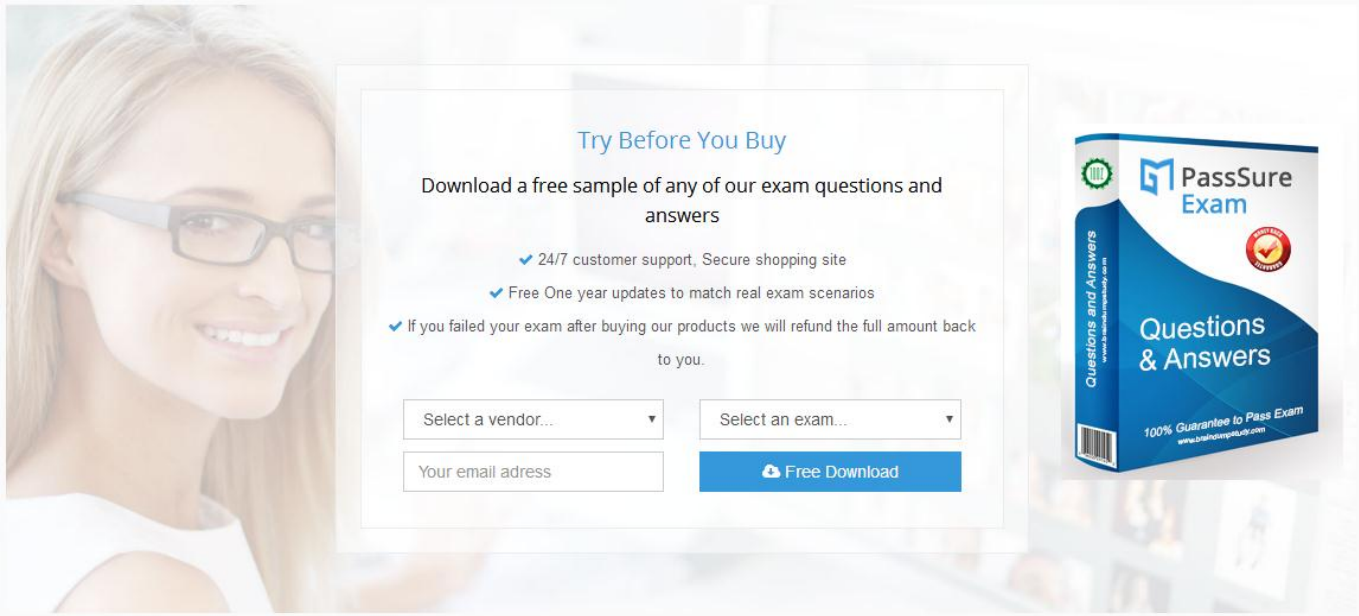
PassSureExam

PassSureExam



QUALITY AND VALUE

VCEPrep Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

TESTED AND APPROVED

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

EASY TO PASS

If you prepare for the exams using our VCEPrep testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

TRY BEFORE BUY

VCEPrep offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

HAPPY CUSTOMERS	DOWNLOADS	TEAM MEMBERS	SHARES
68263	68263	68263	68263

http://www.passsureexam.com

Best Exam Questions & Valid Exam Torrent & Pass for Sure

Exam : **AWS-Security-Specialty-KR**

Title : AWS Certified Security - Specialty (SCS-C01 Korean Version)

Vendor : Amazon

Version : DEMO

QUESTION NO: 1
회사에서 AWS Organizations를 사용하여 여러 AWS 계정을 관리합니다. 회사는 대량의 민감한 데이터를 처리합니다. 이 회사는 마이크로서비스에 서버리스 접근 방식을 사용합니다. 회사는 모든 데이터를 Amazon S3 또는 Amazon DynamoDB에 저장합니다. 회사는 AWS Fargate의 Amazon Elastic Kubernetes Service(Amazon EKS)에서 회사가 호스팅하는 컨테이너 기반 서비스 또는 AWS Lambda 함수를 사용하여 데이터를 읽습니다.
회사는 미사용 데이터를 모두 암호화하고 최소 권한 데이터 액세스 제어를 적용하는 솔루션을 구현해야 합니다. 회사는 AWS Key Management Service(AWS KMS) 고객 관리형 키를 생성합니다.
이러한 요구 사항을 충족하기 위해 회사는 다음에 무엇을 해야 합니까?
A. Amazon S3 및 DynamoDB에 대해서만 kms:Decrypt 작업을 허용하는 키 정책을 생성합니다. 키로 암호화되지 않은 S3 버킷 및 DynamoDB 테이블 생성을 거부하는 SCP를 생성합니다.
B. 키에 대한 kms:Decrypt 작업을 거부하는 1AM 정책을 만듭니다. 정책을 새 역할에 연결하기 위해 일정에 따라 실행되는 Lambda 함수를 생성합니다. 키로 암호화되지 않은 리소스에 대한 알림을 보내는 AWS Config 규칙을 생성합니다.
C. Amazon S3, DynamoDB, Lambda 및 Amazon EKS에 대해서만 kms:Decrypt 작업을 허용하는 키 정책을 생성합니다. 키로 암호화되지 않은 S3 버킷 및 DynamoDB 테이블 생성을 거부하는 SCP를 생성합니다.
D. Amazon S3, DynamoDB, Lambda 및 Amazon EKS에 대해서만 kms:Decrypt 작업을 허용하는 키 정책을 생성합니다. 키로 암호화되지 않은 리소스에 대한 알림을 보내는 AWS Config 규칙을 생성합니다.
Answer: B

