

Amazon EBS와 Amazon EC2 인스턴스 스토어 비교



Amazon EBS

- Amazon EBS 볼륨에 저장된 데이터는 인스턴스의 수명과 무관하게 유지될 수 있습니다.
- 스토리지는 영구적입니다.

Amazon EC2 인스턴스 스토어

- 로컬 인스턴스 스토어에 저장된 데이터는 인스턴스가 활성화되어 있는 동안만 유지됩니다.
- 스토리지는 휘발성입니다.

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

로컬 인스턴스 스토어는 임시 데이터에만 사용합니다. 더 높은 수준의 내구성이 필요한 데이터는 Amazon EBS 볼륨을 사용하거나 데이터를 Amazon S3로 백업합니다. Amazon EBS 볼륨을 루트 파티션으로 사용하고 있고 Amazon EBS 볼륨이 인스턴스 수명을 초과하여 유지되길 원한다면, [Delete on termination flag]를 "No"로 설정하십시오.

재부팅, 중단 및 종료 비교				
특성	재부팅	중단/시작 (EBS 지원 인스턴스만 해당)	종료	최대 절전 모드
호스트 컴퓨터	인스턴스가 동일 호스트 컴퓨터에서 유지됩니다.	대부분의 경우 인스턴스가 새 호스트 컴퓨터에서 실행됩니다.		인스턴스가 새 호스트 컴퓨터에서 실행됩니다.
퍼블릭 IP 주소	변경 없음	새 주소가 지정됨		새 주소가 지정됨
탄력적 IP 주소	인스턴스와 연결된 상태로 유지됩니다.	인스턴스와 연결된 상태로 유지됩니다.	인스턴스와의 연결이 끊어졌습니다.	인스턴스와 연결된 상태로 유지됩니다.
인스턴스 스토리지 볼륨	보존됨	삭제됨	삭제됨	지원하지 않음
EBS 볼륨	보존됨	보존됨	부트 볼륨이 기본적으로 삭제됩니다.	보존됨
결제	인스턴스 청구 시간이 변경되지 않습니다.	상태가 중지 중으로 변경되는 즉시 비용 발생이 중단됩니다.	상태가 종료 중으로 변경되는 즉시 비용 발생이 중단됩니다.	최대 절전 모드로 전환하는 즉시 요금이 부과되지 않습니다.

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

이 표에는 인스턴스 재부팅, 중단 및 종료의 주요 차이점이 요약되어 있습니다.

자세한 내용은 다음을 참조하십시오:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html>

지식 확인



Q: 정적 자산을 호스팅하고 사용자가 업로드한 이미지와 비디오를 오프 인스턴스가 아닌 곳에 저장하여 웹 애플리케이션을 지원하는 AWS 서비스는 무엇입니까?

Amazon S3

Q: Amazon EC2 인스턴스는 어떻게 프라이빗 및 퍼블릭 IP 주소를 찾습니까?

인스턴스 메타데이터를 검색합니다: <http://169.254.169.254/latest/meta-data/>

Q: VPC의 서브넷 수준에서 보안 추가 계층의 역할을 하는 것은 무엇입니까?

네트워크 ACL

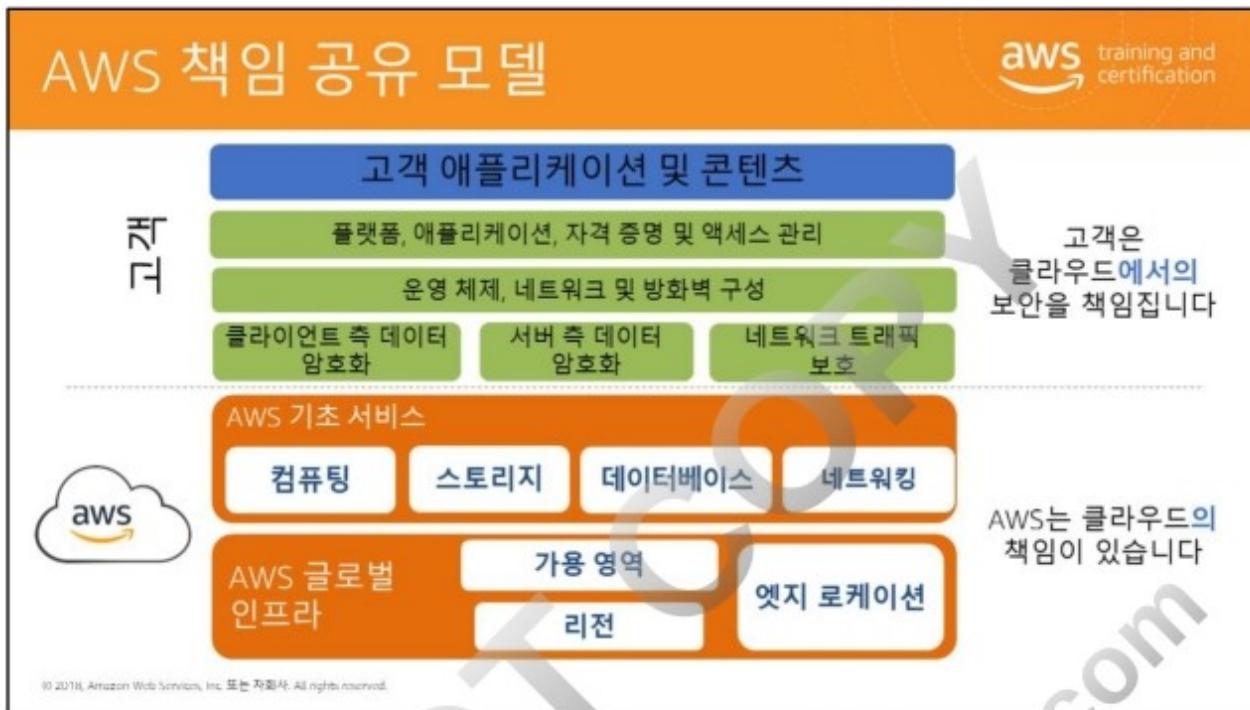
참 또는 거짓: Amazon S3는 저장할 수 있는 총 금액을 제한합니다.
거짓 (객체당 5 TB의 제한이 있음)

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

지식 확인에 대한 정답은 슬라이드에 나와 있습니다.







클라우드 보안을 설명할 때, AWS에서는 책임 공유 모델에 대한 논의부터 시작합니다. AWS에서는 기본 클라우드 인프라를 프로비저닝하고 유지 관리하지만, 클라우드에서의 안전을 보장하기 위해서는 고객도 몇 가지 보안 구성 작업을 직접 수행해야 합니다. 처음부터 하이퍼바이저까지가 AWS의 책임입니다. AWS에서는 제품 및 서비스 일체를 실행하는 하드웨어, 소프트웨어, 시설 및 네트워크를 보호합니다. 고객은 가입하는 서비스를 안전하게 구성할 책임이 있고 해당 서비스에 추가하는 모든 것에 책임을 집니다.

또한, AWS에서는 다음과 같은 책임을 수행합니다.

- 산업 인증 및 독립적인 타사 인증 획득
- 백서와 웹 사이트 콘텐츠를 통한 AWS 보안 및 규제 관행에 대한 정보 공개.
- NDA 체결 후, AWS 고객사에 인증서, 보고서 및 기타 문서 직접 제공(필요한 경우)

수행해야 할 보안 구성 작업의 양은 보유한 데이터의 민감도 및 선택한 서비스에 따라 달라집니다. 예를 들어 Amazon EC2 및 Amazon S3와 같은 AWS 서비스는 사용자가 전적으로 제어할 수 있으며 사용자가 직접 필요한 모든 보안 구성 및 관리 작업을 수행해야 합니다. Amazon EC2의 경우 사용자는 게스트 운영 체제(업데이트 및 보안 패치 포함)를 비롯하여 인스턴스에 설치한 모든 애플리케이션 소프트웨어나 유ти리티의 관리, 그리고 각 인스턴스에 대해 AWS에서 제공한 방화벽(보안

그룹이라고 부름)의 구성을 책임져야 합니다.

