AWS Certified Solutions Architect Professional

NO.138
A large education company recently introduced Amazon Workspaces to provide access to internal applications across multiple universities.
The company is storing user proxies on an Amazon FSx for Windows File Server tile system.
The system is configured with a DNS alias and is connected to a self-managed Active Directory.
As more users begin to use the Workspaces login time increases to unacceptable levels.
An investigation reveals a degradation in performance of the file system.
The company created the file system on HDD storage with a throughput of 16 MBps.
A solutions architect must improve the performance of the file system during a defined maintenance window.
What should the solutions architect do to meet these requirements with the LEAST administrative effort?

(A). Use AWS Backup to create a point-in-time backup of the file system.
Restore the backup to a new FSx for Windows File Server file system.
Select SSD as the storage type Select 32 MBps as the throughput capacity.
When the backup and restore process is completed adjust the DNS alias accordingly.
Delete the original file system.

(B). Disconnect users from the file system In the Amazon FSx console, update the throughput capacity to 32 MBps.
Update the storage type to SSD Reconnect users to the file system.

(C). Deploy an AWS DataSync agent onto a new Amazon EC2 instance.
Create a task. Configure the existing file system as the source location.
Configure a new FSx for Windows File Server file system with SSD storage and 32 MBps of throughput as the target location.
Schedule the task When the task is completed adjust the DNS alias accordingly Delete the original file system.

(D). Enable shadow copies on the existing file system by using a Windows PowerShell command.
Schedule the shadow copy job to create a point-in-time backup of the file system.
Choose to restore previous versions Create a new FSx for Windows File Server file system with SSD storage and 32 MBps of throughput When the copy job is completed, adjust the DNS alias Delete the original file system.

Answer: C

NO.138
큰 교육 회사가 최근 여러 대학의 내부 애플리케이션에 대한 액세스를 제공하기 위해 Amazon Workspaces를 도입했습니다.
회사는 Windows 파일 서버 타일 시스템용 Amazon FSx에 사용자 프록시를 저장하고 있습니다.
시스템은 DNS 별칭으로 구성되며 자체 관리되는 Active Directory에 연결됩니다.
더 많은 사용자가 작업 공간을 사용하기 시작하면 로그인 시간이 허용할 수 없는 수준으로 늘어납니다. 조사 결과 파일 시스템의 성능 저하가 드러났습니다.
회사는 16MBps의 처리량으로 HDD 스토리지에 파일 시스템을 만들었습니다.
솔루션 아키텍트는 정의된 유지 관리 기간 동안 파일 시스템의 성능을 개선해야 합니다.
솔루션 아키텍트는 최소한의 관리 노력으로 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

(A). AWS Backup을 사용하여 파일 시스템의 특정 시점 백업을 생성합니다.
백업을 Windows 파일 서버용 새 FSx 파일 시스템으로 복원합니다.
스토리지 유형으로 SSD 선택 처리 용량으로 32MBps를 선택합니다.
백업 및 복원 프로세스가 완료되면 그에 따라 DNS 별칭을 조정합니다.
원본 파일 시스템을 삭제합니다.

(B). Amazon FSx 콘솔에서 파일 시스템에서 사용자 연결을 끊고, 처리 용량을 32MBps로 업데이트합니다.
스토리지 유형을 SSD로 업데이트합니다. 사용자를 파일 시스템에 다시 연결합니다.

(C). 새 Amazon EC2 인스턴스에 AWS DataSync 에이전트를 배포합니다.
작업을 만듭니다. 기존 파일 시스템을 원본 위치로 구성합니다.
대상 위치로 SSD 스토리지 및 32MBps의 처리량을 사용하여 Windows 파일 서버 파일 시스템용 새 FSx를 구성합니다.
작업 예약 작업이 완료되면 그에 따라 DNS 별칭을 조정합니다. 원본 파일 시스템을 삭제합니다.

(D). Windows PowerShell 명령을 사용하여 기존 파일 시스템에서 shadow copies 를 활성화합니다.
shadow copy 작업을 예약하여 파일 시스템의 특정 시점 백업을 생성합니다.
이전 버전을 복원하도록 선택 SSD 스토리지 및 32MBps의 처리량으로 Windows 파일 서버용 새 FSx 생성 복사 작업이 완료되면 DNS 별칭을 조정합니다. 원본 파일 시스템을 삭제합니다.

Answer: C

NO.138
A company is using Amazon WorkSpaces to provide access to its corporate applications across multiple global locations.
User profile data is stored on an Amazon FSx for Windows File Server file system that is configured with a DNS alias.
The file system is linked to an existing Active Directory service.
Recently, the company added a new application that unexpectedly caused user profiles to grow significantly. The company increased the FSx for Windows File Server file system size from 3 TB to 6 TB to prevent any issues.
A few days later, the company made changes to the application's configuration. The user profile storage usage decreased significantly, leaving a large amount of free space on the file system.
A solutions architect needs to reduce the size of the file system to avoid unnecessary costs.
What should the solutions architect do to achieve this goal?

A. During an agreed upon maintenance window, use AWS Backup to create a point-in-time backup of the file system.
Restore the backup to a new, smaller FSx for Windows File Server file system.
Adjust the DNS alias after the restore is completed. Delete the original file system.

B. During an agreed upon maintenance window, disconnect users from the file system.
In the Amazon FSx console, update the storage capacity of the file system.
Enter an absolute value of 3 TB. Reconnect users to the file system.

C. Deploy an AWS DataSyne agent onto a new Amazon EC2 instance. Create a DataSync task. Configure the existing file system as the source location. Configure a new, smaller FSx for Windows File Server file system as the target location. Schedule the task. Adjust the DNS alias after the task is completed. Delete the original file system.

D. Enable shadow copies on the existing file system by using a Windows PowerShell command. Schedule a shadow copy job to create a point-in-time backup of the file system. Choose to restore previous versions, and create a new, smaller FSx for Windows File Server file system. Adjust the DNS alias after the copy job is completed. Delete the original file system.

Answer: C

NO.138
회사는 Amazon WorkSpaces를 사용하여 여러 글로벌 위치에서 회사 애플리케이션에 대한 액세스를 제공하고 있습니다.
사용자 프로필 데이터는 DNS 별칭으로 구성된 Windows 파일 서버용 Amazon FSx 파일 시스템에 저장됩니다.
파일 시스템은 기존 Active Directory 서비스에 연결됩니다.
최근에 회사는 예기치 않게 사용자 프로필이 크게 증가하는 새 응용 프로그램을 추가했습니다.
회사는 문제를 방지하기 위해 Windows 파일 서버용 FSx 파일 시스템 크기를 3TB에서 6TB로 늘렸습니다.
며칠 후 회사에서 애플리케이션 구성을 변경했습니다.
사용자 프로필 저장소 사용량이 크게 감소하여 파일 시스템에 많은 여유 공간이 남습니다.
솔루션 아키텍트는 불필요한 비용을 피하기 위해 파일 시스템의 크기를 줄여야 합니다.
솔루션 아키텍트는 이 목표를 달성하기 위해 무엇을 해야 합니까?

A. 합의된 유지 관리 기간 동안 AWS Backup을 사용하여 파일 시스템의 특정 시점 백업을 생성합니다.
백업을 Windows 파일 서버용 더 작은 새 FSx 파일 시스템으로 복원합니다.
복원이 완료된 후 DNS 별칭을 조정합니다. 원본 파일 시스템을 삭제합니다.

B. 합의된 유지 관리 기간 동안 파일 시스템에서 사용자의 연결을 끊습니다.
Amazon FSx 콘솔에서 파일 시스템의 스토리지 용량을 업데이트합니다.
절대값 3TB를 입력합니다. 사용자를 파일 시스템에 다시 연결합니다.

C. AWS DataSyne 에이전트를 새 Amazon EC2 인스턴스에 배포합니다.
DataSync 작업을 만듭니다. 기존 파일 시스템을 원본 위치로 구성합니다.
대상 위치로 Windows 파일 서버 파일 시스템용 더 작은 새 FSx를 구성합니다.
작업을 예약합니다. 작업이 완료된 후 DNS 별칭을 조정합니다.
원본 파일 시스템을 삭제합니다.

D. Windows PowerShell 명령을 사용하여 기존 파일 시스템에서shadow copies를 활성화합니다.
shadow copy작업을 예약하여 파일 시스템의 특정 시점 백업을 생성합니다.
이전 버전을 복원하고 Windows 파일 서버 파일 시스템용 더 작은 새 FSx를 생성하도록 선택합니다.
복사 작업이 완료된 후 DNS 별칭을 조정합니다. 원본 파일 시스템을 삭제합니다.

Answer: C

NO.139
A company runs a software-as-a-service (SaaS) application on AWS. The application consists of AWS Lambda functions and an Amazon RDS for MySQL Multi-AZ database.
During market events, the application has a much higher workload than normal.
Users notice slow response times during the peak periods because of many database connections.
The company needs to improve the scalable performance and availability of the database.
Which solution meets these requirements?

A. Create an Amazon CloudWatch alarm action that triggers a Lambda function to add an Amazon RDS for MySQL read replica when resource utilization hits a threshold.

B. Migrate the database to Amazon Aurora, and add a read replica. Add a database connection pool outside of the Lambda handler function.

C. Migrate the database to Amazon Aurora, and add a read replica. Use Amazon Route 53 weighted records.

D. Migrate the database to Amazon Aurora, and add an Aurora Replica. Configure Amazon RDS Proxy to manage database connection pools.

NO.139
회사는 AWS에서 SaaS(Software-as-a-Service) 애플리케이션을 실행합니다. 애플리케이션은 AWS Lambda 함수와 MySQL 다중 AZ 데이터베이스용 Amazon RDS로 구성됩니다.
market 이벤트 중에는 애플리케이션의 워크로드가 평소보다 훨씬 높습니다.
사용자는 많은 데이터베이스 연결로 인해 피크 기간 동안 느린 응답 시간을 알 수 있습니다.
회사는 데이터베이스의 확장 가능한 성능과 가용성을 개선해야 합니다.

A. 리소스 사용률이 임계값에 도달할 때 MySQL용 Amazon RDS 읽기 전용 복제본을 추가하는 Lambda 함수를 트리거하는 Amazon CloudWatch 경보 작업을 생성합니다.

B. 데이터베이스를 Amazon Aurora로 마이그레이션하고 읽기 전용 복제본을 추가합니다. Lambda 핸들러 함수 외부에 데이터베이스 연결 풀을 추가합니다.

C. 데이터베이스를 Amazon Aurora로 마이그레이션하고 읽기 전용 복제본을 추가합니다. Amazon Route 53 가중 레코드를 사용합니다.

D. 데이터베이스를 Amazon Aurora로 마이그레이션하고 Aurora 복제본을 추가합니다. 데이터베이스 연결 풀을 관리하도록 Amazon RDS 프록시를 구성합니다.

Answer: D

NO.140
A company hosts a photography website on AWS that has global visitors.
The website has experienced steady increases in traffic during the last 12 months, and users have reported a delay in displaying images.
The company wants to configure Amazon CloudFront lo deliver photos to visitors with minimal latency.
Which actions will achieve this goal? (Select TWO.)

A. Set the Minimum TTL and Maximum TTL to 0 in the CloudFront distribution.

B. Set the Minimum TTL and Maximum TTL to a high value in the CloudFront distribution.

C. Set the CloudFront distribution to forward all headers, all cookies, and all query strings to the origin.

D. Set up additional origin servers that are geographically closer to the requesters. Configure latency-based routing in Amazon Route 53.

E. Select Price Class 100 on Ihe CloudFront distribution.

Answer: B,D

NO.140
전 세계 방문자가 있는 AWS에서 사진 웹사이트를 호스팅하는 회사가 있습니다.
웹사이트는 지난 12개월 동안 트래픽이 꾸준히 증가했으며 사용자는 이미지 표시가 지연된다고 보고했습니다.
회사는 최소 지연 시간으로 방문자에게 사진을 제공하도록 Amazon CloudFront를 구성하려고 합니다. 어떤 행동이 이 목표를 달성할 것인가? (2개를 선택하십시오.)

A. CloudFront 배포에서 최소 TTL 및 최대 TTL을 0으로 설정합니다.

B. CloudFront 배포에서 최소 TTL 및 최대 TTL을 높은 값으로 설정합니다.

C. 모든 헤더, 모든 쿠키 및 모든 쿼리 문자열을 오리진으로 전달하도록 CloudFront 배포를 설정합니다.

D. 요청자에게 지리적으로 더 가까운 추가 원본 서버를 설정합니다. Amazon Route 53에서 지연 시간 기반 라우팅을 구성합니다.

E. CloudFront 배포에서 Price Class 100을 선택합니다.

Answer: B,D

NO.141
A company recently deployed an application on AWS. The application uses Amazon DynamoDB.
The company measured the application load and configured the RCUs and WCUs on the DynamoDB table to match the expected peak load.
The peak load occurs once a week for a 4-hour period and is double the average load.
The application load is close to the average load tor the rest of the week.
The access pattern includes many more writes to the table than reads of the table.
A solutions architect needs to implement a solution to minimize the cost of the table.
Which solution will meet these requirements?

(A). Use AWS Application Auto Scaling to increase capacity during the peak period.
Purchase reserved RCUs and WCUs to match the average load.

(B). Configure on-demand capacity mode for the table.

(C). Configure DynamoDB Accelerator (DAX) in front of the table.
Reduce the provisioned read capacity to match the new peak load on the table.

(D). Configure DynamoDB Accelerator (DAX) in front of the table.
Configure on-demand capacity mode for the table.
Answer: D

NO.141
한 회사가 최근 AWS에 애플리케이션을 배포했습니다. 애플리케이션은 Amazon DynamoDB를 사용합니다. 회사는 애플리케이션 로드를 측정하고 예상되는 피크 로드와 일치하도록 DynamoDB 테이블에서 RCU 및 WCU를 구성했습니다.
최대 부하는 4시간 동안 일주일에 한 번 발생하며 평균 부하의 두 배입니다.
애플리케이션 로드는 나머지 주의 평균 로드에 가깝습니다.
액세스 패턴에는 테이블 읽기보다 테이블에 대한 쓰기가 더 많이 포함됩니다.
솔루션 아키텍트는 테이블 비용을 최소화하는 솔루션을 구현해야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. AWS Application Auto Scaling을 사용하여 피크 기간 동안 용량을 늘립니다.
평균 부하와 일치하도록 예약된 RCU 및 WCU를 구입합니다.

B. 테이블에 대한 주문형 용량 모드를 구성합니다.

C. 테이블 앞에 DynamoDB Accelerator(DAX)를 구성합니다.
테이블의 새로운 최대 로드에 맞게 프로비저닝된 읽기 용량을 줄입니다.

D. 테이블 앞에 DynamoDB Accelerator(DAX)를 구성합니다. 테이블에 대한 주문형 용량 모드를 구성합니다.
Answer: D

NO.142
A company has many AWS accounts and uses AWS Organizations to manage all of them.
A solutions architect must implement a solution that the company can use to share a common network across multiple accounts.
The company's infrastructure team has a dedicated infrastructure account that has a VPC.
The infrastructure team must use this account to manage the network.
Individual accounts cannot have the ability to manage their own networks.
However, individual accounts must be able to create AWS resources within subnets.
Which combination of actions should the solutions architect perform to meet these requirements? (Select TWO.)

A. Create a transit gateway in the infrastructure account.

B. Enable resource sharing from the AWS Organizations management account.

C. Create VPCs in each AWS account within the organization in AWS Organizations.
Configure the VPCs to share the same CIDR range and subnets as the VPC in the infrastructure account.
Peer the VPCs in each individual account with the VPC in the infrastructure account.

D. Create a resource share in AWS Resource Access Manager in the infrastructure account.
Select the specific AWS Organizations OU that will use the shared network.
Select each subnet to associate with the resource share.

E. Create a resource share in AWS Resource Access Manager in the infrastructure account.
Select the specific AWS Organizations OU that will use the shared network.
Select each prefix list to associate with the resource share.

Answer: B, D

NO.142
회사에는 많은 AWS 계정이 있으며 AWS Organizations를 사용하여 모든 계정을 관리합니다.
솔루션 아키텍트는 회사가 여러 계정에서 공통 네트워크를 공유하는 데 사용할 수 있는
솔루션을 구현해야 합니다.
회사의 인프라 팀에는 VPC가 있는 전용 인프라 계정이 있습니다.
인프라 팀은 이 계정을 사용하여 네트워크를 관리해야 합니다.
개별 계정은 자체 네트워크를 관리할 수 없습니다.
그러나 개별 계정은 서브넷 내에서 AWS 리소스를 생성할 수 있어야 합니다.
이러한 요구 사항을 충족하기 위해 솔루션 아키텍트는 어떤 작업 조합을 수행해야 합니까?
(2개를 선택하십시오.)

A. 인프라 계정에서 전송 게이트웨이를 생성합니다.

B. AWS Organizations 관리 계정에서 리소스 공유를 활성화합니다.

C. AWS Organizations의 조직 내 각 AWS 계정에 VPC를 생성합니다.
인프라 계정의 VPC와 동일한 CIDR 범위 및 서브넷을 공유하도록 VPC를 구성합니다.
인프라 계정의 VPC와 각 개별 계정의 VPC를 피어링합니다.

D. 인프라 계정의 AWS Resource Access Manager에서 리소스 공유를 생성합니다.
공유 네트워크를 사용할 특정 AWS Organizations OU를 선택합니다.
리소스 공유와 연결할 각 서브넷을 선택합니다.

E. 인프라 계정의 AWS Resource Access Manager에서 리소스 공유를 생성합니다.
공유 네트워크를 사용할 특정 AWS Organizations OU를 선택합니다.
리소스 공유와 연결할 각 접두사 목록을 선택합니다.

Answer: B, D

NO.142
A company has many AWS accounts and uses AWS Organizations to manage all of them.
A solutions architect must implement a solution that the company can use to share a common network across multiple accounts.
The company's infrastructure team has a dedicated infrastructure account that has a VPC.
The infrastructure team must use this account to manage the network.
Individual accounts cannot have the ability to manage their own networks.
However, individual accounts must be able to create AWS resources within subnets.
Which combination of actions should the solutions architect perform to meet these requirements? (Select TWO.)

