.
D. Use AWS Glue with a PySpark job.
Answer: C

설명
AWS Lambda 는 호출 수와 함수 실행 시간에 따라 요금을 부과합니다. 데이터 처리 작업이 상대적으로 작기 때문에(데이터 2MB) Lambda 가 비용 효율적인 선택입니다. 인프라를 프로비저닝하고 유지 관리할 필요 없이 실제 사용량에 대해서만 비용을 지불하면 됩니다.

Q656
A company wants to use high-performance computing and artificial intelligence to improve its fraud prevention and detection technology. The company requires distributed processing to complete a single workload as quickly as possible.
Which solution will meet these requirements?
A. Use Amazon Elastic Kubernetes Service (Amazon EKS) and multiple containers.
B. Use AWS ParallelCluster and the Message Passing Interface (MPI) libraries.
C. Use an Application Load Balancer and Amazon EC2 instances.
D. Use AWS Lambda functions.
Answer: B

설명
AWS ParallelCluster 는 AWS 에서 고성능 컴퓨팅(HPC) 클러스터를 생성하고 관리할 수 있는 서비스입니다. 여러 EC2 인스턴스에서 분산 워크로드를 실행할 수 있는 AWS Batch 를 비롯한 여러 스케줄러를 지원합니다.
MPI 는 병렬 컴퓨팅에서 프로세스 간 메시지 전달을 위한 표준입니다. 데이터 송수신, 프로세스 동기화, 통신 그룹 관리 등의 기능을 제공합니다.
AWS ParallelCluster 및 MPI 라이브러리를 사용하면 다음과 같은 이점을 얻을 수 있습니다.
* 인스턴스 유형, 노드 수, 네트워크 구성 및 스토리지 옵션과 같은 특정 요구 사항을 충족하는 HPC 클러스터를 쉽게 생성하고 구성할 수 있습니다.
* AWS 의 확장성과 탄력성을 활용하여 서버 프로비저닝이나 관리에 대한 걱정 없이 대규모 병렬 워크로드를 실행할 수 있습니다.
* MPI 라이브러리를 사용하여 프로세스 간 통신 및 데이터 교환을 활성화하여 병렬 애플리케이션의 성능과 효율성을 최적화할 수 있습니다.
* Open MPI, Intel MPI 및 MPICH 와 같이 AWS ParallelCluster 와 호환되는 다양한 MPI 구현 중에서 선택할 수 있습니다.

Q657

A company runs a container application by using Amazon Elastic Kubernetes Service (Amazon EKS). The application includes microservices that manage customers and place orders. The company needs to route incoming requests to the appropriate microservices.
Which solution will meet this requirement MOST cost-effectively?
A. Use the AWS Load Balancer Controller to provision a Network Load Balancer.
B. Use the AWS Load Balancer Controller to provision an Application Load Balancer.
C. Use an AWS Lambda function to connect the requests to Amazon EKS.
D. Use Amazon API Gateway to connect the requests to Amazon EKS.
Answer: B

설명
Application Load Balancer 는 OSI 모델의 애플리케이션 계층(계층 7)에서 작동하는 일종의 Elastic Load Balancer 입니다. Amazon EC2 인스턴스, 컨테이너, IP 주소 및 Lambda 함수와 같은 여러 대상에 수신 트래픽을 분산할 수 있습니다. 호스트 이름, 경로 또는 쿼리 매개변수와 같은 요청 내용을 기반으로 요청을 라우팅할 수도 있습니다. AWS 로드 밸런서 컨트롤러는 Kubernetes 클러스터의 Elastic Load Balancer 를 관리하는 데 도움이 되는 컨트롤러입니다. Kubernetes 수신 또는 서비스 리소스를 생성할 때 Application Load Balancer 또는 Network Load Balancer 를 프로비저닝할 수 있습니다.
AWS Load Balancer Controller 를 사용하여 Amazon EKS 클러스터용 Application Load Balancer 를 프로비저닝하면 다음과 같은 이점을 얻을 수 있습니다.
* Ingress 리소스에서 정의한 규칙에 따라 수신 요청을 적절한 마이크로서비스로 라우팅할 수 있습니다. 예를 들어 호스트 이름이나 경로가 다른 요청을 고객과 주문을 처리하는 다른 마이크로 서비스로 라우팅할 수 있습니다.
* 여러 대상에 부하를 분산하고 상태 확인 및 자동 조정을 활성화하여 컨테이너 애플리케이션의 성능과 가용성을 개선할 수 있습니다.
* Amazon EKS 및 Kubernetes 와 통합되는 단일 컨트롤러를 사용하여 로드 밸런서 관리 비용과 복잡성을 줄일 수 있습니다. 로드 밸런서를 수동으로 생성 또는 구성하거나 클러스터가 변경될 때 업데이트할 필요가 없습니다.