Amazon RDS, Amazon Redshift 또는 Amazon WorkDocs와 같은 AWS Managed Services를 사용할 때에는 인스턴스의 시작 및 유지 관리 또는 게스트 운영 체제나 애플리케이션의 패치 작업에 대해 걱정할 필요 없습니다. AWS에서 대신 모두 처리해 드립니다. 이러한 관리형 서비스의 기본 보안 구성 작업, 즉 데이터 백업, 데이터베이스 복제, 방화벽 구성 등의 작업은 자동으로 이루어집니다.

하지만 IAM 사용자 계정 및 자격 증명, 데이터 전송을 위한 SSL, 사용자 활동 로깅 등의 특정 보안 기능은 어떤 AWS 서비스를 사용하든 사용자가 구성해야 합니다.

AWS Support는 기술 지원을 원하는 고객에게 고도로 개인화된 수준의 서비스를 제공합니다.

자세한 내용은 다음을 참조하십시오.

- <https://aws.amazon.com/premiumsupport/>
- http://d0.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf
- <https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf>

물리적 보안



- 연중무휴 숙련된 경비 요원
- 평범해 보이는 비공개 시설에 위치한 AWS 데이터 센터
- 허가받은 직원에 대한 이중-팩터 인증
- 데이터 센터 액세스에 대한 권한 부여

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

AWS의 주요 보안 책임 중 하나는 AWS 클라우드 인프라를 수용하고 있는 데이터 센터의 물리적 보안입니다. Amazon은 대규모 데이터 센터를 설계, 구축 및 운영하는데 있어 오랜 경험을 축적해 왔습니다.

이러한 데이터 센터를 보호하는 물리적 보안 조치는 업계에서 가장 포괄적인 조치 중 하나이며, 연중무휴의 숙련된 경비 요원의 경비, 평범해 보이는 위치, 비공개 시설, 출입 시 이중-팩터 인증, 특정 승인된 요구에 한정된 데이터 센터 액세스 허용, 물리적 액세스 통제에 대한 지속적인 모니터링, 로깅 및 감사 등이 포함됩니다.

자세한 내용은 다음을 참조하십시오: 보안 센터 - <http://aws.amazon.com/security/>

하드웨어, 소프트웨어 및 네트워크

aws training and certification

- ▣ 자동 변경 제어 프로세스
- ▣ 모든 액세스 시도를 기록하는 배스천(Bastion) 서버
- ▣ 방화벽과 기타 경계 디바이스
- ▣ AWS 모니터링 도구



© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

AWS 클라우드 서비스를 지원하는 하드웨어 및 소프트웨어는 가용성과 중복성이 매우 높을 뿐 아니라 매우 안전하게 설계되었습니다. AWS 하드웨어 및 소프트웨어의 모든 변경 사항은 중앙 집중식 자동 변경 제어 프로세스를 통해 관리되며 하드웨어나 소프트웨어에 대한 모든 액세스는 승인을 받아야 합니다.

소프트웨어 및 시스템에 대한 액세스 권한이 있는 경우 SSH 로그인이 필요하며, 모든 액세스 시도를 기록하는 배스천 서버를 통해서만 액세스할 수 있습니다. 방화벽 및 기타 경계 디바이스를 비롯한 AWS 네트워크 디바이스는 네트워크 외부 경계 및 주요 내부 경계에서 통신을 모니터링하고 제어합니다.

AWS 모니터링 도구는 인바운드 및 아웃바운드 통신 지점에서 비정상적이거나 승인되지 않은 활동 및 조건을 감지하도록 설계되어 있습니다. 이러한 도구는 서버 및 네트워크 사용, 포트 스캐닝 활동, 애플리케이션 사용 및 무단 침입 시도를 모니터링합니다. AWS 보안 모니터링 도구는 분산, 플러팅 및 소프트웨어/로직 공격을 비롯한 다양한 유형의 서비스 거부(DoS) 공격을 파악하는데 도움이 됩니다.

자세한 내용은 다음을 참조하십시오: <http://aws.amazon.com/security/>



AWS는 여러 가지 감사, 인가 및 인증을 성공적으로 완료하였습니다. AWS는 SOC 2-보안 및 SOC 3 보고서와 마찬가지로 SSAE 16 및 ISAE 3402 전문 표준에 따라 Service Organization Controls SOC 1 보고서를 발행합니다.

또한, AWS는 ISO 9001, ISO 27001, ISO 27017 및 ISO 27018 인증을 획득하였고, Payment Card Industry(PCI) Data Security Standard(DSS)에 따라 성공적으로 Level 1 서비스 공급자로 검증받았으며, 현재 HIPAA의 적용을 받는 피보험 단체 및 기업 관련자에게 HIPAA Business Associate Agreements를 제공합니다.

공공 부문 인증의 경우, AWS는 FedRAMP 규정을 준수하고, 미국 총무청으로부터 FISMA Moderate 등급으로 운영할 수 있도록 승인을 받았으며, Defense Information Assurance Certification and Accreditation Program(DIACAP)에 따라 Authorities to Operate(ATOs)를 획득한 애플리케이션용 플랫폼이기도 합니다.

AWS는 그 외에도 NIST, FIPS 140-2, CJIS, DoD SRG Levels 2 및 4를 획득했습니다.

자세한 내용은 다음을 참조하십시오: <http://aws.amazon.com/compliance/>

SSL 엔드포인트



SSL 엔드포인트	보안 그룹	VPC
보안 전송 안전한 엔드포인트를 사용하여 보안 통신 세션(HTTPS)을 설정.	인스턴스 방화벽 보안 그룹을 사용하여 인스턴스에 대한 방화벽 규칙을 구성.	네트워크 제어 Virtual Private Cloud에서 퍼블릭 및 프라이빗 서브넷, NAT 및 VPN 지원을 사용하여 리소스 액세스에 대한 낮은 수준의 네트워킹 제약 조건을 생성.

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

AWS에서는 HTTPS 액세스가 가능한 고객 액세스 지점(API 엔드포인트라고도 부름)을 제공하므로, AWS 서비스에 SSL과 TLS를 비롯한 보안 통신 세션을 설정할 수 있습니다. SSL은 전송을 암호화하여 각 요청이나 응답이 전송 중에 외부에 노출되지 않도록 보호합니다.