QUESTION NO: 2
회사에서 Amazon S3에 데이터 레이크를 구축하고 있습니다. 데이터는 민감한 정보가 포함된 수백만 개의 작은 파일로 구성됩니다. 보안 팀의 아키텍처 요구 사항은 다음과 같습니다.
* 데이터는 전송 중에 암호화되어야 합니다.
* 미사용 데이터는 암호화해야 합니다.
* 버킷은 비공개여야 하지만 버킷이 실수로 공개된 경우 데이터는 기밀로 유지되어야 합니다.
어떤 단계 조합이 요구 사항을 충족합니까? (3개를 선택하세요.)
A. S3 버킷에서 Amazon S3 관리형 암호화 키(SSE-S3)로 서버 측 암호화를 사용하여 AES-256 암호화를 활성화합니다.
B. S3 버킷에서 IAM KMS 관리형 키(SSE-KMS)를 사용한 서버 측 암호화로 기본 암호화를 활성화합니다.
C. PutObject 요청에 IAMiSecureTcanspoct가 포함되지 않은 경우 거부를 포함하는 버킷 정책을 추가합니다.
D. 회사 인트라넷에서만 업로드 및 다운로드를 허용하는 ws: Sourcelp로 버킷 정책을 추가합니다.
E. PutObject 요청에 s3:x-amz-sairv9r-side-enctyption: "IAM: kms"가 포함되지 않은 경우 거부를 포함하는 버킷 정책을 추가합니다.
F. Amazon Macie가 데이터 레이크의 S3 버킷에 대한 변경 사항을 모니터링하고 조치를 취할 수 있도록 합니다.
Answer: B,D,F

QUESTION NO: 3
회사의 애플리케이션 팀은 IAM에서 MySQL 데이터베이스를 호스팅해야 합니다. 회사의 보안 정책에 따라 IAM에 저장되는 모든 데이터는 유휴 상태에서 암호화되어야 합니다. 또한 모든 암호화 자료는 FIPS 140-2 레벨 3 검증을 준수해야 합니다.
애플리케이션 팀은 회사의 보안 요구 사항을 충족하고 운영 오버헤드를 최소화하는 솔루션이 필요합니다.
이러한 요구 사항을 충족하는 솔루션은 무엇입니까?
A. Amazon RDS에서 데이터베이스를 호스팅합니다. 암호화에 Amazon Elastic Block Store(Amazon EBS)를 사용합니다. 키 관리를 위해 IAM CloudHSM에서 지원하는 IAM KMS(IAM Key Management Service) 사용자 지정 키 스토어를 사용합니다.
B. Amazon RDS에서 데이터베이스를 호스팅합니다. 암호화에 Amazon Elastic Block Store(Amazon EBS)를 사용합니다. 키 관리를 위해 IAM KMS(IAM Key Management Service)에서 IAM 관리형 CMK를 사용합니다.
D. Amazon EC2 인스턴스에서 데이터베이스를 호스팅합니다. 암호화에 Amazon Elastic Block Store(Amazon EBS)를 사용합니다. 키 관리를 위해 IAM KMS(IAM Key Management Service)에서 고객 관리형 CMK를 사용합니다.
E. Amazon EC2 인스턴스에서 데이터베이스를 호스팅합니다. 암호화 및 키 관리에 TDE(투명한 데이터 암호화)를 사용합니다.
Answer: B

QUESTION NO: 4
보안 엔지니어는 Amazon S3 버킷 정책을 생성하여 User=1, User2라는 IAM 사용자 계정에 대한 최소 권한 읽기 액세스 권한을 부여해야 합니다. 및 사용자3. 이러한 IAM 사용자 계정은 AuthorizedPeople IAM 그룹의 구성원입니다. 보안 엔지니어는 다음 S3 버킷 정책의 초안을 작성합니다.

```
{
    "Version": "2012-10-17",
    "Id": "AuthorizedPeoplePolicy",
    "Statement": [
        {
            "Sid": "Actions-Authorized-People",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::authorized-people-bucket/*"
        }
    ]
}
```

보안 엔지니어가 정책을 S3 버킷에 추가하려고 하면 "Missing required field Principal." 오류 메시지가 나타납니다. 보안 엔지니어가 정책에 Principal 요소를 추가하고 있습니다. 추가는 User1에게만 읽기 액세스 권한을 제공해야 합니다. 사용자2 및 사용자3. 어떤 솔루션이 이러한 요구 사항을 충족합니까?

A.

```
"Principal": {
    "AWS": [
        "arn:aws:iam::1234567890:user/User1",
        "arn:aws:iam::1234567890:user/User2",
        "arn:aws:iam::1234567890:user/User3"
    ]
}
```

B.

```
"Principal": {
    "AWS": [
        "arn:aws:iam::1234567890:root"
    ]
}
```

C.

```
"Principal": {
    "AWS": [
        "*"
    ]
}
```

D.

```
"Principal": {
    "AWS": "arn:aws:iam::1234567890:group/AuthorizedPeople"
}
```

Answer: A

QUESTION NO: 5
IAM KMS(IAM Key Management Service) 키 정책을 검토하던 보안 엔지니어가 회사 IAM 계정의 각 키 정책에서 이 설명을 발견했습니다.

```
{
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "kms:*",
      "Resource": "*"
}
```

진술은 무엇을 허용합니까?

A. 모든 IAM 계정의 모든 보안 주체가 키를 사용합니다.
B. 계정 111122223333의 루트 사용자만 키를 사용합니다.
C. 계정 111122223333의 모든 보안 주체는 Amazon S3에서만 키를 사용합니다.
D. 키를 사용할 수 있도록 이 키에 대한 액세스 권한을 부여하는 IAM 정책이 적용된 계정 111122223333의 보안 주체만 해당됩니다.
Answer: D

