1. Amazon Linux EC2 인스턴스에서 실행되는 애플리케이션은 AWS 인프라를 관리해야 합니다.

   AWS API를 안전하게 호출하도록 EC2 인스턴스를 구성하려면 어떻게 해야 합니까?

   > 필요한 권한이 있는 EC2 인스턴스의 역할을 지정합니다.

- "We designed IAM roles so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use.

2. AWS X-Ray로 Lambda 기반 애플리케이션을 추적하려면 무엇이 필요합니까?

   > IAM 실행 역할을 사용하여 Lambda 함수 권한을 부여하고 추적을 활성화합니다.

- Your function needs permission to upload trace data to X-Ray. When you enable active tracing in the Lambda console, Lambda adds the required permissions to your function's execution role. Otherwise, add the AWSXRayDaemonWriteAccess policy to the execution role.

3. 회사는 AWS Fargate 컨테이너에서 수백 개의 보안 서비스를 실행하는 Amazon Elastic Container Service(Amazon ECS) 클러스터에 웹 애플리케이션을 가지고 있습니다. 서비스는 ALB(Application Load Balancer)가 라우팅하는 대상 그룹에 있습니다. 애플리케이션 사용자는 웹사이트에 익명으로 로그인하지만 보안 서비스에 액세스하려면 OpenID Connect 프로토콜 호환 ID 공급자(IdP)를 사용하여 인증되어야 합니다.

   최소한의 노력으로 이러한 요구 사항을 충족하는 인증 방법은 무엇입니까?

> Amazon Cognito를 사용하도록 서비스를 구성합니다.

4. 여러 AWS 계정을 감사하기 위한 애플리케이션을 개발 중입니다. 애플리케이션은 계정 A에서 실행되며 계정 B와 C의 AWS 서비스에 액세스해야 합니다.

   애플리케이션이 각 감사 계정에서 AWS 서비스를 호출할 수 있도록 하는 가장 안전한 방법은 무엇입니까?

   > 각 감사 계정에서 교차 계정 역할을 구성합니다. 해당 역할을 맡는 계정 A에 코드 작성

- This tutorial teaches you how to use a role to delegate access to resources that are in different AWS accounts that you own (Production and Development). You share resources in one account with users in a different account. By setting up cross-account access in this way, you don't need to create individual IAM users in each account. In addition, users don't have to sign out of one account and sign into another in order to access resources in different AWS accounts. After configuring the role, you see how to use the role from the AWS Management Console, the AWS CLI, and the API."

5. 개발자는 Amazon DynamoDB 테이블과 상호 작용하는 AWS Lambda 함수로 Amazon API Gateway REST API 백엔드를 사용하여 애플리케이션을 구축하고 있습니다. 테스트하는 동안 개발자는 API에 요청할 때 높은 대기 시간을 관찰합니다.

   개발자는 종단 간 대기 시간을 어떻게 평가하고 성능 병목 현상을 식별할 수 있습니까?

   > API Gateway 및 Lambda 함수에서 AWS X-Ray 추적을 활성화하고 구성합니다. X-Ray를 사용하여 사용자 요청을 추적하고 분석합니다.

   - X-ray is the right tool to analyze lambda

6. 회사에서 AWS CodePipeline을 사용하여 애플리케이션 중 하나를 제공하고 있습니다. 전달 파이프라인은 AWS CodeCommit 리포지토리 의 마스터 브랜치에 대한 변경으로 트리거되며 AWS CodeBuild를 사용하여 프로세스의 테스트 및 빌드 단계를 구현하고 AWS CodeDeploy를 사용하여 애플리케이션을 배포합니다.

   파이프라인은 몇 달 동안 성공적으로 운영되었으며 수정 사항이 없습니다. 애플리케이션 소스 코드에 대한 최근 변경 사항에 따라 AWS CodeDeploy가 업데이트 애플리케이션을 예상대로 배포하지 않았습니다.

   가능한 원인은 무엇입니까? (2개를 선택하세요.)

   > AWS CodeCommit 리포지토리의 마스터 브랜치에서 변경 사항이 적용되지 않았습니다.
   >
   > 파이프라인의 초기 단계 중 하나가 실패하여 파이프라인이 종료되었습니다.

- -If one of the stages fail before getting to code deploy, application will not deploy
- -If the code is not committed to master branch, the pipeline will not be orchestrated

7. 애플리케이션이 다음 오류와 함께 작동을 중지합니다.

   The specified bucket does not exist.

   근본 원인 분석을 시작하기에 가장 좋은 곳은 어디입니까?