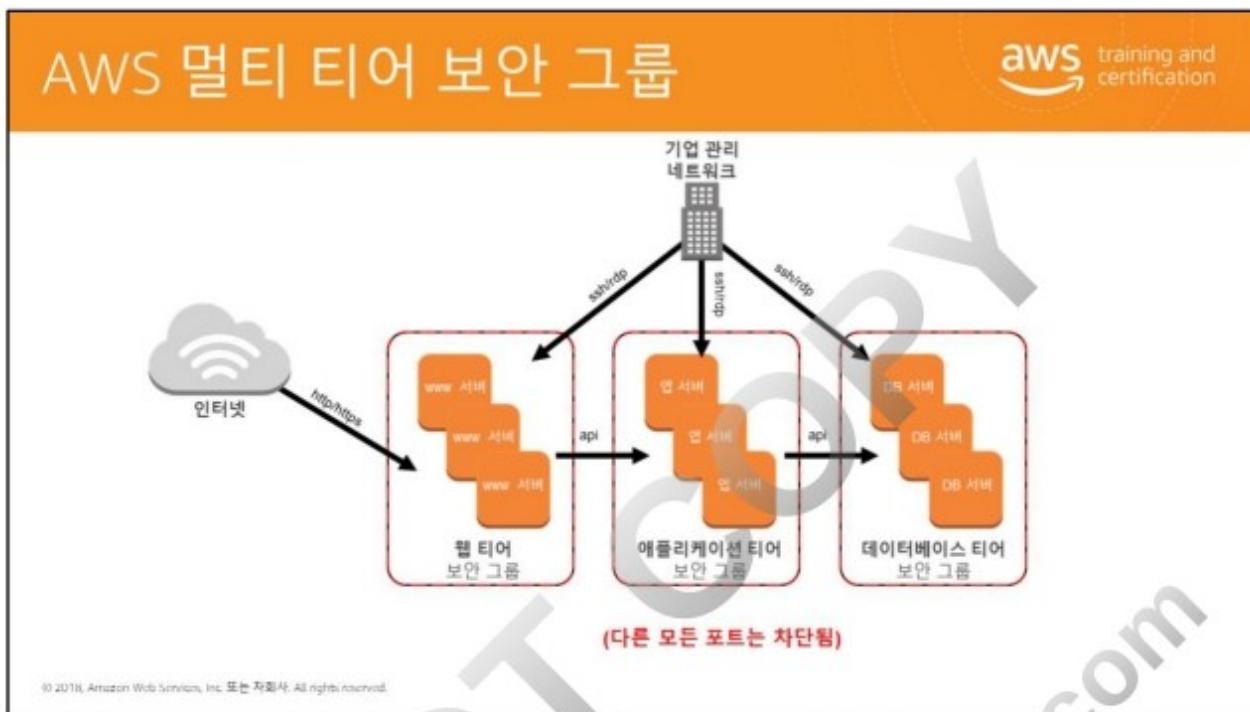
보안 그룹

The diagram illustrates three AWS security services:

- SSL 엔드포인트**:
 - 보안 전송**: An SSL endpoint is used to secure communication (HTTPS) between the user and the instance.
 - 설명: 안전한 엔드포인트를 사용하여 보안 통신 세션(HTTPS)을 설정.
- 보안 그룹**:
 - 인스턴스 방화벽**: A security group is used to define network traffic rules for instances.
 - 설명: 보안 그룹을 사용하여 인스턴스에 대한 방화벽 규칙을 구성.
- VPC**:
 - 네트워크 제어**: Network traffic is controlled within a Virtual Private Cloud (VPC).
 - 설명: Virtual Private Cloud에서 퍼블릭 및 프라이빗 서브넷, NAT 및 VPN 지원을 사용하여 리소스 액세스에 대한 낮은 수준의 네트워킹 제약 조건을 생성.

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

AWS는 사용자의 가상 서버에 내장 방화벽처럼 작동하는 보안 그룹도 제공합니다. 사용자는 완전 공개, 완전 비공개, 또는 중간 수준의 보안 그룹 규칙을 구성하여 인스턴스에 대한 액세스 수준을 제어할 수 있습니다. 인스턴스가 Virtual Private Cloud(VPC) 서브넷 내에 위치하는 경우 수신과 송신 트래픽을 모두 제어할 수 있습니다. 또한, 보안 그룹은 Amazon RDS, Amazon Redshift, Amazon EMR 및 Amazon ElastiCache와 같은 AWS 서비스에서 사용할 수 있습니다.



EC2 인스턴스에 대한 보안 그룹 규칙을 설정해 기존 방식의 멀티 티어 웹 아키텍처를 만들 수 있습니다.

소스 0.0.0.0/0을 선택하면 트래픽이 인터넷의 어디에서 들어오든지 80/443번 포트를 통해 웹 계층 보안 그룹에서 트래픽을 받을 수 있습니다.

마찬가지로 애플리케이션 계층은 웹 계층으로부터, DB 계층은 애플리케이션 계층으로부터의 트래픽만 허용할 수 있습니다.

마지막으로 SSH 포트 22를 통한 원격 관리를 가능하게 하는 규칙도 추가했습니다. 앱 티어를 통해 모든 트래픽을 전달하고 특정 IP의 액세스만 허용함으로써 원격 액세스를 제한했습니다. SSH를 사용하여 앱 티어 서버에 액세스한 후에, 웹 및 DB 보안 그룹의 머신에 연결할 수 있습니다.

Amazon Virtual Private Cloud

The diagram illustrates three methods for securing AWS resources:

- SSL 엔드포인트**:
 - 보안 전송**: An SSL endpoint is used to set up a secure communication session (HTTPS) between the user and the instance.
 - 설명: 안전한 엔드포인트를 사용하여 보안 통신 세션(HTTPS)을 설정.
- 보안 그룹**:
 - 인스턴스 방화벽**: A security group is used to define firewall rules for the instances.
 - 설명: 보안 그룹을 사용하여 인스턴스에 대한 방화벽 규칙을 구성.
- VPC**:
 - 네트워크 제어**: Network traffic is controlled within a VPC, supporting both public and private subnets, NAT, and VPN.
 - 설명: Virtual Private Cloud에서 퍼블릭 및 프라이빗 서브넷, NAT 및 VPN 지원을 사용하여 리소스 액세스에 대한 낮은 수준의 네트워킹 제약 조건을 생성.

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

Amazon Virtual Private Cloud(VPC) 서비스를 사용하면 프라이빗 서브넷을 생성하고 회사 네트워크와 VPC 사이에 IPsec VPN 터널을 추가함으로써, 인스턴스에 또 다른 네트워크 보안 계층을 추가할 수 있습니다. Amazon VPC를 사용하면 서브넷 정의, 네트워크 액세스 제어 목록, 인터넷 게이트웨이, 라우팅 테이블 및 가상 프라이빗 게이트웨이에 대한 정의를 비롯하여 자신만의 네트워크 토폴로지를 정의할 수 있습니다. 생성하는 서브넷은 프라이빗 또는 퍼블릭으로 정의할 수 있습니다.

자세한 내용은 다음을 참조하십시오: <http://aws.amazon.com/vpc/>



AWS IAM을 사용하면 AWS 사용자 및 그룹을 만들고 관리하며 AWS 리소스에 대한 액세스를 허용 및 거부할 수 있습니다. 새로운 AWS 자격 증명을 생성하지 않고도 기존 사내 자격 증명을 이용해 Amazon S3 버킷과 같은 AWS 리소스에 안전하게 액세스하도록 권한을 부여할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html



AWS 서비스 및 리소스는 AWS Management Console이나 AWS CLI를 사용하거나 지원되는 플랫폼의 API 및 SDK를 사용하여 액세스할 수 있습니다. 사용자와 시스템은 먼저 인증을 받아야 AWS 서비스 및 리소스에 액세스할 수 있습니다.

AWS Management Console은 AWS 서비스를 관리하는 웹 기반 방식을 제공합니다. 계정 소유자라면, 직접 AWS 루트 계정을 사용하여 콘솔에 로그인할 수 있습니다. 하지만 사용자별로 개별 IAM 사용자를 생성하고, 개별 자격 증명을 사용하여 로그인하는 것이 좋습니다.

IAM은 무료 서비스입니다.