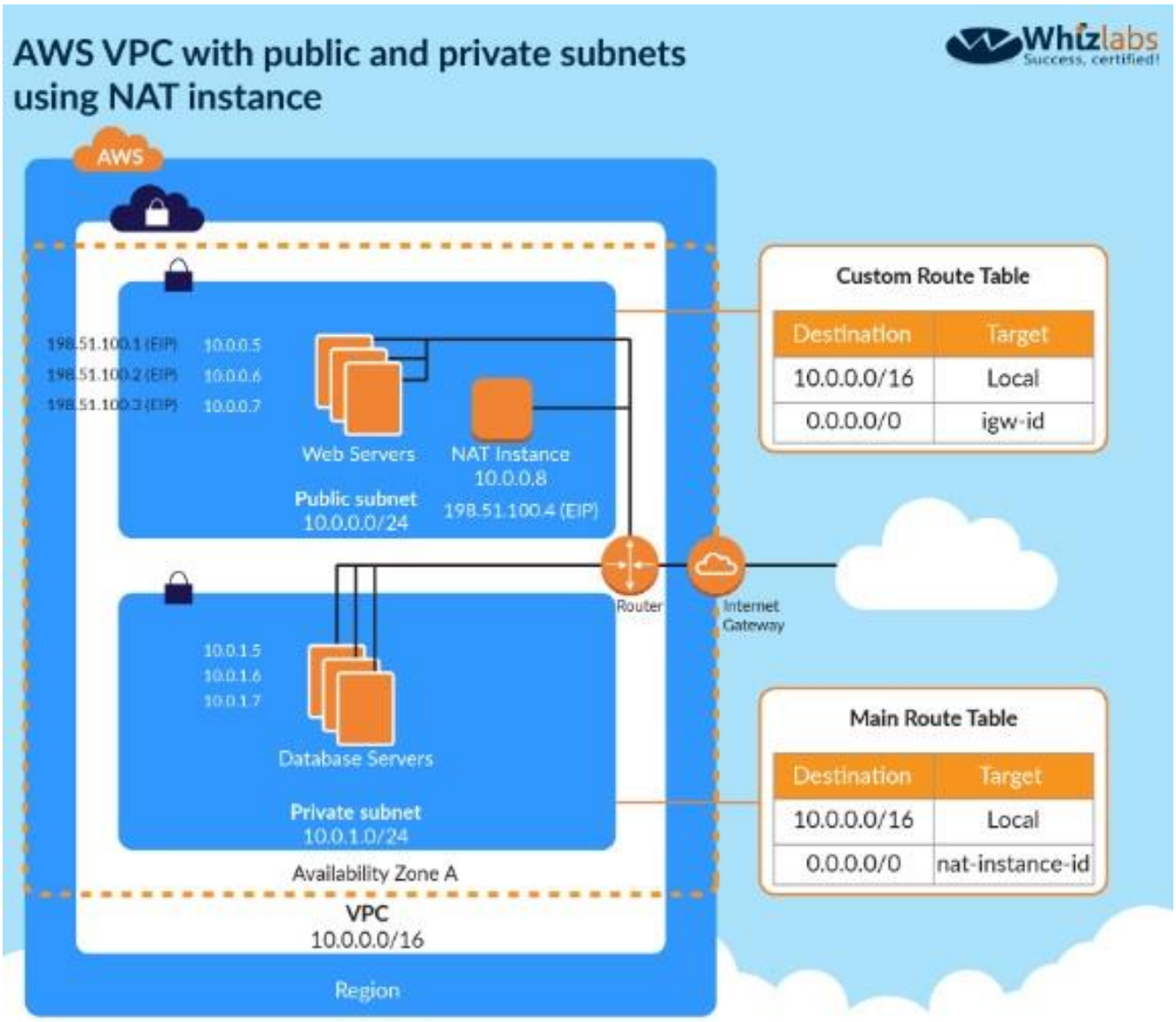
QUESTION NO: 6
웹 애플리케이션은 사용자에게 로그인하여 멤버십의 유효성을 확인하고 Amazon S3 버킷에 저장된 아티팩트를 찾아볼 수 있는 기능을 제공합니다. 사용자가 객체를 다운로드하려고 하면 애플리케이션은 객체에 액세스할 수 있는 권한을 확인하고 사용자가 example com과 같은 사용자 지정 도메인 이름에서 객체를 다운로드할 수 있도록 허용해야 합니다.
보안 엔지니어가 이 기능을 구현하는 가장 안전한 방법은 무엇입니까?
A. 버킷 ACL을 사용하여 객체에 대한 읽기 전용 액세스를 구성합니다. 설정한 시간 경과 후 접근 권한을 제거합니다.
B. 사용자에게 S3 버킷에 대한 읽기 액세스 권한을 부여하는 IAM 정책을 구현합니다.
C. S3 미리 서명된 URL 생성 애플리케이션을 통해 S3 미리 서명된 URL을 사용자에게 제공합니다.
D. Amazon CloudFront 서명 URL을 생성합니다. 애플리케이션을 통해 사용자에게 CloudFront 서명 URL을 제공합니다.
Answer: D
Explanation:
For this scenario you would need to set up static website hosting because a custom domain name is listed as a requirement. "Amazon S3 website endpoints do not support HTTPS or access points. If you want to use HTTPS, you can use Amazon CloudFront to serve a static website hosted on Amazon S3." This is not secure.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/website-hosting-custom-domain-walkthrough.html CloudFront signed URLs allow much more fine-grained control as well as HTTPS access with custom domain names:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html

QUESTION NO: 7
회사는 Amazon API Gateway를 사용하여 REST API를 사용자에게 제공합니다. API 개발자는 로그 파일을 구문 분석할 필요 없이 API 액세스 패턴을 분석하려고 합니다.
최소한의 노력으로 이러한 요구 사항을 충족하는 단계 조합은 무엇입니까? (2개를 선택하세요.)
A. 필요한 API 단계에 대한 액세스 로깅을 구성합니다.
B. API Gateway 이벤트에 대한 AWS CloudTrail 추적 대상을 구성합니다. userIdentity, userAgent 및 sourceIPAddress 필드에 대한 필터를 구성합니다.
C. API 게이트웨이 로그에 대한 Amazon S3 대상을 구성합니다. Amazon Athena 쿼리를 실행하여 API 액세스 정보를 분석합니다.
D. Amazon CloudWatch Logs Insights를 사용하여 API 액세스 정보를 분석합니다.
E. 필요한 API 단계에서 자세한 CloudWatch 지표 활성화 옵션을 선택합니다.

Answer: C,D

QUESTION NO: 8
나열하는 주간 보고서를 생성해야 합니다 . 또한 엔지니어는 승인된 최신 업데이트가 적용되지 않고 시스템이 30일 이상 작동하지 않도록 해야 합니다. 이러한 목표를 달성하는 가장 효율적인 방법은 무엇입니까?
A. Amazon inspector를 사용하여 최신 패치가 적용되지 않은 시스템을 확인하고 30일 후에 해당 인스턴스를 최신 AMI 버전으로 재배포합니다.
B. 정의된 유지 관리 기간 동안 인스턴스 패치 규정 준수를 보고하고 업데이트를 시행하도록 Amazon EC2 Systems Manager를 구성합니다.
C. IAM CloudTrail 토그를 검사하여 지난 30일 동안 인스턴스가 다시 시작되지 않았는지 확인하고 해당 인스턴스를 재배포합니다.
D. 최신 승인 패치로 AML을 업데이트하고 정의된 유지 관리 기간 동안 각 인스턴스를 재배포합니다.
Answer: B

