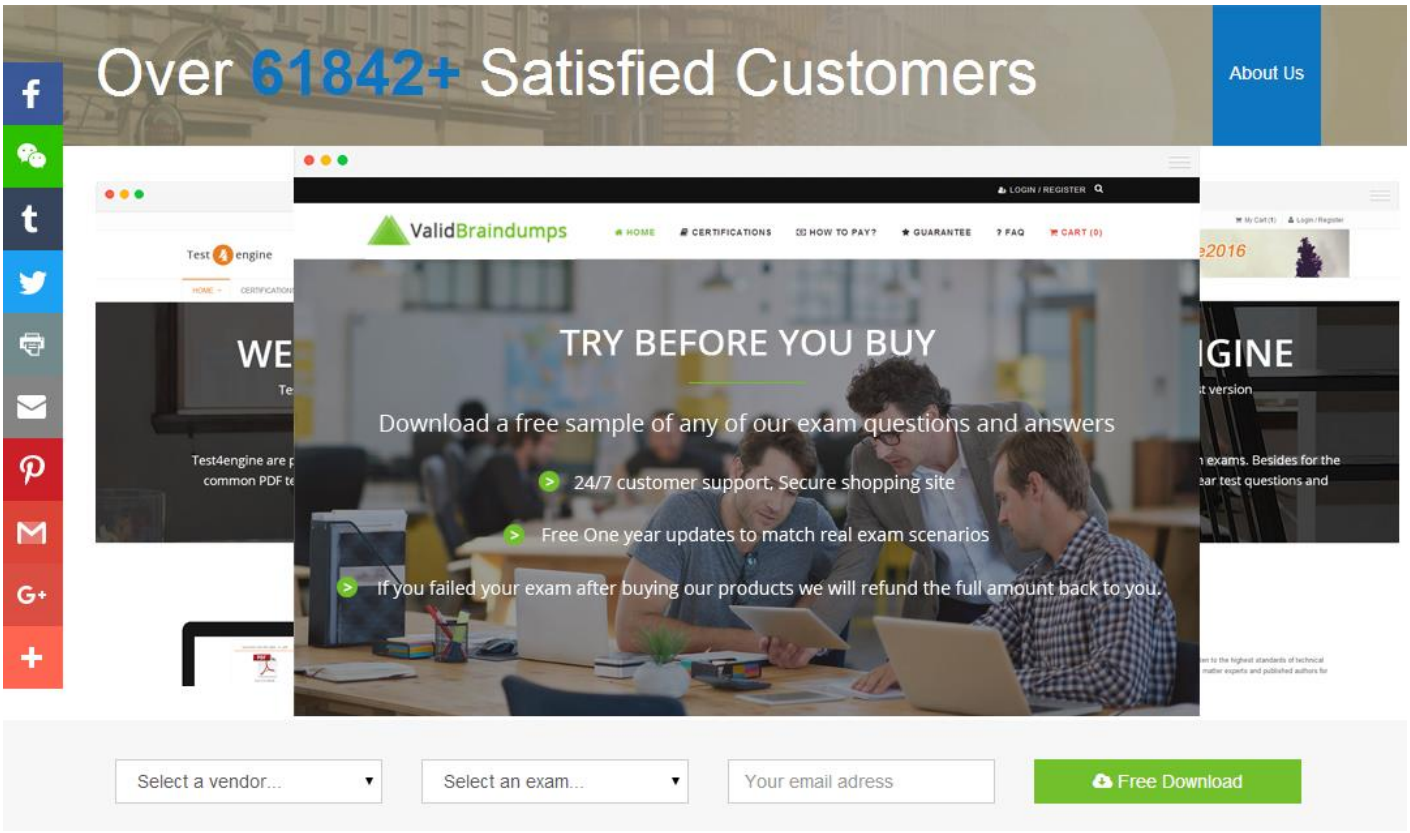
# ValidBraindumps




## Try Before You Buy

Download a free sample of any of our exam questions and answers

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

http://www.validbraindumps.com

Free valid test braindumps for IT certification valid exam

**Exam** : **DOP-C02-KR**

Title : AWS Certified DevOps Engineer - Professional (DOP-C02 Korean Version)

**Vendor** : Amazon

**Version** : DEMO

**QUESTION NO: 1**
회사에는 20개의 서비스 학습이 있습니다. 각 서비스 팀은 자체 마이크로서비스를 담당합니다. 각 서비스 팀은 192 168 0 0/22 CIDR 블록이 있는 마이크로서비스 및 VPC에 별도의 AWS 계정을 사용합니다. 회사는 AWS Organizations로 AWS 계정을 관리합니다.
각 서비스 팀은 Application Load Balancer 뒤에 있는 여러 Amazon EC2 인스턴스에서 마이크로서비스를 호스팅합니다. 마이크로서비스는 공용 인터넷을 통해 서로 통신합니다.
회사의 보안 팀은 마이크로 서비스 간의 모든 통신이 사설 네트워크 연결을 통해 HTTPS를 사용해야 하며 공용 인터넷을 통과할 수 없다는 새로운 지침을 발표했습니다.
DevOps 엔지니어는 이러한 의무를 이행하고 각 서비스 팀의 변경 수를 최소화하는 솔루션을 구현해야 합니다. 어떤 솔루션이 이러한 요구 사항을 충족합니까?
**A.** AWS Organizations에서 새 AWS 계정을 생성합니다. 이 계정에서 VPC를 생성하고 AWS Resource Access Manager를 사용하여 이 VPC의 프라이빗 서브넷을 조직과 공유합니다. 서비스 팀에 새 계정을 시작하도록 지시합니다. 공유 프라이빗 서브넷을 사용하는 NLB(Network Load Balancer) 및 EC2 인스턴스 마이크로 서비스 간의 통신에 NLB DNS 이름을 사용합니다.
**B.** 각 마이크로 서비스 VPC에서 NLB(Network Load Balancer) 생성 AWS PrivateLink를 사용하여 NLB에 대한 각 AWS 계정에 VPC 엔드포인트 생성 다른 각 AWS 계정에서 각 VPC 엔드포인트에 대한 구독 생성 VPC 엔드포인트 DNS 사용 마이크로서비스 간의 통신을 위한 이름입니다.
**C.** 각 마이크로서비스 VPC에 NLB(Network Load Balancer)를 생성합니다. 각 마이크로서비스 VPC 간에 VPC 피어링 연결을 생성합니다. 피어링 링크를 사용하도록 각 VPC의 라우팅 테이블을 업데이트합니다. 마이크로서비스 간 통신에 NLB DNS 이름을 사용합니다.
**D.** AWS Organizations에서 새 AWS 계정 생성 이 계정에서 전송 게이트웨이를 생성하고 AWS Resource Access Manager를 사용하여 조직과 전송 게이트웨이를 공유합니다. 각 마이크로서비스 VPC에서. 공유 Transit Gateway에 Transit Gateway 연결 생성 Transit Gateway를 사용하도록 각 VPC의 라우팅 테이블 업데이트 각 마이크로서비스 VPC에서 NLB(Network Load Balancer) 생성 마이크로서비스 간 통신에 NLB DNS 이름을 사용합니다.
***Answer:*** B
Explanation:
https://aws.amazon.com/blogs/networking-and-content-delivery/connecting-networks-with-overlapping-ip- ranges/ Private link is the best option because Transit Gateway doesn ' t support overlapping CIDR ranges.

**QUESTION NO: 2**
한 회사의 애플리케이션 팀은 애플리케이션 개발을 위해 AWS CodeCommit 리포지토리를 사용합니다. 이 애플리케이션 팀들은 여러 AWS 계정에 리포지토리를 보유하고 있으며, 모든 계정은 AWS Organizations 내의 조직에 속해 있습니다.
각 애플리케이션 팀은 외부 IdP(ID 공급자)로 구성된 AWS IAM Identity Center(AWS Single Sign-On)를 사용하여 개발자 IAM 역할을 수임합니다. 이 개발자 역할을 통해 애플리케이션 팀은 Git을 사용하여 리포지토리의 코드를 작업할 수 있습니다.
보안 감사 결과 애플리케이션 팀이 모든 저장소의 메인 브랜치를 수정할 수 있는 것으로 나타났습니다. DevOps 엔지니어는 애플리케이션 팀이 자신이 관리하는 저장소의 메인 브랜치만 수정할 수 있도록 하는 솔루션을 구현해야 합니다.
다음 요구사항을 충족하는 단계 조합은 무엇입니까? (세 가지를 선택하십시오.)
**A.** SAML 어설션을 업데이트하여 사용자의 팀 이름을 전달하도록 합니다. IAM 역할의 신뢰

정책을 업데이트하여 팀 이름이 포함된 access-team 세션 태그를 추가합니다.
**B.** 조직 관리 계정의 각 팀에 대한 승인 규칙 템플릿을 생성합니다. 템플릿을 모든 저장소와 연결합니다. 개발자 역할 ARN을 승인자로 추가합니다.
**C.** 각 계정에 대한 승인 규칙 템플릿을 생성합니다. 모든 저장소에 템플릿을 연결합니다. 추가합니다.
" aws:ResourceTag/access-team " : " $ ;{aws:PrincipalTag/access-team} " 승인 규칙 템플릿에 대한 조건입니다.
**D.** 각 CodeCommit 저장소에 대해 연결된 팀의 이름으로 값이 설정된 access-team 태그를 추가합니다.
**E.** 계정에 SCP를 첨부하세요. 다음 문구를 포함하세요.
**F.** 각 계정에 IAM 권한 경계를 생성합니다. 다음 문장을 포함하세요.
***Answer:*** A D F
Explanation:
Short Explanation: To meet the requirements, the DevOps engineer should update the SAML assertion to pass the user's team name, update the IAM role's trust policy to add an access-team session tag that has the team name, create an IAM permissions boundary in each account, and for each CodeCommit repository, add an access-team tag that has the value set to the name of the associated team.
Updating the SAML assertion to pass the user's team name allows the DevOps engineer to use IAM tags to identify which team a user belongs to. This can help enforce fine-grained access control based on the user's team membership1.
Updating the IAM role's trust policy to add an access-team session tag that has the team name allows the DevOps engineer to use IAM condition keys to restrict access based on the session tag value2. For example, the DevOps engineer can use the aws:PrincipalTag condition key to match the access-team tag of the user with the access-team tag of the repository3.
Creating an IAM permissions boundary in each account allows the DevOps engineer to set the maximum permissions that an identity-based policy can grant to an IAM entity. An entity's permissions boundary allows it to perform only the actions that are allowed by both its identity-based policies and its permissions boundaries4. For example, the DevOps engineer can use a permissions boundary policy to limit the actions that a user can perform on CodeCommit repositories based on their access-team tag5.
For each CodeCommit repository, adding an access-team tag that has the value set to the name of the associated team allows the DevOps engineer to use resource tags to identify which team manages a repository. This can help enforce fine-grained access control based on the resource tag value6.
The other options are incorrect because:
Creating an approval rule template for each team in the Organizations management account is not a valid option, as approval rule templates are not supported by AWS Organizations. Approval rule templates are specific to CodeCommit and can only be associated with one or more repositories in the same AWS Region where they are created7.
Creating an approval rule template for each account is not a valid option, as approval rule templates are not designed to restrict access to modify branches. Approval rule templates are designed to require approvals from specified users or groups before merging pull requests8.

Attaching an SCP to the accounts is not a valid option, as SCPs are not designed to restrict access based on tags. SCPs are designed to restrict access based on service actions and resources across all users and roles in an organization's account9.