A. Create a transit gateway in the infrastructure account.

B. Enable resource sharing from the AWS Organizations management account.

C. Create VPCs in each AWS account within the organization in AWS Organizations.
Configure the VPCs to share the same CIDR range and subnets as the VPC in the infrastructure account.
Peer the VPCs in each individual account with the VPC in the infrastructure account,

D. Create a resource share in AWS Resource Access Manager in the infrastructure account.
Select the specific AWS Organizations OU that will use the shared network.
Select each subnet to associate with the resource share.

E. Create a resource share in AWS Resource Access Manager in the infrastructure account.
Select the specific AWS Organizations OU that will use the shared network. Select each prefix list to associate with the resource share.

Answer: C,E

https://docs.aws.amazon.com/vpc/latest/userguide/sharing-managed-prefix-lists.html

NO.142
회사에는 많은 AWS 계정이 있으며 AWS Organizations를 사용하여 모든 계정을 관리합니다.
솔루션 아키텍트는 회사가 여러 계정에서 공통 네트워크를 공유하는 데 사용할 수 있는 솔루션을 구현해야 합니다.
회사의 인프라 팀에는 VPC가 있는 전용 인프라 계정이 있습니다.
인프라 팀은 이 계정을 사용하여 네트워크를 관리해야 합니다.
개별 계정은 자체 네트워크를 관리할 수 없습니다.
그러나 개별 계정은 서브넷 내에서 AWS 리소스를 생성할 수 있어야 합니다.
이러한 요구 사항을 충족하기 위해 솔루션 아키텍트는 어떤 작업 조합을 수행해야 합니까?
(2개를 선택하십시오.)

A. 인프라 계정에서 전송 게이트웨이를 생성합니다.

B. AWS Organizations 관리 계정에서 리소스 공유를 활성화합니다.

C. AWS Organizations의 조직 내 각 AWS 계정에 VPC를 생성합니다.
인프라 계정의 VPC와 동일한 CIDR 범위 및 서브넷을 공유하도록 VPC를 구성합니다.
인프라 계정의 VPC와 각 개별 계정의 VPC를 피어링합니다.

D. 인프라 계정의 AWS Resource Access Manager에서 리소스 공유를 생성합니다.
공유 네트워크를 사용할 특정 AWS Organizations OU를 선택합니다.
리소스 공유와 연결할 각 서브넷을 선택합니다.

E. 인프라 계정의 AWS Resource Access Manager에서 리소스 공유를 생성합니다.
공유 네트워크를 사용할 특정 AWS Organizations OU를 선택합니다. 리소스 공유와 연결할 각 접두사 목록을 선택합니다.

Answer: B, D

https://docs.aws.amazon.com/vpc/latest/userguide/sharing-managed-prefix-lists.html

NO.143
A finance company is storing financial records in an Amazon S3 bucket.
The company persists a record for every financial transaction.
According to regulatory requirements, the records cannot be modified for at least 1 year after they are written.
The records are read on a regular basis and must be immediately accessible.
Which solution will meet these requirements?

A. Create a new S3 bucket.
Turn on S3 Object Lock, set a default retention period of 1 year, and set the retention mode to compliance mode.
Store all records in the new S3 bucket.

B. Create an S3 Lifecycle rule to immediately transfer new objects to the S3 Glacier storage tier.
Create an S3 Glacier Vault Lock policy that has a retention period of 1 year.

C. Create an S3 Lifecycle rule to immediately transfer new objects to the S3 Intelligent-Tiering storage tier.
Set a retention period of 1 year.

D. Create an S3 bucket policy with a Deny action for PutObject operations with a condition where the s3:x-amz-object-retention header is not equal to 1 year.

Answer: A

NO.143
금융 회사가 Amazon S3 버킷에 재무 기록을 저장하고 있습니다.
회사는 모든 금융 거래에 대한 기록을 유지합니다. 규제 요건에 따라 기록은 작성된 후 최소 1년 동안 수정할 수 없습니다.기록은 정기적으로 읽고 즉시 액세스할 수 있어야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 새 S3 버킷을 생성합니다.
S3 객체 잠금을 켜고 기본 보존 기간을 1년으로 설정하고 보존 모드를 규정 준수 모드로 설정합니다. 모든 레코드를 새 S3 버킷에 저장합니다.

B. 새 객체를 S3 Glacier 스토리지 계층으로 즉시 전송하는 S3 수명 주기 규칙을 생성합니다.
보존 기간이 1년인 S3 Glacier 볼트 잠금 정책을 생성합니다.

C. 새 객체를 S3 Intelligent-Tiering 스토리지 계층으로 즉시 전송하는 S3 수명 주기 규칙을 생성합니다. 보존 기간을 1년으로 설정합니다.

D. s3:x-amz-object-retention 헤더가 1년이 아닌 조건으로 PutObject 작업에 대한 Deny 작업을 사용하여 S3 버킷 정책을 생성합니다.
Answer: A

NO.144
A company is migrating its infrastructure to the AWS Cloud.
The company must comply with a variety of regulatory standards for different projects.
The company needs a multi-account environment.
A solutions architect needs to prepare the baseline infrastructure.
The solution must provide a consistent baseline of management and security but it must allow flexibility for different compliance requirements within various AWS accounts.
The solution also needs to integrate with the existing onpremises Active Directory Federation Services (AD FS) server.
Which solution meets these requirements with the LEAST amount of operational overhead?

(A). Create an organization In AWS Organizations.
Create a single SCP for least privilege access across all accounts.
Create a single OU for all accounts.
Configure an IAM identity provider tor federation with the on-premises AD FS server.
Configure a central logging account with a defined process for log generating services to send log events to the central account.
Enable AWS Config in the central account with conformance packs for all accounts.

(B). Create an organization In AWS Organizations.
Enable AWS Control Tower on the organization.
Review included guardrails for SCPs.
Check AWS Config for areas that require additions.
Add OUs as necessary.
Connect AWS Single Sign-On to the on-premises AD FS server.

(C). Create an organization in AWS Organizations.
Create SCPs for least privilege access.
Create an OU structure, and use it to group AWS accounts.
Connect AWS Single Sign-On to the on-premises AD FS server.
Configure a central logging account with a defined process for log generating services to send log events to the central account.
Enable AWS Config in the central account with aggregators and conformance packs.

(D). Create an organization in AWS Organizations.
Enable AWS Control Tower on the organization.
Review included guardrails for SCPs.
Check AWS Config for areas that require additions.
Configure an IAM identity provider for federation with the on-premises AD FS server.

Answer: A

NO.144
회사에서 인프라를 AWS 클라우드로 마이그레이션하고 있습니다.
회사는 다양한 프로젝트에 대한 다양한 규제 표준을 준수해야 합니다.
회사는 다중 계정 환경이 필요합니다.
솔루션 아키텍트는 기본 인프라를 준비해야 합니다.
솔루션은 일관된 관리 및 보안 기준을 제공해야 하지만 다양한 AWS 계정 내에서 다양한 규정 준수 요구 사항에 대한 유연성을 허용해야 합니다.
솔루션은 또한 기존 온프레미스 AD FS(Active Directory Federation Services) 서버와 통합해야 합니다. 최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

(A). AWS Organizations에서 조직을 생성합니다.
모든 계정에서 최소 권한 액세스를 위해 single SCP를 만듭니다.
모든 계정에 대해 single OU를 만듭니다.
IAM 자격 증명 공급자를 온프레미스 AD FS 서버와 연동하도록 구성합니다.
중앙 계정에 로그 이벤트를 보내기 위해 로그 생성 서비스에 대해 정의된 프로세스로 중앙 로깅 계정을 구성합니다.
모든 계정에 대한 적합성 팩을 사용하여 중앙 계정에서 AWS Config를 활성화합니다.

(B). AWS Organizations에서 조직을 생성합니다.
조직에서 AWS Control Tower를 활성화합니다.
SCP용 가드레일을 검토합니다.
추가가 필요한 영역은 AWS Config를 확인하십시오.
필요에 따라 OU를 추가합니다.
AWS Single Sign-On을 온프레미스 AD FS 서버에 연결합니다.

(C). AWS Organizations에서 조직을 생성합니다.
최소 권한 액세스를 위해 SCP를 만듭니다.
OU 구조를 생성하고 이를 사용하여 AWS 계정을 그룹화합니다.
AWS Single Sign-On을 온프레미스 AD FS 서버에 연결합니다.
전송할 로그 생성 서비스에 대해 정의된 프로세스로 중앙 로깅 계정을 구성합니다.
중앙 계정에 이벤트를 기록합니다.
central 계정에서 aggregators 및 conformance pack이 있는 AWS Config를 활성화합니다.

(D). AWS Organizations에서 조직을 생성합니다.
조직에서 AWS Control Tower를 활성화합니다.

SCP용 가드레일을 검토합니다.
추가가 필요한 영역은 AWS Config를 확인하십시오.
온프레미스 AD FS 서버와의 연동을 위해 IAM 자격 증명 공급자를 구성합니다.

Answer: A

NO.145
A company has an organization that has many AWS accounts in AWS Organizations.
A solutions architect must improve how the company manages common security group rules for the AWS accounts in the organization.
The company has a common set of IP CIDR ranges in an allow list in each AWS account to allow access to and from the company's on-premises network.
Developers within each account are responsible for adding new IP CIDR ranges to their security groups.
The security team has its own AWS account. Currently, the security team notifies the owners of the other AWS accounts when changes are made to the allow list.
The solutions architect must design a solution that distributes the common set of CIDR ranges across all accounts.
Which solution meets these requirements with the LEAST amount of operational overhead?

A. Set up an Amazon Simple Notification Service (Amazon SNS) topic in the security team's AWS account. Deploy an AWS Lambda function in each AWS account.
Configure the Lambda function to run every time an SNS topic receives a message.
Configure the Lambda function to take an IP address as input and add it to a list of security groups in the account.
Instruct the security team to distribute changes by publishing messages to its SNS topic.

B. Create new customer-managed prefix lists in each AWS account within the organization.
Populate the prefix lists in each account with all internal CIDR ranges.
Notify the owner of each AWS account to allow the new customer-managed prefix list IDs in their accounts in their security groups.
Instruct the security team to share updates with each AWS account owner.

C. Create a new customer-managed prefix list in the security team's AWS account.
Populate the customer-managed prefix list with all internal CIDR ranges.
Share the customer-managed prefix list with the organization by using AWS Resource Access Manager.
Notify the owner of each AWS account to allow the new customer-managed prefix list ID in their security groups.

D. Create an IAM role in each account in the organization.
Grant permissions to update security groups.
Deploy an AWS Lambda function in the security team's AWS account.
Configure the Lambda function to take a list of internal IP addresses as input, assume a role in each organization account, and add the list of IP addresses to the security groups in each account.

Answer: C

https://www.examtopics.com/discussions/amazon/view/74258-exam-aws-certified-solutions-architect-professional-topic-1/

https://docs.aws.amazon.com/vpc/latest/userguide/managed-prefix-lists.html

A managed prefix list is a set of one or more CIDR blocks. You can use prefix lists to make it easier to configure and maintain your security groups and route tables.

NO.145
회사에는 AWS Organizations에 많은 AWS 계정이 있는 조직이 있습니다.
솔루션 아키텍트는 회사가 조직의 AWS 계정에 대한 공통 보안 그룹 규칙을 관리하는 방법을 개선해야 합니다.
회사는 회사의 온프레미스 네트워크에 대한 액세스를 허용하기 위해 각 AWS 계정의 허용 목록에 공통 IP CIDR 범위 세트를 가지고 있습니다.
각 계정 내의 개발자는 보안 그룹에 새 IP CIDR 범위를 추가할 책임이 있습니다.
보안 팀에는 자체 AWS 계정이 있습니다. 현재 보안 팀은 허용 목록이 변경되면 다른 AWS 계정의 소유자에게 알립니다.
솔루션 아키텍트는 모든 계정에 공통 CIDR 범위 집합을 배포하는 솔루션을 설계해야 합니다.
최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 보안 팀의 AWS 계정에서 Amazon Simple Notification Service(Amazon SNS) 주제를 설정합니다. 각 AWS 계정에 AWS Lambda 함수를 배포합니다.
SNS 주제가 메시지를 수신할 때마다 실행되도록 Lambda 함수를 구성합니다.
IP 주소를 입력으로 받아 계정의 보안 그룹 목록에 추가하도록 Lambda 함수를 구성합니다.
보안 팀에 SNS 주제에 메시지를 게시하여 변경 사항을 배포하도록 지시합니다.

B. 조직 내의 각 AWS 계정에 새로운 고객 관리 접두사 목록을 생성합니다.
모든 내부 CIDR 범위로 각 계정의 접두사 목록을 채웁니다.
보안 그룹의 계정에서 새로운 고객 관리형 접두사 목록 ID를 허용하도록 각 AWS 계정의 소유자에게 알립니다.
보안 팀에 각 AWS 계정 소유자와 업데이트를 공유하도록 지시합니다.

C. 보안 팀의 AWS 계정에서 새로운 고객 관리 접두사 목록을 생성합니다.
모든 내부 CIDR 범위로 고객 관리 접두사 목록을 채웁니다.
AWS Resource Access Manager를 사용하여 고객 관리 접두사 목록을 조직과 공유합니다.
보안 그룹에서 새로운 고객 관리형 접두사 목록 ID를 허용하도록 각 AWS 계정의 소유자에게 알립니다.

D. 조직의 각 계정에서 IAM 역할을 생성합니다.
보안 그룹을 업데이트할 수 있는 권한을 부여합니다.
보안 팀의 AWS 계정에 AWS Lambda 함수를 배포합니다.
내부 IP 주소 목록을 입력으로 받고, 각 조직 계정에서 역할을 수임하고, 각 계정의 보안 그룹에 IP 주소 목록을 추가하도록 Lambda 함수를 구성합니다.

Answer: C

■ 관리형 접두사 목록

관리형 접두사 목록은 하나 이상의 CIDR 블록 세트입니다. 접두사 목록을 사용하면 보안 그룹과 라우팅 테이블을 보다 쉽게 구성하고 유지 관리할 수 있습니다.
자주 사용하는 IP 주소에서 접두사 목록을 만들고, 이를 개별적으로 참조하지 않고 보안 그룹 규칙 및 경로의 집합으로 참조할 수 있습니다.
예를 들어, 서로 다른 CIDR 블록은 있지만 포트와 프로토콜은 동일한 보안 그룹 규칙을 접두사 목록을 사용하는 단일 규칙으로 통합할 수 있습니다.
네트워크를 확장하고 다른 CIDR 블록의 트래픽을 허용해야 하는 경우, 관련 접두사 목록을 업데이트할 수 있으며 그러면 접두사 목록을 사용하는 모든 보안 그룹이 업데이트됩니다.
Resource Access Manager(RAM)를 사용하여 다른 AWS 계정과 함께 관리형 접두사 목록을 사용할 수도 있습니다.

접두사 목록에는 두 가지 유형이 있습니다.

- 고객 관리형 접두사 목록 — 사용자가 정의하고 관리하는 IP 주소 범위 세트입니다. 접두사 목록을 다른 AWS 계정과 공유하여 해당 계정이 자체 리소스의 접두사 목록을 참조하도록 할 수 있습니다.
- AWS 관리형 접두사 목록 - AWS 서비스의 IP 주소 범위 세트입니다. AWS 관리형 접두사 목록은 생성, 수정, 공유 또는 삭제할 수 없습니다.

NO.146
A fleet of Amazon ECS instances is used to poll an Amazon SQS queue and update items in an Amazon DynamoDB database.
Items in the table are not being updated, and the SQS queue is filling up.
Amazon CloudWatch Logs are showing consistent 400 errors when attempting to update the table.
The provisioned write capacity units are appropriately configured, and no throttling is occurring.
What is the LIKELY cause of the failure?

A. The ECS service was deleted.

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

C. The ECS instance task execution IAM role was modified.

D. The ECS task role was modified.

Answer: D

https://www.examtopics.com/discussions/amazon/view/27791-exam-aws-certified-solutions-architect-professional-topic-1/

D. Between executionRoleArn (option C) and taskRoleArn (D), only the latter is used to interact with DynamoDB. The former is used to download images or write logs to Cloudwatch.

Status 400 with DynamoDB. Here,probably an authn failure due to someone messing up the role.

NO.146
Amazon ECS 인스턴스 집합은 Amazon SQS 대기열을 폴링하고 Amazon DynamoDB 데이터베이스의 항목을 업데이트하는 데 사용됩니다.
테이블의 항목이 업데이트되지 않고 SQS 대기열이 채워지고 있습니다.
Amazon CloudWatch Logs는 테이블 업데이트를 시도할 때 일관된 400 오류를 표시합니다.
프로비저닝된 쓰기 용량 단위가 적절하게 구성되었으며 조절이 발생하지 않습니다.
실패의 가능한 원인은 무엇입니까?

A. ECS 서비스가 삭제되었습니다.
B. ECS 구성에는 Auto Scaling 그룹이 포함되어 있지 않습니다.
C. ECS 인스턴스 작업 실행 IAM 역할이 수정되었습니다.
D. ECS 태스크 역할이 수정되었습니다.

Answer: D

■ 태스크 정의

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

태스크 정의는 태스크 패밀리, IAM 태스크 역할, 네트워크 모드, 컨테이너 정의, 볼륨, 작업 배치 제약, 시작 유형 등의 부분으로 나뉩니다. 태스크 정의에는 패밀리 및 컨테이너 정의가 필요합니다.

하지만 태스크 역할, 네트워크 모드, 볼륨, 작업 배치 제약 및 시작 유형은 선택 사항입니다.