Q658
A company is migrating its multi-tier on-premises application to AWS. The application consists of a single-node MySQL database and a multi-node web tier. The company must minimize changes to the application during the migration. The company wants to improve application resiliency after the migration.
Which combination of steps will meet these requirements? (Select TWO)

A. Migrate the web tier to Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer.
B. Migrate the database to Amazon EC2 instances in an Auto Scaling group behind a Network Load Balancer.
C. Migrate the database to an Amazon RDS Multi-AZ deployment.
D. Migrate the web tier to an AWS Lambda function.
E. Migrate the database to an Amazon DynamoDB table.
Answer: A, C
설명:
Auto Scaling 그룹은 유사한 특성을 공유하고 수요에 따라 자동으로 확장 또는 축소될 수 있는 EC2 인스턴스 모음입니다. Auto Scaling 그룹은 여러 가용 영역의 여러 대상에 수신 트래픽을 분산시키는 Elastic Load Balancing 로드 밸런서의 일종인 Application Load Balancer 뒤에 배치될 수 있습니다. 이 솔루션은 고가용성, 확장성 및 내결함성을 제공하여 웹 계층의 복원성을 향상시킵니다. Amazon RDS 다중 AZ 배포는 기본 데이터베이스 인스턴스를 자동으로 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제하는 구성입니다. 오류가 발생하면 Amazon RDS 는 수동 개입 없이 자동으로 대기 인스턴스로 장애 조치됩니다. 이 솔루션은 데이터 중복성, 백업 지원 및 가용성을 제공하여 데이터베이스 계층의 복원성을 향상시킵니다. 이 단계 조합은 마이그레이션 중에 애플리케이션을 최소한으로 변경하여 요구 사항을 충족합니다.

Q659
A company is developing an application that will run on a production Amazon Elastic Kubernetes Service (Amazon EKS) cluster The EKS cluster has managed node groups that are provisioned with On-Demand Instances.
The company needs a dedicated EKS cluster for development work. The company will use the development cluster infrequently to test the resiliency of the application. The EKS cluster must manage all the nodes.
Which solution will meet these requirements MOST cost-effectively?
A. Create a managed node group that contains only Spot Instances.
B. Create two managed node groups. Provision one node group with On-Demand Instances.
Provision the second node group with Spot Instances.
C. Create an Auto Scaling group that has a launch configuration that uses Spot Instances. Configure the user data to add the nodes to the EKS cluster.
D. Create a managed node group that contains only On-Demand Instances.

Answer: A
설명:
스팟 인스턴스는 온디맨드 가격에 비해 최대 90% 할인된 가격으로 제공되는 EC2 인스턴스입니다. 스팟 인스턴스는 중단을 허용할 수 있는 상태 비저장, 내결함성 및 유연한 워크로드에 적합합니다. 온디맨드 용량에 대한 수요가 증가하면 스팟 인스턴스를 EC2 에서 회수할 수 있지만 종료되기 2 분 전에 경고를 제공합니다. EKS 관리형 노드 그룹은 EKS 클러스터에 대한 노드의 프로비저닝 및 수명주기 관리를 자동화합니다. 관리형 노드 그룹은 스팟 인스턴스를 사용하여 비용을 절감하고 수요에 따라 클러스터를 확장할 수 있습니다. 관리형 노드 그룹은 스팟 인스턴스의 가용성과 복원력을 향상시키기 위해 용량 재조정 및 용량 최적화 할당 전략과 같은 기능도 지원합니다. 이 솔루션은 가장 저렴한 EC2 용량을 활용하고 수동 개입이 필요하지 않으므로 가장 비용 효율적으로 요구 사항을 충족합니다.