**QUESTION NO: 3**
회사는 해당 애플리케이션에 대한 장애 조치를 구현해야 합니다. 애플리케이션에는 AWS 리전의 Amazon CloudFront 배포와 퍼블릭 ALB(Application Load Balancer)가 포함되어 있습니다. 회사는 ALB를 배포의 기본 원본으로 구성했습니다.
최근 일부 애플리케이션 중단 이후 회사는 0초 RTO를 원합니다. 회사는 웜 대기 구성으로 보조 지역에 애플리케이션을 배포합니다. DevOps 엔지니어는 HTTP GET 요청이 원하는 RTO를 충족하도록 보조 리전에 대한 애플리케이션 장애 조치를 자동화해야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?
**A.** 보조 ALB를 기본 오리진으로 사용하는 두 번째 CloudFront 배포를 생성합니다. 두 CloudFront 배포 모두에 대해 장애 조치 정책 및 대상 상태 평가가 예로 설정된 Amazon Route 53 별칭 레코드를 생성합니다. 새 레코드 세트를 사용하도록 애플리케이션을 업데이트합니다.
**B.** 보조 ALB에 대한 배포판에 새 오리진을 생성합니다. 새 원본 그룹을 만듭니다. 원본 ALB를 기본 원본으로 설정합니다. HTTP 5xx 상태 코드에 대해 장애 조치를 수행하도록 원본 그룹을 구성합니다.
원본 그룹을 사용하도록 기본 동작을 업데이트합니다.
**C.** 두 ALB에 대해 장애 조치 정책 및 대상 상태 평가가 예로 설정된 Amazon Route 53 별칭 레코드를 생성합니다. 두 레코드의 TTL을 0으로 설정합니다. 새 레코드 세트를 사용하도록 배포 원본을 업데이트합니다.
**D.** HTTP 5xx 상태 코드를 감지하는 CloudFront 함수를 생성합니다. 함수가 5xx 상태 코드를 감지하는 경우 보조 ALB에 307 임시 리디렉션 오류 응답을 반환하도록 함수를 구성합니다.
원본 응답을 함수에 보내도록 배포의 기본 동작을 업데이트합니다.
***Answer:*** B
Explanation:
The best solution to implement failover for the application is to use CloudFront origin groups. Origin groups allow CloudFront to automatically switch to a secondary origin when the primary origin is unavailable or returns specific HTTP status codes that indicate a failure1. This way, CloudFront can serve the requests from the secondary ALB in the secondary Region without any delay or redirection. To set up origin groups, the DevOps engineer needs to create a new origin on the distribution for the secondary ALB, create a new origin group with the original ALB as the primary origin and the secondary ALB as the secondary origin, and configure the origin group to fail over for HTTP 5xx status codes. Then, the DevOps engineer needs to update the default behavior to use the origin group instead of the single origin2.
The other options are not as effective or efficient as the solution in option B. Option A is not suitable because creating a second CloudFront distribution will increase the complexity and cost of the application. Moreover, using Route 53 alias records with a failover policy will introduce some delay in detecting and switching to the secondary CloudFront distribution, which may not meet the zero-second RTO requirement. Option C is not feasible because CloudFront does not support using Route 53 alias records as origins3. Option D is not advisable because using a CloudFront function to redirect the requests to the secondary ALB will add an extra round-trip and latency to the failover process, which may also not meet the

zero-second RTO requirement.
1: Optimizing high availability with CloudFront origin failover - Amazon CloudFront
2: Creating an origin group - Amazon CloudFront
3: Values That You Specify When You Create or Update a Web Distribution - Amazon CloudFront

**QUESTION NO: 4**
DevOps 엔지니어는 AWS Cloud Formation 사용자 지정 리소스를 사용하여 AD Connector를 설정했습니다. AWS Lambda 함수가 실행되어 AD 커넥터를 생성했지만 Cloud Formation이 CREATE_IN_PROGRESS에서 CREATE_COMPLETE로 전환되지 않습니다.
엔지니어는 이 문제를 해결하기 위해 어떤 조치를 취해야 합니까?
**A.** Lambda 함수 코드가 성공적으로 종료되었는지 확인하십시오.
**B.** Lambda 함수 코드가 미리 서명된 URL에 대한 응답을 반환하는지 확인합니다.
**C.** Lambda 함수 IAM 역할에 스택 ARN에 대한 cloudformation UpdateStack 권한이 있는지 확인합니다.
**D.** Lambda 함수 IAM 역할에 AWS 계정에 대한 ds ConnectDirectory 권한이 있는지 확인합니다.
***Answer:*** B
Reference: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/crpg-ref-responses.html

**QUESTION NO: 5**
한 회사가 여러 AWS 계정에서 자사 애플리케이션 환경을 관리합니다. 각 환경 계정은 AWS Organizations에서 서로 다른 OU에 속해 있습니다.
DevOps 팀은 여러 환경에 걸쳐 애플리케이션 배포 프로세스를 담당합니다. 이 배포 프로세스는 공유 서비스 계정의 AWS CodePipeline 파이프라인을 사용합니다. DevOps 팀 구성원은 모두 동일한 사용자 그룹에 속해 있으며, AWS IAM Identity Center를 통해 모든 계정에 대한 관리자 권한을 가지고 있습니다.
최근 개발 환경에서 발생한 배포 문제로 인해 DevOps 팀이 수동으로 작업을 수행해야 했습니다. 그 결과, 프로덕션 환경으로의 배포 과정에서 파이프라인 오류가 발생하여 몇 시간 동안 새로운 배포가 차단되었습니다.
DevOps 엔지니어는 파이프라인만이 프로덕션 환경에 배포를 수행할 수 있도록 보장해야 합니다. 또한 비상 상황 발생 시 DevOps 엔지니어는 해당 환경에 접근할 수 있어야 합니다.
어떤 솔루션이 가장 높은 운영 효율성을 보이면서 이러한 요구 사항을 충족할까요?
**A.** 프로덕션 OU에서 DevOps 팀 구성원의 모든 쓰기 작업을 거부하는 SCP를 생성합니다. CodePipeline에서 프로비저닝하는 리소스에 특정 태그를 지정합니다. DevOps 엔지니어 이외의 다른 주체가 태그가 지정된 리소스를 수정하지 못하도록 하는 SCP를 추가합니다.
**B.** DevOps 그룹에 프로덕션 계정에 대한 읽기 전용 액세스 권한이 설정되도록 업데이트합니다.
DevOps 엔지니어 사용자에게 AdministratorAccess 권한을 부여하고 파이프라인 역할을 수행할 수 있도록 하는 새로운 권한 집합을 구성합니다. 파이프라인 역할 이외의 다른 주체가 리소스를 수정하지 못하도록 하는 SCP를 추가합니다.
**C.** DevOps 그룹이 프로덕션 계정에 대한 파이프라인 역할을 수임할 수 있도록 업데이트합니다. DevOps 엔지니어를 위해 IAM Identity Center에 관리자 액세스 권한이 있는 새 권한 집합을 가진 새 사용자를 구성합니다. DevOps 엔지니어 이외의 다른 엔터티가

리소스를 수정하지 못하도록 하는 SCP를 추가합니다.
**D.** 프로덕션 OU에서 DevOps 팀 구성원의 모든 쓰기 작업을 거부하는 SCP를 생성합니다. DevOps 엔지니어를 위해 IAM Identity Center에서 AdministratorAccess 권한이 포함된 새 권한 집합을 가진 새 사용자를 구성합니다. 파이프라인 역할 이외의 모든 엔터티가 리소스를 수정하지 못하도록 하는 SCP를 추가합니다.
***Answer:*** B

**QUESTION NO: 6**
데브옵스 엔지니어가 아마존 리눅스에서 호스팅되는 프로젝트를 진행하고 있는데, 해당 프로젝트가 보안 검토에서 불합격 판정을 받았습니다.
DevOps 관리자는 AWS CodeBuild 프로젝트의 buildspec.yaml 파일을 검토하고 권장 사항을 제시해 달라는 요청을 받았습니다. buildspec.yaml 파일은 다음과 같이 구성되어 있습니다.
AWS 보안 모범 사례를 준수하기 위해 어떤 변경 사항을 권장해야 합니까? (세 가지를 선택하십시오.)
**A.** db_password를 AWS Systems Manager 파라미터 스토어에 SecureString 값으로 저장한 다음 환경 변수에서 db_password를 제거합니다.
**B.** 환경 변수를 'db.-deploy-bucket' Amazon S3 버킷으로 이동하고, 변수를 다운로드한 다음 내보내는 사전 빌드 단계를 추가합니다.
**C.** 다른 CodeBuild 사용자가 임시 파일을 볼 수 없도록 종료 전에 컨테이너에서 임시 파일을 제거하는 빌드 후 명령을 추가합니다.
**D.** 인스턴스에 직접 sec 및 ssh 명령을 사용하는 대신 AWS Systems Manager 실행 명령을 사용하십시오.
**E.** CodeBuild 프로젝트 역할에 필요한 권한을 부여한 다음 환경 변수에서 AWS 자격 증명을 제거합니다.
***Answer:*** A,D,E

**QUESTION NO: 7**
DevOps 엔지니어는 컨테이너 이미지를 빌드하고, 이를 ECR에 저장하고, 이미지의 취약점을 스캔하고, 업스트림 소스 이미지 저장소의 중단에 대한 복원력을 갖춘 탄력적인 CI/CD 파이프라인이 필요합니다.
어떤 솔루션이 이를 충족합니까?
**A.** 개인 ECR 저장소를 만들고, 푸시 시 이미지를 스캔하고, 복제 규칙에 따라 업스트림 저장소에서 이미지를 복제합니다.
**B.** 업스트림 저장소의 이미지를 캐시하기 위한 공개 ECR 저장소를 만들고, 이미지를 저장하기 위한 비공개 저장소를 만들고, 푸시 시 이미지를 스캔합니다.
**C.** 공개 ECR 저장소를 만들고, 풀스루 캐시 규칙을 구성하고, 이미지를 저장할 개인 저장소를 만들고, 기본 스캐닝을 활성화합니다.
**D.** 개인 ECR 저장소를 만들고, 기본 스캐닝을 활성화하고, 풀스루 캐시 규칙을 만듭니다.
***Answer:*** D
* ECR pull-through cache caches images from upstream repositories for resilience.
* Private repo with basic scanning ensures vulnerability detection on pushed images.
* Enabling pull-through caching on a private repo combines caching and vulnerability scanning seamlessly.
* Public repos do not support pull-through caching of upstream images.