QUESTION NO: 9
프라이빗 서브넷이 있는 Amazon VPC와 NAT 인스턴스 서버가 있는 퍼블릭 서브넷이 있습니다. GIT를 통해 애플리케이션을 배포하는 S3에서 부트 스트랩 스크립트를 다운로드 하여 시작시 스스로 구성하는 EC2 인스턴스 그룹을 생성했습니다.
다음 설정 중 가장 높은 수준의 보안을 제공하는 것은 무엇입니까?
아래 주어진 옵션에서 정답을 선택하십시오.
선택 해주세요:
A. 퍼블릭 서브넷의 EC2 인스턴스, EIP 없음, IGW를 통해 나가는 트래픽 라우팅
B. 퍼블릭 서브넷의 EC2 인스턴스, 할당 된 EIP, NAT를 통해 나가는 트래픽 라우팅
C. 프라이빗 서브넷의 EC2 인스턴스, 할당 된 EIP, IGW를 통해 나가는 트래픽 라우팅
D. 프라이빗 서브넷의 EC2 인스턴스, EIP 없음, NAT를 통해 나가는 트래픽 라우팅
Answer: D
Explanation:
The below diagram shows how the NAT instance works. To make EC2 instances very secure, they need to be in a private sub such as the database server shown below with no EIP and all traffic routed via the NAT.



Options A and B are invalid because the instances need to be in the private subnet Option C is invalid because since the instance needs to be in the private subnet, you should not attach an EIP to the instance For more information on NAT instance, please refer to the below Link: http://docs.IAM.amazon.com/AmazonVPC/latest/UserGuideA/PC Instance.html!
The correct answer is: EC2 instances in our private subnet no EIPs, route outgoing traffic via the NAT Submit your Feedback/Queries to our Experts

QUESTION NO: 10
IAM KMS 서비스를 사용하여 정의된 키 세트가 있습니다. 몇 개의 키 사용을 중지하고 싶지만 현재 어떤 서비스에서 키를 사용하고 있는지 확실하지 않습니다. 다음 중 추가 사용에서 키 사용을 중지하는 안전한 옵션은 무엇입니까?
선택 해주세요:
A. 어쨌든 삭제하기 전에 7일의 대기 기간이 있으므로 키를 삭제합니다.
B. 키 비활성화
C. 키의 별칭 설정
D. 키에 대한 키 자료 변경

Answer: B
Explanation:
Option A is invalid because once you schedule the deletion and waiting period ends, you cannot come back from the deletion process.
Option C and D are invalid because these will not check to see if the keys are being used or not The IAM Documentation mentions the following Deleting a customer master key (CMK) in IAM Key Management Service (IAM KMS) is destructive and potentially dangerous. It deletes the key material and all metadata associated with the CMK, and is irreversible. After a CMK is deleted you can no longer decrypt the data that was encrypted under that CMK, which means that data becomes unrecoverable. You should delete a CMK only when you are sure that you don't need to use it anymore. If you are not sure, consider disabling the CMK instead of deleting it. You can re-enable a disabled CMK if you need to use it again later, but you cannot recover a deleted CMK.
For more information on deleting keys from KMS, please visit the below URL:
https://docs.IAM.amazon.com/kms/latest/developereuide/deleting-keys.html The correct answer is: Disable the keys Submit your Feedback/Queries to our Experts

QUESTION NO: 11
회사는 단일 AWS 리전에서 워크로드를 실행하고 AWS Organizations를 사용합니다. 보안 엔지니어는 사용자가 다른 리전에서 리소스를 시작하지 못하도록 방지하는 솔루션을 구현해야 합니다.
최소한의 운영 오버헤드로 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?
A. 지정된 지역에서만 작업을 허용하는 aws RequestedRegion 조건이 있는 IAM 정책을 생성합니다. 정책을 모든 사용자에게 연결합니다.
B. 지정된 지역에 없는 작업을 거부하는 aws RequestedRegion 조건이 있는 I AM 정책을 생성합니다. 정책을 AWS Organizations의 AWS 계정에 연결합니다.
C. 원하는 작업을 허용하는 aws RequestedRegion 조건이 있는 IAM 정책을 생성합니다. 지정된 지역에 있는 사용자에게만 정책을 연결합니다.
D. 지정된 지역에 없는 작업을 거부하는 aws RequestedRegion 조건이 있는 SCP를 생성합니다. AWS Organizations의 AWS 계정에 SCP를 연결합니다.
Answer: D
Explanation:
Although you can use a IAM policy to prevent users launching resources in other regions. The best practice is to use SCP when using AWS organizations.
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_general.html#example-scp-deny-region

QUESTION NO: 12
한 개발자가 자신의 계정에서 IAM CloudTrail이 비활성화되었다고 보고했습니다. 보안 엔지니어가 계정을 조사한 결과 현재 보안 솔루션에서 이벤트를 감지하지 못했다는 사실을 발견했습니다. 보안 엔지니어는 CloudTrail 구성에 대한 향후 변경 사항을 감지하고 변경 사항이 발생하면 알림을 보내는 솔루션을 추천해야 합니다.
보안 엔지니어는 이러한 요구 사항을 충족하기 위해 무엇을 해야 합니까?
A. IAM 리소스 액세스 관리자(IAM RAM)를 사용하여 IAM CloudTrail 구성을 모니터링합니다. Amazon SNS를 사용하여 알림을 보냅니다.