Q660
A company runs an SMB file server in its data center. The file server stores large files that the company frequently accesses for up to 7 days after the file creation date. After 7 days, the company needs to be able to access the files with a maximum retrieval time of 24 hours.
Which solution will meet these requirements?
A. Use AWS DataSync to copy data that is older than 7 days from the SMB file server to AWS.
B. Create an Amazon S3 File Gateway to increase the company's storage space. Create an S3 Lifecycle policy to transition the data to S3 Glacier Deep Archive after 7 days.
C. Create an Amazon FSx File Gateway to increase the company's storage space. Create an Amazon S3 Lifecycle policy to transition the data after 7 days.
D. Configure access to Amazon S3 for each user. Create an S3 Lifecycle policy to transition the data to S3 Glacier Flexible Retrieval after 7 days.
Answer: B
설명:
Amazon S3 파일 게이트웨이는 네트워크 파일 공유로 표시되는 Amazon S3 에 파일 기반 인터페이스를 제공하는 서비스입니다. SMB 와 같은 표준 파일 스토리지 프로토콜을 통해 Amazon S3 객체를 저장하고 검색할 수 있습니다. S3 파일 게이트웨이는 짧은 액세스 지연을 위해 자주 액세스하는 데이터를 로컬로 캐시할 수도 있습니다. S3 수명 주기 정책은 수명 주기 전반에 걸쳐 객체 관리를 자동화하는 규칙을 정의할 수 있는 기능입니다. S3 수명 주기 정책을 사용하면 객체의 수명과 액세스 패턴에 따라 객체를 다양한 스토리지 클래스로 전환할 수 있습니다. S3 Glacier Deep Archive 는 검색 시간이 12 시간 또는 48 시간으로 가장 저렴한 장기 데이터 보관 비용을 제공하는 스토리지 클래스입니다. 이 솔루션은 회사가 SMB 파일 액세스를 통해 S3 에 대용량 파일을 저장하고, 비용 절감 및

규정 준수를 위해 7 일 후에 파일을 S3 Glacier Deep Archive 로 이동할 수 있도록 하므로 요구 사항을 충족합니다.

Q661

A solutions architect needs to copy files from an Amazon S3 bucket to an Amazon Elastic File System (Amazon EFS) file system and another S3 bucket. The files must be copied continuously. New files are added to the original S3 bucket consistently. The copied files should be overwritten only if the source file changes.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create an AWS DataSync location for both the destination S3 bucket and the EFS file system.

Create a task for the destination S3 bucket and the EFS file system. Set the transfer mode to transfer only data that has changed.

B. Create an AWS Lambda function. Mount the file system to the function. Set up an S3 event notification to invoke the function when files are created and changed in Amazon S3. Configure the function to copy files to the file system and the destination S3 bucket.

C. Create an AWS DataSync location for both the destination S3 bucket and the EFS file system.

Create a task for the destination S3 bucket and the EFS file system. Set the transfer mode to transfer all data.

D. Launch an Amazon EC2 instance in the same VPC as the file system. Mount the file system. Create a script to routinely synchronize all objects that changed in the origin S3 bucket to the destination S3 bucket and the mounted file system.

Answer: A

설명:

AWS DataSync 는 AWS 스토리지 서비스와 온프레미스 스토리지 시스템 간에 대량의 데이터를 쉽게 이동할 수 있게 해주는 서비스입니다. AWS DataSync 는 S3 버킷에서 EFS 파일 시스템 및 다른 S3 버킷으로 파일을 지속적으로 복사할 수 있을 뿐만 아니라 소스에서 변경된 파일만 덮어쓸 수 있습니다. 이 솔루션은 코드 개발이나 수동 개입이 필요하지 않으므로 최소한의 운영 오버헤드로 요구 사항을 충족합니다.

Q662

A global company runs its applications in multiple AWS accounts in AWS Organizations. The company's applications use multipart uploads to upload data to multiple Amazon S3 buckets

across AWS Regions. The company wants to report on incomplete multipart uploads for cost compliance purposes.
Which solution will meet these requirements with the LEAST operational overhead?
A. Configure AWS Config with a rule to report the incomplete multipart upload object count.
B. Create a service control policy (SCP) to report the incomplete multipart upload object count.
C. Configure S3 Storage Lens to report the incomplete multipart upload object count.
D. Create an S3 Multi-Region Access Point to report the incomplete multipart upload object count.
Answer: C
설명:
S3 Storage Lens 는 AWS Organizations 의 여러 AWS 계정에 걸친 객체 스토리지 사용 및 활동에 대한 조직 전체의 가시성을 제공하는 클라우드 스토리지 분석 기능입니다. S3 스토리지 렌즈는 수집하여 S3 콘솔의 대화형 대시보드에 표시하는 지표 중 하나로 불완전한 멀티파트 업로드 객체 수를 보고할 수 있습니다. S3 Storage Lens 는 추가 분석을 위해 CSV 또는 Parquet 형식의 지표를 S3 버킷으로 내보낼 수도 있습니다. 이 솔루션은 코드 개발이나 정책 변경이 필요하지 않으므로 최소한의 운영 오버헤드로 요구 사항을 충족합니다.