* Replication rules are for multi-Region replication, not upstream caching.
References:
Amazon ECR Pull Through Cache
Amazon ECR Image Scanning

**QUESTION NO: 8**
회사는 전자상거래 웹 애플리케이션을 통해 제품을 판매합니다. 회사는 제품 거래 세부 정보를 파이 차트로 표시하는 대시보드를 원합니다. 회사는 대시보드를 회사의 기존 Amazon CloudWatch 대시보드와 통합하려고 합니다. 어떤 솔루션이 이러한 요구 사항을 가장 효율적인 운영 효율성으로 충족합니까?
**A.** 처리된 각 트랜잭션에 대해 JSON 객체를 CloudWatch 로그 그룹으로 내보내도록 전자상거래 애플리케이션을 업데이트합니다. CloudWatch Logs Insights를 사용하여 로그 그룹을 쿼리하고 결과를 원형 차트 형식으로 시각화합니다. 결과를 원하는 CloudWatch 대시보드에 연결합니다.
**B.** 처리된 각 트랜잭션에 대해 JSON 객체를 Amazon S3 버킷으로 내보내도록 전자상거래 애플리케이션을 업데이트합니다. Amazon Athena를 사용하여 S3 버킷을 쿼리하고 결과를 원형 차트 형식으로 시각화합니다. Athena에서 결과 내보내기 원하는 CloudWatch 대시보드에 결과 연결
**C.** 계측에 AWS X-Ray를 사용하도록 전자상거래 애플리케이션을 업데이트합니다. 새로운 X-Ray 하위 세그먼트를 생성합니다. 처리된 각 트랜잭션에 대한 주석을 추가합니다. X-Ray 추적을 사용하여 데이터를 쿼리하고 원형 차트 형식으로 결과를 시각화합니다. 결과를 원하는 CloudWatch 대시보드에 연결합니다.
**D.** 처리된 각 트랜잭션에 대해 CloudWatch 로그 그룹에 JSON 객체를 내보내도록 전자상거래 애플리케이션을 업데이트합니다. AWS Lambda 함수를 생성하여 결과를 집계하고 Amazon DynamoDB에 기록합니다. 로그 파일에 대한 Lambda 구독 필터를 생성합니다. 원하는 CloudWatch 대시보드에 결과를 연결합니다.
***Answer:*** A
Explanation:
The correct answer is A.
Option A is correct because it meets the requirements with the most operational efficiency. Updating the ecommerce application to emit a JSON object to a CloudWatch log group for each processed transaction is a simple and cost-effective way to collect the data needed for the dashboard. Using CloudWatch Logs Insights to query the log group and to visualize the results in a pie chart format is also a convenient and integrated solution that leverages the existing CloudWatch dashboards. Attaching the results to the desired CloudWatch dashboard is straightforward and does not require any additional steps or services.
Option B is incorrect because it introduces unnecessary complexity and cost. Updating the ecommerce application to emit a JSON object to an Amazon S3 bucket for each processed transaction is a valid way to store the data, but it requires creating and managing an S3 bucket and its permissions. Using Amazon Athena to query the S3 bucket and to visualize the results in a pie chart format is also a valid way to analyze the data, but it incurs charges based on the amount of data scanned by each query. Exporting the results from Athena and attaching them to the desired CloudWatch dashboard is also an extra step that adds more overhead and latency.
Option C is incorrect because it uses AWS X-Ray for an inappropriate purpose. Updating the

ecommerce application to use AWS X-Ray for instrumentation is a good practice for monitoring and tracing distributed applications, but it is not designed for aggregating product transaction details. Creating a new X-Ray subsegment and adding an annotation for each processed transaction is possible, but it would clutter the X- Ray service map and make it harder to debug performance issues. Using X-Ray traces to query the data and to visualize the results in a pie chart format is also possible, but it would require custom code and logic that are not supported by X-Ray natively. Attaching the results to the desired CloudWatch dashboard is also not supported by X-Ray directly, and would require additional steps or services.
Option D is incorrect because it introduces unnecessary complexity and cost. Updating the ecommerce application to emit a JSON object to a CloudWatch log group for each processed transaction is a simple and cost-effective way to collect the data needed for the dashboard, as in option A. However, creating an AWS Lambda function to aggregate and write the results to Amazon DynamoDB is redundant, as CloudWatch Logs Insights can already perform aggregation queries on log data. Creating a Lambda subscription filter for the log file is also redundant, as CloudWatch Logs Insights can already access log data directly. Attaching the results to the desired CloudWatch dashboard would also require additional steps or services, as DynamoDB does not support native integration with CloudWatch dashboards.
References:
CloudWatch Logs Insights
Amazon Athena
AWS X-Ray
AWS Lambda
Amazon DynamoDB

**QUESTION NO: 9**
한 회사에서 AWS CDK와 CodePipeline, 그리고 CodeBuild를 사용하여 애플리케이션을 배포합니다. 이 회사는 배포 전에 단위 테스트를 시행하고, 테스트를 통과한 경우에만 배포를 진행하려고 합니다.
어떤 단계에서 이를 시행합니까? (두 가지를 선택하세요.)
**A.** 테스트를 실행한 다음 배포하도록 CodeBuild 빌드 명령을 업데이트하고 OnFailure를 ABORT로 설정합니다.
**B.** 테스트를 실행한 후 배포하도록 CodeBuild 명령을 업데이트하고, cdk deploy에 --rollback true를 추가합니다.
**C.** 테스트를 실행한 다음 배포하도록 CodeBuild 명령을 업데이트하고 --require-approval any-change 플래그를 추가합니다.
**D.** template.hasResourceProperties 어설션을 사용하여 AWS CDK 어설션 모듈로 테스트를 만듭니다.
**E.** cdk diff를 사용하고 리소스 변경이 감지되면 실패하는 테스트를 만듭니다.
***Answer:*** A D
* Running unit tests in the build phase and aborting on failure (OnFailure=ABORT) prevents deployment if tests fail.
* AWS CDK assertions module provides programmatic unit tests against synthesized templates (Option D).

* The --rollback flag relates to CloudFormation stack rollback, not test gating.
* The --require-approval flag controls manual approvals, not test outcomes.
* cdk diff checks for changes but is not a unit test and may not catch logical errors.
References:
Testing AWS CDK Applications
CodeBuild Buildspec OnFailure

**QUESTION NO: 10**
DevOps 엔지니어가 AWS Fargate의 Amazon Elastic Container Service(Amazon ECS) 클러스터에서 실행되는 Java 기반 애플리케이션을 관리합니다. 이 애플리케이션에는 자동 확장이 구성되어 있지 않습니다. DevOps 엔지니어는 Java Virtual Machine(JVM) 스레드 수가 애플리케이션 확장 시기를 알려주는 좋은 지표라고 판단했습니다. 이 애플리케이션은 8080 포트에서 고객 트래픽을 처리하고 9404 포트에서 JVM 메트릭을 제공합니다. 최근 애플리케이션 사용량이 증가했습니다. DevOps 엔지니어는 이 애플리케이션에 자동 확장을 구성해야 합니다. 운영 오버헤드를 최소화하면서 이러한 요구 사항을 충족하는 솔루션은 무엇일까요?

**A.** Amazon CloudWatch 에이전트를 컨테이너 사이드카로 배포합니다. CloudWatch 에이전트가 포트 9404에서 JVM 메트릭을 검색하도록 구성합니다. JVM 스레드 수 메트릭에 대한 CloudWatch 알람을 생성하여 애플리케이션을 확장합니다. Fargate에 단계적 확장 정책을 추가하여 CloudWatch 알람에 따라 확장 및 축소합니다.

**B.** Amazon CloudWatch 에이전트를 컨테이너 사이드카로 배포합니다. CloudWatch 에이전트의 CloudWatch 로그 그룹에서 JVM 스레드 수 메트릭에 대한 메트릭 필터를 구성합니다. Fargate에 대상 추적 정책을 추가합니다. 메트릭 필터에서 해당 메트릭을 확장 대상으로 선택합니다.

**C.** Amazon Managed Service for Prometheus 작업 영역을 생성합니다. AWS Distro for OpenTelemetry를 컨테이너 사이드카로 배포하여 포트 9404에서 Prometheus 작업 영역으로 JVM 메트릭을 게시합니다. 작업 영역에서 JVM 스레드 수 메트릭을 사용하여 애플리케이션을 확장하도록 규칙을 구성합니다. Fargate에 단계적 확장 정책을 추가합니다. 확장 및 축소할 Prometheus 규칙을 선택합니다.

**D.** Amazon Managed Service for Prometheus 작업 영역을 생성합니다. AWS Distro for OpenTelemetry를 컨테이너 사이드카로 배포하여 포트 9404에서 JVM 메트릭을 검색하고, 포트 9404에서 Prometheus 작업 영역에 JVM 메트릭을 게시합니다. Fargate에서 대상 추적 정책을 추가합니다. Prometheus 메트릭을 확장 대상으로 선택합니다.

***Answer:*** A

**QUESTION NO: 11**
한 회사가 AWS Organizations의 조직을 사용하여 여러 AWS 계정을 관리합니다. 회사는 조직의 모든 기능을 활성화했습니다. AWS CloudFormation StackSets를 사용하여 계정에 구성을 배포합니다. 또한 AWS Config를 사용하여 Amazon S3 버킷을 모니터링합니다. 회사는 S3 버킷에 업로드되는 모든 객체에 AWS Key Management Service(AWS KMS) 암호화를 사용해야 합니다. 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?

**A.** s3-bucket-server-side-encryption-enabled 규칙을 포함하는 AWS Config 적합성 팩을 생성합니다. 적합성 팩을 계정에 배포합니다. Amazon Simple Notification Service(Amazon SNS) 주제를 대상으로 규칙을 구성합니다.

**B.** s3:createBucket 작업에 대한 거부 명령문과 s3:x-amz-server-side-encryption이 aws:kms가

아닌 조건문을 포함하는 SCP를 생성합니다. SCP를 조직의 루트에 연결합니다.
**C.** 조직의 S3 데이터 이벤트를 캡처할 수 있도록 AWS CloudTrail 트레일을 활성화하는 AWS CloudFormation 스택 세트를 생성합니다. 스택 세트에서 AWS KMS 암호화를 사용하지 않는 S3 PutObject 이벤트와 일치하는 Amazon EventBridge 규칙을 생성합니다. Amazon Simple Notification Service(Amazon SNS) 주제를 대상으로 규칙을 구성합니다.
**D.** s3:putObject 작업에 대한 거부 명령과 s3:x-amz-server-side-encryption이 aws:kms가 아닌 조건을 포함하는 SCP를 생성합니다. SCP를 조직의 루트에 연결합니다.
***Answer:*** D

**QUESTION NO: 12**
한 회사가 새로운 기능 개발에 걸리는 시간을 단축하고자 합니다. 이 회사는 AWS CodeBuild와 AWS CodeDeploy를 사용하여 애플리케이션을 빌드하고 배포합니다. 또한 AWS CodePipeline을 사용하여 각 마이크로서비스를 자체 CI/CD 파이프라인으로 배포합니다. 이 회사는 새로운 기능 출시까지의 평균 시간과 배포 실패 후 복구하는 데 걸리는 평균 시간에 대한 가시성을 높여야 합니다. 어떤 솔루션이 가장 적은 구성 작업으로 이러한 가시성을 제공할 수 있을까요?
**A.** 각 파이프라인의 성공 및 실패한 실행 정보를 사용하여 Amazon CloudWatch 사용자 지정 지표를 생성하는 AWS Lambda 함수를 프로그래밍합니다. 5분마다 Lambda 함수를 호출하는 Amazon EventBridge 규칙을 생성합니다. 이 지표를 사용하여 CloudWatch 대시보드를 구축합니다.
**B.** 각 파이프라인의 성공 및 실패한 실행 정보를 사용하여 Amazon CloudWatch 사용자 지정 지표를 생성하는 AWS Lambda 함수를 프로그래밍합니다. 모든 성공 및 실패 실행 후 Lambda 함수를 호출하는 Amazon EventBridge 규칙을 생성합니다. 이 지표를 사용하여 CloudWatch 대시보드를 구축합니다.
**C.** 성공한 실행과 실패한 실행에 대한 정보를 Amazon DynamoDB에 기록하는 AWS Lambda 함수를 프로그래밍합니다. 모든 성공한 실행과 실패한 실행 후에 Lambda 함수를 호출하는 Amazon EventBridge 규칙을 생성합니다. DynamoDB의 정보를 표시하는 Amazon QuickSight 대시보드를 구축합니다.
**D.** Amazon DynamoDB에 성공 및 실패한 실행에 대한 정보를 기록하는 AWS Lambda 함수를 프로그래밍합니다. 5분마다 Lambda 함수를 호출하는 Amazon EventBridge 규칙을 생성합니다. DynamoDB의 정보를 표시하는 Amazon QuickSight 대시보드를 구축합니다.
***Answer:*** B

**QUESTION NO: 13**
회사는 AWS Organizations를 사용하여 각 부서에 대해 별도의 AWS 계정을 생성하고 있습니다. 회사는 다음 작업을 자동화해야 합니다.
* 정기적으로 새로운 패치로 Linux AMI를 업데이트하고 골든 이미지를 생성합니다.
* 골든 이미지의 Chef 에이전트에 새 버전 설치 가능
* 새로 생성된 AMI를 부서 계정에 제공
최소한의 관리 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?
**A.** 이전 골든 이미지에서 Amazon EC2 인스턴스를 시작하는 스크립트 작성 패치 업데이트 적용 새 버전의 Chef 에이전트를 설치하고 새 골든 이미지를 생성한 다음 새 골든 이미지만 공유하도록 AMI 권한을 수정합니다. 부서의 계정이 포함된 이미지입니다.
**B.** Amazon EC2 Image Builder를 사용하여 기본 Linux AMI와 Chef 에이전트를 설치하는 구성

요소로 구성된 이미지 파이프라인을 생성합니다. AWS Resource Access Manager를 사용하여 EC2 Image Builder 이미지를 부서 계정과 공유합니다.