   > AWS CloudTrail에서 DeleteBucket 이벤트를 확인합니다.

- Amazon S3 is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon S3. By default, CloudTrail logs bucket-level actions. Amazon S3 records are written together with other AWS service records in a log file. CloudTrail determines when to create and write to a new file based on a time period and file size. The tables in this section list the Amazon S3 bucket-level actions that are supported for logging by CloudTrail. Amazon S3 bucket-level API actions tracked by CloudTrail logging will show up as the following event names suchbas Delete Bucket

8. Amazon RDS 데이터베이스 인스턴스는 많은 애플리케이션에서 기록 데이터를 조회하는 데 사용됩니다. 쿼리 비율은 비교적 일정합니다. 기록 데이터가 매일 업데이트되면 결과 쓰기 트래픽으로 인해 읽기 쿼리 성능이 느려지고 모든 애플리케이션 사용자에게 영향을 미칩니다.

   애플리케이션 사용자에 대한 성능 영향을 제거하려면 어떻게 해야 합니까?

   > RDS 읽기 전용 복제본을 만들고 모든 읽기 트래픽을 복제본으로 보냅니다.

- Pick AWS Elasticache If the same read query is performed over and over again. AWS RDS Read Replica if the read query changes dynamically.

9. 온프레미스 레거시 애플리케이션은 데이터 파일을 로컬로 캐싱하고 공유 이미지를 로컬 디스크에 기록합니다.

   애플리케이션을 AWS로 마이그레이션할 때 수평적 확장을 허용하려면 무엇이 필요합니까?

   > 공유 이미지를 제공하기 위해 Amazon S3를 사용하도록 애플리케이션을 수정합니다. 그런 다음 캐시 데이터를 로컬 디스크에 쓸 수 있습니다.

    - cache is for quicker access and we can afford to recreate if instance dies. Not the images, so image in S3 and cache on local makes sense.

10. Amazon EC2 인스턴스에서 실행되는 애플리케이션은 AWS KMS 암호화 키(SSE-KMS)를 사용하는 서버 측 암호화를 사용하여 암호화된 Amaon S3 버스킷 내의 객체에 액세스해야 합니다 . 애플리케이션은 객체를 해독하기 위해 고객 마스터 키(CMK)에 액세스할 수 있어야 합니다.

    애플리케이션 액세스 권한을 부여하는 단계 조합은 무엇입니까? (2개를 선택하십시오.)

    > 애플리케이션의 EC2 인스턴스에 연결된 IAM EC2 역할의 키에 대한 액세스 권한을 부여합니다.
    >
    > IAM 정책이 키에 대한 액세스 권한을 부여할 수 있도록 하는 키 정책을 작성합니다.

    - IAM role needs access to the keys to decrypt the object and key policies must allow role access to the key. Key policies are the primary way to control access to customer master keys (CMKs) in AWS KMS. You need the permission to decrypt the AWS KMS key. When a user sends a GET request, Amazon S3 checks if the AWS Identity and Access Management (IAM) user or role that sent the request is authorized to decrypt the key associated with the object. If the IAM user or role belongs to the same AWS account as the key, then the permission to decrypt must be granted on the AWS KMS key's policy. Even if the user has permission to decrypt the key in their IAM policy, the user still needs the permission on the key policy for the download to work.

11. 회사에서는 시스템 관리자가 문제를 보다 효과적으로 해결할 수 있도록 개발자가 작성한 AWS Lambda 함수가 오류를 기록하도록 요구합니다.

    개발자는 이 요구 사항을 충족하기 위해 무엇을 구현해야 합니까?

> Lambda 함수 코드의 로깅 문을 통해 오류를 보고합니다.

- You can insert logging statements into your code to help you validate that your code is working as expected. Lambda automatically integrates with CloudWatch Logs and pushes all logs from your code to a CloudWatch Logs group associated with a Lambda function, which is named /aws/lambda/.

12. 개발자는 Amazon ECS 환경에서 실행되는 보안 애플리케이션에 대해 AWS X-Ray를 활성화하려고 합니다.

    어떤 단계의 조합으로 X-Ray를 사용할 수 있습니까? (3개를 선택하세요.)

    > X-Ray 데몬을 실행하는 Docker 이미지를 생성합니다.
    >
    > X-Ray용 애플리케이션 코드에 계측을 추가합니다.
    >
    > 작업에 대한 IAM 역할을 구성하고 사용합니다.