자세한 내용은 다음을 참조하십시오:

<http://docs.aws.amazon.com/IAM/latest/UserGuide/console.html>

AWS IAM 인증

aws training and certification

- 인증
- AWS CLI 또는 SDK API
- 액세스 키와 보안 키

액세스 키 ID: AKIAIOSFODNN7EXAMPLE
보안 액세스 키: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

AWS CLI

```
:$ aws configure
AWS Access Key ID [*****022A]:
AWS Secret Access Key [*****4m8i]:
Default region name [ap-southeast-1]:
Default output format [json]:
```

AWS SDK 및 API

Java Python .NET

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

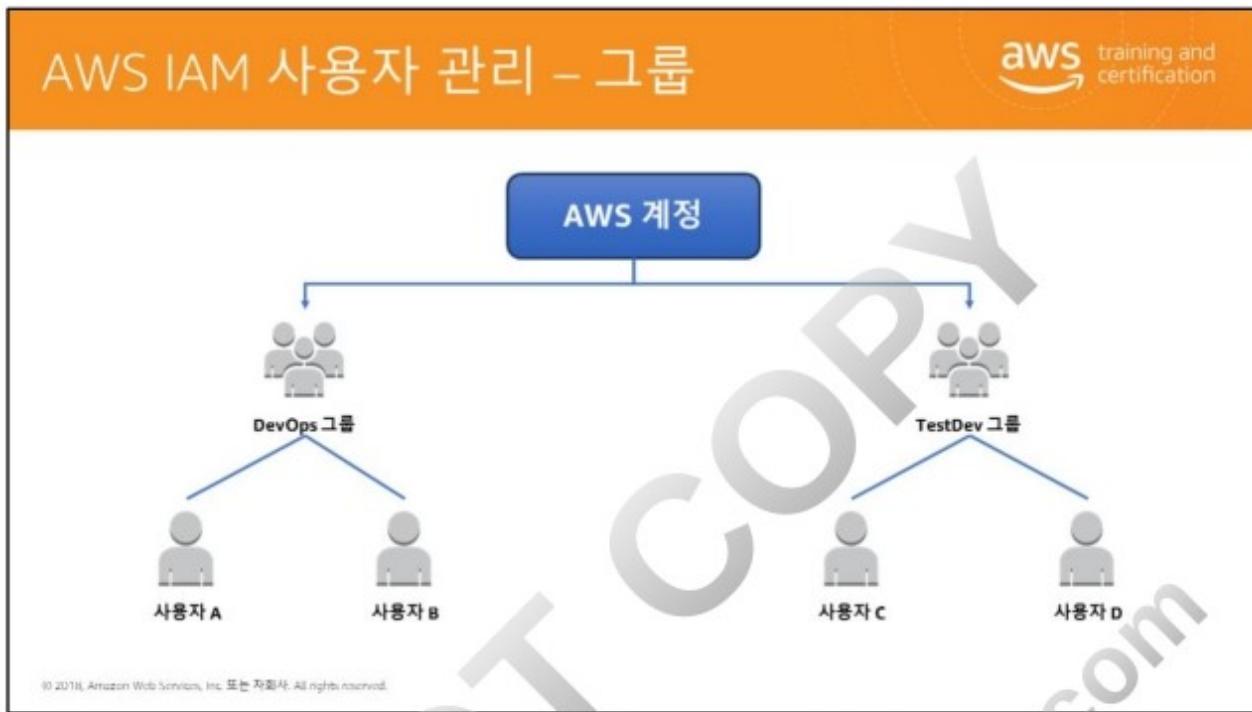
AWS CLI는 AWS 서비스를 관리하는 통합 도구입니다. AWS CLI에서는 여러 AWS 서비스를 명령줄에서 관리하고 스크립트를 통해 자동화할 수 있습니다.

AWS CLI는 Windows, Linux, macOS 및 Unix 플랫폼에서 지원됩니다.

AWS는 .NET, Java, Python 등과 같은 다양한 프로그래밍 플랫폼에 대한 지원을 제공합니다.

자세한 내용은 다음을 참조하십시오:

<http://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html>



AWS 환경을 관리하는 사용자 수가 늘어남에 따라, IAM 그룹을 사용하여 여러 IAM 사용자에 대한 권한을 관리하는 것이 도움이 됩니다.

자세한 내용은 다음을 참조하십시오:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html

AWS IAM 권한 부여

aws training and certification

권한 부여

정책:

- 권한을 설명하는 JSON 문서입니다.
- 사용자, 그룹 또는 역할에 지정됩니다.

IAM 사용자
IAM 그룹
IAM 역할

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

사용자 또는 시스템이 인증을 받으면, AWS 서비스에 액세스할 수 있는 권한을 부여받아야 합니다. 사용자, 그룹, 역할 또는 리소스에 권한을 할당하려면, 권한을 명시적으로 나열하는 문서인 정책을 생성합니다.

IAM 역할은 자격 증명이 AWS에서 무엇을 할 수 있고 무엇을 할 수 없는지 결정하는 권한 정책이 있는 AWS 자격 증명이라는 점에서 사용자와 비슷합니다. 하지만 한 명에게 고유하게 연결되는 대신, 역할은 필요한 누구나 이를 맡을 수 있게 되어 있습니다. 또한, 역할은 이와 연결된 자격 증명(암호 또는 액세스 키)이 전혀 없습니다. 대신, 사용자가 역할을 맡게 되면, 액세스 키가 동적으로 생성되어 사용자에게 제공됩니다.

정책 및 역할은 다음 슬라이드에서 좀 더 자세히 다룹니다.