**C.** AWS Systems Manager Automation Runbook을 사용하여 이전 이미지를 사용하여 Linux AMI를 업데이트합니다. Chef 에이전트를 업데이트할 스크립트에 대한 URL을 제공합니다. AWS Organizations를 사용하여 부서 계정의 이전 골든 이미지를 교체합니다.

**D.** Amazon EC2 Image Builder를 사용하여 기본 Linux AMI와 Chef 에이전트를 설치할 구성 요소로 구성된 이미지 파이프라인을 생성합니다. AWS Systems Manager Parameter Store에서 매개변수를 생성하여 참조할 수 있는 새 AMI ID를 저장합니다. 부서의 회계

***Answer:*** B

Explanation:

Amazon EC2 Image Builder is a service that automates the creation, management, and deployment of customized, secure, and up-to-date server images that are pre-installed with software and configuration settings tailored to meet specific IT standards. EC2 Image Builder simplifies the creation and maintenance of golden images, and makes it easy to generate images for multiple platforms, such as Amazon EC2 and on- premises. EC2 Image Builder also integrates with AWS Resource Access Manager, which allows you to share your images across accounts within your organization or with external AWS accounts. This solution meets the requirements of automating the tasks of updating the Linux AMIs, installing the Chef agent, and providing the images to the department's accounts with the least management overhead. References:

Amazon EC2 Image Builder

Sharing EC2 Image Builder images

**QUESTION NO: 14**

비디오 공유 회사는 비디오를 Amazon S3에 저장합니다. 회사는 동영상 액세스 요청이 갑자기 증가한 것을 관찰했지만 어떤 동영상이 가장 인기가 있는지 회사는 알지 못합니다. 회사는 동영상 파일에 대한 일반적인 액세스 패턴을 식별해야 합니다. 이 패턴에는 특정 날짜에 특정 파일에 액세스하는 사용자 수와 n이 포함됩니다.umb DevOps 엔지니어는 Amazon EC2에서 실행되는 대규모 상업용 웹 사이트를 관리합니다. 웹 사이트는 Amazon Kinesis Data Streams를 사용하여 웹 토그를 수집하고 처리합니다. DevOps 엔지니어는 Amazon EC2에서도 실행되는 Kinesis 소비자 애플리케이션을 관리합니다. 레코드를 처리하기 전에 모든 뒤의 애플리케이션과 Kinesis 데이터 스트림이 레코드를 드롭합니다. DevOps 엔지니어는 스트림 처리를 개선하기 위한 솔루션을 구현해야 합니다.

회사는 어떻게 최소한의 노력으로 이러한 요구 사항을 충족할 수 있습니까?

**A.** S3 서버 액세스 로깅을 활성화합니다. 액세스 로그를 Amazon Aurora 데이터베이스로 가져옵니다. Aurora SQL 쿼리를 사용하여 액세스 패턴을 분석합니다.

**B.** S3 서버 액세스 로깅을 활성화합니다. Amazon Athena를 사용하여 로그 파일이 있는 외부 테이블을 생성합니다. Athena를 사용하여 SQL 쿼리를 생성하여 액세스 패턴을 분석합니다.

**C.** 모든 S3 객체 액세스 이벤트에 대해 AWS Lambda 함수를 호출합니다. 사용자와 같은 파일 액세스 정보를 쓰도록 Lambda 함수를 구성합니다. Amazon Aurora 데이터베이스에 대한 S3 버킷 및 파일 키. Aurora SQL 쿼리를 사용하여 액세스 패턴을 분석합니다.

**D.** 모든 S3 객체 액세스 이벤트에 대한 Amazon CloudWatch Logs 로그 메시지를 기록합니다. 사용자, S3 버킷 및 파일 키와 같은 파일 액세스 정보를 SQL 애플리케이션용 Amazon Kinesis Data Analytics에 쓰도록 CloudWatch Logs 로그 스트림을 구성합니다. 슬라이딩 윈도우 분석을 수행합니다.

***Answer:*** B
Explanation:
Activating S3 server access logging and using Amazon Athena to create an external table with the log files is the easiest and most cost-effective way to analyze access patterns. This option requires minimal setup and allows for quick analysis of the access patterns with SQL queries. Additionally, Amazon Athena scales automatically to match the query load, so there is no need for additional infrastructure provisioning or management.

**QUESTION NO: 15**
한 회사에 Auto Scaling 그룹의 Amazon EC2 인스턴스에서 실행되는 애플리케이션이 있습니다. 이 애플리케이션은 Amazon Simple Queue Service(Amazon SQS) 대기열에서 대량의 메시지를 처리합니다.
DevOps 엔지니어가 애플리케이션이 SQS 대기열의 메시지 그룹을 처리하는 데 몇 시간이 걸린다는 것을 발견했습니다. 메시지를 처리할 때 Auto Scaling 그룹의 평균 CPU 사용률이 대상 추적 확장 정책의 임계값을 넘지 않았습니다. SQS 대기열을 처리하는 애플리케이션은 Amazon CloudWatch Logs에 로그를 게시합니다.
DevOps 엔지니어는 대기열이 빠르게 처리되는지 확인해야 합니다.
어떤 솔루션이 운영 오버헤드를 최소화하면서 이러한 요구 사항을 충족시킬 수 있을까요?
**A.** AWS Lambda 함수를 생성합니다. ApproximateNumberOfMessagesVisible SQS 대기열 속성과 GroupIn-ServiceInstances Auto Scaling 그룹 속성을 사용하여 각 인스턴스의 대기열 메시지를 게시하는 사용자 지정 지표를 Lambda 함수에 게시하도록 구성합니다. Lambda 함수를 매시간 실행하도록 Amazon EventBridge 규칙을 예약합니다. 사용자 지정 지표를 사용하여 확장 및 축소하는 Auto Scaling 그룹에 대한 대상 추적 확장 정책을 생성합니다.
**B.** AWS Lambda 함수를 생성합니다. ApproximateNumberOfMessagesVisible SQS 대기열 속성과 GroupIn-ServiceInstances Auto Scaling 그룹 속성을 사용하여 각 인스턴스의 대기열 메시지를 게시하는 사용자 지정 지표를 Lambda 함수에 게시하도록 구성합니다. Lambda 함수를 대상으로 애플리케이션 로그에 대한 CloudWatch 구독 필터를 생성합니다. 사용자 지정 지표를 사용하여 확장 및 축소하는 Auto Scaling 그룹에 대한 대상 추적 확장 정책을 생성합니다.
**C.** 자동 확장 그룹에 대한 대상 추적 확장 정책을 생성합니다. 대상 추적 정책에서 ApproximateNumberOfMessagesVisible SQS 대기열 속성과 GroupIn-ServiceInstances 자동 확장 그룹 속성을 사용하여 메트릭 연산을 통해 각 인스턴스 수에 대해 대기열에 있는 메시지 수를 계산합니다. calculated 속성을 사용하여 확장 및 축소합니다.
**D.** SQS 대기열의 ApproximateNumberOfMessagesVisible 속성을 CloudWatch Logs 로그 그룹에 로깅하는 AWS Lambda 함수를 생성합니다. Amazon EventBridge 규칙을 예약하여 Lambda 함수를 5분마다 실행합니다. CloudWatch Logs 그룹의 로그 이벤트 수를 계산하는 메트릭 필터를 생성합니다. 사용자 지정 메트릭을 사용하여 확장 및 축소하는 Auto Scaling 그룹에 대한 대상 추적 확장 정책을 생성합니다.
***Answer:*** C
Explanation:
The default CPU utilization metric does not reflect the processing backlog in the SQS queue, so the Auto Scaling group is not scaling properly to handle the workload.
To scale the Auto Scaling group based on queue length, you can create a target tracking scaling policy that uses a custom metric that combines the SQS queue ' s ApproximateNumberOfMessagesVisible and the number of instances (GroupIn-

ServiceInstances) metric using CloudWatch metric math. This allows the scaling policy to calculate the average number of messages per instance and scale accordingly.
This approach requires no additional Lambda functions or log processing, thus minimizing operational overhead.
Option A and B require Lambda functions to publish custom metrics, which increases operational complexity.
Option D also adds complexity with logging and metric filters.
Reference:
Scaling based on SQS queue length using metric math: " You can create CloudWatch metric math expressions combining SQS and Auto Scaling group metrics to enable target tracking scaling policies that respond to queue backlog. " (AWS Auto Scaling with SQS) Target Tracking Scaling Policies: " Target tracking policies can use metric math expressions as a source to make scaling decisions. " (AWS Auto Scaling Target Tracking)

**QUESTION NO: 16**
DevOps 엔지니어는 AWS 계정에 CI/CD 파이프라인을 구현해야 합니다. 이 파이프라인은 AWS Systems Manager 파라미터 스토어에 저장된 민감한 데이터베이스 자격 증명을 사용해야 합니다. 파라미터 스토어 파라미터는 별도의 중앙 계정에 있습니다. DevOps 엔지니어는 해당 파라미터를 생성하고 CI/CD 계정과 통합해야 합니다.
다음 요구사항을 충족하는 단계 조합은 무엇입니까? (세 가지를 선택하십시오.)
**A.** 고급 계층 파라미터 스토어 파라미터를 사용하여 데이터베이스 자격 증명을 중앙 AWS 계정에 저장합니다.
**B.** CI/CD 파이프라인을 호스팅하는 AWS 계정에 IAM 역할을 생성합니다. 해당 IAM 역할과 연결된 IAM 정책에 파라미터의 전체 ARN을 추가합니다.
**C.** 표준 계층 파라미터 스토어 파라미터를 사용하여 데이터베이스 자격 증명을 중앙 AWS 계정에 저장합니다.
**D.** AWS KMS 관리형 키를 사용하여 파라미터를 암호화합니다. CI/CD 파이프라인을 호스팅하는 AWS 계정에 KMS 키에 대한 복호화 권한을 부여합니다.
**E.** 고객 관리형 AWS KMS 키를 사용하여 파라미터를 암호화합니다. CI/CD 파이프라인을 호스팅하는 AWS 계정에 고객 관리형 키에 대한 복호화 권한을 부여합니다.
**F.** 중앙 AWS 계정에 AWS Resource Access Manager(AWS RAM) 리소스 공유를 생성합니다. CI/CD 파이프라인을 호스팅하는 계정과 파라미터를 공유합니다.
***Answer:*** A E F
Explanation:
---
###
The requirement is to securely consume cross-account sensitive parameters from AWS Systems Manager Parameter Store in a CI/CD pipeline. AWS imposes specific constraints and features for cross-account parameter access, and the correct solution must align with those constraints.
First, cross-account sharing of Parameter Store parameters is supported only for Advanced tier parameters.
Standard tier parameters cannot be shared across accounts. Therefore, Option A is required, and Option C is invalid.
Second, cross-account access to Parameter Store parameters is implemented using AWS

Resource Access Manager (AWS RAM). RAM allows the central account to explicitly share the parameter resource with the CI
/CD account. Without RAM, the parameter is not visible or accessible across accounts. This makes Option F mandatory.
Third, because the parameter stores sensitive credentials, encryption must be handled securely. When sharing encrypted parameters across accounts, AWS requires the use of a customer managed AWS KMS key, not an AWS managed key. The key policy must explicitly grant `kms:Decrypt` permission to the consuming account. AWS managed keys cannot be shared across accounts, which makes Option D invalid and Option E correct.
Although the CI/CD pipeline's IAM role must ultimately have permission to read the parameter, that permission is implicit in the consuming account once the parameter is shared and the KMS key policy allows decryption. The critical cross-account enablers are Advanced tier, RAM sharing, and a customer managed KMS key.
Therefore, the correct combination is A, E, and F.