B. Amazon GuardDuty 결과를 모니터링하는 Amazon CloudWatch Events 규칙을 생성합니다. Amazon SNS를 사용하여 이메일 알림을 보냅니다.
C. IAM 지원이 의심스러운 활동이 감지되면 경고를 보내도록 IAM 계정 설정에서 보안 연락처 세부 정보를 업데이트합니다.
D. Amazon Inspector를 사용하여 보안 문제를 자동으로 감지합니다. Amazon SNS를 사용하여 알림을 보냅니다.
Answer: B

QUESTION NO: 13
수도 유틸리티 회사는 여러 Amazon EC2 인스턴스를 사용하여 수질을 모니터링하는 2,000개의 IoT(사물 인터넷) 필드 디바이스에 대한 업데이트를 관리합니다. 이러한 장치에는 각각 고유한 액세스 자격 증명이 있습니다.
운영 안전 정책에서는 특정 자격 증명에 대한 액세스를 독립적으로 감사할 수 있어야 합니다. 자격 증명 저장소를 관리하는 가장 비용 효율적인 방법은 무엇입니까?
A. IAM Systems Manager를 사용하여 보안 문자열 매개변수로 자격 증명을 저장합니다. IAM KMS 키를 사용하여 보호합니다.
B. IAM 키 관리 시스템을 사용하여 자격 증명을 암호화하는 데 사용되는 마스터 키를 저장합니다. 암호화된 자격 증명은 Amazon RDS 인스턴스에 저장됩니다.
C. IAM Secrets Manager를 사용하여 자격 증명을 저장합니다.
D. 서버 측 암호화를 사용하여 Amazon S3의 JSON 파일에 자격 증명을 저장합니다.
Answer: A
Explanation:
https://docs.IAM.amazon.com/systems-manager/latest/userguide/parameter-store-advanced-parameters.html

QUESTION NO: 14
귀사는 IAM에서 많은 EC2 인스턴스 섹션을 호스팅합니다. EC2 인스턴스를 관리하는 엄격한 보안 규칙이 있습니다. 잠재적인 보안 침해가 발생하는 동안 기본 EC2 인스턴스를 신속하게 조사해야 합니다. 다음 중 위반된 인스턴스를 조사하기 위해 테스트 환경을 신속하게 프로비저닝하는 데 도움이 되는 서비스는 무엇입니까?
선택 해주세요:
A. IAM 클라우드워치
B. IAM 클라우드포메이션
C. IAM 클라우드 트레일
D. IAM 구성
Answer: B
Explanation:
The IAM Security best practises mentions the following
Unique to IAM, security practitioners can use CloudFormation to quickly create a new, trusted environment in which to conduct deeper investigation. The CloudFormation template can pre-configure instances in an isolated environment that contains all the necessary tools forensic teams need to determine the cause of the incident This cuts down on the time it takes to gather necessary tools, isolates systems under examination, and ensures that the team is operating in a clean room.

Option A is incorrect since this is a logging service and cannot be used to provision a test environment Option C is incorrect since this is an API logging service and cannot be used to provision a test environment Option D is incorrect since this is a configuration service and cannot be used to provision a test environment For more information on IAM Security best practises, please refer to below URL:
https://d1.IAMstatic.com/whitepapers/architecture/IAM-Security-Pillar.pd1 The correct answer is: IAM Cloudformation Submit your Feedback/Queries to our Experts

QUESTION NO: 15
팀이 응용 프로그램의 API 게이트웨이 서비스를 실험하고 있습니다. API 게이트웨이에 대한 호출의 인증 / 권한 부여에 사용할 수 있는 사용자 정의 모듈을 구현해야 합니다. 이것이 어떻게 달성 될 수 있습니까?
선택 해주세요:
A. 권한 부여에 요청 매개 변수 사용
B. Lambda 인증 자 사용
C. 게이트웨이 권한 부 여기 사용
D. API 게이트웨이에서 CORS 사용
Answer: B
Explanation:
The IAM Documentation mentions the following
An Amazon API Gateway Lambda authorizer (formerly known as a custom authorize?) is a Lambda function that you provide to control access to your API methods. A Lambda authorizer uses bearer token authentication strategies, such as OAuth or SAML. It can also use information described by headers, paths, query strings, stage variables, or context variables request parameters.
Options A,C and D are invalid because these cannot be used if you need a custom authentication/authorization for calls made to the API gateway For more information on using the API gateway Lambda authorizer please visit the URL:
https://docs.IAM.amazon.com/apisateway/latest/developerguide/apieateway-use-lambda-authorizer.htmll The correct answer is: Use a Lambda authorizer Submit your Feedback/Queries to our Experts

QUESTION NO: 16
한 회사에서 새로운 Amazon RDS 데이터베이스 애플리케이션을 개발했습니다. 회사는 전송 중 암호화 및 미사용 암호화를 위해 ROS 데이터베이스 자격 증명을 보호해야 합니다. 또한 회사는 자격 증명을 정기적으로 자동 교체해야 합니다.
어떤 솔루션이 이러한 요구 사항을 충족합니까?
A. IAM Systems Manager Parameter Store를 사용하여 데이터베이스 자격 증명을 저장합니다. 자격 증명의 자동 회전을 구성합니다.
B. IAM Secrets Manager를 사용하여 데이터베이스 자격 증명을 저장합니다. 자격 증명의 자동* 회전 구성
C. S3 관리형 암호화 키(SSE-S3)를 사용한 서버 측 암호화로 구성된 Amazon S3 버킷에 데이터베이스 자격 증명을 저장합니다. IAM 데이터베이스 인증으로 자격 증명을 교체합니다.
D. 데이터베이스 자격 증명을 Amazon S3 Glacier에 저장하고 S3 Glacier Vault Lock을 사용합니다. 예약된 bast에서 자격 증명을 교체하도록 IAM Lambda 함수를 구성합니다.

Answer: A

QUESTION NO: 17
Amazon SQS에서 메시지를 검색하는 Amazon EC2 인스턴스로 애플리케이션이 구축되었습니다.
최근에 IAM이 변경되어 인스턴스가 더 이상 메시지를 검색 할 수 없습니다.
최소 권한을 유지하면서 문제를 해결하기 위해 취해야 할 조치 (2 개 선택)
A. MFA 디바이스를 구성하고 인스턴스가 사용하는 역할에 할당하십시오.
B. SQS 자원 정책이 인스턴스가 사용하는 역할에 대한 액세스를 명시 적으로 거부하지 않는지 확인하십시오.
C. 인스턴스가 사용하는 역할에 연결된 액세스 키가 활성화되어 있는지 확인하십시오.
D. AmazonSQSFullAccess 관리 형 정책을 인스턴스가 사용하는 역할에 연결합니다.
E. 인스턴스에 연결된 역할에 큐에 대한 액세스를 허용하는 정책이 포함되어 있는지 확인하십시오.
Answer: B,E