JSON 파일에서 이러한 파라미터를 사용하여 태스크 정의를 구성할 수 있습니다.

```
{
    "family": "firelens-example-cloudwatch",
    "taskRoleArn": "arn:aws:iam::123456789012:role/ecs_task_iam_role",
    "containerDefinitions": [
        {
            "essential": true,
            "image": "906394416424.dkr.ecr.us-west-2.amazonaws.com/aws-for-fluent-bit:latest",
            "name": "log_router",
            "firelensConfiguration": {
                "type": "fluentbit"
            },
            "logConfiguration": {
                "logDriver": "awslogs",
                "options": {
                    "awslogs-group": "firelens-container",
                    "awslogs-region": "us-west-2",
                    "awslogs-create-group": "true",
                    "awslogs-stream-prefix": "firelens"
                }
            },
            "memoryReservation": 50
        },
        {
            "essential": true,
            "image": "httpd",
            "name": "app",
            "logConfiguration": {
                "logDriver":"awsfirelens",
                "options": {
                    "Name": "cloudwatch",
                    "region": "us-west-2",
                    "log_group_name": "firelens-blog",
                    "auto_create_group": "true",
                    "log_stream_prefix": "from-fluent-bit",
                    "log-driver-buffer-limit": "2097152"
                }
            },
            "memoryReservation": 100
            }
    ]
}
```

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Programming.Errors.html#Programming.Errors.MessagesAndCodes

HTTP 상태 코드 400

HTTP 400 상태 코드는 인증 실패, 필수 파라미터 누락, 테이블의 할당 처리량 초과 등 요청에 문제가 있음을 의미합니다. 요청을 다시 제출하기 전에 애플리케이션의 문제를 해결해야 합니다.

NO.147
A company built an ecommerce website on AWS using a three-tier web architecture.
The application is Java-based and composed of an Amazon CloudFront distribution, an Apache web server layer of Amazon EC2 instances in an Auto Scaling group, and a backend Amazon Aurora MySQL database.
Last month, during a promotional sales event, users reported errors and timeouts while adding items to their shopping carts.
The operations team recovered the logs created by the web servers and reviewed Aurora DB cluster performance metrics.
Some of the web servers were terminated before logs could be collected and the Aurora metrics were not sufficient for query performance analysis.
Which combination of steps must the solutions architect take to improve application performance visibility during peak traffic events? (Choose three.)

A. Configure the Aurora MySQL DB cluster to publish slow query and error logs to Amazon CloudWatch Logs.

B. Implement the AWS X-Ray SDK to trace incoming HTTP requests on the EC2 instances and implement tracing of SQL queries with the X-Ray SDK for Java.

C. Configure the Aurora MySQL DB cluster to stream slow query and error logs to Amazon Kinesis

D. Install and configure an Amazon CloudWatch Logs agent on the EC2 instances to send the Apache logs to CloudWatch Logs.

E. Enable and configure AWS CloudTrail to collect and analyze application activity from Amazon EC2 and Aurora.

F. Enable Aurora MySQL DB cluster performance benchmarking and publish the stream to AWS X-Ray.

Answer: A, B, D

https://www.examtopics.com/discussions/amazon/view/47553-exam-aws-certified-solutions-architect-professional-topic-1/

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_LogAccess.Concepts.MySQL.html#USER_LogAccess.MySQLDB.PublishAuroraMySQLtoCloudWatchLogs

https://aws.amazon.com/blogs/mt/simplifying-apache-server-logs-with-amazon-cloudwatch-logs-insights/

https://docs.aws.amazon.com/xray/latest/devguide/xray-sdk-dotnet-messagehandler.html

https://docs.aws.amazon.com/xray/latest/devguide/xray-sdk-java-sqlclients.html

NO.147
한 회사는 3계층 웹 아키텍처를 사용하여 AWS에서 전자 상거래 웹 사이트를 구축했습니다. 이 애플리케이션은 Java 기반이며 Amazon CloudFront 배포, Auto Scaling 그룹에 있는 Amazon EC2 인스턴스의 Apache 웹 서버 계층 및 백엔드 Amazon Aurora MySQL 데이터베이스로 구성됩니다.
지난 달 프로모션 판매 이벤트 중에 사용자가 장바구니에 항목을 추가하는 동안 오류 및 시간 초과를 보고했습니다.
운영팀은 웹 서버에서 생성된 로그를 복구하고 Aurora DB 클러스터 성능 지표를 검토했습니다. 일부 웹 서버가 로그를 수집하기 전에 종료되었고 Aurora 지표가 쿼리 성능 분석에 충분하지 않았습니다.
최대 트래픽 이벤트 동안 애플리케이션 성능 가시성을 개선하기 위해 솔루션 아키텍트가 취해야 하는 단계의 조합은 무엇입니까? (3개를 선택하세요.)

A. 느린 쿼리 및 오류 로그를 Amazon CloudWatch Logs에 게시하도록 Aurora MySQL DB 클러스터를 구성합니다.

B. AWS X-Ray SDK를 구현하여 EC2 인스턴스에서 들어오는 HTTP 요청을 추적하고 X-Ray SDK for Java로 SQL 쿼리 추적을 구현합니다.

C. 느린 쿼리 및 오류 로그를 Amazon Kinesis로 스트리밍하도록 Aurora MySQL DB 클러스터 구성합니다.

D. Amazon CloudWatch Logs 에이전트를 EC2 인스턴스에 설치 및 구성하여 Apache 로그를 CloudWatch Logs로 보냅니다.

E. Amazon EC2 및 Aurora에서 애플리케이션 활동을 수집하고 분석하도록 AWS CloudTrail을 활성화하고 구성합니다.

F. Aurora MySQL DB 클러스터 성능 벤치마킹을 활성화하고 스트림을 AWS X-Ray에 게시합니다.

Answer: A, B, D

https://www.examtopics.com/discussions/amazon/view/47553-exam-aws-certified-solutions-architect-professional-topic-1/

NO.148
A large multinational company runs a timesheet application on AWS that is used by staff across the world.
The application runs on Amazon EC2 instances in an Auto Scaling group behind an Elastic Load Balancing (ELB) load balancer, and stores data in an Amazon RDS MySQL Multi-AZ database instance.
The CFO is concerned about the impact on the business if the application is not available. The application must not be down for more than two hours, but he solution must be as cost-effective as possible.
How should the Solutions Architect meet the CFO's requirements while minimizing data loss?

A. In another region, configure a read replica and create a copy of the infrastructure.
When an issue occurs, promote the read replica and configure as an Amazon RDS Multi-AZ database instance.
Update the DNS record to point to the other region's ELB.

B. Configure a 1-day window of 60-minute snapshots of the Amazon RDS Multi-AZ database instance.
Create an AWS CloudFormation template of the application infrastructure that uses the latest snapshot.
When an issue occurs, use the AWS CloudFormation template to create the environment in another region.
Update the DNS record to point to the other region's ELB.

C. Configure a 1-day window of 60-minute snapshots of the Amazon RDS Multi-AZ database instance which is copied to another region.
Create an AWS CloudFormation template of the application infrastructure that uses the latest copied snapshot.
When an issue occurs, use the AWS CloudFormation template to create the environment in another region. Update the DNS record to point to the other region's ELB.

D. Configure a read replica in another region.
Create an AWS CloudFormation template of the application infrastructure.
When an issue occurs, promote the read replica and configure as an Amazon RDS Multi-AZ database instance and use the AWS CloudFormation template to create the environment in another region using the promoted Amazon RDS instance.
Update the DNS record to point to the other region's ELB.

Answer: D

https://www.examtopics.com/discussions/amazon/view/5593-exam-aws-certified-solutions-architect-professional-topic-1/

NO.148
대규모 다국적 회사는 전 세계 직원이 사용하는 AWS에서 작업표 애플리케이션을 실행합니다. 애플리케이션은 Elastic Load Balancing(ELB) 로드 밸런서 뒤에 있는 Auto Scaling 그룹의 Amazon EC2 인스턴스에서 실행되고 Amazon RDS MySQL 다중 AZ 데이터베이스 인스턴스에 데이터를 저장합니다.
CFO는 애플리케이션을 사용할 수 없는 경우 비즈니스에 미치는 영향에 대해 우려하고 있습니다. 애플리케이션은 2시간 이상 중단되어서는 안 되지만 솔루션은 가능한 한 비용 효율적이어야 합니다.
Solutions Architect는 데이터 손실을 최소화하면서 CFO의 요구 사항을 어떻게 충족해야 합니까?

A. 다른 지역에서 읽기 전용 복제본을 구성하고 인프라의 복사본을 만듭니다.
문제가 발생하면 읽기 전용 복제본을 승격하고 Amazon RDS 다중 AZ 데이터베이스 인스턴스로 구성합니다.
다른 지역의 ELB를 가리키도록 DNS 레코드를 업데이트합니다.

B. Amazon RDS 다중 AZ 데이터베이스 인스턴스의 60분 스냅샷의 1일 창을 구성합니다.
최신 스냅샷을 사용하는 애플리케이션 인프라의 AWS CloudFormation 템플릿을 생성합니다.
문제가 발생하면 AWS CloudFormation 템플릿을 사용하여 다른 리전에 환경을 생성하십시오.
다른 지역의 ELB를 가리키도록 DNS 레코드를 업데이트합니다.

C. 다른 리전에 복사되는 Amazon RDS 다중 AZ 데이터베이스 인스턴스의 60분 스냅샷의 1일 창을 구성합니다.
가장 최근에 복사한 스냅샷을 사용하는 애플리케이션 인프라의 AWS CloudFormation 템플릿을 생성합니다.
문제가 발생하면 AWS CloudFormation 템플릿을 사용하여 다른 리전에 환경을 생성하십시오.
다른 지역의 ELB를 가리키도록 DNS 레코드를 업데이트합니다.

D. 다른 지역에서 읽기 전용 복제본을 구성합니다.
애플리케이션 인프라의 AWS CloudFormation 템플릿을 생성합니다.
문제가 발생하면 읽기 전용 복제본을 승격하고 Amazon RDS 다중 AZ 데이터베이스 인스턴스로 구성하고 AWS CloudFormation 템플릿을 사용하여 승격된 Amazon RDS 인스턴스를 사용하는 다른 리전에 환경을 생성합니다.
다른 지역의 ELB를 가리키도록 DNS 레코드를 업데이트합니다.

Answer: D

https://www.examtopics.com/discussions/amazon/view/5593-exam-aws-certified-solutions-architect-professional-topic-1/

NO.149
A company is running an application in the AWS Cloud.
The application consists of microservices that run on a fleet of Amazon EC2 instances in multiple Availability Zones behind an Application Load Balancer.
The company recently added a new REST API that was implemented in Amazon API Gateway.
Some of the older microservices that run on EC2 instances need to call this new API.
The company does not want the API to be accessible from the public internet and does not want proprietary data to traverse the public internet.
What should a solutions architect do to meet these requirements?

A. Create an AWS Site-to-Site VPN connection between the VPC and the API Gateway.
Use API Gateway to generate a unique API key for each microservice. Configure the API methods to require the key.

B. Create an interface VPC endpoint for API Gateway, and set an endpoint policy to only allow access to the specific API.
Add a resource policy to API Gateway to only allow access from the VPC endpoint. Change the API Gateway endpoint type to private.

C. Modify the API Gateway to use IAM authentication Update the IAM policy for the IAM role that is assigned to the EC2 instances to allow access to the API Gateway Move the API Gateway into a new VPC.
Deploy a transit gateway and connect the VPCs.

D. Create an accelerator in AWS Global Accelerator, and connect the accelerator to the API Gateway.
Update the route table for all VPC subnets with a route to the created Global Accelerator endpoint IP address. Add an API key for each service to use for authentication.

Answer: B

https://www.examtopics.com/discussions/amazon/view/74172-exam-aws-certified-solutions-architect-professional-topic-1/

NO.149
회사에서 AWS 클라우드에서 애플리케이션을 실행하고 있습니다.
애플리케이션은 Application Load Balancer 뒤의 여러 가용 영역에 있는 Amazon EC2 인스턴스 집합에서 실행되는 마이크로서비스로 구성됩니다.
이 회사는 최근 Amazon API Gateway에 구현된 새로운 REST API를 추가했습니다.
EC2 인스턴스에서 실행되는 일부 이전 마이크로서비스는 이 새 API를 호출해야 합니다.
회사는 API가 퍼블릭 인터넷에서 액세스되는 것을 원하지 않으며 자산 데이터(proprietary data)가 퍼블릭 인터넷을 통과하는 것을 원하지 않습니다.
솔루션 아키텍트는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?

A. VPC와 API Gateway 간에 AWS Site-to-Site VPN 연결을 생성합니다.
API Gateway를 사용하여 각 마이크로서비스에 대해 고유한 API 키를 생성합니다. 키가 필요하도록 API 메서드를 구성합니다.

B. API Gateway에 대한 인터페이스 VPC 엔드포인트를 생성하고 특정 API에 대한 액세스만 허용하도록 엔드포인트 정책을 설정합니다.
VPC 엔드포인트의 액세스만 허용하도록 API Gateway에 리소스 정책을 추가합니다.
API Gateway 엔드포인트 유형을 프라이빗으로 변경합니다.

C. IAM 인증을 사용하도록 API 게이트웨이 수정 API 게이트웨이에 대한 액세스를 허용하도록 EC2 인스턴스에 할당된 IAM 역할에 대한 IAM 정책을 업데이트합니다.
API 게이트웨이를 새 VPC로 이동합니다.
Transit Gateway를 배포하고 VPC를 연결합니다.

D. AWS Global Accelerator에서 액셀러레이터를 생성하고 액셀러레이터를 API Gateway에 연결합니다.
생성된 Global Accelerator 엔드포인트 IP 주소에 대한 경로를 사용하여 모든 VPC 서브넷에 대한 라우팅 테이블을 업데이트합니다.
인증에 사용할 각 서비스에 대한 API 키를 추가합니다.

Answer: B

https://www.examtopics.com/discussions/amazon/view/74172-exam-aws-certified-solutions-architect-professional-topic-1/

NO.150
A company is moving a business-critical, multi-tier application to AWS. The architecture consists of a desktop client application and server infrastructure.
The server infrastructure resides in an on-premises data center that frequently fails to maintain the application uptime SLA of 99.95%.
A Solutions Architect must re- architect the application to ensure that it can meet or exceed the SLA.
The application contains a PostgreSQL database running on a single virtual machine.
The business logic and presentation layers are load balanced between multiple virtual machines.
Remote users complain about slow load times while using this latency-sensitive application.
Which of the following will meet the availability requirements with little change to the application while improving user experience and minimizing costs?

A. Migrate the database to a PostgreSQL database in Amazon EC2.
Host the application and presentation layers in automatically scaled Amazon ECS containers behind an Application Load Balancer.
Allocate an Amazon WorkSpaces WorkSpace for each end user to improve the user experience.

B. Migrate the database to an Amazon RDS Aurora PostgreSQL configuration.
Host the application and presentation layers in an Auto Scaling configuration on Amazon EC2 instances behind an Application Load Balancer.
Use Amazon AppStream 2.0 to improve the user experience.

C. Migrate the database to an Amazon RDS PostgreSQL Multi-AZ configuration.
Host the application and presentation layers in automatically scaled AWS Fargate containers behind a Network Load Balancer.
Use Amazon ElastiCache to improve the user experience.

D. Migrate the database to an Amazon Redshift cluster with at least two nodes.
Combine and host the application and presentation layers in automatically scaled Amazon ECS containers behind an Application Load Balancer.
Use Amazon CloudFront to improve the user experience.

Answer: B

https://www.examtopics.com/discussions/amazon/view/5224-exam-aws-certified-solutions-architect-professional-topic-1/

Aurora would improve availability that can replicate to multiple AZ (6 copies).
Auto scaling would improve the performance together with a ALB.
AppStream is like Citrix that deliver hosted Apps to users.

NO.150
한 회사에서 비즈니스 크리티컬한 다중 계층 애플리케이션을 AWS로 이전하고 있습니다.
아키텍처는 데스크톱 클라이언트 애플리케이션과 서버 인프라로 구성됩니다.
서버 인프라는 99.95%의 애플리케이션 가동 시간 SLA를 유지하는 데 자주 실패하는
온프레미스 데이터 센터에 있습니다.
Solutions Architect는 SLA를 충족하거나 초과할 수 있도록 애플리케이션을 재설계해야 합니다.
애플리케이션에는 단일 가상 머신에서 실행되는 PostgreSQL 데이터베이스가 포함되어
있습니다. 비즈니스 로직 및 프레젠테이션 계층은 여러 가상 머신 간에 로드 밸런싱됩니다.
원격 사용자는 이 지연 시간에 민감한 애플리케이션을 사용하는 동안 느린 로드 시간에 대해
불평합니다.다음 중 사용자 경험을 개선하고 비용을 최소화하면서 애플리케이션을 거의
변경하지 않고 가용성 요구 사항을 충족하는 것은 무엇입니까?

A. 데이터베이스를 Amazon EC2의 PostgreSQL 데이터베이스로 마이그레이션합니다.
Application Load Balancer 뒤에서 자동으로 조정되는 Amazon ECS 컨테이너에서
애플리케이션 및 프레젠테이션 계층을 호스팅합니다.
각 최종 사용자에 대해 Amazon WorkSpaces WorkSpace를 할당하여 사용자 경험을
개선합니다.

B. 데이터베이스를 Amazon RDS Aurora PostgreSQL 구성으로 마이그레이션합니다.
Application Load Balancer 뒤의 Amazon EC2 인스턴스에서 Auto Scaling 구성으로
애플리케이션 및 프레젠테이션 계층을 호스팅합니다.
Amazon AppStream 2.0을 사용하여 사용자 경험을 개선하십시오.

C. 데이터베이스를 Amazon RDS PostgreSQL 다중 AZ 구성으로 마이그레이션합니다.
Network Load Balancer 뒤에서 자동으로 확장되는 AWS Fargate 컨테이너에서 애플리케이션
및 프레젠테이션 계층을 호스팅합니다.
Amazon ElastiCache를 사용하여 사용자 경험을 개선하십시오.

D. 데이터베이스를 두 개 이상의 노드가 있는 Amazon Redshift 클러스터로
마이그레이션합니다.
Application Load Balancer 뒤에서 자동으로 조정되는 Amazon ECS 컨테이너에서
애플리케이션 및 프레젠테이션 계층을 결합하고 호스팅합니다.
Amazon CloudFront를 사용하여 사용자 경험을 개선하십시오.