**QUESTION NO: 17**
한 회사가 AWS CodePipeline의 파이프라인을 사용하여 애플리케이션을 배포합니다. 이 회사는 애플리케이션의 복원력을 테스트하기 위해 AWS Fault Injection Service(AWS FIS) 실험 템플릿을 만들었습니다. DevOps 엔지니어는 이 실험을 파이프라인에 통합해야 합니다. 어떤 솔루션이 이 요구 사항을 충족시킬까요?
**A.** AWS FIS 작업을 포함하는 파이프라인의 새 단계를 구성합니다. AWS FIS 실험 템플릿을 참조하도록 작업을 구성합니다. 파이프라인에 실험을 시작할 수 있는 권한을 부여합니다.
**B.** Amazon EventBridge 스케줄러를 생성합니다. 스케줄러에 AWS FIS 실험을 시작할 수 있는 권한을 부여합니다. 파이프라인에 EventBridge 스케줄러를 호출하는 작업이 포함된 새 단계를 구성합니다.
**C.** AWS FIS 실험을 시작하는 AWS Lambda 함수를 생성합니다. Lambda 함수에 실험 시작 권한을 부여합니다. 파이프라인에 Lambda 작업이 있는 새 단계를 생성합니다. Lambda 함수를 호출하도록 작업을 설정합니다.
**D.** AWS FIS 실험 템플릿을 Amazon S3 버킷으로 내보냅니다. AWS FIS 실험을 시작하는 빌드 사양이 포함된 AWS CodeBuild 단위 테스트 프로젝트를 생성합니다. CodeBuild 프로젝트에 실험을 시작할 수 있는 권한을 부여합니다. CodeBuild 단위 테스트 프로젝트를 실행하는 작업이 포함된 파이프라인의 새 단계를 구성합니다.
***Answer:*** C

**QUESTION NO: 18**
IT 팀은 회사의 다른 사람들이 애플리케이션을 빠르고 안정적으로 배포하고 종료할 수 있도록 AWS CloudFormation 템플릿을 구축했습니다. 이 템플릿은 사용자 데이터 스크립트를 사용하여 Amazon EC2 인스턴스를 생성하여 애플리케이션을 설치하고 애플리케이션이 실행 중인 동안 정적 웹 페이지를 제공하는 데 사용하는 Amazon S3 버킷을 생성합니다.
CloudFormation 스택이 삭제되면 모든 리소스를 제거해야 합니다. 그러나 팀은 CloudFormation이 스택 삭제 중에 오류를 보고하고 스택에 의해 생성된 S3 버킷이 삭제되지 않음을 관찰합니다.
모든 리소스가 오류 없이 삭제되도록 팀에서 가장 효율적인 방식으로 오류를 해결하려면 어떻게 해야 합니까?
**A.** S3 버킷 리소스에 DelelionPolicy 속성을 추가합니다. Delete 값은 스택이 삭제될 때 버킷이

강제로 제거되도록 합니다.
**B.** S3 버킷 및 IAM 역할을 지정하는 DependsOn 속성이 있는 AWS Lambda 함수로 사용자 지정 리소스를 추가합니다. RequestType이 Delete일 때 버킷에서 모든 객체를 삭제하도록 Lambda 함수를 작성합니다.
**C.** 삭제되지 않은 리소스를 식별합니다. S3 버킷을 수동으로 비운 다음 삭제합니다.
**D.** EC2 및 S3 버킷 리소스를 단일 AWS OpsWorks Stacks 리소스로 교체합니다. 스택에 대한 사용자 지정 레시피를 정의하여 EC2 인스턴스 및 S3 버킷을 생성하고 삭제합니다.
***Answer:*** B
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/cloudformation-s3-custom-resources/

**QUESTION NO: 19**
한 회사가 Amazon EC2 노드 그룹과 함께 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터를 구축했습니다. 이 회사의 DevOps 팀은 Kubernetes Horizontal Pod Autoscaler를 사용하고 있으며, 최근 지원되는 EKS 클러스터 Autoscaler를 설치했습니다.
DevOps 팀은 성능 기준선을 설정하기 위해 EKS 클러스터의 지표와 로그를 수집하는 솔루션을 구현해야 합니다. DevOps 팀은 특정 지표에 대한 초기 임계값을 설정하고, 클러스터 사용에 따라 임계값을 업데이트합니다. 초기 임계값을 초과하거나 EKS 클러스터 Autoscaler가 제대로 작동하지 않는 경우, DevOps 팀은 Amazon Simple Notification Service(Amazon SNS) 이메일 알림을 받아야 합니다.
솔루션은 클러스터, 노드 및 Pod 메트릭을 수집해야 합니다. 또한 Amazon CloudWatch의 로그도 캡처해야 합니다.
이러한 요구 사항을 충족하기 위해 DevOps 팀은 어떤 단계 조합을 거쳐야 합니까? (3가지 선택)
**A.** CloudWatch 에이전트와 Fluent Bit를 클러스터에 배포합니다. EKS 클러스터에 CloudWatch로 메트릭과 로그를 전송할 수 있는 적절한 권한이 있는지 확인합니다.
**B.** AWS Distro for OpenTelemetry를 클러스터에 배포합니다. EKS 클러스터에 CloudWatch로 메트릭과 로그를 전송할 수 있는 적절한 권한이 있는지 확인합니다.
**C.** 클러스터의 CPU, 메모리 및 노드 오류 메트릭을 모니터링하기 위해 CloudWatch 알람을 생성합니다.
임계값을 초과하면 DevOps 팀에 SNS 이메일 알림을 보내도록 알람을 구성합니다.
**D.** 클러스터의 CPU, 메모리 및 노드 메트릭에 대한 메트릭 로그 필터를 모니터링하는 CloudWatch 복합 알람을 생성합니다. 이상 징후가 감지되면 DevOps 팀에 SNS 이메일 알림을 전송하도록 알람을 구성합니다.
**E.** Autoscaler 배포 로그에서 오류를 모니터링하는 CloudWatch 알람을 생성합니다. 임계값을 초과하면 DevOps 팀에 SNS 이메일 알림을 보내도록 알람을 구성합니다.
**F.** Autoscaler 배포의 메트릭 로그 필터를 모니터링하여 오류를 찾아내는 CloudWatch 알람을 생성합니다. 임계값을 초과하면 DevOps 팀에 SNS 이메일 알림을 보내도록 알람을 구성합니다.
***Answer:*** A C F
Explanation:
Deploy CloudWatch Agent + Fluent Bit (supported by Amazon EKS integration) to forward metrics and logs.

Create CloudWatch Alarms for CPU/memory/node metrics and metric log filters for Autoscaler logs, triggering SNS notifications when anomalies occur. This pattern matches AWS guidance on "Monitoring EKS clusters with CloudWatch Container Insights and alarms. "

**QUESTION NO: 20**
성장하는 회사는 AWS Organizations의 조직에서 50개 이상의 계정을 관리합니다. 회사는 로그를 Amazon CloudWatch Logs로 보내도록 애플리케이션을 구성했습니다.
DevOps 엔지니어는 회사가 향후 보안 사고에 대응하기 위해 로그를 빠르게 검색할 수 있도록 로그를 집계해야 합니다. DevOps 엔지니어가 중앙 집중식 모니터링을 위해 새로운 AWS 계정을 만들었습니다.
모니터링 계정에서 애플리케이션 로그를 검색할 수 있도록 DevOps 엔지니어가 수행해야 하는 단계 조합은 무엇입니까? (3개를 선택하세요.)
**A.** 모니터링 계정에서 조직에서 사용할 CloudWatch의 AWS CloudFormation 템플릿을 다운로드합니다. 조직의 마스터 계정에서 CloudFormation StackSets를 사용하여 CloudFormation 템플릿을 전체 조직에 배포합니다.
**B.** IAM 역할을 정의하는 AWS CloudFormation 템플릿을 생성합니다. aws:ResourceAccount 속성이 모니터링 계정 ID와 동일한 경우 로그-amazonaws.com이 로그:링크 작업을 수행할 수 있도록 역할을 구성합니다. 조직의 마스터 계정에서 CloudFormation StackSets를 사용하여 CloudFormation 템플릿을 전체 조직에 배포합니다.
**C.** 모니터링 계정에 IAM 역할을 생성합니다. aws:PrincipalOrgId 속성이 조직 ID와 동일한 경우 log.amazonaws.com이 iam:CreateSink 작업을 수행하도록 허용하는 신뢰 정책을 연결합니다.
**D.** 조직의 마스터 계정에서 조직에 대한 로깅 정책을 활성화합니다.
**E.** 모니터링 계정에서 CloudWatch Observability Access Manager를 사용하여 싱크를 생성합니다. 로그가 모니터링 계정과 공유되도록 허용합니다. 조직 ID에서 관찰 가능성 데이터를 보려면 모니터링 계정 데이터 선택을 구성합니다.
**F.** 모니터링 계정에서 로그 검색을 맡을 수 있는 IAM 역할에 CloudWatchLogsReadOnlyAccess AWS 관리형 정책을 연결합니다.
***Answer:*** B C F
Explanation:
To aggregate logs from multiple accounts in an organization, the DevOps engineer needs to create a cross- account subscription1 that allows the monitoring account to receive log events from the sharing accounts.
To enable cross-account subscription, the DevOps engineer needs to create an IAM role in each sharing account that grants permission to CloudWatch Logs to link the log groups to the destination in the monitoring account2. This can be done using a CloudFormation template and StackSets3 to deploy the role to all accounts in the organization.
The DevOps engineer also needs to create an IAM role in the monitoring account that allows CloudWatch Logs to create a sink for receiving log events from other accounts4. The role must have a trust policy that specifies the organization ID as a condition.
Finally, the DevOps engineer needs to attach the CloudWatchLogsReadOnlyAccess policy5 to an IAM role in the monitoring account that can be used to search the logs from the cross-account subscription.
1: Cross-account log data sharing with subscriptions 2: Create an IAM role for CloudWatch

Logs in each sharing account 3: AWS CloudFormation StackSets 4: Create an IAM role for CloudWatch Logs in your monitoring account 5: CloudWatchLogsReadOnlyAccess policy

**QUESTION NO: 21**
한 회사가 Amazon Elastic Kubernetes Service(Amazon EKS)에서 마이크로서비스 애플리케이션을 운영하고 있습니다. 최근 사용자들은 계정 요약 기능에 접속하는 데 상당한 지연이 발생했다고 보고했는데, 특히 업무량이 많은 시간대에 지연이 심화되었다고 합니다. DevOps 엔지니어는 Amazon CloudWatch 지표와 로그를 사용하여 문제를 해결했습니다. 로그는 EKS 노드의 CPU 및 메모리 사용률이 정상임을 나타냈습니다. DevOps 엔지니어는 마이크로서비스 아키텍처 내에서 지연이 발생한 위치를 파악하지 못했습니다.
DevOps 엔지니어는 지연이 발생하는 지점을 정확히 파악하기 위해 애플리케이션의 관찰성을 높여야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족할까요?
**A.** AWS X-Ray 데몬을 EKS 클러스터에 DaemonSet으로 배포합니다. X-Ray SDK를 사용하여 애플리케이션 코드를 계측합니다. 애플리케이션을 다시 배포합니다.
**B.** EKS 클러스터에 대해 CloudWatch Container Insights를 활성화합니다. Container Insights 데이터를 사용하여 지연을 진단합니다.
**C.** 기존 CloudWatch 지표를 기반으로 알람을 생성합니다. 이메일 알림을 전송하기 위해 Amazon Simple Notification Service(Amazon SNS) 주제를 설정합니다.
**D.** 네트워크 작업에 대한 애플리케이션 코드의 시간 초과 설정을 늘려 작업이 완료될 때까지 더 많은 시간을 확보합니다.
***Answer:*** A
Explanation:
AWS X-Ray provides distributed tracing for microservice-based applications. Deploying the X-Ray daemon as a DaemonSet in the EKS cluster and instrumenting the application with the X-Ray SDK enables end-to-end tracing across microservices, helping identify performance bottlenecks. This method is documented in "Using AWS X-Ray with Amazon EKS" (AWS Observability Guide).