QUESTION NO: 18
회사의 애플리케이션은 Amazon EC2에서 실행되고 Amazon S3 버킷에 데이터를 저장합니다. 회사는 데이터가 외부 당사자에게 우발적으로 노출될 가능성을 제한하기 위해 추가 보안 제어를 원합니다. 이 요구 사항을 충족하는 작업 조합은 무엇입니까? (3개를 선택하세요.)
A. Amazon S3 관리 암호화 키(SSE-S3)로 서버 측 암호화를 사용하여 Amazon S3의 데이터를 암호화합니다.
B. IAM KMS 관리형 암호화 키(SSE-KMS)로 서버 측 암호화를 사용하여 Amazon S3의 데이터를 암호화합니다.
C. 새 Amazon S3 VPC 엔드포인트를 생성하고 새 엔드포인트를 사용하도록 VPC의 라우팅 테이블을 수정합니다.
D. Amazon S3 공개 액세스 차단 기능을 사용합니다.
E. 애플리케이션 인스턴스에서만 액세스를 허용하도록 버킷 정책을 구성합니다.
F. NACL을 사용하여 Amazon S3에 대한 트래픽 필터링
Answer: B,C,E

QUESTION NO: 19
보안 엔지니어는 Amazon S3 버킷 예제 버킷에서 암호화가 활성화되었지만 버킷에 대한 액세스 권한이 있는 사람은 누구나 파일을 검색할 수 있음을 발견했습니다. 엔지니어는 각 IAM 사용자가 할당된 폴더에만 액세스할 수 있도록 액세스를 제한하려고 합니다.
보안 엔지니어는 이를 달성하기 위해 무엇을 해야 합니까?
A. IAM 관리형 CMK IAM/s3와 함께 봉투 암호화를 사용합니다.
B. 다음을 기반으로 "kms:Decrypt"를 부여하는 키 정책을 사용하여 고객 관리형 CMK를 생성합니다.
"${IAM:사용자 이름}" 변수.
C. 각 사용자에 대해 고객 관리형 CMK를 생성합니다. 해당 키 정책에서 각 사용자를 키 사용자로 추가합니다.
D. "리소스"에 대한 S3 액세스 권한을 부여하도록 해당 IAM 정책을 변경합니다.
"arn:IAM:s3:::examplebucket/${IAM:사용자 이름}/*"

Answer: B

QUESTION NO: 20
정보 기술 부서는 Classic Load Balancer 사용을 중단하고 Application Load Balancer로 전환하여 비용을 절감했습니다. 전환 후 구형 장치의 일부 사용자는 더 이상 웹 사이트에 연결할 수 없습니다.
이 상황의 원인은 무엇입니까?
A. Application Load Balancer는 이전 웹 브라우저를 지원하지 않습니다.
B. Perfect Forward Secrecy 설정이 올바르게 구성되지 않았습니다.
C. 중간 인증서는 Application Load Balancer 내에 설치됩니다.
D. Application Load Balancer의 암호화 제품군이 연결을 차단하고 있습니다.
Answer: D
Explanation:
https://docs.IAM.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html

QUESTION NO: 21
애플리케이션은 IAM SDK를 사용하여 IAM 서비스를 호출합니다. 애플리케이션은 연결된 IAM 역할이 있는 Amazon EC2 인스턴스에서 실행됩니다. 애플리케이션이 Amazon S3 버킷 내의 객체에 액세스하려고 시도하는 경우 관리자는 다음과 같은 오류 메시지를 받습니다. HTTP 403: 액세스가 거부되었습니다.
관리자는 이 문제를 해결하기 위해 어떤 조합의 단계를 수행해야 합니까? (3개를 선택합니다.)
A. EC2 인스턴스의 보안 그룹이 S3 액세스 권한을 부여하는지 확인합니다.
B. KMS 키 정책이 이 IAM 원칙에 대해 KMS 키에 대한 암호 해독 액세스를 허용하는지 확인합니다.
C. 개체에 대한 액세스를 거부하는 문에 대한 S3 버킷 정책을 확인합니다.
D. EC2 인스턴스가 올바른 키 쌍을 사용하고 있는지 확인합니다.
E. EC2 인스턴스와 연결된 IAM 역할에 적절한 권한이 있는지 확인합니다.
F. 인스턴스와 S3 버킷이 동일한 리전에 있는지 확인합니다.
Answer: B,C,E

QUESTION NO: 22
회사는 IAM Secrets Manager를 사용하여 CMK를 사용하여 암호화되고 보안 계정 111122223333에 저장되는 비밀을 저장합니다. 회사의 프로덕션 계정 중 하나입니다. 444455556666은 보안 계정 111122223333에서 비밀 값을 검색해야 합니다. 프로덕션 계정이 비밀 값만 검색할 수 있도록 보안 엔지니어는 최소 권한 액세스를 기반으로 보안 계정의 비밀에 정책을 적용해야 합니다.
보안 엔지니어는 어떤 정책을 적용해야 합니까?

A.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:*",
            "Principal": {"AWS": "444455556666"},
            "Resource": "*"
        }
    ]
}
```

B.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:*",
            "Principal": {"AWS": "111122223333"},
            "Resource": "*"
        }
    ]
}
```

C.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Principal": {"AWS": "111122223333"},
            "Resource": "*"
        }
    ]
}
```

D.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Principal": {"AWS": "444455556666"},
            "Resource": "*"
        }
    ]
```