AWS IAM 정책 요소

The screenshot shows the AWS IAM Policy Editor interface. On the left, a JSON policy document is displayed:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "Stmt1453690971587",  
            "Action": [  
                "ec2:Describe*",  
                "ec2:StartInstances",  
                "ec2:StopInstances"  
            ],  
            "Effect": "Allow",  
            "Resource": "*",  
            "Condition": {  
                "IpAddress": {  
                    "aws:SourceIp": "54.64.34.65/32"  
                }  
            }  
        },  
        {  
            "Sid": "Stmt1453690998327",  
            "Action": [  
                "s3:GetObject"  
            ],  
            "Effect": "Allow",  
            "Resource": "arn:aws:s3:::example_bucket/*"  
        }  
    ]  
}
```

On the right, there is a visual representation of the policy, showing a blue arrow pointing to a box labeled "IAM 정책" (IAM Policy) which contains three green checkmarks and one red X.

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

정책은 JavaScript Object Notation(JSON)을 사용해 생성된 문서입니다. 정책은 각각 하나의 권한 집합을 설명하는 하나 이상의 문으로 구성됩니다.

IAM 정책은 다음으로 구성될 수 있습니다.

- **버전**
- **Id**
- **Statement**
- **SID**
- **Effect**: 사용자가 액세스를 요청할 때 나타나는 결과(허용 또는 거부)를 정의합니다. 기본적으로 사용자는 리소스에 대한 액세스가 거부되어 있으므로, 사용자가 리소스에 액세스하는 것을 허용한다고 지정하는 것이 일반적입니다.
- **Principal**
- **NotPrincipal**
- **Actions**: 허용하려는 작업을 정의합니다. 각 AWS 서비스에는 자체 작업 세트가 있습니다. 명시적으로 허용하지 않은 작업은 모두 거부됩니다.
- **NotAction**
- **Resources**: 작업을 허용하는 리소스를 정의합니다. 사용자는 관련 권한이

명시적으로 부여되지 않은 어떠한 리소스에도 액세스할 수 없습니다.

- **NotResource**
- 조건
- 지원 데이터 형식

AWS 정책 생성기: AWS 정책 생성기를 사용하여 간편하게 정책을 생성할 수 있습니다.

AWS 정책 검사기: 정책 검사기는 IAM 정책 문법을 준수하는지 확인하기 위해 기존 IAM 액세스 제어 정책을 자동으로 검사합니다.

AWS 정책 시뮬레이터: 시뮬레이터는 사용자가 선택한 정책을 평가하고, 지정한 각 작업에 대한 효과적인 권한을 결정합니다. 이 시뮬레이터는 AWS 서비스에 대한 실제 요청에 사용되는 것과 동일한 정책 평가 엔진을 사용합니다.

관리형 정책: AWS 계정의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. 관리형 정책은 리소스가 아니라 자격 증명(사용자, 그룹 및 역할)에만 적용됩니다. 두 가지 유형의 관리형 정책을 사용할 수 있습니다.

- **AWS 관리형 정책:** AWS에서 생성하고 관리하는 관리형 정책. 정책 사용이 처음이라면, AWS 관리형 정책을 사용하여 시작하는 것이 좋습니다.
- **고객 관리형 정책:** 고객이 AWS 계정에서 생성하고 관리하는 관리형 정책. 고객 관리형 정책을 사용하면, AWS 관리형 정책을 사용할 때보다 좀 더 정밀하게 정책을 제어할 수 있습니다.

인라인 정책: 사용자가 생성하고 관리하며, 단일 사용자, 그룹 또는 역할에 직접 포함되는 정책입니다.

자세한 내용은 다음을 참조하십시오.

- [AWS 정책 생성기 - http://awspolicygen.s3.amazonaws.com/policygen.html](http://awspolicygen.s3.amazonaws.com/policygen.html)
- [정책 시뮬레이터에 액세스 - https://policysim.aws.amazon.com/home/index.jsp](https://policysim.aws.amazon.com/home/index.jsp)
- [IAM 정책 개요 - http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html)
- [IAM 정책 요소 참조 - http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements.html)



IAM 정책은 IAM 사용자와 그룹에 지정됩니다. 이러한 사용자는 IAM 정책에 정의된 권한의 제한을 받습니다.



IAM 정책은 IAM 역할에 지정될 수도 있습니다.

자세한 내용은 다음을 참조하십시오:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

AWS IAM 역할

aws training and certification

- IAM 역할은 정책을 사용합니다.
- IAM 역할에는 연결된 자격 증명이 없습니다.
- IAM 사용자, 애플리케이션 및 서비스는 IAM 역할을 맡을 수 있습니다.



IAM 역할

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