- with Amazon ECS you need to create a separated X-Ray daemon instance and configure a IAM task role, as stated in https://docs.aws.amazon.com/xray/latest/devguide/xray-daemon-ecs.html.
- B is correct because it is using the correct name convention "instrument" used by Amazon, that says you have to instrument your application code to use X-Ray, as stated in https://docs.aws.amazon.com/xray/latest/devguide/xray-usage.html.
- C is incorrect because you do not have control of your EC2 instances with ECS, and cannot install X-Ray daemon on it.
- D is incorrect because you don't configure and IAM instance role for X-Ray, you configure a task role.

- E is incorrect because it is not using the correct naming "instrument".

13. 회사에서 사용자가 AWS 서비스에 액세스하고 자신의 암호를 재설정하도록 허용하는 애플리케이션을 만들고 있습니다.

    다음 중 사용자가 자신의 비밀번호를 재설정하도록 허용하면서 회사에서 사용자 및 권한을 관리할 수 있는 것은 무엇입니까?

> Amazon Cognito 사용자 풀 및 자격 증명 풀

14. 기업 웹 애플리케이션은 Amazon Virtual Private Cloud(VPC) 내에 배포되며 IPSec VPN을 통해 기업 데이터 센터에 연결됩니다. 애플리케이션은 온프레미스 LDAP 서버에 대해 인증해야 합니다. 인증 후 로그인한 각 사용자는 해당 사용자와 관련된 Amazon Simple Storage Space(S3) 키 스페이스에만 액세스할 수 있습니다 .

    이러한 목표를 충족할 수 있는 두 가지 접근 방식은 무엇입니까? (2개를 선택하세요.)

> 애플리케이션은 LDAP에 대해 인증하고 사용자와 연결된 IAM 역할의 이름을 검색합니다. 그런 다음 애플리케이션은 IAM 보안 토큰 서비스를 호출하여 해당 IAM 역할을 수임합니다. 애플리케이션은 임시 자격 증명을 사용하여 적절한 S3 버킷에 액세스할 수 있습니다.

> LDAP에 대해 인증한 다음 IAM 보안 토큰 서비스를 호출하여 IAM 연동 사용자 자격 증명을 가져오는 자격 증명 브로커를 개발합니다. 애플리케이션은 자격 증명 브로커를 호출하여 적절한 S3 버킷에 대한 액세스 권한이 있는 IAM 연동 사용자 자격 증명을 가져옵니다.

14. 개발자가 Lambda 함수를 생성하고 있으며 표준 Lambda 라이브러리에 포함되지 않은 외부 라이브러리를 사용할 것입니다.

    사용되는 Lambda 컴퓨팅 시간을 최소화하는 작업은 무엇입니까?

> 모든 Lambda 함수에서 사용할 수 있도록 Lambda에 외부 라이브러리를 설치합니다.

    - 외부 라이브러리를 포함하는 Lambda 배포 패키지를 생성합니다. 와 의견이 분분하지만 D에 조금 더 많은 표가 몰려있음

15. 개발자는 AWS Lambda 함수로 작성된 프로덕션 분산 애플리케이션의 성능 문제를 분석해야 합니다. 이러한 분산 Lambda 애플리케이션은 애플리케이션을 구성하는 다른 구성 요소를 호출합니다.

    개발자는 프로덕션에서 성능 문제의 근본 원인을 어떻게 식별하고 해결해야 합니까?

> AWS X-Ray를 사용하여 세그먼트 및 오류를 검사합니다.

16. 개발자가 Amazon DynamoDB 테이블에서 글로벌 보조 인덱스의 항목 목록을 찾으려고 합니다.

    가장 적은 수의 읽기 용량 단위를 사용하기 위해 개발자가 사용할 수 있는 DynamoDB API 호출은 무엇입니까?

> 최종 일관성 읽기를 사용한 쿼리 작업

- Strongly consistent reads are not supported on global secondary indexes.
- Strongly consistent reads use more throughput capacity than eventually consistent reads.

17. 개발자가 특정 Amazon S3 버킷에 쓸 수 있는 s3:putObject 권한이 있는 새 AWS IAM 사용자를 생성했습니다. 이 S3 버킷은 AWS KMS 관리형 키(SSE-KMS)를 기본 암호화로 사용하는 서버 측 암호화를 사용합니다. IAM 사용자의 액세스 키와 비밀 키를 사용하여 PutObject API를 호출할 때 애플리케이션이 액세스 거부 오류를 수신했습니다.

    이 문제를 어떻게 해결할 수 있습니까?

> kms:GenerateDataKey 작업을 허용하도록 IAM 사용자의 정책을 업데이트합니다.