A. 옵션 A

B. 옵션 B
C. 옵션 C
D. 옵션 D
Answer: A

QUESTION NO: 23
감사 결과 회사의 Amazon EC2 인스턴스 보안 그룹이 무제한 수신 SSH 트래픽을 허용하여 회사 정책을 위반한 것으로 확인되었습니다. 보안 엔지니어는 이러한 위반을 관리자에게 알리는 거의 실시간 모니터링 및 경고 솔루션을 구현해야 합니다.
가장 운영 효율성이 높은 이러한 요구 사항을 충족하는 솔루션은 무엇입니까?
A. 매일 실행되고 Network Reachability 패키지를 사용하는 반복 Amazon Inspector 평가 실행을 만듭니다. 평가 실행이 시작될 때 IAM Lambda 함수를 호출하는 Amazon CloudWatch 규칙을 생성합니다. 완료되면 평가 실행 보고서를 검색하고 평가하도록 Lambda 함수를 구성합니다. 무제한 수신 SSH 트래픽에 대한 위반이 있는 경우 Amazon Simple Notification Service(Amazon SNS) 알림을 게시하도록 Lambda 함수도 구성합니다.
B. 규정을 준수하지 않는 보안 그룹 구성 변경에 의해 호출되는 제한된 ssh IAM 구성 관리 규칙을 사용합니다. IAM 구성 수정 기능을 사용하여 Amazon Simple Notification Service(Amazon SNS) 주제에 메시지를 게시합니다.
C. VPC에 대한 VPC 흐름 로그를 구성합니다. Amazon CloudWatch Logs 그룹을 지정합니다. 새 로그 항목을 구문 분석하고, 포트 22에서 성공적인 연결을 감지하고, Amazon Simple Notification Service(Amazon SNS)를 통해 알림을 게시하는 IAM Lambda 함수에 CloudWatch Logs 그룹을 구독합니다.
D. 매일 실행되고 보안 모범 사례 패키지를 사용하는 반복 Amazon Inspector 평가 실행을 생성합니다. 평가 실행이 시작될 때 IAM Lambda 함수를 호출하는 Amazon CloudWatch 규칙을 생성합니다. 완료되면 평가 실행 보고서를 검색하고 평가하도록 Lambda 함수를 구성합니다. 무제한 수신 SSH 트래픽에 대한 위반이 있는 경우 Amazon Simple Notification Service(Amazon SNS) 알림을 게시하도록 Lambda 함수도 구성합니다.
Answer: A

QUESTION NO: 24
한 회사가 Auto Scaling 그룹의 Amazon EC2 인스턴스에서 애플리케이션을 실행하고 있습니다. 애플리케이션이 로그를 로컬에 저장합니다. 보안 엔지니어가 축소 이벤트 후 로그가 손실되었음을 발견했습니다. 보안 엔지니어는 로그 데이터의 내구성과 가용성을 보장하는 솔루션을 권장해야 합니다. 모든 로그는 감사 목적으로 최소 1 년 동안 보관해야 합니다. 보안 엔지니어는 무엇을 권장해야 합니까?
A. Auto Scaling 수명주기 내에서 EC2 인스턴스가 생성 될 때마다 Amazon Elastic Block Store (Amazon EBS) 로그 볼륨을 생성하고 연결하는 후크를 추가합니다. 인스턴스가 종료되면 로그 검토를 위해 EBS 볼륨을 다른 인스턴스에 다시 연결할 수 있습니다.
B. Amazon Elastic File System (Amazon EFS) 파일 시스템을 생성하고 Auto Scaling 시작 템플릿의 사용자 데이터 섹션에 명령을 추가하여 EC2 인스턴스 생성 중에 EFS 파일 시스템을 탑재합니다. 로그를 한 번 복사하도록 인스턴스에서 프로세스를 구성합니다. 인스턴스 Amazon Elastic Block Store (Amazon EBS) 볼륨에서 EFS 파일 시스템의 디렉터리로 하루.
C. Auto Scaling 그룹에서 사용되는 AMI에 Amazon CloudWatch 에이전트를 빌드합니다. 검토를 위해 Amazon CloudWatch Logs에 로그를 보내도록 CloudWatch 에이전트를

구성합니다.
D. Auto Scaling 수명주기 내에서 종료 상태 전환시 수명주기 후크를 추가하고 Amazon Simple Notification Service (Amazon SNS)에 수명주기 알림을 사용하여 엔지니어링 팀에 알립니다. 인스턴스 종료 전에 보안 로그를 수동으로 검토 할 수 있도록 후크를 Terminating : Wait 상태로 1 시간 동안 유지하도록 구성합니다.
Answer: B

QUESTION NO: 25
회사의 IAM 계정은 약 300명의 IAM 사용자로 구성됩니다. 이제 100명의 IAM 사용자가 S3에 대한 무제한 권한을 가지려면 액세스 변경이 필요하다는 의무가 있습니다. 시스템 관리자로서 개별 사용자 수준에서 정책을 적용할 필요가 없도록 이를 효과적으로 구현하는 방법은 무엇입니까?
선택 해주세요:
A. 새 역할을 생성하고 각 사용자를 IAM 역할에 추가
B. IAM 그룹을 사용하고 역할에 따라 사용자를 다른 그룹에 추가하고 그룹에 정책을 적용합니다.
C. 정책을 생성하고 JSON 스크립트를 사용하여 여러 사용자에게 적용
D. 각 사용자의 IAM 계정 ID를 포함하는 무제한 액세스 권한이 있는 S3 버킷 정책을 생성합니다.
Answer: B
Explanation:
Option A is incorrect since you don't add a user to the IAM Role
Option C is incorrect since you don't assign multiple users to a policy Option D is incorrect since this is not an ideal approach An IAM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group For more information on IAM Groups, just browse to the below URL:
https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_eroups.html
The correct answer is: Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group Submit your Feedback/Queries to our Experts

QUESTION NO: 26
회사에는 각 비즈니스 단위에 대한 전용 계정을 포함하는 AWS Organizations의 조직이 있습니다. 회사는 최상위 계정의 단일 Amazon S3 버킷에 있는 계정에서 모든 AWS CloudTrail 로그를 수집하고 있습니다. 회사의 IT 거버넌스 팀은 최상위 계정에 액세스할 수 있습니다. 보안 엔지니어는 각 사업부가 자체 CloudTrail 로그에 액세스할 수 있도록 허용해야 합니다.
보안 엔지니어는 각각의 다른 계정에 대한 최상위 계정에서 IAM 역할을 생성합니다. 각 역할에 대해 보안 엔지니어는 각 로그의 접두사가 있는 S3 버킷의 객체에 대한 읽기 전용 권한을 허용하는 IAM 정책을 생성합니다.
해당 계정의 IAM 사용자가 로그를 읽을 수 있도록 각 사업부 계정에서 보안 엔지니어가 수행해야 하는 조치는 무엇입니까?
A. IAM 사용자에게 정책을 연결하여 사용자가 최상위 계정에서 생성된 역할을 맡도록 허용합니다. 정책에서 역할의 ARN을 지정합니다.
B. 최상위 계정에 권한을 부여하는 SCP를 생성합니다.