IAM 정책은 IAM 역할에 지정될 수도 있습니다.

IAM 역할은 자격 증명이 AWS에서 무엇을 할 수 있고 무엇을 할 수 없는지 결정하는 권한 정책이 있는 AWS 자격 증명이라는 점에서 사용자와 비슷합니다. 역할은 이와 연결된 자격 증명(암호 또는 액세스 키)이 전혀 없습니다. 대신, 사용자가 역할을 맡게 되면, 액세스 키가 동적으로 생성되어 사용자에게 제공됩니다.

자세한 내용은 다음을 참조하십시오:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html



보통은 AWS 리소스에 대한 액세스 권한이 없는 사용자, 애플리케이션 또는 서비스에 역할을 사용해 액세스 권한을 위임할 수 있습니다.

예: AWS 리소스에 대한 애플리케이션 액세스

Amazon EC2 인스턴스에 호스팅된 Python 애플리케이션은 Amazon S3와 상호 작용해야 합니다.

AWS 자격 증명이 필요합니다.

- 옵션 1: AWS 자격 증명을 Amazon EC2 인스턴스에 저장
- 옵션 2: AWS 자격 증명을 AWS 서비스 및 애플리케이션에 안전하게 배포

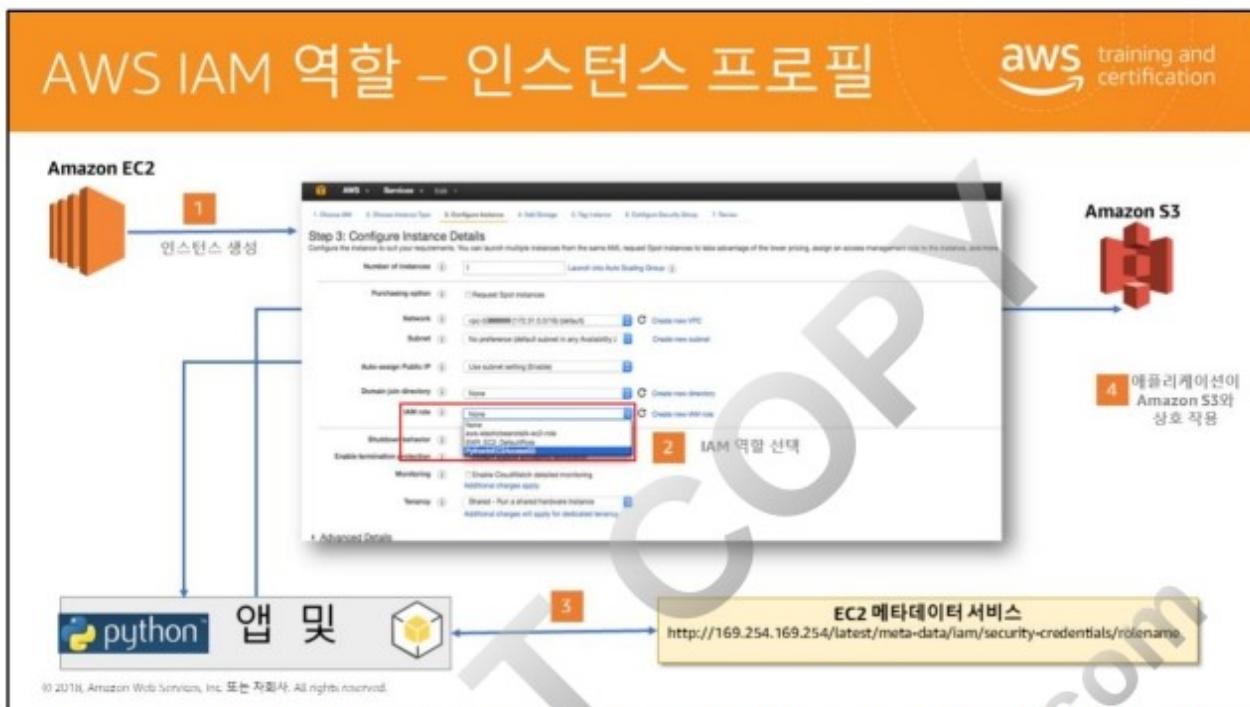
 IAM 역할

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

위의 예에서 Python으로 작성되고 Amazon EC2 인스턴스에 호스팅된 사용자 정의 애플리케이션은 Amazon S3 버킷에 저장된 객체와 상호 작용해야 합니다. 애플리케이션은 다양한 방법으로 AWS 리소스에 액세스할 수 있습니다. 그중 하나는 AWS 액세스 키 ID와 보안 액세스 키를 애플리케이션 코드 또는 애플리케이션에서 지원하는 구성 파일에 포함하는 것입니다. 하지만 이렇게 하면 사용자 자격 증명이 손상될 수 있습니다. 사용자 자격 증명을 변경하거나 교체할 때마다 코드 업데이트가 필요하게 됩니다. 이러한 접근 방식은 많은 경우에 안전하지도 실현 가능하지도 않습니다. 안전한 다른 옵션은 IAM 역할을 사용하여 인스턴스 프로필의 일부로 임시 보안 자격 증명을 전달하는 것입니다.

자세한 내용은 다음을 참조하십시오.

- 인스턴스 프로필 사용 –
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2_instance-profiles.html
- Amazon EC2에 대한 IAM 역할 –
<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>



인스턴스 프로필은 인스턴스가 시작될 때 역할 정보를 EC2 인스턴스에 전달하는 데 사용할 수 있는 IAM 역할용 컨테이너입니다.

이 예에서는 `PythonInEC2AccessS3`라는 이름의 IAM 역할이 IAM 사용자에 의해 생성되었습니다. 이 역할은 Amazon S3 버킷에 대한 액세스 권한을 부여합니다.

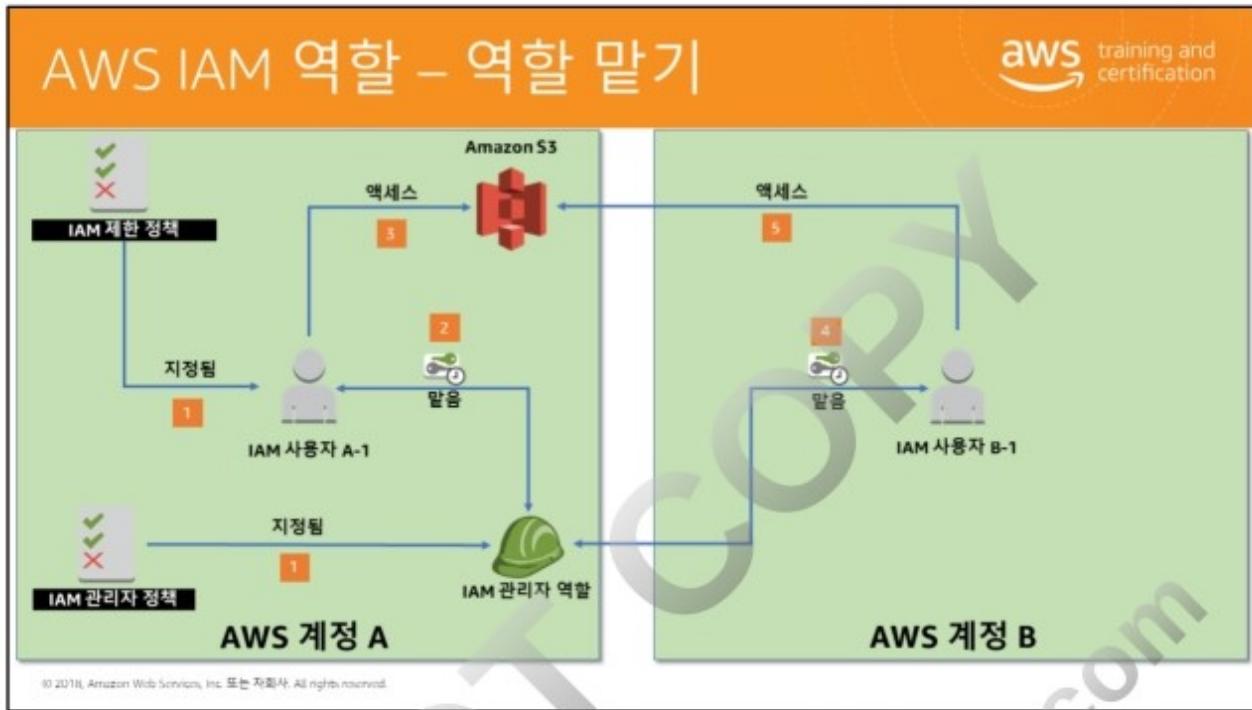
1. 애플리케이션 개발자는 Amazon EC2 인스턴스를 생성하면서 `PythonInEC2AccessS3` 역할을 선택합니다. 인스턴스는 Python 애플리케이션을 호스팅하게 되고, 이 애플리케이션은 Amazon S3 버킷에 액세스해야 합니다.

참고: IAM 역할은 생성 도중에만 EC2 인스턴스에 연결될 수 있습니다. 역할에 연결된 정책은 언제든 변경할 수 있습니다. EC2 인스턴스를 시작하는 사용자는 IAM 역할을 EC2 인스턴스에 연결하기 위한 적절한 권한이 필요합니다.

2. Python 애플리케이션이 EC2 인스턴스에 설치됩니다. Python용 AWS SDK(Boto3)도 인스턴스에 설치됩니다. 애플리케이션에서 Amazon S3 버킷에 대한 액세스를 시도합니다. 하지만 인스턴스에서는 AWS 자격 증명이 지원되지 않습니다.
3. Python 애플리케이션이 EC2 메타데이터 서비스를 사용하여 임시 보안 자격 증명에 액세스합니다.
4. 애플리케이션이 `PythonInEC2AccessS3` 역할에 지정된 Amazon S3 버킷과 상호 작용합니다.

자세한 내용은 다음을 참조하십시오:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html#instance-metadata-security-credentials>



또한, IAM 역할은 사용자에게 연결할 수 있습니다.

위의 예에는 A와 B라는 2개의 AWS 계정이 있습니다. IAM User A-1은 계정 A의 일부이고, IAM User B-1은 계정 B의 일부입니다.

1. Amazon S3 버킷에 대한 액세스 권한이 있는 IAM 관리자 정책이라는 IAM 정책은 IAM 관리자 역할이라는 IAM 역할에 연결되어 있습니다. User A-1은 제한적 액세스가 적용된 IAM 정책을 가지고 있습니다. 일반적으로 User A-1은 관리자 권한이 필요 없으므로 이처럼 제한적 액세스가 적용되었습니다. 하지만 User A-1은 가끔 관리자 권한이 필요한 작업을 수행해야 합니다.
2. 필요한 경우, User A-1이 IAM 관리자 역할을 맡습니다. 그렇게 함으로써 User A-1은 S3 버킷에 액세스할 수 있습니다. 역할을 맡은 사용자는 자체 권한을 임시로 포기하고, 대신 해당 역할의 권한을 맡게 됩니다. 사용자가 역할을 끝내거나 사용을 중단하면, 원래 사용자 권한이 복구됩니다. 따라서 변경이 필요할 때마다 사용자 정책을 변경하는 대신 IAM 역할을 사용하는 것이 유용합니다.

참고 : User A-1의 정책에는 역할을 맡을 수 있는 권한이 포함되어 있어야 합니다.

3. User A-1이 Amazon S3 버킷에 액세스할 수 있습니다.
4. IAM 역할의 경우, 신뢰하는 계정과 다른 AWS 신뢰할 수 있는 계정 간에 신뢰 관계를 설정할 수 있습니다. 신뢰하는 계정은 액세스할 리소스를 소유하고, 신뢰할 수 있는 계정은 해당 리소스에 액세스해야 하는 사용자를 포함합니다. 계정 B의

User B-1은 계정 A의 IAM 관리자 역할을 맡습니다.

5. User B-1이 계정 A가 소유한 Amazon S3 버킷에 액세스할 수 있습니다.

자세한 내용은 다음을 참조하십시오:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user.html

DO NOT COPY
zlagusdbs@gmail.com