- An error occurred (AccessDenied) when calling the PutObject operation: Access Denied" Add permission to the kms:GenerateDataKey action. This permission is required for buckets that use default encryption with a custom AWS KMS key.

18. Amazon EBS 지원 인스턴스와 인스턴스 스토어 지원 인스턴스의 주요 차이점은 무엇입니까?

> Amazon EBS 지원 인스턴스를 중지하고 다시 시작할 수 있습니다.

19. 개발자가 Amazon API Gateway를 통해 API를 호출하는 애플리케이션을 시작했습니다. 하루에도 몇 번씩 바뀌는 정보를 제공하지만 실시간으로 업데이트되지는 않습니다. 애플리케이션이 너무 대중화되어 API 엔드포인트에 과부하가 걸리고 엔드포인트에 대한 트래픽을 줄여야 합니다.

    개발자는 성능 문제를 해결하기 위해 무엇을 할 수 있습니까?

> Amazon ElastiCache에서 API 캐싱을 활성화합니다.

20. 애플리케이션은 Lambda 함수를 사용하여 S3 버킷에 업로드된 파일에서 메타데이터를 추출합니다. 메타데이터는 Amazon DynamoDB에 저장됩니다. 애플리케이션이 예기치 않게 작동하기 시작하고 개발자는 오류가 있는지 Lambda 함수 코드의 로그를 검사하려고 합니다.

    이 시스템 구성을 기반으로 개발자는 어디에서 로그를 찾을 수 있습니까?

> Amazon CloudWatch

- Lambda automatically integrates with CloudWatch Logs and pushes all logs from your code to a CloudWatch Logs group associated with a Lambda function

21. 개발자는 SAML(Security Assertion Markup Language) 및 Facebook 인증을 지원하는 애플리케이션을 만들어야 합니다. 또한 Amazon DynamoDB와 같은 AWS 서비스에 대한 액세스를 허용해야 합니다 .

    최소한의 추가 코딩으로 이러한 요구 사항을 충족하는 AWS 서비스 또는 기능은 무엇입니까?

> Amazon Cognito 자격 증명 풀

- user pools is for authentication but identity pools authorize the application to access resources.

22. 회사는 AWS CodePipeline에서 애플리케이션에 대한 지속적 통합/지속적 전달(CI/CD) 파이프라인을 실행합니다. 개발자는 테스트를 위해 아티팩트를 준비하기 전에 단위 테스트를 작성하고 파이프라인의 일부로 실행해야 합니다.

    개발자는 단위 테스트를 CI/CD 파이프라인의 일부로 통합해야 합니까?

> 단위 테스트 실행 단계를 포함하도록 AWS CodeBuild 사양 업데이트

- With codebuild repots one can see reports generated by functional or integration tests

23. EC2 인스턴스에서 실행되는 애플리케이션이 S3 버킷에 데이터를 저장하고 있습니다. 보안 정책에 따라 모든 데이터는 전송 중에 암호화되어야 합니다.

    개발자는 S3 버킷에 대한 모든 트래픽이 암호화되었는지 어떻게 확인할 수 있습니까?

    > SecureTransport가 false인 트래픽을 거부하는 버킷 정책을 생성합니다.

- The following bucket policy allows access to Amazon S3 objects only through HTTPS (the policy was generated with the AWS Policy Generator). Here the bucket policy explicitly denies ("Effect": "Deny") all read access ("Action": "s3:GetObject") from anybody who browses ("Principal": "*") to Amazon S3 objects within an Amazon S3 bucket if they are not accessed through HTTPS ("aws:SecureTransport": "false").

```
{
    "Version": "2012-10-17",
 "Id": "Policy1504640911349",
 "Statement": [
     { "Sid": "Stmt1504640908907",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::/*",
      "Condition": {
          "Bool": {
              "aws:SecureTransport": "false"
          }
      }
```

24. 애플리케이션은 수백 개의 사무실에 있는 많은 직원을 위해 매일 밤 DynamoDB에 급여 정보를 저장합니다. 항목 속성은 개인 이름, 사무실 식별자 및 누적 일일 시간으로 구성됩니다.

    관리자는 사무실에서 일하는 다양한 이름에 대한 보고서를 실행합니다. 하나의 쿼리입니다. "A에서 E로 시작하는 이름에 대해 이 사무실의 모든 항목을 반환합니다."

    이 쿼리에 대해 프로비저닝된 처리량에 미치는 영향이 가장 적은 테이블 구성은 무엇입니까?