**QUESTION NO: 22**
한 회사가 AWS CodeConnections 호환 Git 저장소에 애플리케이션 코드를 보관하고 있습니다. 이 회사는 풀 리퀘스트가 열릴 때 단위 테스트가 실행되도록 구성하려고 합니다. 또한, 테스트가 완료되면 풀 리퀘스트에 테스트 상태가 표시되도록 하려고 합니다. 또한, 테스트가 완료된 후 테스트에서 생성된 출력 데이터 파일을 Amazon S3 버킷에 저장하려고 합니다. 이러한 요구 사항을 충족하는 솔루션 조합은 무엇입니까? (세 가지 선택)
**A.** 테스트를 실행하는 데 필요한 리소스에 대한 액세스를 허용하는 IAM 서비스 역할을 만듭니다.
**B.** AWS CodePipeline에 테스트 단계가 있는 파이프라인을 생성합니다. 풀 리퀘스트가 생성되거나 업데이트될 때 파이프라인을 실행하는 트리거를 생성합니다. 테스트 결과를 보고하는 소스 작업을 추가합니다.
**C.** 테스트를 실행할 AWS CodeBuild 프로젝트를 생성합니다. 풀 리퀘스트가 생성되거나 업데이트될 때 테스트를 실행하려면 웹훅 트리거를 활성화합니다. 테스트 결과를 보고하려면 빌드 상태 보고를 활성화합니다.
**D.** 테스트 실행이 완료되면 출력 파일을 업로드할 보고서 섹션이 있는 buildspec.yml 파일을 만듭니다.

**E.** 테스트 실행이 완료되면 아티팩트를 업로드할 아티팩트 섹션이 있는 buildspec.yml 파일을 만듭니다.
**F.** 테스트 실행이 완료되면 출력 파일을 업로드할 파일 섹션이 있는 appspec.yml 파일을 만듭니다.
***Answer:*** A C E

**QUESTION NO: 23**
한 회사는 컨테이너화된 인프라의 모든 이미지에 Amazon Elastic Container Registry(Amazon ECR)를 사용합니다. 회사는 외부 이미지 레지스트리에서 이미지를 가져올 때 제한을 방지하기 위해 /external 접두사가 붙은 풀스루 캐시 기능을 사용합니다. 또한, AWS Organizations를 계정 관리에 사용합니다.
레지스트리의 모든 이미지는 사전 프로비저닝된 특정 AWS Key Management Service(AWS KMS) 키로 암호화되어야 합니다. 회사에서 내부적으로 생성한 이미지는 이미 이 정책을 준수하고 있습니다.
하지만 캐시된 외부 이미지는 Amazon S3 관리 키(SSE-S3)를 사용하는 서버 측 암호화를 사용합니다.
회사는 규정을 준수하지 않는 캐시 저장소를 제거해야 합니다. 또한 모든 새로운 풀스루 캐시 저장소가 필수 KMS 키로 자동 암호화되도록 하는 보안 솔루션을 구현해야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족시킬까요?
**A.** AWS Config를 구성합니다. Guard 구문을 사용하는 사용자 지정 규칙을 추가합니다. 새 저장소에 KMS 암호화를 활성화하는 규칙을 작성합니다.
**B.** 접두사에 대한 ECR 저장소 생성 템플릿을 구성합니다. KMS 키를 지정합니다. 저장소가 다시 채워질 때까지 기다립니다.
**C.** 모든 ECR 저장소가 KMS 암호화되도록 요구하는 모든 AWS 계정에 대한 SCP를 구성합니다.
**D.** 모든 "ECR Pull Through Cache Action" 이벤트에서 트리거되는 새로운 Amazon EventBridge 규칙을 만듭니다. AWS KMS를 규칙 대상으로 설정합니다.
***Answer:*** B
Explanation:
For pull through cache repositories, Amazon ECR now supports repository creation templates that can be applied to a registry prefix, such as /external . These templates define default settings, including encryption configuration with a specific KMS key , tag immutability, scan on push, and more. When new cache repositories are auto-created under that prefix, they inherit the template settings automatically.
In this scenario, existing external cache repositories are noncompliant because they use SSE-S3. The company can delete those repositories (removing the noncompliant caches) and configure an ECR repository creation template for the /external prefix that specifies the required customer managed KMS key. As new images are pulled, ECR recreates the cache repositories under that prefix with KMS encryption using the specified key , guaranteeing compliance going forward.
Option A (AWS Config) would only detect noncompliance after creation and cannot enforce encryption at creation time. Option C (SCP) cannot directly control repository encryption properties. Option D misuses EventBridge; KMS cannot be a "target" that retroactively encrypts repositories.
Therefore, using an ECR repository creation template with the desired KMS key is the

correct, automatic, and secure solution.

**QUESTION NO: 24**
한 회사가 AWS Organizations에 조직을 보유하고 있습니다. DevOps 엔지니어는 조직 내 여러 OU에 속한 여러 AWS 계정을 관리해야 합니다. 계정 내의 1AM 정책 및 Amazon S3 정책을 포함한 모든 리소스는 AWS CloudFormation을 통해 배포됩니다. 모든 템플릿과 코드는 AWS CodeCommit 리포지토리에 저장됩니다. 최근 일부 개발자들이 조직 내 특정 계정에서 S3 버킷에 접근할 수 없는 문제가 발생하고 있습니다.
다음 정책이 S3 버킷에 연결됩니다.
DevOps 엔지니어는 이 접근 권한 문제를 해결하기 위해 무엇을 해야 할까요?
**A.** S3 버킷 정책을 수정합니다. S3 버킷에서 "S3 공개 액세스 차단" 설정을 해제합니다. S3 정책에 awsSourceAccount 조건을 추가합니다. 문제가 발생하는 모든 개발자의 AWS 계정 ID를 추가합니다.
**B.** 1AM 권한 경계로 인해 개발자가 S3 버킷에 액세스할 수 없는지 확인합니다. 필요한 경우 IAM 권한 경계를 변경합니다. 문제가 발생하는 개별 개발자 계정에서 AWS Config 레코더를 사용하여 액세스를 차단하는 변경 사항을 되돌립니다.
수정 사항을 CodeCommit 저장소에 다시 커밋합니다. Cloud Formation을 통해 배포를 실행하여 변경 사항을 적용합니다.
**C.** 개발자 OU에서 1AM 리소스를 수정하지 못하도록 SCP를 구성합니다. S3 정책에 awsSourceAccount 조건을 추가합니다. 문제가 발생하는 모든 개발자의 AWS 계정 ID를 추가합니다. 수정 사항을 CodeCommit 저장소에 커밋합니다. CloudFormation을 통해 배포를 실행하여 변경 사항을 적용합니다.
**D.** SCP가 개발자의 S3 버킷 접근을 차단하지 않는지 확인합니다. 1AM 정책 권한 경계가 개발자 1AM 사용자의 접근을 거부하지 않는지 확인합니다. CodeCommit 저장소에서 SCP 및 1AM 정책 권한 경계를 필요한 대로 변경합니다. CloudFormation을 통해 배포를 실행하여 변경 사항을 적용합니다.
***Answer:*** D
Explanation:
Verify No SCP Blocking Access:
Ensure that no Service Control Policy (SCP) is blocking access for developers to the S3 bucket. SCPs are applied at the organization or organizational unit (OU) level in AWS Organizations and can restrict what actions users and roles in the affected accounts can perform.
Verify No IAM Policy Permissions Boundaries Blocking Access:
IAM permissions boundaries can limit the maximum permissions that a user or role can have. Verify that these boundaries are not restricting access to the S3 bucket.
Make Necessary Changes to SCP and IAM Policy Permissions Boundaries:
Adjust the SCPs and IAM permissions boundaries if they are found to be the cause of the access issue. Make sure these changes are reflected in the code maintained in the AWS CodeCommit repository.
Invoke Deployment Through CloudFormation:
Commit the updated policies to the CodeCommit repository.
Use AWS CloudFormation to deploy the changes across the relevant accounts and resources to ensure that the updated permissions are applied consistently.
By ensuring no SCPs or IAM policy permissions boundaries are blocking access and making

necessary changes if they are, the DevOps engineer can resolve the access issue for developers trying to access the S3 bucket.
References:
AWS SCPs
IAM Permissions Boundaries
Deploying CloudFormation Templates

**QUESTION NO: 25**
회사에는 단일 공유 AWS 계정에서 작업하는 여러 개발 그룹이 있습니다. 그룹의 수석 관리자는 리소스 생성이 계정의 서비스 제한에 접근할 때 타사 API 호출을 통해 경고를 받기를 원합니다.
최소한의 개발 노력으로 이를 달성할 수 있는 솔루션은 무엇입니까?
**A.** 주기적으로 실행되고 AWS Lambda 함수를 대상으로 하는 Amazon CloudWatch 이벤트 규칙을 생성합니다. Lambda 함수 내에서 AWS 환경의 현재 상태를 평가하고 배포된 리소스 값을 계정의 리소스 제한과 비교합니다. 계정이 서비스 한도에 가까워지면 고위 관리자에게 알리십시오.
**B.** AWS Trusted Advisor 검사를 새로 고치는 AWS Lambda 함수를 배포하고 Lambda 함수를 주기적으로 실행하도록 Amazon CloudWatch Events 규칙을 구성합니다. Trusted Advisor 이벤트 및 대상 Lambda 함수와 일치하는 이벤트 패턴을 사용하여 또 다른 CloudWatch 이벤트 규칙을 생성합니다. 대상 Lambda 함수에서 수석 관리자에게 알립니다.
**C.** AWS Personal Health Dashboard 검사를 새로 고치는 AWS Lambda 함수를 배포하고 Lambda 함수를 주기적으로 실행하도록 Amazon CloudWatch Events 규칙을 구성합니다. Personal Health Dashboard 이벤트 및 대상 Lambda 함수와 일치하는 이벤트 패턴을 사용하여 또 다른 CloudWatch 이벤트 규칙을 생성합니다. 대상 Lambda 함수에서 수석 관리자에게 알립니다.
**D.** 주기적으로 실행되고, AWS 서비스 제한 상태를 확인하고, 알림을 Amazon SNS 주제로 스트리밍하는 AWS Config 사용자 지정 규칙을 추가합니다. 선임 관리자에게 알리는 AWS Lambda 함수를 배포하고 SNS 주제에 Lambda 함수를 구독합니다.
***Answer:*** B
Explanation:
To meet the requirements, the company needs to create a solution that alerts the Senior Manager when the creation of resources approaches the service limits for the account with the least amount of development effort. The company can use AWS Trusted Advisor, which is a service that provides best practice recommendations for cost optimization, performance, security, and service limits. The company can deploy an AWS Lambda function that refreshes Trusted Advisor checks, and configure an Amazon CloudWatch Events rule to run the Lambda function periodically. This will ensure that Trusted Advisor checks are up to date and reflect the current state of the account. The company can then create another CloudWatch Events rule with an event pattern matching Trusted Advisor events and a target Lambda function. The event pattern can filter for events related to service limit checks and their status. The target Lambda function can notify the Senior Manager via a third-party API call if the event indicates that the account is approaching or exceeding a service limit.