임시 보안 자격 증명 (AWS STS)

aws training and certification

세션

- 액세스 키 ID
- 보안 액세스 키
- 세션 토큰
- 만료

임시 보안 자격 증명
15분에서 36시간

사용 사례

- 교차 계정 액세스
- 연동
- 모바일 사용자
- Amazon EC2 기반 앱을 위한 키 교체

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

AWS Security Token Service(AWS STS)는 신뢰할 수 있는 사용자에게 AWS 리소스에 대한 액세스를 제어할 수 있는 임시 보안 자격 증명을 제공합니다. 이러한 자격 증명은 단기용이며, 장기 액세스 키 자격 증명과 거의 동일하게 작동합니다. 이러한 자격 증명은 요청 시 동적으로 생성되어 사용자에게 제공됩니다.

AWS STS로 설정된 세션은 액세스 키 ID, 보안 액세스 키, 세션 토큰 및 만료 시간으로 구성됩니다. 만료 시간은 15분에서 36시간이 될 수 있습니다. API 요청에 서명하고 추가 파라미터로서 토큰을 전달하는데 키가 사용되며, AWS에서는 이를 사용하여 임시 액세스 키가 유효한지 확인합니다.

자세한 내용은 다음을 참조하십시오:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html



AWS IAM은 운영 체제 및 애플리케이션 인증용으로 부적합합니다.

AWS IAM 인증 및 권한 부여

aws training and certification

인증

- AWS Management Console
 - 사용자 이름 및 비밀번호
- AWS CLI 또는 SDK API
 - 액세스 키와 보안 키

권한 부여

- 정책

The diagram shows three icons representing IAM entities: a single user icon labeled 'IAM 사용자' (User), a group icon labeled 'IAM 그룹' (Group), and a role icon labeled 'IAM 역할' (Role).

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

IAM은 사용자와 AWS 리소스를 인증하고 권한을 부여하는 강력한 서비스입니다.

AWS IAM 모범 사례



- ▣ AWS 계정(루트) 액세스 키를 삭제.
- ▣ 개별 IAM 사용자를 생성합니다.
- ▣ 그룹을 사용하여 IAM 사용자에게 권한을 지정.
- ▣ 최소한의 권한 부여.
- ▣ 강력한 암호 정책 구성.
- ▣ 권한 있는 사용자에 대해 멀티 팩터 인증(MFA)을 활성화합니다.

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.



이 슬라이드는 IAM을 사용할 때 따라야 하는 일부 모범 사례를 보여줍니다.

AWS IAM 모범 사례(계속)



- ▣ Amazon EC2 인스턴스에서 실행되는 애플리케이션에 역할 사용.
- ▣ 자격 증명을 공유하기보다는 역할을 사용하여 위임.
- ▣ 자격 증명을 주기적으로 교체.
- ▣ 불필요한 사용자와 자격 증명을 제거합니다.
- ▣ 보안 강화를 위해 정책 조건을 사용합니다.
- ▣ AWS 계정 내 활동을 모니터링.

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

자세한 내용은 다음을 참조하십시오:

<http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

AWS CloudTrail



- ▣ 계정에 대한 AWS API 호출을 기록합니다.
- ▣ 정보와 함께 로그 파일을 Amazon S3 버킷에 전송합니다.
- ▣ AWS Management Console, AWS SDK, AWS CLI 및 상위 수준의 AWS 서비스를 사용하여 호출을 수행합니다.



The diagram illustrates the AWS CloudTrail architecture. On the left, there is a green cube icon labeled "AWS CloudTrail". A horizontal line labeled "로그" (Log) connects it to a red bucket icon labeled "Amazon S3 버킷" (Amazon S3 Bucket).

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

AWS CloudTrail은 계정에서 지원되는 AWS 서비스에 대한 API 호출을 기록하고 로그 파일을 사용자에게 전달하는 웹 서비스입니다.

지식 확인



Q: 보유한 웹 애플리케이션에서는 Amazon DynamoDB 테이블 및 Amazon S3 버킷을 읽고 써야 합니다. 이 작업에는 AWS 자격 증명과 AWS 서비스 사용에 대한 권한 부여가 필요합니다. 어떤 IAM 엔터티를 사용해야 합니까?

- 사용자
- 그룹
- 역할
- 정책

A: 역할

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

3교시 교육을 이수하셨습니다. 새로 익힌 기술을 테스트해 보십시오!



강사는 IAM 역할을 사용하여 사용자, 역할, 그룹 및 정책을 생성하는 방법을 시연합니다.





다음과 같은 기본 AWS 데이터베이스 서비스의 개념을 이해:

- Amazon Relational Database Service (Amazon RDS)
 - DB 인스턴스
 - 보안 그룹
 - RDS 인터페이스
- Amazon DynamoDB
 - Amazon DynamoDB 데이터 모델
 - 지원되는 작업
 - 프로비저닝된 처리량
 - DynamoDB 액세스하기

SQL 및 NoSQL 데이터베이스

aws training and certification

	SQL	NoSQL
데이터 스토리지	행 및 열	키-값
스키마	고정	동적
쿼리	SQL 사용	문서 수집에 집중
확장성	수직적	수평적

SQL

ISBN	Title	Author	Format
9182932465265	Cloud Computing Concepts	Wilson, Joe	Paperback
3142536475869	The Databasc Guru	Gomez, Maria	eBook

NoSQL