Q663
A company deployed a serverless application that uses Amazon DynamoDB as a database layer The application has experienced a large increase in users. The company wants to improve database response time from milliseconds to microseconds and to cache requests to the database.
Which solution will meet these requirements with the LEAST operational overhead?
A. Use DynamoDB Accelerator (DAX).
B. Migrate the database to Amazon Redshift.
C. Migrate the database to Amazon RDS.
D. Use Amazon ElastiCache for Redis.
Answer: A
설명:
DynamoDB Accelerator(DAX)는 Amazon DynamoDB 용으로 구축된 완전 관리형 고가용성 캐싱 서비스입니다. DAX 는 초당 수백만 건의 요청에서도 밀리초에서 마이크로초로 최대 10 배의 성능 향상을 제공합니다. DAX 는 개발자가 캐시 무효화, 데이터 채우기 또는 클러스터 관리를 관리할 필요 없이 DynamoDB 테이블에 인 메모리 가속을 추가하는 데

필요한 모든 무거운 작업을 수행합니다. 이제 대규모 성능에 대한 걱정 없이 고객을 위한 훌륭한 애플리케이션을 구축하는 데 집중할 수 있습니다. DAX 는 기존 DynamoDB API 호출과 호환되므로 애플리케이션 로직을 수정할 필요가 없습니다. 이 솔루션은 코드 개발이나 수동 개입이 필요하지 않으므로 최소한의 운영 오버헤드로 요구 사항을 충족합니다.

Q664

A company uses an on-premises network-attached storage (NAS) system to provide file shares to its high performance computing (HPC) workloads. The company wants to migrate its latency-sensitive HPC workloads and its storage to the AWS Cloud. The company must be able to provide NFS and SMB multi-protocol access from the file system.

Which solution will meet these requirements with the LEAST latency? (Select TWO)

A. Deploy compute optimized EC2 instances into a cluster placement group.

B. Deploy compute optimized EC2 instances into a partition placement group.

C. Attach the EC2 instances to an Amazon FSx for Lustre file system.

D. Attach the EC2 instances to an Amazon FSx for OpenZFS file system.

E. Attach the EC2 instances to an Amazon FSx for NetApp ONTAP file system.

Answer: A, E

설명:

클러스터 배치 그룹은 네트워크 지연 시간을 최소화하기 위해 서로 가깝게 배치되는 단일 가용 영역 내 EC2 인스턴스의 논리적 그룹입니다. 이는 높은 네트워크 성능이 요구되는 대기 시간에 민감한 HPC 워크로드에 적합합니다. 컴퓨팅 최적화 EC2 인스턴스는 vCPU 대 메모리 비율이 높은 인스턴스 유형으로, 컴퓨팅 집약적인 애플리케이션에 이상적입니다.

NetApp ONTAP 용 Amazon FSx 는 파일 시스템에서 NFS 및 SMB 다중 프로토콜 액세스는 물론 데이터 중복 제거, 압축, 씬 프로비저닝, 스냅샷과 같은 기능을 제공하는 완전관리형 서비스입니다. 이 솔루션은 AWS 의 짧은 지연 시간 네트워크 및 스토리지 성능을 활용하므로 가장 짧은 지연 시간으로 요구 사항을 충족합니다.

Q665

A company wants to migrate its on-premises Microsoft SQL Server Enterprise edition database to AWS. The company's online application uses the database to process transactions. The data analysis team uses the same production database to run reports for analytical processing. The company wants to reduce operational overhead by moving to managed services wherever possible.