Answer: B

https://www.examtopics.com/discussions/amazon/view/5224-exam-aws-certified-solutions-architect-professional-topic-1/
Aurora would improve availability that can replicate to multiple AZ (6 copies).
Auto scaling would improve the performance together with a ALB.
AppStream is like Citrix that deliver hosted Apps to users.

NO.151
A company is running an application in the AWS Cloud.
The company's security team must approve the creation of all new IAM users.
When a new IAM user is created, all access for the user must be removed automatically.
The security team must then receive a notification to approve the user. The company has a multi-Region AWS CloudTrail trail in the AWS account.
Which combination of steps will meet these requirements? (Choose three.)

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule.
Define a pattern with the detail-type value set to AWS API Call via CloudTrail and an eventName of CreateUser.

B. Configure CloudTrail to send a notification for the CreateUser event to an Amazon Simple Notification Service (Amazon SNS) topic.

C. Invoke a container that runs in Amazon Elastic Container Service (Amazon ECS) with AWS Fargate technology to remove access.

D. Invoke an AWS Step Functions state machine to remove access.

E. Use Amazon Simple Notification Service (Amazon SNS) to notify the security team.

F. Use Amazon Pinpoint to notify the security team.

Answer: A, D, E

https://www.examtopics.com/discussions/amazon/view/79898-exam-aws-certified-solutions-architect-professional-topic-1/

NO.151
회사에서 AWS 클라우드에서 애플리케이션을 실행하고 있습니다.
회사의 보안 팀은 모든 새 IAM 사용자 생성을 승인해야 합니다.
새 IAM 사용자가 생성되면 해당 사용자에 대한 모든 액세스 권한이 자동으로 제거되어야 합니다.
그런 다음 보안 팀은 사용자를 승인하라는 알림을 받아야 합니다.
이 회사는 AWS 계정에 다중 리전 AWS CloudTrail 추적이 있습니다.
이러한 요구 사항을 충족하는 단계 조합은 무엇입니까? (3개를 선택하세요.)

A. Amazon EventBridge(Amazon CloudWatch Events) 규칙을 생성합니다.
CloudTrail을 통한 AWS API 호출 및 CreateUser의 eventName으로 설정된 세부 유형 값으로 패턴을 정의합니다.

B. CreateUser 이벤트에 대한 알림을 Amazon Simple Notification Service(Amazon SNS) 주제로 보내도록 CloudTrail을 구성합니다.

C. AWS Fargate 기술로 Amazon Elastic Container Service(Amazon ECS)에서 실행되는 컨테이너를 호출하여 액세스를 제거합니다.

D. AWS Step Functions 상태 머신을 호출하여 액세스를 제거합니다.

E. Amazon Simple Notification Service(Amazon SNS)를 사용하여 보안 팀에 알립니다.

F. Amazon Pinpoint를 사용하여 보안 팀에 알립니다.

Answer: A, D, E

NO.152
A company is serving files to its customer through an SFTP server that is accessible over the Internet.
The SFTP server is running on a single Amazon EC2 instance with an Elastic IP address attached.
Customers connect to the SFTP server through its Elastic IP address and use SSH for authentication.
The EC2 instance also has an attached security group that allows access from all customer IP addresses.
A solutions architect must implement a solution to improve availability, minimize the complexity of infrastructure management, and minimize the disruption to customers who access files.
The solution must not change the way customers connect.
Which solution will meet these requirements?

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

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

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

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

the EC2 instances that the Auto Scaling group launches.
Sync all files from the SFTP server to the new multi-attach EBS volume.

Answer: B
https://www.examtopics.com/discussions/amazon/view/60092-exam-aws-certified-solutions-architect-professional-topic-1/

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

NO.152
회사는 인터넷을 통해 액세스할 수 있는 SFTP 서버를 통해 고객에게 파일을 제공하고 있습니다.
SFTP 서버는 탄력적 IP 주소가 연결된 단일 Amazon EC2 인스턴스에서 실행됩니다.
고객은 탄력적 IP 주소를 통해 SFTP 서버에 연결하고 인증을 위해 SSH를 사용합니다.
EC2 인스턴스에는 모든 고객 IP 주소에서 액세스를 허용하는 연결된 보안 그룹도 있습니다.
솔루션 아키텍트는 가용성을 개선하고 인프라 관리의 복잡성을 최소화하며 파일에 액세스하는 고객의 중단을 최소화하는 솔루션을 구현해야 합니다.
솔루션은 고객이 연결하는 방식을 변경해서는 안 됩니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. EC2 인스턴스에서 탄력적 IP 주소를 연결 해제합니다.
SFTP 파일 호스팅에 사용할 Amazon S3 버킷을 생성합니다.
AWS Transfer Family 서버를 생성합니다.
공개적으로 액세스 가능한 엔드포인트로 Transfer Family 서버를 구성합니다.
SFTP 탄력적 IP 주소를 새 엔드포인트와 연결합니다.
Transfer Family 서버가 S3 버킷을 가리키도록 합니다.
SFTP 서버의 모든 파일을 S3 버킷으로 동기화합니다.

B. EC2 인스턴스에서 탄력적 IP 주소를 연결 해제합니다.
SFTP 파일 호스팅에 사용할 Amazon S3 버킷을 생성합니다.
AWS Transfer Family 서버를 생성합니다.
VPC에서 호스팅하는 인터넷 연결 엔드포인트로 Transfer Family 서버를 구성합니다.
SFTP 탄력적 IP 주소를 새 엔드포인트와 연결합니다.
고객 IP 주소가 있는 보안 그룹을 새 엔드포인트에 연결합니다.
Transfer Family 서버가 S3 버킷을 가리키도록 합니다.
SFTP 서버의 모든 파일을 S3 버킷으로 동기화합니다.

C. EC2 인스턴스에서 탄력적 IP 주소를 연결 해제합니다.

SFTP 파일 호스팅에 사용할 새 Amazon Elastic File System(Amazon EFS) 파일 시스템을 생성합니다.
SFTP 서버를 실행하기 위한 AWS Fargate 작업 정의를 생성합니다.
작업 정의에서 EFS 파일 시스템을 마운트로 지정합니다.
작업 정의를 사용하여 Fargate 서비스를 생성하고 서비스 앞에 NLB(Network Load Balancer)를 배치합니다.
서비스를 구성할 때 고객 IP 주소가 있는 보안 그룹을 SFTP 서버를 실행하는 작업에 연결합니다.
탄력적 IP 주소를 NLB와 연결합니다. SFTP 서버의 모든 파일을 S3 버킷으로 동기화합니다.

D. EC2 인스턴스에서 탄력적 IP 주소를 연결 해제합니다.
SFTP 파일 호스팅에 사용할 다중 연결 Amazon Elastic Block Store(Amazon EBS) 볼륨을 생성합니다.
탄력적 IP 주소가 연결된 NLB(Network Load Balancer)를 생성합니다.
SFTP 서버를 실행하는 EC2 인스턴스로 Auto Scaling 그룹을 생성합니다.
시작되는 인스턴스가 새로운 다중 연결 EBS 볼륨을 연결해야 하는 Auto Scaling 그룹을 정의합니다.
NLB 뒤에 인스턴스를 자동으로 추가하도록 Auto Scaling 그룹을 구성합니다.
Auto Scaling 그룹이 시작하는 EC2 인스턴스에 대한 고객 IP 주소를 허용하는 보안 그룹을 사용하도록 Auto Scaling 그룹을 구성합니다.
SFTP 서버의 모든 파일을 새로운 다중 연결 EBS 볼륨으로 동기화합니다.

Answer: B

NO.153
A company has developed a web application. The company is hosting the application on a group of Amazon EC2 instances behind an Application Load Balancer.
The company wants to improve the security posture of the application and plans to use AWS WAF web ACLs. The solution must not adversely affect legitimate traffic to the application.
How should a solutions architect configure the web ACLs to meet these requirements?

A. Set the action of the web ACL rules to Count. Enable AWS WAF logging. Analyze the requests for false positives. Modify the rules to avoid any false positive. Over time, change the action of the web ACL rules from Count to Block.

B. Use only rate-based rules in the web ACLs, and set the throttle limit as high as possible. Temporarily block all requests that exceed the limit. Define nested rules to narrow the scope of the rate tracking.

C. Set the action of the web ACL rules to Block. Use only AWS managed rule groups in the web ACLs. Evaluate the rule groups by using Amazon CloudWatch metrics with AWS WAF sampled requests or AWS WAF logs.

D. Use only custom rule groups in the web ACLs, and set the action to Allow. Enable AWS WAF logging. Analyze the requests for false positives. Modify the rules to avoid any false positive. Over time, change the action of the web ACL rules from Allow to Block.

Answer: B
https://www.examtopics.com/discussions/amazon/view/74273-exam-aws-certified-solutions-architect-professional-topic-1/

https://aws.amazon.com/ko/premiumsupport/knowledge-center/waf-analyze-count-action-rules/

NO.153
회사에서 웹 응용 프로그램을 개발했습니다. 이 회사는 Application Load Balancer 뒤의 Amazon EC2 인스턴스 그룹에서 애플리케이션을 호스팅하고 있습니다. 이 회사는 애플리케이션의 보안 태세를 개선하기를 원하며 AWS WAF 웹 ACL을 사용할 계획입니다. 솔루션은 애플리케이션에 대한 합법적인 트래픽에 부정적인 영향을 미치지 않아야 합니다. 솔루션 아키텍트는 이러한 요구 사항을 충족하도록 웹 ACL을 어떻게 구성해야 합니까?

A. 웹 ACL 규칙의 작업을 Count로 설정합니다. AWS WAF 로깅을 활성화합니다. false positive에 대한 요청을 분석합니다. false positive을 방지하기 위해 규칙을 수정합니다. 시간이 지남에 따라 웹 ACL 규칙의 작업을 Count에서 Block으로 변경합니다.

B. 웹 ACL에서는 비율 기반 규칙만 사용하고 스로틀 제한을 최대한 높게 설정합니다. 제한을 초과하는 모든 요청을 일시적으로 차단합니다. 비율 추적 범위를 좁히기 위해 중첩 규칙을

정의합니다.

C. 웹 ACL 규칙의 동작을 차단으로 설정합니다. 웹 ACL에는 AWS 관리형 규칙 그룹만 사용하십시오. AWS WAF 샘플링 요청 또는 AWS WAF 로그와 함께 Amazon CloudWatch 지표를 사용하여 규칙 그룹을 평가합니다.

D. 웹 ACL에서 사용자 지정 규칙 그룹만 사용하고 작업을 허용으로 설정합니다.
AWS WAF 로깅을 활성화합니다. false positive에 대한 요청을 분석합니다.
false positive을 방지하기 위해 규칙을 수정합니다.
시간이 지나면서 웹 ACL 규칙의 동작을 허용에서 차단으로 변경합니다.

Answer: B

NO.154
An enterprise company wants to allow its developers to purchase third-party software through AWS Marketplace.
The company uses an AWS Organizations account structure with full features enabled, and has a shared services account in each organizational unit (OU) that will be used by procurement managers.
The procurement team's policy indicates that developers should be able to obtain third-party software from an approved list only and use Private Marketplace in AWS Marketplace to achieve this requirement.
The procurement team wants administration of Private Marketplace to be restricted to a role named procurement- manager-role, which could be assumed by procurement managers.
Other IAM users, groups, roles, and account administrators in the company should be denied Private Marketplace administrative access.
What is the MOST efficient way to design an architecture to meet these requirements?

A. Create an IAM role named procurement-manager-role in all AWS accounts in the organization.
Add the PowerUserAccess managed policy to the role.
Apply an inline policy to all IAM users and roles in every AWS account to deny permissions on the AWSPrivateMarketplaceAdminFullAccess managed policy.

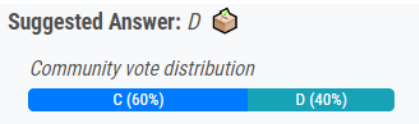
B. Create an IAM role named procurement-manager-role in all AWS accounts in the organization.
Add the AdministratorAccess managed policy to the role.
Define a permissions boundary with the AWSPrivateMarketplaceAdminFullAccess managed policy and attach it to all the developer roles.

C. Create an IAM role named procurement-manager-role in all the shared services accounts in the organization.
Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role.
Create an organization root-level SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role.
Create another organization root-level SCP to deny permissions to create an IAM role named procurement-manager-role to everyone in the organization.

D. Create an IAM role named procurement-manager-role in all AWS accounts that will be used by developers.
Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role. Create an SCP in Organizations to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role.
Apply the SCP to all the shared services accounts in the organization.

Answer: D

https://www.examtopics.com/discussions/amazon/view/28410-exam-aws-certified-solutions-architect-professional-topic-1/



NO.154
엔터프라이즈 회사는 개발자가 AWS Marketplace를 통해 타사 소프트웨어를 구매할 수 있도록 허용하려고 합니다. 이 회사는 모든 기능이 활성화된 AWS Organizations 계정 구조를 사용하며 조달 관리자가 사용할 각 OU(조직 단위)에 공유 서비스 계정이 있습니다.
조달 팀의 정책에 따르면 개발자는 승인된 목록에서만 타사 소프트웨어를 구하고 AWS Marketplace의 Private Marketplace를 사용하여 이 요구사항을 충족할 수 있습니다.
조달 팀은 Private Marketplace의 관리가 조달 관리자가 맡을 수 있는 procurement-manager-role이라는 역할로 제한되기를 원합니다. 회사의 다른 IAM 사용자, 그룹, 역할 및 계정 관리자는 Private Marketplace administrative access가 거부되어야 합니다.
이러한 요구 사항을 충족하도록 아키텍처를 설계하는 가장 효율적인 방법은 무엇입니까?

A. 조직의 모든 AWS 계정에서 procurement-manager-role이라는 IAM 역할을 생성합니다.
PowerUserAccess 관리형 정책을 역할에 추가합니다.
모든 AWS 계정의 모든 IAM 사용자 및 역할에 AWSPrivateMarketplaceAdminFullAccess 관리형 정책에 대한 deny permissions 인라인 정책을 적용합니다.

B. 조직의 모든 AWS 계정에서 procurement-manager-role이라는 IAM 역할을 생성합니다.
역할에 AdministratorAccess 관리형 정책을 추가합니다.
AWSPrivateMarketplaceAdminFullAccess 관리형 정책으로 권한 경계를 정의하고 모든 개발자 역할에 연결합니다.

C. 조직의 모든 공유 서비스 계정에서 procurement-manager-role이라는 IAM 역할을 생성합니다.
역할에 AWSPrivateMarketplaceAdminFullAccess 관리형 정책을 추가합니다.
procurement-manager-role이라는 역할을 제외한 모두에게 Private Marketplace 관리 권한을 거부하는 조직루트수준 SCP를 만듭니다.
조직의 모든 사람에게 procurement-manager-role이라는 IAM 역할을 생성할 수 있는 권한을 거부하는 조직루트수준 SCP를 만듭니다.

D. 개발자가 사용할 모든 AWS 계정에서 procurement-manager-role이라는 IAM 역할을 생성합니다.
역할에 AWSPrivateMarketplaceAdminFullAccess 관리형 정책을 추가합니다.
조직에 SCP를 만들어 procurement-manager-role이라는 역할을 제외한 모든 사람에게 Private Marketplace를 관리할 수 있는 권한을 거부합니다.
조직의 모든 공유 서비스 계정에 SCP를 적용합니다.

Answer: D

NO.155
A company is hosting a critical application on a single Amazon EC2 instance.
The application uses an Amazon ElastiCache for Redis single-node cluster for an in-memory data store.
The application uses an Amazon RDS for MariaDB DB instance for a relational database.
For the application to function, each piece of the infrastructure must be healthy and must be in an active state.
A solutions architect needs to improve the application's architecture so that the infrastructure can automatically recover from failure with the least possible downtime.
Which combination of steps will meet these requirements? (Select THREE.)

(A). Use an Elastic Load Balancer to distribute traffic across multiple EC2 instances.
Ensure that the EC2 instances are part of an Auto Scaling group that has a minimum capacity of two instances.

(B). Use an Elastic Load Balancer to distribute traffic across multiple EC2 instances Ensure that the EC2 instances are configured in unlimited mode.

(C). Modify the DB instance to create a read replica in the same Availability Zone.
Promote the read replica to be the primary DB instance in failure scenarios.

(D). Modify the DB instance to create a Multi-AZ deployment that extends across two Availability Zones.

(E). Create a replication group for the ElastiCache for Redis cluster.
Configure the cluster to use an Auto Scaling group that has a minimum capacity of two instances.

(F). Create a replication group for the ElastiCache for Redis cluster. Enable Multi-AZ on the cluster.

Answer: A, D, E

NO.155
회사에서 단일 Amazon EC2 인스턴스에서 중요한 애플리케이션을 호스팅하고 있습니다.
애플리케이션은 인메모리 데이터 스토어에 대해 Redis 단일 노드 클러스터용 Amazon ElastiCache를 사용합니다.
애플리케이션은 관계형 데이터베이스에 Amazon RDS for MariaDB DB 인스턴스를 사용합니다.
애플리케이션이 작동하려면 인프라의 각 부분이 정상이어야 하고 활성 상태여야 합니다.
솔루션 아키텍트는 가능한 최소한의 다운타임으로 인프라가 장애로부터 자동으로 복구할 수 있도록 애플리케이션의 아키텍처를 개선해야 합니다.
이러한 요구 사항을 충족하는 단계 조합은 무엇입니까? (3개를 선택하세요.)

(A). Elastic Load Balancer를 사용하여 여러 EC2 인스턴스에 트래픽을 분산합니다.
EC2 인스턴스는 최소 2개의 인스턴스 용량이 있는 Auto Scaling 그룹의 파트가 되도록합니다.

(B). Elastic Load Balancer를 사용하여 여러 EC2 인스턴스에 트래픽을 분산합니다.
EC2 인스턴스는 무제한 모드로 구성됩니다.