C. 사업부 계정의 루트 계정을 사용하여 최상위 계정에서 생성된 역할을 맡습니다. 정책에서 역할의 ARN을 지정합니다.
D. 최상위 계정의 IAM 역할 자격 증명을 사업부 계정의 IAM 사용자에게 전달합니다.
Answer: A
Explanation:
To allow an IAM user in one AWS account to access resources in another AWS account using IAM roles, the following steps are required:
Create a role in the AWS account that contains the resources (the trusting account) and specify the AWS account that contains the IAM user (the trusted account) as a trusted entity in the role's trust policy. This allows users from the trusted account to assume the role and access resources in the trusting account.
Attach a policy to the IAM user in the trusted account that allows the user to assume the role in the trusting account. The policy must specify the ARN of the role that was created in the trusting account.
The IAM user can then switch roles or use temporary credentials to access the resources in the trusting account.
Verified Reference:
https://repost.aws/knowledge-center/cross-account-access-iam
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

QUESTION NO: 27
회사의 보안 정책에 따라 모든 VPC에서 VPC 흐름 로그를 활성화해야 합니다. 보안 엔지니어는 규정 준수를 위해 VPC 리소스를 감사하는 프로세스를 자동화하려고 합니다. 엔지니어는 어떤 조합의 조치를 취해야 합니까? (두 가지를 선택하세요.)
A. 지정된 VPC에 대해 흐름 로그가 활성화되었는지 여부를 결정하는 IAM Lambda 함수를 생성합니다.
B. 회사 IAM 계정의 각 VPC에 대한 IAM 구성 구성 항목을 생성합니다.
C. 리소스 유형이 IAM:: Lambda:: Function인 IAM Config 관리형 규칙을 생성합니다.
D. IAM Config에서 내보낸 이벤트를 트리거하는 Amazon CloudWatch 이벤트 규칙을 생성합니다.
E. IAM Config 사용자 지정 규칙을 생성하고 이를 평가 로직이 포함된 IAM Lambda 함수와 연결합니다.
Answer: A,E
Explanation:
https://medium.com/mudita-misra/how-to-audit-your-aws-resources-for-security-compliance-by-using-custom-IAM-config-rules-2e53b09006de

QUESTION NO: 28
회사는 S3 버킷에서 중요한 데이터를 호스팅합니다. 버킷에 적절한 권한을 할당했지만 여전히 데이터 삭제가 걱정됩니다. 버킷에서 데이터 삭제 위험을 제한하기 위해 취할 수 있는 조치 아래의 옵션 중에서 2 개의 답변을 선택하십시오. 선택하십시오 :
A. S3 버킷에서 버전 관리 활성화

B. 버킷의 객체에 대해 유휴 데이터 사용
C. 버킷 정책에서 MFA 삭제 활성화
D. 버킷의 객체에 대해 전송중인 데이터를 활성화합니다
Answer: A,C
Explanation:
One of the IAM Security blogs mentions the followinj
You can add another layer of protection by enabling MFA Delete on a versioned bucket. Once you do so, you must provide your IAM accounts access keys and a valid code from the account's MFA device in order to permanently delete an object version or suspend or reactivate versioning on the bucket.
Option B is invalid because enabling encryption does not guarantee risk of data deletion.
Option D is invalid because this option does not guarantee risk of data deletion.
For more information on IAM S3 versioning and MFA please refer to the below URL:
https://IAM.amazon.com/blogs/security/securing-access-to-IAM-using-mfa-part-3/ The correct answers are: Enable versioning on the S3 bucket Enable MFA Delete in the bucket policy
Submit your Feedback/Queries to our Experts

QUESTION NO: 29
한 회사에 수백 개의 IAM 계정과 이러한 모든 계정에 대한 IAM CloudTrail을 수집하는 데 사용되는 중앙 집중식 Amazon S3 버킷이 있습니다. 보안 엔지니어는 추적이 회사의 IAM 계정에서 처음 활성화된 시점으로부터 3년 전의 CloudTrail 로그에 대해 임시 대기열을 실행할 수 있는 솔루션을 만들고자 합니다.
최소한의 관리 오버헤드로 이를 달성하려면 어떻게 해야 합니까?
A. CloudTrail 추적을 검사하기 위해 MapReduce 작업을 사용하는 Amazon EMP 클러스터를 실행합니다.
B. CloudTrail 콘솔의 이벤트 기록/기능을 사용하여 CloudTrail 추적을 쿼리합니다.
C. CloudTrail 추적을 쿼리하는 IAM Lambda 함수를 작성합니다. CloudTrail S3 버킷에 새 파일이 생성될 때마다 실행되도록 Lambda 함수를 구성합니다.
D. S3 버킷에서 CloudTrail 추적이 기록되는 Amazon Athena 테이블을 생성합니다. Athena를 사용하여 추적에 대해 쿼리를 실행합니다.
Answer: D

QUESTION NO: 30
귀사는 데이터 저장을 위해 S3 버킷을 사용합니다. 모든 서비스에 로깅을 활성화해야 한다는 회사 정책이 있습니다. IAM 계정에서 생성된 S3 버킷에 대해 로깅이 항상 활성화되도록 하려면 어떻게 해야 합니까?
선택 해주세요:
A. IAM Inspector를 사용하여 모든 S3 버킷을 검사하고 활성화되지 않은 버킷에 대한 로깅을 활성화합니다.
B. IAM 구성 규칙을 사용하여 버킷에 대한 로깅이 활성화되었는지 확인
C. IAM Cloudwatch 메트릭을 사용하여 버킷에 대한 로깅이 활성화되었는지 확인
D. IAM Cloudwatch 로그를 사용하여 버킷에 대한 로깅이 활성화되었는지 확인
Answer: B
Explanation:

This is given in the IAM Documentation as an example rule in IAM Config Example rules with triggers Example rule with configuration change trigger
1. You add the IAM Config managed rule, S3_BUCKET_LOGGING_ENABLED, to your account to check whether your Amazon S3 buckets have logging enabled.
2. The trigger type for the rule is configuration changes. IAM Config runs the evaluations for the rule when an Amazon S3 bucket is created, changed, or deleted.
3. When a bucket is updated, the configuration change triggers the rule and IAM Config evaluates whether the bucket is compliant against the rule.
Option A is invalid because IAM Inspector cannot be used to scan all buckets Option C and D are invalid because Cloudwatch cannot be used to check for logging enablement for buckets.
For more information on Config Rules please see the below Link:
https://docs.IAM.amazon.com/config/latest/developerguide/evaluate-config-rules.html The correct answer is: Use IAM Config Rules to check whether logging is enabled for buckets
Submit your Feedback/Queries to our Experts