> 이름 속성에 대한 범위 인덱스와 사무실 식별자에 대한 해시 인덱스를 갖도록 테이블 구성

- A primary key is consists of a hash key and an optional range key. Hash key is used to select the DynamoDB partition. Partitions are parts of the table data. Range keys are used to sort the items in the partition, if they exist."

25. 한 개발자가 매우 민감한 데이터가 포함된 10MB 문서를 처리하는 응용 프로그램에서 작업하고 있습니다. 애플리케이션은 AWS KMS를 사용하여 클라이언트 측 암호화를 수행합니다.

    어떤 단계를 따라야 합니까?

    > GenerateDataKey API를 호출하여 데이터 암호화 키의 일반 텍스트 버전을 검색하여 데이터를 암호화합니다.

- Invoke the GenerateDataKey API to retrieve the plaintext version of the data encryption key to encrypt the data
- #> https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html
- #> When uploading an object—Using the customer master key (CMK) ID, the client first sends a request to AWS KMS for a CMK that it can use to encrypt your object data. AWS KMS returns two versions of a randomly generated data key:
- #> 1. A plaintext version of the data key that the client uses to encrypt the object data
- #> 2. A cipher blob of the same data key that the client uploads to Amazon S3 as object metadata

26. 회사는 거래 요청을 처리하는 데 밀리초 미만의 대기 시간이 필요한 주식 거래 애플리케이션을 구축하고 있습니다. Amazon DynamoDB는 각 요청을 처리하는 데 사용되는 모든 거래 데이터를 저장하는 데 사용됩니다. 애플리케이션을 로드 테스트한 후 개발 팀은 데이터 검색 시간으로 인해 대기 시간 요구 사항이 충족되지 않음을 발견했습니다. 요청 수가 갑자기 급증하기 때문에 제한을 피하기 위해 DynamoDB 읽기 용량을 상당히 과도하게 프로비저닝해야 합니다.

    대기 시간 요구 사항을 충족하고 애플리케이션 실행 비용을 줄이려면 어떤 조치를 취해야 합니까?

> DynamoDB Accelerator를 사용하여 거래 데이터를 캐시합니다.

- "sub-millisecond latency" --> Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for Amazon DynamoDB that delivers up to a 10 times performance improvement—from milliseconds to microseconds—even at millions of requests per second.

27. 회사에서 기존 3계층 웹 애플리케이션을 컨테이너화 하여 Amazon ECS Fargate에 배포하려고 합니다. 애플리케이션이 세션 데이터를 사용하여 사용자 활동을 추적하고 있습니다.

    어떤 접근 방식이 최고의 사용자 경험을 제공할까요?

> Amazon ElastiCache에서 Redis 클러스터를 프로비저닝하고 클러스터에 세션 데이터를 저장합니다.

- Session data should always saved in elasticache or DB

28. 고객이 AWS Elastic Beanstalk 환경에 소스 코드를 배포하려고 합니다. 고객은 중단을 최소화하면서 배포를 수행해야 하며 기존 인스턴스만 사용하여 애플리케이션 액세스 로그를 보관해야 합니다.

    이러한 요구 사항을 충족하는 배포 정책은 무엇입니까?

> Rolling

- All at once – The quickest deployment method. Suitable if you can accept a short loss of service, and if quick deployments are important to you. With this method, Elastic Beanstalk deploys the new application version to each instance. Then, the web proxy or application server might need to restart. As a result, your application might be unavailable to users (or have low availability) for a short time.
- Rolling – Avoids downtime and minimizes reduced availability, at a cost of a longer deployment time. Suitable if you can't accept any period of completely lost service. With this method, your application is deployed to your environment one batch of instances at a time. Most bandwidth is retained throughout the deployment.

29. 응용 프로그램은 많은 수의 작은 메시지를 수집하여 데이터베이스에 저장합니다. 애플리케이션은 AWS Lambda를 사용합니다. 개발 팀이 애플리케이션 처리 로직을 변경하고 있습니다. 테스트에서 각 메시지를 처리하는 데 15분 이상 걸립니다. 팀은 현재 백엔드가 시간 초과될 수 있다고 우려하고 있습니다.

각 메시지가 가장 확장 가능한 방식으로 처리되도록 하려면 백엔드 시스템에서 어떤 변경을 해야 합니까?

> Amazon SQS 대기열에 메시지를 추가합니다. Auto Scaling 그룹에서 Amazon EC2 인스턴스를 설정하여 대기열을 폴링하고 메시지가 도착하면 처리합니다.

- Add the messages to an Amazon SQS queue. Set up Amazon EC2 instances in an Auto Scaling group to poll the queue and process the messages as they arrive.