(C). 동일한 가용 영역에 읽기 전용 복제본을 생성하도록 DB 인스턴스를 수정합니다.
장애 시나리오에서 읽기 전용 복제본을 기본 DB 인스턴스로 승격합니다.

(D). DB 인스턴스를 수정하여 2개의 가용 영역에 걸쳐 확장되는 다중 AZ 배포를 생성합니다.

(E). Redis용 ElastiCache 클러스터에 대한 복제 그룹을 생성합니다.
최소 2개의 인스턴스 용량이 있는 Auto Scaling 그룹을 사용하도록 클러스터를 구성합니다.

(F). Redis용 ElastiCache 클러스터에 대한 복제 그룹을 생성합니다.
클러스터에서 다중 AZ를 활성화합니다.

Answer: A, D, E

NO.156
A company uses AWS Organizations with a single OU named Production to manage multiple accounts. All accounts are members of the Production OU.
Administrators use deny list SCPs in the root of the organization to manage access to restricted services.
The company recently acquired a new business unit and invited the new unit's existing AWS account to the organization.
Once onboarded, the administrators of the new business unit discovered that they are not able to update existing AWS Config rules to meet the company's policies.
Which option will allow administrators to make changes and continue to enforce the current policies without introducing additional long-term maintenance?

A. Remove the organization's root SCPs that limit access to AWS Config.
Create AWS Service Catalog products for the company's standard AWS Config rules and deploy them throughout the organization, including the new account.

B. Create a temporary OU named Onboarding for the new account.
Apply an SCP to the Onboarding OU to allow AWS Config actions.
Move the new account to the Production OU when adjustments to AWS Config are complete.

C. Convert the organization's root SCPs from deny list SCPs to allow list SCPs to allow the required services only.
Temporally apply an SCP to the organization's root that allows AWS Config actions for principals only in the new account.

D. Create a temporary OU named Onboarding for the new account. Apply an SCP to the Onboarding OU to allow AWS Config actions.
Move the organization's root SCP to the Production OU.
Move the new account to the Production OU when adjustments to AWS Config are complete.

Answer: B

https://www.examtopics.com/discussions/amazon/view/36360-exam-aws-certified-solutions-architect-professional-topic-1/

NO.156
회사는 Production이라는 단일 OU와 함께 AWS Organizations를 사용하여 여러 계정을 관리합니다. 모든 계정은 Production OU의 구성원입니다.
관리자는 조직의 루트에 있는 거부 목록 SCP를 사용하여 제한된 서비스에 대한 액세스를 관리합니다.
이 회사는 최근 새 사업부를 인수하고 새 사업부의 AWS 계정을 조직에 초대했습니다.
온보딩된 후 새 사업부의 관리자는 회사 정책을 충족하도록 기존 AWS Config 규칙을 업데이트할 수 없다는 것을 발견했습니다.
관리자가 추가적인 장기 유지 관리를 도입하지 않고 현재 정책을 변경하고 계속 적용할 수 있는 옵션은 무엇입니까?

A. AWS Config에 대한 액세스를 제한하는 조직의 루트 SCP를 제거합니다.
회사의 표준 AWS Config 규칙에 대한 AWS Service Catalog 제품을 생성하고 새 계정을 포함하여 조직 전체에 배포합니다.

B. 새 계정에 대해 Onboarding이라는 임시 OU를 만듭니다.
AWS Config 작업을 허용하려면 SCP를 온보딩 OU에 적용합니다.
AWS Config 조정이 완료되면 새 계정을 프로덕션 OU로 이동합니다.

C. 조직의 루트 SCP를 거부 목록 SCP에서 허용 목록 SCP가 필요한 서비스만 허용하도록 변환합니다. 새 계정의 보안 주체에 대해서만 AWS Config 작업을 허용하는 SCP를 조직의 루트에 임시로 적용합니다.

D. 새 계정에 대해 Onboarding이라는 임시 OU를 만듭니다.
AWS Config 작업을 허용하려면 SCP를 온보딩 OU에 적용합니다.
조직의 루트 SCP를 프로덕션 OU로 이동합니다.
AWS Config 조정이 완료되면 새 계정을 프로덕션 OU로 이동합니다.

Answer: B

NO.157
A mobile gaming company is expanding into the global market. The company's game servers run in the us-east-1 Region.
The game's client application uses UDP to communicate with the game servers and needs to be able to connect to a set of static IP addresses.
The company wants its game to be accessible on multiple continents.
The company also wants the game to maintain its network performance and global availability.
Which solution meets these requirements?

(A). Provision an Application Load Balancer (ALB) in front of the game servers.
Create an Amazon CloudFront distribution that has no geographical restrictions.
Set the ALB as the origin.
Perform DNS lookups for the cloudfront net domain name.
Use the resulting IP addresses in the game's client application.

(B). Provision game servers in each AWS Region.
Provision an Application Load Balancer in front of the game servers.
Create an Amazon Route 53 latency-based routing policy for the game's client application to use with DNS lookups.

(C). Provision game servers in each AWS Region.
Provision a Network Load Balancer (NLB) in front of the game servers.
Create an accelerator in AWS Global Accelerator, and configure endpoint groups in each Region.
Associate the NLBs with the corresponding Regional endpoint groups.
Point the game client's application to the Global Accelerator endpoints.

(D). Provision game servers in each AWS Region.
Provision a Network Load Balancer (NLB) in front of the game servers.
Create an Amazon CloudFront distribution that has no geographical restrictions.
Set the NLB as the origin.
Perform DNS lookups for the cloudfront net domain name.
Use the resulting IP addresses in the game's client application.

Answer: C

NO.157
모바일 게임 회사가 글로벌 시장으로 확장하고 있습니다.
회사의 게임 서버는 us-east-1 리전에서 실행됩니다.
게임의 클라이언트 응용 프로그램은 UDP를 사용하여 게임 서버와 통신하고 고정 IP 주소 집합에 연결할 수 있어야 합니다.
회사는 게임을 여러 대륙에서 액세스할 수 있기를 원합니다.
회사는 또한 게임이 네트워크 성능과 글로벌 가용성을 유지하기를 원합니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?

(A). 게임 서버 앞에 ALB(Application Load Balancer)를 프로비저닝합니다.
지리적 제한이 없는 Amazon CloudFront 배포를 생성합니다.
ALB를 오리진으로 설정합니다.
cloudfront net 도메인 이름에 대한 DNS 조회를 수행합니다.
게임의 클라이언트 애플리케이션에서 결과 IP 주소를 사용합니다.

(B). 각 AWS 리전에서 게임 서버를 프로비저닝합니다.
게임 서버 앞에 Application Load Balancer를 프로비저닝합니다.
게임의 클라이언트 애플리케이션이 DNS 조회에 사용할 Amazon Route 53 지연 시간 기반 라우팅 정책을 생성합니다.

(C). 각 AWS 리전에서 게임 서버를 프로비저닝합니다.
게임 서버 앞에 NLB(Network Load Balancer)를 프로비저닝합니다.
AWS Global Accelerator에서 액셀러레이터를 생성하고 각 리전에서 엔드포인트 그룹을 구성합니다. NLB를 해당 리전 엔드포인트 그룹과 연결합니다.
게임 클라이언트의 애플리케이션이 Global Accelerator 엔드포인트를 가리키도록 합니다.

(D). 각 AWS 리전에서 게임 서버를 프로비저닝합니다.
게임 서버 앞에 NLB(Network Load Balancer)를 프로비저닝합니다.
지리적 제한이 없는 Amazon CloudFront 배포를 생성합니다.
NLB를 원점으로 설정합니다.
cloudfront net 도메인 이름에 대한 DNS 조회를 수행합니다.
게임의 클라이언트 애플리케이션에서 결과 IP 주소를 사용합니다.

Answer: C

NO.158
A company uses AWS Organizations to manage more than 1,000 AWS accounts.
The company has created a new developer organization.
There are 540 developer member accounts that must be moved to the new developer organization.
All accounts are set up with all the required information so that each account can be operated as a standalone account.
Which combination of steps should a solutions architect take to move all of the developer accounts to the new developer organization? (Choose three.)

A. Call the MoveAccount operation in the Organizations API from the old organization's management account to migrate the developer accounts to the new developer organization.

B. From the management account, remove each developer account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API.

C. From each developer account, remove the account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API.

D. Sign in to the new developer organization's management account and create a placeholder member account that acts as a target for the developer account migration.

E. Call the InviteAccountToOrganization operation in the Organizations API from the new developer organization's management account to send invitations to the developer accounts.

F. Have each developer sign in to their account and confirm to join the new developer organization.

Answer: B, E, F
https://www.examtopics.com/discussions/amazon/view/74003-exam-aws-certified-solutions-architect-professional-topic-1/

NO.158
회사는 AWS Organizations를 사용하여 1,000개 이상의 AWS 계정을 관리합니다.
회사는 새로운 개발자 조직을 만들었습니다.
새 개발자 조직으로 이동해야 하는 개발자 구성원 계정이 540개 있습니다.
모든 계정은 각 계정이 독립형 계정으로 운영될 수 있도록 필요한 모든 정보로 설정됩니다.
솔루션 아키텍트는 모든 개발자 계정을 새 개발자 조직으로 이동하기 위해 어떤 단계를 조합해야 합니까? (3개를 선택하세요.)

A. 이전 조직의 관리 계정에서 Organizations API의 MoveAccount 작업을 호출하여 개발자 계정을 새 개발자 조직으로 마이그레이션합니다.

B. 관리 계정에서 Organizations API의 RemoveAccountFromOrganization 작업을 사용하여 이전 조직의 각 개발자 계정을 제거합니다.

C. 각 개발자 계정에서 Organizations API의 RemoveAccountFromOrganization 작업을 사용하여 이전 조직의 계정을 제거합니다.

D. 새 개발자 조직의 관리 계정에 로그인하고 개발자 계정 마이그레이션의 대상 역할을 하는 자리 표시자 구성원 계정을 만듭니다.

E. 새 개발자 조직의 관리 계정에서 Organizations API의 InviteAccountToOrganization 작업을 호출하여 개발자 계정에 초대를 보냅니다.

F. 각 개발자가 자신의 계정에 로그인하고 새 개발자 조직에 가입하도록 확인합니다.

Answer: B, E, F

NO.159
A company is in the process of implementing AWS Organizations to constrain its developers to use only Amazon EC2, Amazon S3, and Amazon DynamoDB.
The Developers account resides in a dedicated organizational unit (OU).
The Solutions Architect has implemented the following SCP on the Developers account:

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

When this policy is deployed, IAM users in the Developers account are still able to use AWS services that are not listed in the policy.
What should the Solutions Architect do to eliminate the Developers' ability to use services outside the scope of this policy?

A. Create an explicit deny statement for each AWS service that should be constrained.
B. Remove the FullAWSAccess SCP from the Developer account's OU.
C. Modify the FullAWSAccess SCP to explicitly deny all services.
D. Add an explicit deny statement using a wildcard to the end of the SCP.

Answer: B

https://www.examtopics.com/discussions/amazon/view/46899-exam-aws-certified-solutions-architect-professional-topic-1/

NO.159
회사는 개발자가 Amazon EC2, Amazon S3 및 Amazon DynamoDB만 사용하도록 제한하기 위해 AWS Organizations를 구현하는 과정에 있습니다.
개발자 계정은 전용 OU(조직 구성 단위)에 있습니다.
Solutions Architect는 개발자 계정에 다음 SCP를 구현했습니다

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

이 정책이 배포되면 개발자 계정의 IAM 사용자는 정책에 나열되지 않은 AWS 서비스를 계속 사용할 수 있습니다.
이 정책 범위를 벗어나는 서비스를 사용할 수 있는 개발자의 능력을 제거하기 위해 Solutions Architect는 무엇을 해야 합니까?

A. 제한해야 하는 각 AWS 서비스에 대해 명시적 거부 문을 생성합니다.

B. 개발자 계정의 OU에서 FullAWSAccess SCP를 제거합니다.

C. 모든 서비스를 명시적으로 거부하도록 FullAWSAccess SCP를 수정합니다.

D. SCP 끝에 와일드카드를 사용하여 명시적 거부 문을 추가합니다.

Answer: B

NO.160
An enterprise runs 103 line-of-business applications on virtual machines in an on-premises data center. Many of the applications are simple PHP, Java, or Ruby web applications, are no longer actively developed, and serve little traffic.
Which approach should be used to migrate these applications to AWS with the LOWEST infrastructure costs?

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

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

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

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

Answer: C
https://www.examtopics.com/discussions/amazon/view/5089-exam-aws-certified-solutions-architect-professional-topic-1/

NO.160
기업은 온프레미스 데이터 센터의 가상 머신에서 103개의 기간 업무 애플리케이션을 실행합니다.
많은 애플리케이션이 단순한 PHP, Java 또는 Ruby 웹 애플리케이션이며 더 이상 활발히 개발되지 않고 트래픽을 거의 제공하지 않습니다.
가장 낮은 인프라 비용으로 이러한 애플리케이션을 AWS로 마이그레이션하려면 어떤 접근 방식을 사용해야 합니까?

A. 로드 밸런서 없이 단일 인스턴스 AWS Elastic Beanstalk 환경에 애플리케이션을 배포합니다.

B. AWS SMS를 사용하여 각 가상 머신에 대한 AMI를 생성하고 Amazon EC2에서 실행합니다.

C. 각 애플리케이션을 Docker 이미지로 변환하고 Application Load Balancer 뒤의 소규모 Amazon ECS 클러스터에 배포합니다.

D. VM Import/Export를 사용하여 각 가상 머신에 대한 AMI를 생성하고 사용자 지정 이미지를 구성하여 단일 인스턴스 AWS Elastic Beanstalk 환경에서 실행합니다.

Answer: C

NO.161
A company has a data lake in Amazon S3 that needs to be accessed by hundreds of applications across many AWS accounts.
The company's information security policy states that the S3 bucket must not be accessed over the public internet and that each application should have the minimum permissions necessary to function.
To meet these requirements, a solutions architect plans to use an S3 access point that is restricted to specific VPCs for each application.
Which combination of steps should the solutions architect take to implement this solution? (Choose two.)

A. Create an S3 access point for each application in the AWS account that owns the S3 bucket.
Configure each access point to be accessible only from the application's VPC.
Update the bucket policy to require access from an access point

B. Create an interface endpoint for Amazon S3 in each application's VPC.
Configure the endpoint policy to allow access to an S3 access point.
Create a VPC gateway attachment for the S3 endpoint

C. Create a gateway endpoint for Amazon S3 in each application's VPC.
Configure the endpoint policy to allow access to an S3 access point.
Specify the route table that is used to access the access point.

D. Create an S3 access point for each application in each AWS account and attach the access points to the S3 bucket.
Configure each access point to be accessible only from the application's VPC. Update the bucket policy to require access from an access point.

E. Create a gateway endpoint for Amazon S3 in the data lake's VPC.
Attach an endpoint policy to allow access to the S3 bucket.
Specify the route table that is used to access the bucket.

Answer: A,C

https://www.examtopics.com/discussions/amazon/view/51217-exam-aws-certified-solutions-architect-professional-topic-1/

https://joe.blog.freemansoft.com/2020/04/protect-data-in-cloud-with-s3-access.html
https://aws.amazon.com/s3/features/access-points/
https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/

NO.161
회사는 Amazon S3에 여러 AWS 계정에 걸쳐 수백 개의 애플리케이션에서 액세스해야 하는 데이터 레이크를 가지고 있습니다.
회사의 정보 보안 정책에는 공용 인터넷을 통해 S3 버킷에 액세스해서는 안 되며 각 애플리케이션이 작동하는 데 필요한 최소한의 권한이 있어야 한다고 명시되어 있습니다.
이러한 요구 사항을 충족하기 위해 솔루션 아키텍트는 각 애플리케이션에 대해 특정 VPC로 제한된 S3 액세스 포인트를 사용할 계획입니다.
솔루션 아키텍트는 이 솔루션을 구현하기 위해 어떤 단계 조합을 취해야 합니까? (2개를 선택하세요.)

A. S3 버킷을 소유한 AWS 계정의 각 애플리케이션에 대해 S3 액세스 포인트를 생성합니다.
애플리케이션의 VPC에서만 액세스할 수 있도록 각 액세스 포인트를 구성합니다.
액세스 포인트에서 액세스해야 하도록 버킷 정책을 업데이트합니다.

B. 각 애플리케이션의 VPC에서 Amazon S3에 대한 인터페이스 엔드포인트를 생성합니다.
S3 액세스 포인트에 대한 액세스를 허용하도록 엔드포인트 정책을 구성합니다.
S3 엔드포인트에 대한 VPC 게이트웨이 연결을 생성합니다.

C. 각 애플리케이션의 VPC에서 Amazon S3용 게이트웨이 엔드포인트를 생성합니다.
S3 액세스 포인트에 대한 액세스를 허용하도록 엔드포인트 정책을 구성합니다.
액세스 포인트에 액세스하는 데 사용되는 라우팅 테이블을 지정합니다.

D. 각 AWS 계정의 각 애플리케이션에 대한 S3 액세스 포인트를 생성하고 액세스 포인트를 S3 버킷에 연결합니다.
애플리케이션의 VPC에서만 액세스할 수 있도록 각 액세스 포인트를 구성합니다.
액세스 포인트에서 액세스해야 하도록 버킷 정책을 업데이트합니다.

E. 데이터 레이크의 VPC에서 Amazon S3용 게이트웨이 엔드포인트를 생성합니다.
S3 버킷에 대한 액세스를 허용하는 엔드포인트 정책을 연결합니다.
버킷에 액세스하는 데 사용되는 라우팅 테이블을 지정합니다.

Answer: A,C

https://www.examtopics.com/discussions/amazon/view/51217-exam-aws-certified-solutions-architect-professional-topic-1/

NO.162
A company runs applications on Amazon EC2 instances.
The company plans to begin using an Auto Scaling group for the instances.
As part of this transition, a solutions architect must ensure that Amazon CloudWatch Logs automatically collects logs from all new instances.
The new Auto Scaling group will use a launch template that includes the Amazon Linux 2 AMI and no key pair.
Which solution meets these requirements?