**QUESTION NO: 26**
회사는 AWS Organizations에서 조직의 모든 기능을 활성화했습니다. 조직에는 10개의 AWS

계정이 있습니다. 회사는 모든 계정에서 AWS CloudTrail을 켰습니다. 이 회사는 내년에 조직의 AWS 계정 수가 500개로 증가할 것으로 예상합니다. 회사는 이러한 계정에 대해 여러 OU를 사용할 계획입니다.
회사는 조직의 각 기존 AWS 계정에서 AWS Config를 활성화했습니다. DevOps 엔지니어는 조직에서 생성되는 모든 향후 AWS 계정에 대해 자동으로 AWS Config를 활성화하는 솔루션을 구현해야 합니다.
이 요구 사항을 충족하는 솔루션은 무엇입니까?

**A.** 조직의 마스터 계정에서 CreateAccount API 호출에 반응하는 Amazon EventBridge 규칙을 생성합니다. 조직의 AWS Config에 대한 신뢰할 수 있는 액세스를 활성화하는 AWS Lambda 함수를 호출하도록 규칙을 구성합니다.

**B.** 조직의 마스터 계정에서 AWS Config를 활성화하도록 설정된 AWS CloudFormation 스택을 생성합니다. 조직을 통해 계정이 생성될 때 자동으로 배포되도록 스택 세트를 구성합니다.

**C.** 조직의 마스터 계정에서 AWS Config를 활성화하기 위해 적절한 AWS Config API 호출을 허용하는 SCP를 생성합니다. SCP를 루트 수준 OU에 적용합니다.

**D.** 조직의 마스터 계정에서 CreateAccount API 호출에 반응하는 Amazon EventBridge 규칙을 생성합니다. 계정에 대해 AWS Config를 활성화하기 위해 AWS Systems Manager Automation Runbook을 호출하는 규칙을 구성합니다.

***Answer:*** B

Explanation:

https://aws.amazon.com/about-aws/whats-new/2020/02/aws-cloudformation-stacksets-introduces-automatic- deployments-across-accounts-and-regions-through-aws-organizations/

**QUESTION NO: 27**

한 회사에서 Amazon EC2 시작 유형으로 Amazon Elastic Container Service(Amazon ECS)를 사용합니다. 이 회사는 모든 로그 데이터를 Amazon CloudWatch에 중앙 집중화해야 합니다. 이 회사의 ECS 작업에는 로그 드라이버 이름으로 awslogs 값을 지정하는 LogConfiguration 객체가 포함됩니다.
회사의 ECS 작업 배포에 실패했습니다. 오류 메시지는 권한 누락으로 인해 실패했음을 나타냅니다. 회사는 컨테이너 인스턴스를 시작하는 데 사용된 IAM 역할에 다음 로그가 포함되어 있음을 확인했습니다.
CreateLogGroup, logs:CreateLogStream, logs:PutLogEvents 권한.
어떤 해결책이 문제를 해결할 수 있을까?

**A.** Amazon ECS를 신뢰할 수 있는 서비스로 설정하는 IAM 역할에 IAM 신뢰 정책을 추가합니다.

**B.** IAM 역할에 적용된 정책에 logs:PutDestination 권한을 추가합니다.

**C.** IAM 역할에 적용된 정책에서 logs:CreateLogStream 권한을 제거합니다.

**D.** CloudWatch를 신뢰할 수 있는 서비스로 설정하는 IAM 역할에 IAM 신뢰 정책을 추가합니다.

***Answer:*** A

Explanation:

When using the awslogs log driver with ECS on EC2, the ECS agent running on the container instance uses the instance's IAM role (container instance role or task execution role, depending on configuration) to write logs to CloudWatch Logs. The policy already grants logs:CreateLogGroup , logs:CreateLogStream , and logs:

PutLogEvents , which are the required CloudWatch Logs actions. However, for the role to be usable by ECS, the role's trust policy must allow the appropriate service principal to assume it.
In this question, the error message indicates "missing permission" during ECS task deployment. If the IAM role is not trusted by the ECS service (for example, ecs-tasks.amazonaws.com for a task execution role or the proper principal for container instances), ECS cannot assume that role and therefore cannot use the granted CloudWatch permissions, causing deployment failures.
Option A addresses this by adding a trust relationship so that Amazon ECS can assume the IAM role. Options B and C mutate the permissions but do not fix the underlying problem: the missing trust. Option D incorrectly attempts to trust CloudWatch, which does not assume roles in this context.
Thus, adding a trust policy that establishes ECS as a trusted service is the correct fix.

**QUESTION NO: 28**
한 회사에서 트렁크 기반 개발 브랜칭 전략을 사용합니다. 이 회사에는 Git 제공자와 통합된 두 개의 AWS CodePipeline 파이프라인이 있습니다. pull_request 파이프라인에는 기능 브랜치와 일치하는 브랜치 필터가 있습니다. main_branch 파이프라인에는 기본 브랜치와 일치하는 브랜치 필터가 있습니다.
풀 리퀘스트가 메인 브랜치에 병합되면, 해당 풀 리퀘스트는 main_branch 파이프라인을 통해 배포됩니다. 회사 개발자들은 제출된 모든 풀 리퀘스트에 대한 테스트 결과를 pull_request 파이프라인에서 최대한 빨리 받아야 합니다. 회사는 다음 파이프라인 실행 전에 main_branch 파이프라인의 테스트 결과가 완료되고 각 배포가 완료되도록 하려고 합니다.
어떤 솔루션이 이러한 요구 사항을 충족할까요?
**A.** SUPERSEDED 모드를 사용하도록 pull_request 파이프라인을 구성합니다. QUEUED 모드를 사용하도록 main_branch 파이프라인을 구성합니다.
**B.** pull_request 파이프라인을 PARALLEL 모드를 사용하도록 구성합니다. main_branch 파이프라인을 QUEUED 모드를 사용하도록 구성합니다.
**C.** pull_request 파이프라인을 PARALLEL 모드를 사용하도록 구성합니다. main_branch 파이프라인을 SUPERSEDED 모드를 사용하도록 구성합니다.
**D.** pull_request 파이프라인을 QUEUED 모드를 사용하도록 구성합니다. main_branch 파이프라인을 SUPERSEDED 모드를 사용하도록 구성합니다.
***Answer:*** B
Explanation:
In CodePipeline's execution mode,
* PARALLEL mode for pull_request pipelines ensures that multiple feature branches can be tested simultaneously for quick feedback.
* QUEUED mode for main_branch ensures deployments run sequentially - each must finish before the next begins, preventing overlap. This configuration aligns with AWS CodePipeline best practices for trunk-based development and concurrent test pipelines.

**QUESTION NO: 29**
전자 건강 기록을 사용하는 회사는 Amazon Linux 운영 체제에서 Amazon EC2 인스턴스 플릿을 실행하고 있습니다. 환자 개인 정보 보호 요구 사항의 일환으로 회사는 EC2 인스턴스에서 실행되는 운영 체제 및 애플리케이션의 패치에 대한 지속적인 규정 준수를

보장해야 합니다.
기본 및 사용자 지정 리포지토리를 사용하여 운영 체제 및 애플리케이션 패치의 배포를 어떻게 자동화할 수 있습니까?

**A.** AWS Systems Manager를 사용하여 사용자 지정 리포지토리를 포함하는 새 패치 기준을 생성합니다. run 명령을 사용하여 AWS-RunPatchBaseline 문서를 실행하여 패치를 확인하고 설치합니다.

**B.** AWS Direct Connect를 사용하여 회사 리포지토리를 통합하고 Amazon CloudWatch 예약 이벤트를 사용하여 패치를 배포한 다음 CloudWatch 대시보드를 사용하여 보고서를 생성합니다.

**C.** yum-config-manager를 사용하여 /etc/yum.repos.d 아래에 사용자 지정 리포지토리를 추가하고 yum-config-manager-enable을 실행하여 리포지토리를 활성화합니다.

**D.** AWS Systems Manager를 사용하여 회사 리포지토리를 포함하는 새 패치 기준을 생성합니다. run 명령을 사용하여 AWS-AmazonLinuxDefaultPatchBaseline 문서를 실행하여 패치를 확인하고 설치합니다.

***Answer:*** A
Explanation:
https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-how-it-works-alt-source- repository.html

**QUESTION NO: 30**
한 회사가 S3를 사용하여 이미지를 저장하고 있으며, 양방향 복제 및 15분 이내의 지연 시간을 지원하는 다중 지역 재해 복구(DR) 환경이 필요합니다.
다음 단계 중 어떤 단계가 요구 사항을 충족합니까? (세 가지를 선택하십시오.)

**A.** 각 복제 규칙에 대해 S3 복제 시간 제어(RTC)를 활성화합니다.

**B.** S3 다중 지역 액세스 포인트(액티브/패시브)를 생성합니다.

**C.** 장애 조치 중에 SubmitMultiRegionAccessPointRoutes를 호출합니다.

**D.** S3 전송 가속을 활성화합니다.

**E.** 53번 경로 ARC 라우팅 제어를 사용합니다.

**F.** 장애 조치 중에 트래픽을 전환하려면 Route 53 ARC를 사용하십시오.

***Answer:*** A B C
* S3 RTC ensures #15-min replication SLA.
* Multi-Region Access Point (MRAP) simplifies active-passive replication access.
* SubmitMultiRegionAccessPointRoutes API manages routing changes during failover. This configuration follows AWS DR best practices for S3 active/passive architectures.

**QUESTION NO: 31**
AWS Organizations의 회사 조직에는 단일 OU가 있습니다. 회사는 OU 계정에서 Amazon EC2 인스턴스를 실행합니다. 회사는 각 EC2 인스턴스의 자격 증명 사용을 자격 증명이 할당된 특정 EC2 인스턴스로 제한해야 합니다. DevOps 엔지니어는 EC2 인스턴스에 대한 보안을 구성해야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족시킬까요?

**A.** VPC CIDR 블록을 지정하는 SCP를 만듭니다. SCP를 구성하여 aws:VpcSourceIp 조건 키의 값이 지정된 블록에 있는지 확인합니다. 동일한 SCP 확인에서 aws:EC2InstanceSourcePrivateIPv4 및 aws:SourceVpc 조건 키의 값이 동일한지 확인합니다.