Which solution will meet these requirements with the LEAST operational overhead?
A. Migrate to Amazon RDS for Microsoft SQL Server. Use read replicas for reporting purposes.
B. Migrate to Microsoft SQL Server on Amazon EC2. Use Always On read replicas for reporting purposes.
C. Migrate to Amazon DynamoDB. Use DynamoDB on-demand replicas for reporting purposes.
D. Migrate to Amazon Aurora MySQL. Use Aurora read replicas for reporting purposes.
Answer: A
설명:
Microsoft SQL Server 용 Amazon RDS 는 SQL Server 2014, 2016, 2017 및 2019 에디션을 제공하는 동시에 백업, 패치, 확장과 같은 데이터베이스 관리 작업을 오프로드하는 완전관리형 서비스입니다. Amazon RDS 는 온라인 애플리케이션의 성능에 영향을 주지 않고 보고 목적으로 사용할 수 있는 기본 데이터베이스의 읽기 전용 복사본인 읽기 전용 복제본을 지원합니다.
이 솔루션은 코드 변경이나 수동 개입이 필요하지 않으므로 최소한의 운영 오버헤드로 요구 사항을 충족합니다.

Q666
A company maintains an Amazon RDS database that maps users to cost centers. The company has accounts in an organization in AWS Organizations. The company needs a solution that will tag all resources that are created in a specific AWS account in the organization. The solution must tag each resource with the cost center ID of the user who created the resource.
Which solution will meet these requirements?
A. Move the specific AWS account to a new organizational unit (OU) in Organizations from the management account. Create a service control policy (SCP) that requires all existing resources to have the correct cost center tag before the resources are created. Apply the SCP to the new OU.
B. Create an AWS Lambda function to tag the resources after the Lambda function looks up the appropriate cost center from the RDS database. Configure an Amazon EventBridge rule that reacts to AWS CloudTrail events to invoke the Lambda function.
C. Create an AWS CloudFormation stack to deploy an AWS Lambda function. Configure the Lambda function to look up the appropriate cost center from the RDS database and to tag resources. Create an Amazon EventBridge scheduled rule to invoke the CloudFormation

stack.
D. Create an AWS Lambda function to tag the resources with a default value. Configure an Amazon EventBridge rule that reacts to AWS CloudTrail events to invoke the Lambda function when a resource is missing the cost center tag.
Answer: B
설명:
AWS Lambda 는 서버를 프로비저닝하거나 관리하지 않고도 코드를 실행할 수 있는 서버리스 컴퓨팅 서비스입니다. Lambda 를 사용하면 사용자를 비용 센터에 매핑하는 RDS 데이터베이스를 쿼리하여 리소스를 생성한 사용자의 비용 센터 ID 로 리소스에 태그를 지정할 수 있습니다. Amazon EventBridge 는 이벤트 중심 아키텍처를 지원하는 서버리스 이벤트 버스 서비스입니다. EventBridge 는 AWS 계정에 의해 또는 AWS 계정을 대신하여 이루어진 기록된 API 호출인 AWS CloudTrail 이벤트에 반응하도록 구성할 수 있습니다. EventBridge 는 특정 AWS 계정에 리소스가 생성될 때 Lambda 함수를 호출하여 사용자 자격 증명 및 리소스 정보를 매개 변수로 전달할 수 있습니다. 이 솔루션은 사용자 및 비용 센터 매핑을 기반으로 리소스에 자동으로 태그를 지정할 수 있으므로 요구 사항을 충족합니다.

Q667
A company uses Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS) volumes to run an application. The company creates one snapshot of each EBS volume every day to meet compliance requirements. The company wants to implement an architecture that prevents the accidental deletion of EBS volume snapshots. The solution must not change the administrative rights of the storage administrator user.
Which solution will meet these requirements with the LEAST administrative effort?
A. Create an IAM role that has permission to delete snapshots. Attach the role to a new EC2 instance. Use the AWS CLI from the new EC2 instance to delete snapshots.
B. Create an IAM policy that denies snapshot deletion. Attach the policy to the storage administrator user.
C. Add tags to the snapshots. Create retention rules in Recycle Bin for EBS snapshots that have the tags.
D. Lock the EBS snapshots to prevent deletion.
Answer: D
설명:
EBS 스냅샷은 데이터를 복원하거나 새 볼륨을 생성하는 데 사용할 수 있는 EBS 볼륨의 특정 시점 백업입니다. EBS 스냅샷 잠금이라는 기능을 사용하여 실수로 삭제되는 것을

방지하기 위해 EBS 스냅샷을 잠글 수 있습니다. 스냅샷이 잠겨 있으면 잠금이 해제될 때까지 루트 사용자를 포함한 어떤 사용자도 삭제할 수 없습니다. 잠금 정책은 스냅샷을 삭제할 수 있는 보존 기간을 지정할 수도 있습니다. 이 솔루션은 코드 개발이나 정책 변경이 필요하지 않으므로 최소한의 관리 노력으로 요구 사항을 충족합니다.