A. Create an Amazon CloudWatch agent configuration for the workload.
Store the CloudWatch agent configuration in an Amazon S3 bucket.
Write an EC2 user data script to fetch the configuration file from Amazon S3.
Configure the CloudWatch agent on the instance during initial boot.

B. Create an Amazon CloudWatch agent configuration for the workload in AWS Systems Manager Parameter Store.
Create a Systems Manager document that installs and configures the CloudWatch agent by using the configuration.
Create an Amazon EventBridge (Amazon CloudWatch Events) rule on the default event bus with a Systems Manager Run Command target that runs the document whenever an instance enters the running state.

C. Create an Amazon CloudWatch agent configuration for the workload.
Create an AWS Lambda function to install and configure the CloudWatch agent by using AWS Systems Manager Session Manager.
Include the agent configuration inside the Lambda package.
Create an AWS Config custom rule to identify changes to the EC2 instances and invoke Lambda function.

D. Create an Amazon CloudWatch agent configuration for the workload.
Save the CloudWatch agent configuration as part of an AWS Lambda deployment package.
Use AWS CloudTrail to capture EC2 tagging events and initiate agent installation.
Use AWS CodeBuild to configure the CloudWatch agent on the instances that run the workload.

Answer: B

https://www.examtopics.com/discussions/amazon/view/68925-exam-aws-certified-solutions-architect-professional-topic-1/

NO.162
회사는 Amazon EC2 인스턴스에서 애플리케이션을 실행합니다.
회사는 인스턴스에 대해 Auto Scaling 그룹을 사용할 계획입니다.
이 전환의 일환으로 솔루션 아키텍트는 Amazon CloudWatch Logs가 모든 새 인스턴스에서 자동으로 로그를 수집하도록 해야 합니다.
새로운 Auto Scaling 그룹은 Amazon Linux 2 AMI를 포함하고 키 페어가 없는 시작템플릿을 사용합니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?

A. 워크로드에 대한 Amazon CloudWatch 에이전트 구성을 생성합니다.
CloudWatch 에이전트 구성을 Amazon S3 버킷에 저장합니다.
EC2 사용자 데이터 스크립트를 작성하여 Amazon S3에서 구성 파일을 가져옵니다.
초기 부팅 중에 인스턴스에서 CloudWatch 에이전트를 구성합니다.

B. AWS Systems Manager Parameter Store에서 워크로드에 대한 CloudWatch agent configuration을 생성합니다. configuration을 사용하여 CloudWatch 에이전트를 설치 및 구성하는 Systems Manager 문서를 생성합니다.
인스턴스가 실행 상태가 될 때, document 를 실행하는 Systems Manager Run Command 대상을 사용하여 기본 이벤트 버스에서 Amazon EventBridge(Amazon CloudWatch Events) 규칙을 생성합니다.

C. 워크로드에 대한 Amazon CloudWatch 에이전트 구성을 생성합니다.
AWS Systems Manager Session Manager를 사용하여 CloudWatch 에이전트를 설치 및 구성하는 AWS Lambda 함수를 생성합니다. Lambda 패키지 내에 에이전트 구성을 포함합니다.
EC2 인스턴스에 대한 변경 사항을 식별하고 Lambda 함수를 호출하는 AWS Config 사용자 지정 규칙을 생성합니다.

D. 워크로드에 대한 Amazon CloudWatch 에이전트 구성을 생성합니다.
CloudWatch 에이전트 구성을 AWS Lambda 배포 패키지의 일부로 저장합니다.
AWS CloudTrail을 사용하여 EC2 태깅 이벤트를 캡처하고 에이전트 설치를 시작합니다.
AWS CodeBuild를 사용하여 워크로드를 실행하는 인스턴스에서 CloudWatch 에이전트를 구성합니다.

Answer: B
https://www.examtopics.com/discussions/amazon/view/68925-exam-aws-certified-solutions-architect-professional-topic-1/

NO.163
A medical company is running a REST API on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group behind an Application Load Balancer (ALB).
The ALB runs in three public subnets, and the EC2 instances run in three private subnets.

The company has deployed an Amazon CloudFront distribution that has the ALB as the only origin. Which solution should a solutions architect recommend to enhance the origin security?

A. Store a random string in AWS Secrets Manager. Create an AWS Lambda function for automatic secret rotation. Configure CloudFront to inject the random string as a custom HTTP header for the origin request. Create an AWS WAF web ACL rule with a string match rule for the custom header. Associate the web ACL with the ALB.

B. Create an AWS WAF web ACL rule with an IP match condition of the CloudFront service IP address ranges. Associate the web ACL with the ALB. Move the ALB into the three private subnets.

C. Store a random string in AWS Systems Manager Parameter Store. Configure Parameter Store automatic rotation for the string. Configure CloudFront to inject the random string as a custom HTTP header for the origin request. Inspect the value of the custom HTTP header, and block access in the ALB.

D. Configure AWS Shield Advanced. Create a security group policy to allow connections from CloudFront service IP address ranges. Add the policy to AWS Shield Advanced, and attach the policy to the ALB.

Answer: A

https://www.examtopics.com/discussions/amazon/view/80083-exam-aws-certified-solutions-architect-professional-topic-1/

NO.163
한 의료 회사가 Amazon EC2 인스턴스 세트에서 REST API를 실행하고 있습니다.
EC2 인스턴스는 ALB(Application Load Balancer) 뒤의 Auto Scaling 그룹에서 실행됩니다.
ALB는 3개의 퍼블릭 서브넷에서 실행되고 EC2 인스턴스는 3개의 프라이빗 서브넷에서 실행됩니다.
이 회사는 ALB가 유일한 오리진인 Amazon CloudFront 배포를 배포했습니다.
솔루션 아키텍트가 오리진 보안을 강화하기 위해 어떤 솔루션을 권장해야 합니까?

A. AWS Secrets Manager에 임의의 문자열을 저장합니다.
자동 보안 암호 교체를 위한 AWS Lambda 함수를 생성합니다.
임의의 문자열을 오리진 요청에 대한 사용자 지정 HTTP 헤더로 삽입하도록 CloudFront를 구성합니다.
사용자 지정 헤더에 대한 문자열 일치 규칙을 사용하여 AWS WAF 웹 ACL 규칙을 생성합니다.
웹 ACL을 ALB와 연결합니다.

B. CloudFront 서비스 IP 주소 범위의 IP 일치 조건으로 AWS WAF 웹 ACL 규칙을 생성합니다.
웹 ACL을 ALB와 연결합니다. ALB를 3개의 프라이빗 서브넷으로 이동합니다.

C. AWS Systems Manager Parameter Store에 임의의 문자열을 저장합니다.
문자열에 대한 Parameter Store 자동 교체를 구성합니다.
임의의 문자열을 오리진 요청에 대한 사용자 지정 HTTP 헤더로 삽입하도록 CloudFront를 구성합니다. 사용자 정의 HTTP 헤더의 값을 검사하고 ALB에서 액세스를 차단하십시오.

D. AWS Shield Advanced를 구성합니다.
CloudFront 서비스 IP 주소 범위에서 연결을 허용하는 보안 그룹 정책을 생성합니다.
AWS Shield Advanced에 정책을 추가하고 ALB에 정책을 연결합니다.

Answer: A

https://www.examtopics.com/discussions/amazon/view/80083-exam-aws-certified-solutions-architect-professional-topic-1/

NO.164
A company is running an application on Amazon EC2 instances in three environments: development, testing, and production.
The company uses AMIs to deploy the EC2 instances.
The company builds the AMIs by using custom deployment scripts and infrastructure orchestration tools for each release in each environment.
The company is receiving errors in its deployment process.
Errors appear during operating system package downloads and during application code installation from a third-party Git hosting service.
The company needs deployments to become more reliable across all environments.
Which combination of steps will meet these requirements? (Choose three.)

A. Mirror the application code to an AWS CodeCommit Git repository. Use the repository to build EC2 AMIs.

B. Produce multiple EC2 AMIs, one for each environment, for each release.

C. Produce one EC2 AMI for each release for use across all environments.

D. Mirror the application code to a third-party Git repository that uses Amazon S3 storage.
Use the repository for deployment.

E. Replace the custom scripts and tools with AWS CodeBuild.
Update the infrastructure deployment process to use EC2 Image Builder.

F. Replace the custom scripts and tools with EC2 Image Builder.
Update the deployment process to use AWS CloudFormation.

Answer: A, C, F

https://www.examtopics.com/discussions/amazon/view/80521-exam-aws-certified-solutions-architect-professional-topic-1/

NO.164
회사는 개발, 테스트 및 프로덕션의 세 가지 환경에서 Amazon EC2 인스턴스에서 애플리케이션을 실행하고 있습니다.
회사는 AMI를 사용하여 EC2 인스턴스를 배포합니다.
회사는 각 환경의 각 릴리스에 대해 사용자 지정 배포 스크립트와 인프라 오케스트레이션 도구를 사용하여 AMI를 구축합니다.
회사는 배포 프로세스에서 오류를 수신하고 있습니다.
운영 체제 패키지를 다운로드하는 동안 및 타사 Git 호스팅 서비스에서 애플리케이션 코드를 설치하는 동안 오류가 나타납니다.
회사는 모든 환경에서 더 안정적이 되기 위한 배포가 필요합니다.
이러한 요구 사항을 충족하는 단계 조합은 무엇입니까? (3개를 선택하세요.)

A. 애플리케이션 코드를 AWS CodeCommit Git repository로 미러링합니다.
리포지토리를 사용하여 EC2 AMI를 빌드합니다.

B. 릴리스마다 환경마다 하나씩 여러 EC2 AMI를 생성합니다.

C. 모든 환경에서 사용할 각 릴리스에 대해 하나의 EC2 AMI를 생성합니다.

D. Amazon S3 스토리지를 사용하는 타사 Git repository에 애플리케이션 코드를 미러링합니다.
배포를 위해 repository를 사용합니다.

E. 사용자 지정 스크립트 및 도구를 AWS CodeBuild로 교체합니다.
EC2 Image Builder를 사용하도록 인프라 배포 프로세스를 업데이트합니다.

F. 사용자 지정 스크립트 및 도구를 EC2 Image Builder로 교체합니다.
AWS CloudFormation을 사용하도록 배포 프로세스를 업데이트합니다.

Answer: A, C, F

https://www.examtopics.com/discussions/amazon/view/80521-exam-aws-certified-solutions-architect-professional-topic-1/

NO.165

A company is developing a new service that will be accessed using TCP on a static port.
A solutions architect must ensure that the service is highly available, has redundancy across Availability Zones, and is accessible using the DNS name my.service.com, which is publicly accessible.
The service must use fixed address assignments so other companies can add the addresses to their allow lists.
Assuming that resources are deployed in multiple Availability Zones in a single Region, which solution will meet these requirements?

A. Create Amazon EC2 instances with an Elastic IP address for each instance.
Create a Network Load Balancer (NLB) and expose the static TCP port.
Register EC2 instances with the NLB.
Create a new name server record set named my.service.com, and assign the Elastic IP addresses of the EC2 instances to the record set.
Provide the Elastic IP addresses of the EC2 instances to the other companies to add to their allow lists.

B. Create an Amazon ECS cluster and a service definition for the application.
Create and assign public IP addresses for the ECS cluster.
Create a Network Load Balancer (NLB) and expose the TCP port.
Create a target group and assign the ECS cluster name to the NLB.
Create a new A record set named my.service.com, and assign the public IP addresses of the ECS cluster to the record set.
Provide the public IP addresses of the ECS cluster to the other companies to add to their allow lists.

C. Create Amazon EC2 instances for the service.
Create one Elastic IP address for each Availability Zone.
Create a Network Load Balancer (NLB) and expose the assigned TCP port.
Assign the Elastic IP addresses to the NLB for each Availability Zone.
Create a target group and register the EC2 instances with the NLB.
Create a new A (alias) record set named my.service.com, and assign the NLB DNS name to the record set.

D. Create an Amazon ECS cluster and a service definition for the application.
Create and assign public IP address for each host in the cluster.
Create an Application Load Balancer (ALB) and expose the static TCP port.
Create a target group and assign the ECS service definition name to the ALB.
Create a new CNAME record set and associate the public IP addresses to the record set.
Provide the Elastic IP addresses of the Amazon EC2 instances to the other companies to add to their allow lists.

Answer: C

https://www.examtopics.com/discussions/amazon/view/28045-exam-aws-certified-solutions-architect-professional-topic-1/

NO.165
회사는 정적 포트에서 TCP를 사용하여 액세스할 새로운 서비스를 개발 중입니다.
솔루션 아키텍트는 서비스가 고가용성이고 가용 영역 전체에 중복성이 있으며 공개적으로 액세스할 수 있는 DNS 이름 my.service.com을 사용하여 액세스할 수 있는지 확인해야 합니다.
다른 회사가 주소를 허용 목록에 추가할 수 있도록 서비스는 고정 주소 할당을 사용해야 합니다.
리소스가 단일 리전의 여러 가용 영역에 배포되어 있다고 가정할 때 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

A. 각 인스턴스에 대해 탄력적 IP 주소를 사용하여 Amazon EC2 인스턴스를 생성합니다.
NLB(Network Load Balancer)를 생성하고 정적 TCP 포트를 노출합니다.
NLB에 EC2 인스턴스를 등록합니다.
my.service.com이라는 이름의 새 이름 서버 레코드 세트를 생성하고 EC2 인스턴스의 탄력적 IP 주소를 레코드 세트에 할당합니다.
EC2 인스턴스의 탄력적 IP 주소를 다른 회사에 제공하여 허용 목록에 추가합니다.

B. Amazon ECS 클러스터와 애플리케이션에 대한 서비스 정의를 생성합니다.
ECS 클러스터에 대한 퍼블릭 IP 주소를 생성하고 할당합니다.
NLB(Network Load Balancer)를 생성하고 TCP 포트를 노출합니다.
target group을 생성하고 NLB에 ECS 클러스터 이름을 할당합니다.
my.service.com이라는 새 A 레코드 세트를 생성하고 ECS 클러스터의 퍼블릭 IP 주소를 레코드 세트에 할당합니다.
ECS 클러스터의 공용 IP 주소를 다른 회사에 제공하여 허용 목록에 추가합니다.

C. 서비스에 대한 Amazon EC2 인스턴스를 생성합니다.
각 가용 영역에 대해 하나의 탄력적 IP 주소를 생성합니다.
NLB(Network Load Balancer)를 생성하고 할당된 TCP 포트를 노출합니다.
각 가용 영역의 NLB에 탄력적 IP 주소를 할당합니다.
target group을 생성하고 NLB에 EC2 인스턴스를 등록합니다.
my.service.com이라는 새 A(별칭) 레코드 세트를 생성하고 NLB DNS 이름을 레코드 세트에 할당합니다.

D. Amazon ECS 클러스터와 애플리케이션에 대한 서비스 정의를 생성합니다.
클러스터의 각 호스트에 대한 공용 IP 주소를 만들고 할당합니다.
ALB(Application Load Balancer)를 생성하고 정적 TCP 포트를 노출합니다.
target group을 생성하고 ECS 서비스 정의 이름을 ALB에 할당합니다.
새 CNAME 레코드 세트를 만들고 공개 IP 주소를 레코드 세트에 연결합니다.
다른 회사의 허용 목록에 추가할 Amazon EC2 인스턴스의 탄력적 IP 주소를 제공합니다.

Answer: C
https://www.examtopics.com/discussions/amazon/view/28045-exam-aws-certified-solutions-architect-professional-topic-1/

NO.166

A company has a three-tier application running on AWS with a web server, an application server, and an Amazon RDS MySQL DB instance.

A solutions architect is designing a disaster recovery (DR) solution with an RPO of 5 minutes.

Which solution will meet the company's requirements?

A. Configure AWS Backup to perform cross-Region backups of all servers every 5 minutes. Reprovision the three tiers in the DR Region from the backups using AWS CloudFormation in the event of a disaster.

B. Maintain another running copy of the web and application server stack in the DR Region using AWS CloudFormation drift detection. Configure cross-Region snapshots of the DB instance to the DR Region every 5 minutes. In the event of a disaster, restore the DB instance using the snapshot in the DR Region.

C. Use Amazon EC2 Image Builder to create and copy AMIs of the web and application server to both the primary and DR Regions. Create a cross-Region read replica of the DB instance in the DR Region. In the event of a disaster, promote the read replica to become the master and reprovision the servers with AWS CloudFormation using the AMIs.

D. Create AMIs of the web and application servers in the DR Region. Use scheduled AWS Glue jobs to synchronize the DB instance with another DB instance in the DR Region. In the event of a disaster, switch to the DB instance in the DR Region and reprovision the servers with AWS CloudFormation using the AMIs.

Answer: C

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

https://www.examtopics.com/discussions/amazon/view/47128-exam-aws-certified-solutions-architect-professional-topic-1/

NO.166
회사에 웹 서버, 애플리케이션 서버 및 Amazon RDS MySQL DB 인스턴스와 함께 AWS에서 실행되는 3계층 애플리케이션이 있습니다.
솔루션 아키텍트는 RPO가 5분인 재해 복구(DR) 솔루션을 설계하고 있습니다.
어떤 솔루션이 회사의 요구 사항을 충족합니까?

A. 5분마다 모든 서버의 교차 리전 백업을 수행하도록 AWS Backup을 구성합니다.
재해 발생 시 AWS CloudFormation을 사용하여 백업에서 DR 리전의 3개 계층을 다시 프로비저닝합니다.

B. AWS CloudFormation 드리프트 감지를 사용하여 DR 리전에서 웹 및 애플리케이션 서버 스택의 실행 중인 다른 복사본을 유지 관리합니다.
5분마다 DB 인스턴스의 교차 리전 스냅샷을 DR 리전에 구성합니다.
재해 발생 시 DR 리전의 스냅샷을 사용하여 DB 인스턴스를 복원합니다.