두 조건 중 하나가 거짓이면 액세스를 거부합니다. SCP를 OU에 적용합니다.
**B.** aws:EC2InstanceSourceVPC 및 aws:SourceVpc 조건 키의 값이 같은지 확인하는 SCP를 만듭니다. 값이 같지 않으면 액세스를 거부합니다. 동일한 SCP 확인에서 aws:EC2InstanceSourcePrivateIPv4 및 awsVpcSourceIp 조건 키의 값이 같은지 확인합니다. 값이 같지 않으면 액세스를 거부합니다. SCP를 OU에 적용합니다.
**C.** 허용 가능한 VPC 값 목록을 포함하고 aws의 값이 다음인지 확인하는 SCP를 만듭니다. SourceVpc 조건 키가 목록에 있습니다. 동일한 SCP 확인에서 허용 가능한 IP 주소 값 목록을 정의하고 aws:VpcSourceIp 조건 키 값이 목록에 있는지 확인합니다. 두 조건 중 하나가 거짓이면 액세스를 거부합니다. 조직의 각 계정에 SCP를 적용합니다.
**D.** aws:EC2InstanceSourceVPC 및 aws:VpcSourceIp 조건 키의 값이 같은지 확인하는 SCP를 만듭니다. 값이 같지 않으면 액세스를 거부합니다. 동일한 SCP 확인에서 aws:EC2InstanceSourcePrivatoIPv4 및 aws:SourceVpc 조건 키의 값이 같은지 확인합니다. 값이 같지 않으면 액세스를 거부합니다. 조직의 각 계정에 SCP를 적용합니다.
***Answer:*** B
Explanation:
Step 1: Using Service Control Policies (SCPs) for EC2 SecurityTo limit the use of EC2 instance credentials to the specific EC2 instance they are assigned to, you can create a Service Control Policy (SCP) that verifies specific conditions, such as whether the EC2 instance ' s source VPC and private IP match expected values.
Action: Create an SCP that checks whether the values of the aws:EC2InstanceSourceVPC and aws:
SourceVpc condition keys are the same. Deny access if they are not.
Why: This ensures that credentials cannot be used outside the designated EC2 instance or VPC.
Step 2: Further Validation with Private IPsThe SCP should also verify that the EC2 instance ' s private IP matches the IP range specified for the VPC. If the instance ' s private IP does not match, access should be denied.
Action: In the same SCP, check whether the values of the aws:EC2InstanceSourcePrivateIP and aws:
VpcSourceIP condition keys are the same. Deny access if they are not.
Why: This ensures that the credentials are only used within the specific EC2 instance and its associated VPC.
Reference: AWS documentation on Service Control Policies (SCPs).
This corresponds to Option B: Create an SCP that checks whether the values of the aws: EC2InstanceSourceVPC and aws:SourceVpc condition keys are the same. Deny access if the values are not the same. In the same SCP check, check whether the values of the aws:EC2InstanceSourcePrivateIP and aws:
VpcSourceIP condition keys are the same. Deny access if the values are not the same. Apply the SCP to the OU.

**QUESTION NO: 32**
한 회사가 AWS에서 웹 애플리케이션을 구축하고 있습니다. 이 애플리케이션은 AWS CodeConnections를 사용하여 Git 저장소에 접근합니다. 회사는 AWS CodePipeline에 파이프라인을 설정하여 메인 브랜치에 코드를 푸시할 때 애플리케이션을 자동으로 빌드하고 스테이징 환경에 배포합니다. 파이프라인에 자동화된 테스트가 통합되어 있지 않아 메인

브랜치에서 버그와 통합 문제가 발생하는 경우가 있습니다.
이 회사는 Git 저장소에서 코드 병합이 발생할 때 자동으로 테스트를 실행하고, 테스트가 실패할 경우 배포가 스테이징 환경에 도달하지 않도록 하려고 합니다. 테스트는 최대 20분까지 실행될 수 있습니다. 이러한 요구 사항을 충족하는 솔루션은 무엇일까요?
**A.** 파이프라인에 AWS CodeBuild 작업을 추가합니다. Git 저장소에 buildspec.yml 파일을 추가하여 테스트 실행 명령을 정의합니다. 테스트가 실패하면 배포를 중지하도록 파이프라인을 구성합니다.
**B.** 각 코드 병합 시 AWS Lambda 함수를 실행하도록 Git 웹훅을 구성합니다. Lambda 함수가 프로그래밍 방식으로 테스트를 실행하고 테스트가 실패하면 파이프라인을 중지하도록 구성합니다.
**C.** 테스트 환경의 Docker 이미지를 사용하도록 AWS Batch를 구성합니다. AWS Batch를 파이프라인에 통합합니다. 배치 작업을 제출하고 테스트가 실패하면 코드 병합을 되돌리는 AWS Lambda 함수를 파이프라인에 추가합니다.
**D.** 각 코드 병합 시 Amazon S3 버킷에 코드를 푸시하도록 Git 저장소를 구성합니다. S3 이벤트 알림을 사용하여 테스트를 시작하고 테스트가 실패할 경우 코드 병합을 되돌립니다.
***Answer:*** A
Explanation:
AWS CodePipeline supports multiple stages including source, build, test, and deploy. The most efficient way to integrate automated testing is by adding an AWS CodeBuild action to the pipeline that runs the tests using a buildspec.yml file. CodeBuild can be configured to fail the pipeline automatically if tests fail, ensuring that deployments do not proceed to the staging environment. This pattern is directly supported and documented in AWS CodePipeline + CodeBuild CI/CD architecture guidance.

**QUESTION NO: 33**
한 회사가 새벽 1시 정책을 검토하고 있습니다. DevOps 엔지니어가 작성한 정책 중 하나가 너무 관대하다는 이유로 보류되었습니다. 이 정책은 주말 동안 Environment: NonProducion 태그가 지정된 Amazon EC2 인스턴스에 중지 명령을 내리는 AWS Lambda 함수에서 사용됩니다. 현재 정책은 다음과 같습니다.
엔지니어는 최소한의 권한 부여 정책을 달성하기 위해 어떤 변경 사항을 적용해야 할까요? (세 가지를 선택하세요.)
**A.** 옵션 A
**B.** 옵션 B
**C.** 옵션 C
**D.** 옵션 D
**E.** 옵션 E
**F.** 옵션 F
***Answer:*** A B D
Explanation:
The engineer should make the following changes to achieve a policy of least permission:
A: Add a condition to ensure that the principal making the request is an AWS Lambda function. This ensures that only Lambda functions can execute this policy.
B: Narrow down the resources by specifying the ARN of EC2 instances instead of allowing all resources. This ensures that the policy only affects EC2 instances.

D: Add a condition to ensure that this policy only applies to EC2 instances tagged with "Environment:
NonProduction". This ensures that production environments are not affected by this policy.
AWS Identity and Access Management (IAM) - AWS Documentation
Certified DevOps Engineer - Professional (DOP-C02) Study Guide (page 179)

**QUESTION NO: 34**
회사는 AWS CloudFormation 스택을 사용하여 애플리케이션에 업데이트를 배포합니다. 스택은 서로 다른 리소스로 구성됩니다. 리소스에는 AWS Auto Scaling 그룹, Amazon EC2 인스턴스, Application Load Balancer(ALB) 및 독립 스택을 시작하고 유지 관리하는 데 필요한 기타 리소스가 포함됩니다. CloudFormation 스택 업데이트 외부의 애플리케이션 리소스에 대한 변경은 허용되지 않습니다.
이 회사는 최근 AWS CLI를 사용하여 애플리케이션 스택 업데이트를 시도했습니다. 스택 업데이트에 실패하고 다음 오류 메시지가 생성되었습니다. 스택은 UPDATE_ROLLBACK_FAILED 상태로 유지됩니다. * 이 문제를 해결하는 솔루션은 무엇입니까?
**A.** ALB에 대해 구성된 서브넷 매핑을 업데이트합니다. aws cloudformation update-stack-set AWS CLI 명령을 실행합니다.
**B.** 스택을 업데이트하는 데 필요한 권한을 제공하여 1AM 역할을 업데이트합니다. aws cloudformation continue-update-rollback AWS CLI 명령을 실행합니다.
**C.** 계정의 EC2 인스턴스 수에 대한 할당량 증가 요청을 제출합니다. aws cloudformation cancel-update-stack AWS CLI 명령을 실행합니다.
**D.** Auto Scaling 그룹 리소스를 삭제합니다. aws cloudformation rollback-stack AWS CLI 명령을 실행합니다.
***Answer:*** B
Explanation:
https://repost.aws/knowledge-center/cloudformation-update-rollback-failed If your stack is stuck in the UPDATE_ROLLBACK_FAILED state after a failed update, then the only actions that you can perform on the stack are the ContinueUpdateRollback or DeleteStack operations.

**QUESTION NO: 35**
회사의 DevOps 팀은 AWS Organizations의 조직에 있는 일련의 AWS 계정을 관리합니다. 회사에는 모든 Amazon EC2 인스턴스가 DevOps 팀이 관리하는 승인된 AMI를 사용하도록 보장하는 솔루션이 필요합니다. 또한 솔루션은 승인되지 않은 AMI의 사용을 수정해야 합니다. 개별 계정 관리자는 승인된 AMI 사용에 대한 제한을 제거할 수 없어야 합니다.
이러한 요구 사항을 충족하는 솔루션은 무엇입니까?
**A.** AWS CloudFormation StackSets를 사용하여 Amazon EventBridge 규칙을 각 계정에 배포합니다. Amazon EC2에 대한 AWS CloudTrail 이벤트에 반응하고 Amazon Simple Notification Service(Amazon SNS) 주제에 알림을 보내도록 규칙을 구성합니다. DevOps 팀의 SNS 주제 구독
**B.** AWS CloudFormation StackSets를 사용하여 Approved-amis-by-id AWS Config 관리형 규칙을 각 계정에 배포합니다. 승인된 AMI 목록을 사용하여 규칙을 구성합니다. 비준수 EC2 인스턴스에 대해 AWS-StopEC2Instance AWS 시스템 관리자 자동화 Runbook을 실행하도록 규칙을 구성합니다.

**C.** Amazon EC2에 대한 AWS CloudTrail 이벤트를 처리하는 AWS Lambda 함수를 생성합니다. Amazon Simple Notification Service(Amazon SNS) 주제에 알림을 보내도록 Lambda 함수를 구성합니다. DevOps 팀의 SNS 주제를 구독하세요. 조직의 각 계정에 Lambda 함수 배포 각 계정에 Amazon EventBridge 규칙 생성 Amazon EC2에 대한 AWS CloudTrail 이벤트에 반응하고 Lambda 함수를 호출하도록 EventBridge 규칙을 구성합니다.
**D.** 조직 전체에서 AWS Config 활성화 승인된 AMI 목록과 함께 승인된 -amis-by-id AWS Config 관리 규칙을 사용하는 적합성 팩을 생성합니다. 조직 전체에 적합성 팩을 배포합니다. 비준수 EC2 인스턴스에 대해 AWS-StopEC2Instance AWS 시스템 관리자 자동화 Runbook을 실행하도록 규칙을 구성합니다.

***Answer:*** D

Explanation:

Enable AWS Config Across the Organization:

AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. It can be used to assess, audit, and evaluate the configurations of your resources. Enabling AWS Config across the organization ensures that all accounts are monitored for compliance.

Create a Conformance Pack Using the approved-amis-by-id AWS Config Managed Rule:

A conformance pack is a collection of AWS Config rules and remediation actions that can be easily deployed across an organization.

The approved-amis-by-id managed rule checks whether running instances are using approved AMIs.

Deploy the Conformance Pack Across the Organization:

Deploying the conformance pack across the organization ensures that all accounts adhere to the policy of using only approved AMIs.

The conformance pack can be deployed via the AWS Management Console, CLI, or SDKs.

Configure the Rule to Run the AWS-StopEC2Instance AWS Systems Manager Automation Runbook for Non- Compliant EC2 Instances:

The AWS-StopEC2Instance runbook can be configured to automatically stop any EC2 instances that are found to be non-compliant (i.e., not using approved AMIs).

This remediation action ensures that any unauthorized instances are promptly stopped, enforcing the policy without manual intervention.

By following these steps, the solution ensures that all EC2 instances across the organization use approved AMIs, and any non-compliant instances are remediated automatically.

References:

AWS Config Conformance Packs

AWS Config Managed Rules

AWS Systems Manager Automation Runbooks