C. Amazon EC2 Image Builder를 사용하여 웹 및 애플리케이션 서버의 AMI를 생성하고 기본 리전과 DR 리전 모두에 복사합니다.
DR 리전에서 DB 인스턴스의 리전 간 읽기 전용 복제본을 생성합니다.
재해 발생 시 읽기 전용 복제본을 마스터로 승격하고 AMI를 사용하여 AWS CloudFormation으로 서버를 다시 프로비저닝하십시오.

D. DR 리전에서 웹 및 애플리케이션 서버의 AMI를 생성합니다.
예약된 AWS Glue 작업을 사용하여 DB 인스턴스를 DR 리전의 다른 DB 인스턴스와 동기화합니다.
재해 발생 시 DR 리전의 DB 인스턴스로 전환하고 AMI를 사용하여 AWS CloudFormation으로 서버를 다시 프로비저닝하십시오.

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

https://www.examtopics.com/discussions/amazon/view/47128-exam-aws-certified-solutions-architect-professional-topic-1/

NO.167
A company has used infrastructure as code (IaC) to provision a set of two Amazon EC2 instances. The instances have remained the same for several years.
The company's business has grown rapidly in the past few months.
In response the company's operations team has implemented an Auto Scaling group to manage the sudden increases in traffic.
Company policy requires a monthly installation of security updates on all operating systems that

are running.
The most recent security update required a reboot.
As a result, the Auto Scaling group terminated the instances and replaced them with new, unpatched instances.
Which combination of steps should a solutions architect recommend to avoid a recurrence of this issue? (Choose two.)

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

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

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

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

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

Answer: A, D

https://www.examtopics.com/discussions/amazon/view/68855-exam-aws-certified-solutions-architect-professional-topic-1/

NO.167
회사는 IaC(Infrastructure as Code)를 사용하여 두 개의 Amazon EC2 인스턴스 세트를 프로비저닝했습니다. 인스턴스 는 몇 년 동안 동일하게 유지되었습니다.
회사의 사업은 지난 몇 달 동안 빠르게 성장했습니다.
이에 대한 대응으로 회사 운영 팀은 갑작스러운 트래픽 증가를 관리하기 위해 Auto Scaling 그룹을 구현했습니다.
회사 정책에 따라 실행 중인 모든 운영 체제에 보안 업데이트를 매월 설치해야 합니다.
가장 최근의 보안 업데이트는 재부팅이 필요했습니다.
결과적으로 Auto Scaling 그룹은 인스턴스를 종료하고 패치되지 않은 새 인스턴스로 교체했습니다. 솔루션 아키텍트는 이 문제의 재발을 피하기 위해 어떤 단계 조합을 권장해야 합니까? (2개를 선택하세요.)

A. 교체할 가장 오래된 launch configuration 을 대상으로 업데이트 정책을 설정하여 Auto Scaling 그룹을 수정합니다.

B. 다음 패치 유지 관리 전에 새 Auto Scaling 그룹을 생성합니다.
유지 관리 기간 동안 두 그룹을 모두 패치하고 인스턴스를 재부팅합니다.

C. Auto Scaling 그룹 앞에 Elastic Load Balancer를 생성합니다.
Auto Scaling 그룹이 종료된 인스턴스를 교체한 후 target group health check가 정상으로 반환되도록 모니터링을 구성합니다.

D. 자동화 스크립트를 생성하여 AMI를 패치하고, 시작 구성을 업데이트하고, Auto Scaling 인스턴스 새로 고침을 호출합니다.

E. Auto Scaling 그룹 앞에 Elastic Load Balancer를 생성합니다. 인스턴스에 종료 방지를 구성합니다.

Answer: A, D

https://www.examtopics.com/discussions/amazon/view/68855-exam-aws-certified-solutions-architect-professional-topic-1/

NO.168
A company is migrating its marketing website and content management system from an on-premises data center to AWS.
The company wants the AWS application to be deployed in a VPC with Amazon EC2 instances used for the web servers and an Amazon RDS instance for the database.
The company has a runbook document that describes the installation process of the on-premises system.
The company would like to base the AWS system on the processes referenced in the runbook document.
The runbook document describes the installation and configuration of the operating systems, network settings, the website, and content management system software on the servers.
After the migration is complete, the company wants to be able to make changes quickly to take advantage of other AWS features.
How can the application and environment be deployed and automated in AWS, while allowing for future changes?

A. Update the runbook to describe how to create the VPC, the EC2 instances, and the RDS instance for the application by using the AWS Console.
Make sure that the rest of the steps in the runbook are updated to reflect any changes that may come from the AWS migration.

B. Write a Python script that uses the AWS API to create the VPC, the EC2 instances, and the RDS instance for the application. Write shell scripts that implement the rest of the steps in the runbook. Have the Python script copy and run the shell scripts on the newly created instances to complete the installation.

C. Write an AWS CloudFormation template that creates the VPC, the EC2 instances, and the RDS instance for the application. Ensure that the rest of the steps in the runbook are updated to reflect any changes that may come from the AWS migration.

D. Write an AWS CloudFormation template that creates the VPC, the EC2 instances, and the RDS instance for the application. Include EC2 user data in the AWS CloudFormation template to install and configure the software.

Answer: D

https://www.examtopics.com/discussions/amazon/view/5179-exam-aws-certified-solutions-architect-professional-topic-1/

NO.168
회사는 마케팅 웹 사이트와 콘텐츠 관리 시스템을 온프레미스 데이터 센터에서 AWS로 마이그레이션하고 있습니다.
이 회사는 AWS 애플리케이션이 웹 서버에 사용되는 Amazon EC2 인스턴스와 데이터베이스에 사용되는 Amazon RDS 인스턴스가 있는 VPC에 배포되기를 원합니다.
회사에는 온-프레미스 시스템의 설치 프로세스를 설명하는 Runbook 문서가 있습니다.
회사는 Runbook 문서에 참조된 프로세스를 기반으로 AWS 시스템을 구축하려고 합니다.
Runbook 문서는 서버의 운영 체제, 네트워크 설정, 웹 사이트 및 콘텐츠 관리 시스템 소프트웨어의 설치 및 구성에 대해 설명합니다.
마이그레이션이 완료된 후 회사는 다른 AWS 기능을 활용하기 위해 빠르게 변경할 수 있기를 원합니다. AWS에서 애플리케이션과 환경을 배포하고 자동화하면서 향후 변경 사항을 허용하려면 어떻게 해야 합니까?

A. AWS 콘솔을 사용하여 애플리케이션에 대한 VPC, EC2 인스턴스 및 RDS 인스턴스를 생성하는 방법을 설명하도록 Runbook을 업데이트합니다.
Runbook의 나머지 단계가 AWS 마이그레이션으로 인해 발생할 수 있는 변경 사항을 반영하도록 업데이트되었는지 확인합니다.

B. AWS API를 사용하여 애플리케이션에 대한 VPC, EC2 인스턴스 및 RDS 인스턴스를 생성하는 Python 스크립트를 작성합니다.
Runbook의 나머지 단계를 구현하는 셸 스크립트를 작성합니다.
Python 스크립트가 새로 생성된 인스턴스에서 셸 스크립트를 복사하고 실행하여 설치를 완료하도록 합니다.

C. 애플리케이션에 대한 VPC, EC2 인스턴스 및 RDS 인스턴스를 생성하는 AWS CloudFormation 템플릿을 작성합니다. Runbook의 나머지 단계가 AWS 마이그레이션으로 인해 발생할 수 있는 변경 사항을 반영하도록 업데이트되었는지 확인합니다.

D. 애플리케이션에 대한 VPC, EC2 인스턴스 및 RDS 인스턴스를 생성하는 AWS CloudFormation 템플릿을 작성합니다. AWS CloudFormation 템플릿에 EC2 사용자 데이터를 포함하여 소프트웨어를 설치 및 구성합니다.

Answer: D

https://www.examtopics.com/discussions/amazon/view/5179-exam-aws-certified-solutions-architect-professional-topic-1/

NO.169
A solution architect is designing an AWS account structure for a company that consists of multiple terms. All the team will work in the same AWS Region.
The company needs a VPC that is connected to the on-premises network.
The company expects less than 50 Mbps of total to and from the on-premises network.
Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO)

(A). Create an AWS CloudFormation template that provisions a VPC and the required subnets. Deploy the template to each AWS account.

(B). Create an AWS CloudFormabon template that provisions a VPC and the required subnets. Deploy the template to a shared services account.
Share the subnets by using AWS Resource Access Manager.

(C). Use AWS Transit Gateway along with an AWS Site-to-Site VPN for connectivity to the on-premises network. Share the transit gateway by using AWS Resource Access Manager

(D). Use AWS Site-to-Site VPN for connectivity to the on-premises network

(E). Use AWS Direct Connect for connectivity to the on-premises network.
Answer: B,D

NO.169
솔루션 아키텍트는 여러 용어로 구성된 회사의 AWS 계정 구조를 설계하고 있습니다.
모든 팀은 동일한 AWS 리전에서 작업합니다. 회사는 온프레미스 네트워크에 연결된 VPC가 필요합니다. 이 회사는 온프레미스 네트워크에서 송수신되는 총 50Mbps 미만을 예상합니다.
이러한 요구 사항을 가장 비용 효율적으로 충족하는 단계 조합은 무엇입니까? (2개 선택)

(A). VPC와 필요한 서브넷을 프로비저닝하는 AWS CloudFormation 템플릿을 생성합니다. 템플릿을 각 AWS 계정에 배포합니다.

(B). VPC와 필요한 서브넷을 프로비저닝하는 AWS CloudFormabon 템플릿을 생성합니다. 템플릿을 공유 서비스 계정에 배포합니다.

(C). 온프레미스 네트워크에 연결하려면 AWS Site-to-Site VPN과 함께 AWS Transit Gateway를 사용하십시오. AWS Resource Access Manager를 사용하여 전송 게이트웨이를 공유합니다.

(D). 온프레미스 네트워크에 연결하려면 AWS Site-to-Site VPN을 사용하십시오.

(E). 온프레미스 네트워크에 연결하려면 AWS Direct Connect를 사용하십시오.
Answer: B, D

NO.170
A company is running a serverless application that consists of several AWS Lambda functions and Amazon DynamoDB tables.
The company has created new functionality that requires the Lambda functions to access an Amazon Neptune DB cluster.
The Neptune DB cluster is located in three subnets in a VPC.
Which of the possible solutions will allow the Lambda functions to access the Neptune DB cluster and DynamoDB tables? (Choose two.)

A. Create three public subnets in the Neptune VPC, and route traffic through an internet gateway. Host the Lambda functions in the three new public subnets.

B. Create three private subnets in the Neptune VPC, and route internet traffic through a NAT gateway. Host the Lambda functions in the three new private subnets.

C. Host the Lambda functions outside the VPC.
Update the Neptune security group to allow access from the IP ranges of the Lambda functions.

D. Host the Lambda functions outside the VPC.
Create a VPC endpoint for the Neptune database, and have the Lambda functions access Neptune over the VPC endpoint.

E. Create three private subnets in the Neptune VPC.
Host the Lambda functions in the three new isolated subnets.
Create a VPC endpoint for DynamoDB, and route DynamoDB traffic to the VPC endpoint.

Answer: B, E

https://www.examtopics.com/discussions/amazon/view/81635-exam-aws-certified-solutions-architect-professional-topic-1/

NO.170
회사에서 여러 AWS Lambda 함수와 Amazon DynamoDB 테이블로 구성된 서버리스 애플리케이션을 실행하고 있습니다.
이 회사는 Amazon Neptune DB 클러스터에 액세스하는 데 Lambda 함수가 필요한 새로운 기능을 만들었습니다.
Neptune DB 클러스터는 VPC의 서브넷 3개에 있습니다.
가능한 솔루션 중 Lambda 함수가 Neptune DB 클러스터 및 DynamoDB 테이블에 액세스할 수 있도록 허용하는 솔루션은 무엇입니까? (2개를 선택하세요.)

A. Neptune VPC에 3개의 퍼블릭 서브넷을 생성하고 인터넷 게이트웨이를 통해 트래픽을 라우팅합니다. 3개의 새로운 퍼블릭 서브넷에서 Lambda 함수를 호스팅합니다.

B. Neptune VPC에 3개의 프라이빗 서브넷을 생성하고 NAT 게이트웨이를 통해 인터넷 트래픽을 라우팅합니다. 3개의 새로운 프라이빗 서브넷에서 Lambda 함수를 호스팅합니다.

C. VPC 외부에서 Lambda 함수를 호스팅합니다.
Lambda 함수의 IP 범위에서 액세스를 허용하도록 Neptune 보안 그룹을 업데이트합니다.

D. VPC 외부에서 Lambda 함수를 호스팅합니다.
Neptune 데이터베이스에 대한 VPC 엔드포인트를 생성하고 Lambda 함수가 VPC 엔드포인트를 통해 Neptune에 액세스하도록 합니다.

E. Neptune VPC에 3개의 프라이빗 서브넷을 생성합니다.
3개의 새로운 격리 서브넷에서 Lambda 함수를 호스팅합니다.
DynamoDB용 VPC 엔드포인트를 생성하고 DynamoDB 트래픽을 VPC 엔드포인트로 라우팅합니다.

Answer: B, E

https://www.examtopics.com/discussions/amazon/view/81635-exam-aws-certified-solutions-architect-professional-topic-1/

NO.171
A company has implemented an ordering system using an event driven architecture.
During initial testing, the system stopped processing orders.
Further log analysis revealed that one order message in an Amazon Simple Queue Service (Amazon SQS) standard queue was causing an error on the backend and blocking all subsequent order messages.
The visibility timeout of the queue is set to 30 seconds, and the backend processing timeout is set to 10 seconds.
A solutions architect needs to analyze faulty order messages and ensure that the system continues to process subsequent messages.
Which step should the solutions architect take to meet these requirements?

A. Increase the backend processing timeout to 30 seconds to match the visibility timeout.

B. Reduce the visibility timeout of the queue to automatically remove the faulty message.

C. Configure a new SQS FIFO queue as a dead-letter queue to isolate the faulty messages.

D. Configure a new SQS standard queue as a dead-letter queue to isolate the faulty messages.

Answer: D

https://www.examtopics.com/discussions/amazon/view/51245-exam-aws-certified-solutions-architect-professional-topic-1/

NO.171
A 회사는 이벤트 드리븐 아키텍처(event driven architecture)를 사용하여 주문 시스템을 구현했습니다.
초기 테스트 중에 시스템이 주문 처리를 중지했습니다.
추가 로그 분석에 따르면 Amazon Simple Queue Service(Amazon SQS) 표준 대기열의 한 주문 메시지가 백엔드에서 오류를 일으키고 모든 후속 주문 메시지를 차단하고 있는 것으로 나타났습니다.
대기열의 가시성 제한 시간은 30초로 설정되고 백엔드 처리 제한 시간은 10초로 설정됩니다.
솔루션 아키텍트는 잘못된 주문 메시지를 분석하고 시스템이 후속 메시지를 계속 처리하도록 해야 합니다. 솔루션 아키텍트는 이러한 요구 사항을 충족하기 위해 어떤 단계를 수행해야 합니까?

A. 가시성 제한 시간과 일치하도록 백엔드 처리 제한 시간을 30초로 늘립니다.

B. 오류 메시지를 자동으로 제거하기 위해 대기열의 가시성 시간 초과를 줄입니다.

C. 새 SQS FIFO 대기열을 배달 못한 편지 대기열로 구성하여 오류 메시지를 격리합니다.

D. 새 SQS 표준 대기열을 배달 못한 편지 대기열(dead-letter queue)로 구성하여 오류 메시지를 격리합니다.

Answer: D

https://www.examtopics.com/discussions/amazon/view/51245-exam-aws-certified-solutions-architect-professional-topic-1/

NO.172
A solutions architect must analyze a company's Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS) volumes to determine whether the company is using resources efficiently. The company is running several large, high-memory EC2 instances to host database clusters that are deployed in active/ passive configurations.
The utilization of these EC2 instances varies by the applications that use the databases, and the company has not identified a pattern.
The solutions architect must analyze the environment and take action based on the findings.
Which solution meets these requirements MOST cost-effectively?

A. Create a dashboard by using AWS Systems Manager OpsCenter.
Configure visualizations for Amazon CloudWatch metrics that are associated with the EC2 instances and their EBS volumes.
Review the dashboard periodically, and identify usage patterns.
Rightsize the EC2 instances based on the peaks in the metrics.

B. Turn on Amazon CloudWatch detailed monitoring for the EC2 instances and their EBS volumes.
Create and review a dashboard that is based on the metrics.
Identify usage patterns. Rightsize the EC2 instances based on the peaks in the metrics.

C. Install the Amazon CloudWatch agent on each of the EC2 instances.
Turn on AWS Compute Optimizer, and let it run for at least 12 hours.
Review the recommendations from Compute Optimizer, and rightsize the EC2 instances as directed.

D. Sign up for the AWS Enterprise Support plan.
Turn on AWS Trusted Advisor. Wait 12 hours.
Review the recommendations from Trusted Advisor, and rightsize the EC2 instances as directed.

Answer: C

https://www.examtopics.com/discussions/amazon/view/68919-exam-aws-certified-solutions-architect-professional-topic-1/

https://aws.amazon.com/compute-optimizer/pricing/
https://aws.amazon.com/systemsmanager/pricing/
https://aws.amazon.com/compute-optimizer/

NO.172
솔루션 아키텍트는 회사의 Amazon EC2 인스턴스와 Amazon Elastic Block Store(Amazon EBS) 볼륨을 분석하여 회사가 리소스를 효율적으로 사용하고 있는지 확인해야 합니다.
이 회사는 active/ passive 구성으로 배포된 데이터베이스 클러스터를 호스팅하기 위해 여러 개의 대용량 대용량 EC2 인스턴스를 실행하고 있습니다.
이러한 EC2 인스턴스의 활용도는 데이터베이스를 사용하는 애플리케이션에 따라 다르며 회사는 패턴을 식별하지 않았습니다.
솔루션 아키텍트는 환경을 분석하고 결과에 따라 조치를 취해야 합니다.
어떤 솔루션이 이러한 요구 사항을 가장 비용 효율적으로 충족합니까?

A. AWS Systems Manager OpsCenter를 사용하여 대시보드를 생성합니다.
EC2 인스턴스 및 해당 EBS 볼륨과 연결된 Amazon CloudWatch 지표에 대한 시각화를 구성합니다.
대시보드를 주기적으로 검토하고 사용 패턴을 식별합니다.
지표의 피크를 기반으로 EC2 인스턴스의 크기를 조정합니다.

B. EC2 인스턴스 및 해당 EBS 볼륨에 대한 Amazon CloudWatch 세부 모니터링을 켭니다.
메트릭을 기반으로 하는 대시보드를 만들고 검토합니다.
사용 패턴을 식별합니다. 지표의 피크를 기반으로 EC2 인스턴스의 크기를 조정합니다.

C. 각 EC2 인스턴스에 Amazon CloudWatch 에이전트를 설치합니다.
AWS Compute Optimizer를 켜고 최소 12시간 동안 실행합니다.
Compute Optimizer의 권장 사항을 검토하고 지시에 따라 EC2 인스턴스의 크기를 적절하게 조정합니다.

D. AWS Enterprise Support 플랜에 가입합니다.
AWS Trusted Advisor를 켭니다. 12시간을 기다립니다.
Trusted Advisor의 권장 사항을 검토하고 지시에 따라 EC2 인스턴스의 크기를 적절하게 조정합니다.

Answer: C

https://www.examtopics.com/discussions/amazon/view/68919-exam-aws-certified-solutions-architect-professional-topic-1/

https://aws.amazon.com/compute-optimizer/pricing/
https://aws.amazon.com/systemsmanager/pricing/
https://aws.amazon.com/compute-optimizer/

NO.173
A public retail web application uses an Application Load Balancer (ALB) in front of Amazon EC2 instances running across multiple Availability Zones (AZs) in a Region backed by an Amazon RDS MySQL Multi-AZ deployment.
Target group health checks are configured to use HTTP and pointed at the product catalog page.
Auto Scaling is configured to maintain the web fleet size based on the ALB health check.
Recently, the application experienced an outage. Auto Scaling continuously replaced the instances during the outage.
A subsequent investigation determined that the web server metrics were within the normal range, but the database tier was experiencing high load, resulting in severely elevated query response times.
Which of the following changes together would remediate these issues while improving monitoring capabilities for the availability and functionality of the entire application stack for future growth? (Select TWO.)

A. Configure read replicas for Amazon RDS MySQL and use the single reader endpoint in the web application to reduce the load on the backend database tier.

B. Configure the target group health check to point at a simple HTML page instead of a product catalog page and the Amazon Route 53 health check against the product page to evaluate full application functionality.
Configure Amazon CloudWatch alarms to notify administrators when the site fails.

C. Configure the target group health check to use a TCP check of the Amazon EC2 web server and the Amazon Route 53 health check against the product page to evaluate full application functionality.
Configure Amazon CloudWatch alarms to notify administrators when the site fails.

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

E. Configure an Amazon ElastiCache cluster and place it between the web application and RDS MySQL instances to reduce the load on the backend database tier.

Answer: B, E

https://www.examtopics.com/discussions/amazon/view/4570-exam-aws-certified-solutions-architect-professional-topic-2/

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

NO.173
퍼블릭 소매 웹 애플리케이션은 Amazon RDS MySQL 다중 AZ 배포가 지원하는 리전의 여러 가용 영역(AZ)에서 실행되는 Amazon EC2 인스턴스 앞에서 애플리케이션 로드 밸런서(ALB)를 사용합니다.
Target group health check는 HTTP를 사용하도록 구성되며 제품 카탈로그 페이지를 가리킵니다.
Auto Scaling은 ALB 상태 확인을 기반으로 web fleet size를 유지하도록 구성됩니다.
최근에 애플리케이션이 중단되었습니다.
Auto Scaling은 중단 중에 인스턴스를 지속적으로 교체했습니다.
후속 조사에서는 웹 서버 메트릭이 정상 범위 내에 있었지만 데이터베이스 계층에 높은 로드가 발생하여 쿼리 응답 시간이 크게 증가한 것으로 확인되었습니다.
다음 변경 사항 중 어떤 것이 이러한 문제를 해결하는 동시에 향후 성장을 위해 전체 애플리케이션 스택의 가용성 및 기능에 대한 모니터링 기능을 개선할 것입니까? (2개를 선택하십시오.)

A. Amazon RDS MySQL에 대한 읽기 전용 복제본을 구성하고 웹 애플리케이션에서 단일 리더 엔드포인트를 사용하여 백엔드 데이터베이스 계층의 부하를 줄입니다.

B. 제품 카탈로그 페이지 대신 간단한 HTML 페이지를 가리키도록 target group health check를 구성하고 전체 애플리케이션 기능을 평가하기 위해 제품 페이지에 대해 Amazon Route 53 상태 확인을 구성합니다.
사이트가 실패할 때 관리자에게 알리도록 Amazon CloudWatch 경보를 구성합니다.

C. Amazon EC2 웹 서버의 TCP 확인 및 제품 페이지에 대한 Amazon Route 53 health check를 사용하여 전체 애플리케이션 기능을 평가하도록 target group health check를 구성합니다.
사이트가 실패할 때 관리자에게 알리도록 Amazon CloudWatch 경보를 구성합니다.

D. 데이터베이스 계층에서 부하가 높고 손상된 RDS 인스턴스를 복구하는 작업으로 Amazon RDS에 대한 Amazon CloudWatch 경보를 구성합니다.

E. Amazon ElastiCache 클러스터를 구성하고 웹 애플리케이션과 RDS MySQL 인스턴스 사이에 배치하여 백엔드 데이터베이스 계층의 부하를 줄입니다.

Answer: B, E

https://www.examtopics.com/discussions/amazon/view/4570-exam-aws-certified-solutions-architect-professional-topic-2/

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

NO.174
A Solutions Architect is building a containerized .NET Core application that will run in AWS Fargate. The backend of the application requires Microsoft SQL Server with high availability.
All tiers of the application must be highly available.
The credentials used for the connection string to SQL Server should not be stored on disk within the .NET Core front-end containers.
Which strategies should the Solutions Architect use to meet these requirements?

A. Set up SQL Server to run in Fargate with Service Auto Scaling.
Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to SQL Server running in Fargate.
Specify the ARN of the secret in AWS Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string.
Set up the .NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.

B. Create a Multi-AZ deployment of SQL Server on Amazon RDS.
Create a secret in AWS Secrets Manager for the credentials to the RDS database.
Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to the RDS database in Secrets Manager.
Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string.
Set up the .NET Core service in Fargate using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.

C. Create an Auto Scaling group to run SQL Server on Amazon EC2.
Create a secret in AWS Secrets Manager for the credentials to SQL Server running on EC2.
Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to SQL Server on EC2.
Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string.
Set up the .NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.

D. Create a Multi-AZ deployment of SQL Server on Amazon RDS.
Create a secret in AWS Secrets Manager for the credentials to the RDS database. Create non-persistent empty storage for the .NET Core containers in the Fargate task definition to store the sensitive information.
Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to the RDS database in Secrets Manager.
Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be written to the non-persistent empty storage on startup for reading into the application to construct the connection string. Set up the .NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones
.

Answer: B

https://www.examtopics.com/discussions/amazon/view/28032-exam-aws-certified-solutions-architect-professional-topic-1/

Secrets Manager natively supports SQL Server on RDS.
No real need to create additional 'ephemeral storage' to fetch credentials, as these can be injected to containers as environment variables.

https://aws.amazon.com/premiumsupport/knowledge-center/ecs-data-security-container-task/

NO.174
Solutions Architect는 AWS Fargate에서 실행할 컨테이너화된 .NET Core 애플리케이션을 구축하고 있습니다.
애플리케이션의 백엔드에는 고가용성을 갖춘 Microsoft SQL Server가 필요합니다.
애플리케이션의 모든 계층은 가용성이 높아야 합니다.
SQL Server에 대한 연결 문자열에 사용되는 자격 증명은 .NET Core 프런트엔드 컨테이너 내의 디스크에 저장하면 안 됩니다.
이러한 요구 사항을 충족하기 위해 Solutions Architect는 어떤 전략을 사용해야 합니까?

A. Service Auto Scaling을 사용하여 Fargate에서 실행되도록 SQL Server를 설정합니다.
Fargate task 정의가 Fargate에서 실행되는 SQL Server에 대한 자격 증명의 암호 값을 가져올 수 있도록 하는 Amazon ECS task 실행 역할을 생성합니다.
Fargate task 정의의 비밀 섹션에서 AWS Secrets Manager의 비밀 ARN을 지정하면 연결 문자열을 구성하기 위해 애플리케이션에서 읽기 위해 시작 시 환경변수로 민감한 데이터를 컨테이너에 주입할 수 있습니다.
여러 가용 영역의 Application Load Balancer 뒤에서 Service Auto Scaling을 사용하여 .NET Core 서비스를 설정합니다.

B. Amazon RDS에서 SQL Server의 다중 AZ 배포를 생성합니다.
AWS Secrets Manager에서 RDS 데이터베이스에 대한 자격 증명에 대한 암호를 생성합니다.
Fargate task 정의가 Secrets Manager의 RDS 데이터베이스에 대한 자격 증명의 암호 값을 가져오도록 허용하는 Amazon ECS task 실행 역할을 생성합니다.
연결 문자열을 구성하기 위해 응용 프로그램으로 읽어 들이기 위해,
Fargate 작업 정의의 비밀 섹션에서 Secrets Manager의 비밀 ARN을 지정하면 민감한 데이터가 시작 시 환경 변수로 컨테이너에 주입될 수 있습니다.
여러 가용 영역의 Application Load Balancer 뒤에서 Service Auto Scaling을 사용하여 Fargate에서 .NET Core 서비스를 설정합니다.

C. Amazon EC2에서 SQL Server를 실행할 Auto Scaling 그룹을 생성합니다.
EC2에서 실행되는 SQL Server에 대한 자격 증명에 대해 AWS Secrets Manager에서 암호를

생성합니다.
Fargate task 정의가 EC2의 SQL Server에 대한 자격 증명의 암호 값을 가져오도록 허용하는 Amazon ECS 작업 실행 역할을 생성합니다.
연결 문자열을 구성하기 위해 응용 프로그램으로 읽어 들이기 위해,
Fargate 작업 정의의 비밀 섹션에서 Secrets Manager의 비밀 ARN을 지정하면 민감한 데이터가 시작 시 환경 변수로 컨테이너에 주입될 수 있습니다.
여러 가용 영역의 Application Load Balancer 뒤에서 Service Auto Scaling을 사용하여 .NET Core 서비스를 설정합니다.

D. Amazon RDS에서 SQL Server의 다중 AZ 배포를 생성합니다.
AWS Secrets Manager에서 RDS 데이터베이스에 대한 자격 증명에 대한 암호를 생성합니다.
중요한 정보를 저장하기 위해 Fargate task 정의에서 .NET Core 컨테이너에 대한 비영구적 빈 스토리지를 생성합니다.
Fargate 작업 정의가 Secrets Manager의 RDS 데이터베이스에 대한 자격 증명의 암호 값을 가져오도록 허용하는 Amazon ECS 작업 실행 역할을 생성합니다.
연결 문자열을 구성하기 위해 응용 프로그램으로 읽어 들이기 위해,
Fargate 작업 정의의 비밀 섹션에서 Secrets Manager의 비밀 ARN을 지정하면 시작 시 중요한 데이터가 비영구적 빈 스토리지에 기록될 수 있습니다.
여러 가용 영역의 Application Load Balancer 뒤에서 Service Auto Scaling을 사용하여 .NET Core 서비스를 설정합니다.

Answer: B

https://www.examtopics.com/discussions/amazon/view/28032-exam-aws-certified-solutions-architect-professional-topic-1/

Secrets Manager natively supports SQL Server on RDS.
No real need to create additional 'ephemeral storage' to fetch credentials, as these can be injected to containers as environment variables.

https://aws.amazon.com/premiumsupport/knowledge-center/ecs-data-security-container-task/

NO.175
A company has built a high performance computing (HPC) cluster in AWS for a tightly coupled workload that generates a large number of shared files stored in Amazon EFS.
The cluster was performing well when the number of Amazon EC2 instances in the cluster was 100. However, when the company increased the cluster size to 1,000 EC2 instances, overall performance was well below expectations.
Which collection of design choices should a solutions architect make to achieve the maximum performance from the HPC cluster? (Choose three.)

A. Ensure the HPC cluster is launched within a single Availability Zone.

B. Launch the EC2 instances and attach elastic network interfaces in multiples of four.

C. Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled.

D. Ensure the clusters is launched across multiple Availability Zones.

E. Replace Amazon EFS win multiple Amazon EBS volumes in a RAID array.

F. Replace Amazon EFS with Amazon FSx for Lustre.

Answer: A, C, F

https://www.examtopics.com/discussions/amazon/view/28275-exam-aws-certified-solutions-architect-professional-topic-1/

NO.175
한 회사는 Amazon EFS에 저장된 많은 수의 공유 파일을 생성하는 긴밀하게 연결된 워크로드를 위해 AWS에 고성능 컴퓨팅(HPC) 클러스터를 구축했습니다.
클러스터의 Amazon EC2 인스턴스 수가 100개일 때 클러스터는 잘 작동하고 있었습니다.
그러나 회사에서 클러스터 크기를 1,000개 EC2 인스턴스로 늘렸을 때 전반적인 성능은 예상보다 훨씬 낮았습니다.
솔루션 아키텍트는 HPC 클러스터에서 최대 성능을 달성하기 위해 어떤 설계 선택을 해야 합니까? (3개를 선택하세요.)

A. HPC 클러스터가 단일 가용 영역 내에서 시작되었는지 확인합니다.

B. EC2 인스턴스를 시작하고 4의 배수로 탄력적 네트워크 인터페이스를 연결합니다.

C. EFA(Elastic Fabric Adapter)가 활성화된 EC2 인스턴스 유형을 선택합니다.

D. 클러스터가 여러 가용 영역에서 시작되었는지 확인합니다.

E. RAID 어레이에서 여러 Amazon EBS 볼륨을 확보한 Amazon EFS를 교체합니다.

F. Amazon EFS를 Lustre용 Amazon FSx로 교체합니다.

Answer: A, C, F

https://www.examtopics.com/discussions/amazon/view/28275-exam-aws-certified-solutions-architect-professional-topic-1/

NO.176
A company is running a line-of-business (LOB) application on AWS to support its users.
The application runs in one VPC, with a backup copy in a second VPC in a different AWS Region for disaster recovery.
The company has a single AWS Direct Connect connection between its on-premises network and AWS.
The connection terminates at a Direct Connect gateway.
All access to the application must originate from the company's on-premises network and traffic must be encrypted in transit through the use of IPsec.
The company is routing traffic through a VPN tunnel over the Direct Connect connection to provide the required encryption.
A business continuity audit determines that the Direct Connect connection represents a potential single point of failure for access to the application. The company needs to remediate this issue as quickly as possible.
Which approach will meet these requirements?

A. Order a second Direct Connect connection to a different Direct Connect location. Terminate the second Direct Connect connection at the same Direct Connect gateway.

B. Configure an AWS Site-to-Site VPN connection over the internet. Terminate the VPN connection at a virtual private gateway in the secondary Region.

C. Create a transit gateway. Attach the VPCs to the transit gateway, and connect the transit gateway to the Direct Connect gateway. Configure an AWS Site-to- Site VPN connection, and terminate it at the transit gateway.

D. Create a transit gateway. Attach the VPCs to the transit gateway, and connect the transit gateway to the Direct Connect gateway. Order a second Direct Connect connection, and terminate it at the transit gateway.

Answer: C

https://www.examtopics.com/discussions/amazon/view/60129-exam-aws-certified-solutions-architect-professional-topic-1/

NO.176
회사는 사용자를 지원하기 위해 AWS에서 기간 업무(LOB) 애플리케이션을 실행하고 있습니다.
애플리케이션은 재해 복구를 위해 다른 AWS 리전의 두 번째 VPC에서 백업 복사본과 함께 하나의 VPC에서 실행됩니다.
이 회사는 온프레미스 네트워크와 AWS 간에 단일 AWS Direct Connect 연결이 있습니다.
연결은 Direct Connect 게이트웨이에서 종료됩니다.
애플리케이션에 대한 모든 액세스는 회사의 온프레미스 네트워크에서 시작되어야 하며 트래픽은 IPsec을 사용하여 전송 중에 암호화되어야 합니다.
회사는 필요한 암호화를 제공하기 위해 Direct Connect 연결을 통해 VPN 터널을 통해 트래픽을 라우팅하고 있습니다.
비즈니스 연속성 감사는 Direct Connect 연결이 애플리케이션 액세스에 대한 잠재적인 단일 실패 지점을 나타내는지 확인합니다.
회사는 가능한 한 빨리 이 문제를 해결해야 합니다.
어떤 접근 방식이 이러한 요구 사항을 충족합니까?

A. 다른 Direct Connect 위치에 대한 두 번째 Direct Connect 연결을 주문하십시오.
동일한 Direct Connect 게이트웨이에서 두 번째 Direct Connect 연결을 종료합니다.

B. 인터넷을 통해 AWS Site-to-Site VPN 연결을 구성합니다.
보조 리전의 가상 프라이빗 게이트웨이에서 VPN 연결을 종료합니다.

C. 전송 게이트웨이를 만듭니다. VPC를 전송 게이트웨이에 연결하고 전송 게이트웨이를 Direct Connect 게이트웨이에 연결합니다.
AWS Site-to-Site VPN 연결을 구성하고 전송 게이트웨이에서 연결을 종료합니다.

D. 전송 게이트웨이를 만듭니다. VPC를 전송 게이트웨이에 연결하고 전송 게이트웨이를 Direct Connect 게이트웨이에 연결합니다.
두 번째 Direct Connect 연결을 주문하고 전송 게이트웨이에서 종료합니다.

Answer: C