```
{  
  ISBN: "9182932465265",  
  Title: "Cloud Computing Concepts",  
  Author: "Wilson, Joe",  
  Format: "Paperback"  
}
```

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved. 2

SQL 데이터베이스는 데이터를 행과 열에 저장합니다. 행은 하나의 항목에 대한 모든 정보를 포함하고, 열은 데이터 요소를 분리하는 속성을 포함합니다. SQL 데이터베이스 스키마는 고정되어 있으며, 열은 데이터 입력 전에 잠겨 있어야 합니다.

데이터베이스가 전체적으로 변경되고 오프라인인 경우, 스키마를 수정할 수 있습니다. SQL 데이터베이스의 데이터는 복잡한 쿼리가 가능한 SQL(Structure Query Language)을 사용하여 쿼리합니다. SQL 데이터베이스는 하드웨어 성능을 높이는 방법으로 수직적으로 확장합니다.

NoSQL 데이터베이스는 키 값 페어, 문서 및 그래프를 비롯한 다양한 스토리지 모델 중 하나를 사용하여 데이터를 저장합니다. NoSQL 스키마는 동적이며, 정보를 신속하게 추가할 수 있습니다. 각 '행'은 각 '열'에 대한 데이터를 포함할 필요가 없습니다. NoSQL 데이터베이스의 데이터는 문서 수집에 집중하여 쿼리합니다. NoSQL 데이터베이스는 서버를 추가하는 방법으로 수평적으로 확장합니다.

데이터 스토리지 고려사항

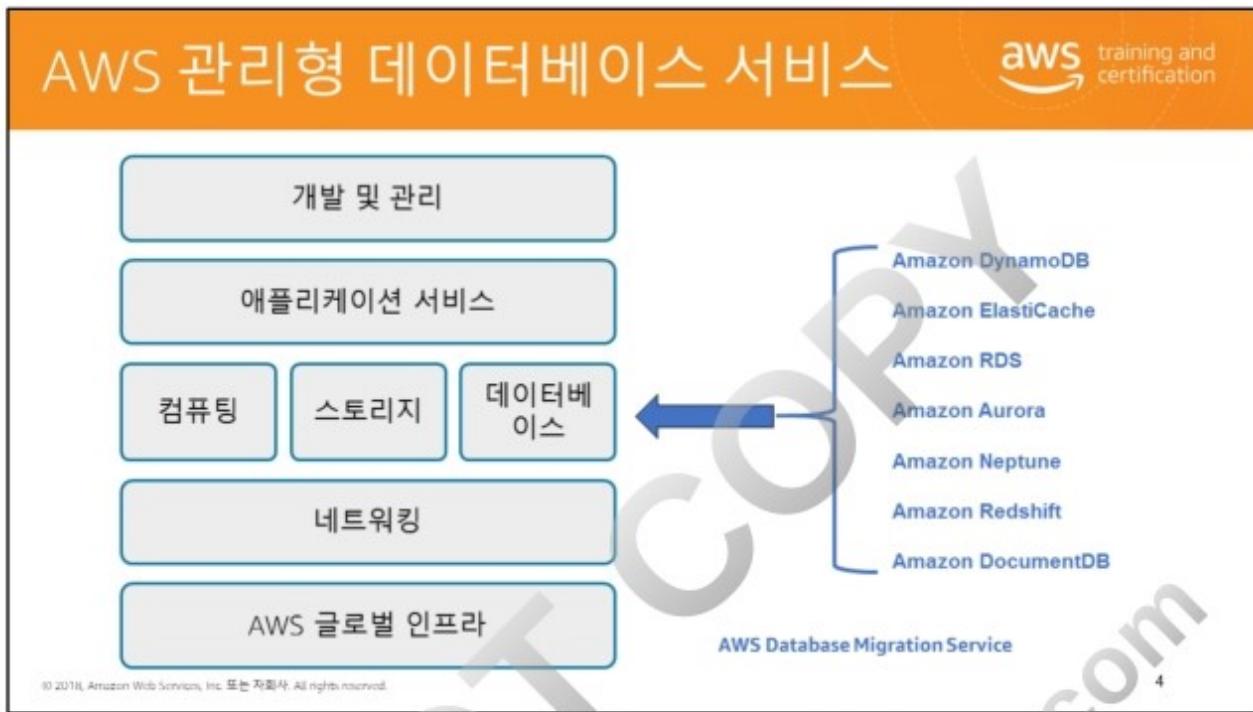


- ▣ 하나로 모든 요건을 충족할 수는 없습니다.
- ▣ 다음을 고려하여 데이터 요구 사항을 분석합니다.
 - ▣ 데이터 형식
 - ▣ 데이터 크기
 - ▣ 쿼리 빈도
 - ▣ 데이터 액세스 속도
 - ▣ 데이터 보존 기간

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

3

데이터베이스 유형을 고려할 때 하나로 모든 요건을 충족하는 데이터베이스는 없다는 것을 기억하시기 바랍니다. 데이터 형식, 데이터 크기, 쿼리 빈도, 데이터가 얼마나 빨리 필요한지, 데이터를 얼마나 오래 유지해야 하는지 등 데이터 요구 사항을 고려해야 합니다.



이 슬라이드는 AWS가 제공하는 데이터베이스 서비스를 보여줍니다.

Amazon Relational Database Service

 Amazon RDS

- 비용 효율적이고 조절 가능한 용량
- 시간 소모적인 데이터베이스 관리 작업을 지원
- Amazon Aurora, MySQL, MariaDB, Microsoft SQL Server, Oracle 및 PostgreSQL 데이터베이스의 전체 기능에 대한 액세스
- VMware에 배포 가능

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved. 5

Amazon RDS를 사용하면 친숙한 MySQL, MariaDB, Microsoft SQL Server, Oracle 또는 PostgreSQL 데이터베이스의 전체 기능에 액세스할 수 있습니다. MySQL용 Amazon RDS는 다중 AZ 배포와 읽기 전용 복제본이라는 서로 다르지만 상호 보완적인 두 가지 복제 기능을 제공합니다. 이 기능들을 함께 사용하면 데이터베이스 가용성이 향상되고, 예기치 않은 장애에 대비해 데이터베이스의 최신 변경 사항을 보호할 수 있습니다. 또한, 단일 DB 인스턴스의 용량을 한도 이상으로 확장해 읽기 중심의 데이터베이스 워크로드도 원활히 처리할 수 있습니다.

Amazon Aurora는 Amazon RDS의 일부인 MySQL 호환 관계형 데이터베이스 엔진입니다.

Relational Database Service (RDS) on VMware를 사용하면 고객이 Amazon RDS 기술을 사용하여 온프레미스 및 하이브리드 환경에 관리형 데이터베이스를 배포할 수 있습니다.

Amazon RDS

aws training and certification

- ▣ 간편하고 빠른 배포
- ▣ 일반적인 데이터베이스 관리 작업을 관리
- ▣ 애플리케이션과 호환됨
- ▣ 빠르고 예상 가능한 성능
- ▣ 간편하고 빠른 확장
- ▣ 보안
- ▣ 비용 효율적

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved. 6

Amazon RDS는 클라우드에서 관계형 데이터베이스를 손쉽게 설치, 운영 및 확장할 수 있게 해주는 웹 서비스입니다. 시간 소모적인 데이터베이스 관리 작업을 관리하는 한편, 효율적인 비용으로 크기 조정이 가능한 용량을 제공하므로 고객은 애플리케이션과 비즈니스에 좀 더 집중할 수 있습니다. Amazon RDS를 사용하면 MySQL, Oracle, SQL Server 또는 Amazon Aurora 데이터베이스 엔진의 전체 기능에 액세스할 수 있습니다. 따라서 기존 데이터베이스에서 이미 사용하고 있는 코드, 애플리케이션 및 도구를 Amazon RDS에서 사용할 수 있습니다. Amazon RDS는 자동으로 데이터베이스 소프트웨어를 패치하고 데이터베이스를 백업하므로, 고객이 정의한 보존 기간 동안 백업을 저장할 수 있고 특정 시점으로 복구가 지원됩니다. 단일 API 호출을 통해 관계형 데이터베이스 인스턴스와 관련된 컴퓨팅 리소스나 스토리지 용량을 유연하게 확장할 수 있는 이점을 활용할 수 있습니다.

DB 인스턴스



- DB 인스턴스는 Amazon RDS의 기본 빌딩 블록입니다.
- DB 인스턴스는 클라우드에 있는 격리된 데이터베이스 환경입니다.
- DB 인스턴스에는 사용자가 생성한 여러 데이터베이스가 포함될 수 있습니다.

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

7

Amazon RDS의 기본 빌딩 블록은 DB 인스턴스입니다. DB 인스턴스는 클라우드에 있는 격리된 데이터베이스 환경입니다. DB 인스턴스에는 사용자가 만든 여러 데이터베이스가 포함될 수 있으며, 독립 실행형 데이터베이스 인스턴스에 사용하는 것과 동일한 도구 및 애플리케이션을 사용해 액세스할 수 있습니다. AWS Management Console, AWS CLI, 또는 Amazon RDS API를 사용하여 DB 인스턴스를 만들고 수정할 수 있습니다.

Amazon RDS 백업 작동 방식

aws training and certification

자동 백업:

- 데이터베이스를 특정 시점으로 복원합니다.
- 기본적으로 활성화되어 있습니다.
- 최대 35일까지 보존 기간을 선택할 수 있습니다.



수동 스냅샷:

- 스냅샷에서 새 데이터베이스 인스턴스를 구축할 수 있습니다.
- 사용자가 시작해야 합니다.
- 사용자가 삭제할 때까지 유지됩니다.
- Amazon S3에 저장됩니다.

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

DB 인스턴스의 자동 백업을 활성화하면 Amazon RDS가 매일 자동으로 데이터에 대한 완전한 스냅샷을 만들고(기본 백업 기간 내에), 트랜잭션 로그를 캡처(DB 인스턴스를 업데이트할 때)합니다. 특정 시점으로 복구를 시작할 때, DB 인스턴스를 사용자가 요청한 특정 시점으로 복구하기 위해 가장 적합한 일일 백업에 트랜잭션 로그가 적용됩니다. Amazon RDS는 보존 기간이라고 부르는 사용자가 지정한 일정 기간 동안 DB 인스턴스의 백업을 보관합니다. 보존 기간은 기본적으로 1일이지만 최대 35일까지 설정할 수 있습니다.

수동 데이터베이스 스냅샷은 사용자가 시작하며, 원하는 빈도로 DB 인스턴스를 일관되게 백업한 다음, 언제든지 그 상태로 복원할 수 있습니다. DB 스냅샷은 AWS Management Console 또는 CreateDBSnapshot API로 생성할 수 있으며, Console 또는 DeleteDBSnapshot API에서 명시적으로 삭제할 때까지 유지됩니다.

수동 데이터베이스 스냅샷은 Amazon Simple Storage Service (Amazon S3)에 보관됩니다. 활성 DB 인스턴스에 사용되는 데이터베이스 스토리지의 최대 100%까지는 백업 스토리지에 대해 추가 비용이 청구되지 않습니다.

교차 리전 스냅샷

aws training and certification

- 다른 AWS 리전에 저장된 데이터베이스 스냅샷 사본입니다.
- 재해 복구를 위한 백업을 제공합니다.
- 다른 리전으로 마이그레이션할 기반으로 사용할 수 있습니다.

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

9

교차 리전 스냅샷 사본은 모든 Amazon RDS 엔진에서 사용할 수 있습니다. 모든 크기의 스냅샷을 복사할 수 있습니다. 사본은 모든 퍼블릭 AWS 리전 간에 이동될 수 있으며, 전송을 하나 이상 실행하여 같은 스냅샷을 여러 리전으로 동시에 복사할 수 있습니다. 복사 작업 자체에는 비용이 부과되지 않으며, 소스 리전에서 송신되는 데이터와 대상 리전의 데이터 스토리지에 대해서만 비용을 지불합니다.

Amazon RDS 보안



- ▣ **Amazon VPC**에서 DB 인스턴스 실행.
- ▣ IAM 정책을 사용하여 RDS 리소스에 대한 액세스 권한을 부여.
- ▣ 보안 그룹을 사용.
- ▣ DB 인스턴스(Amazon Aurora, Oracle, MySQL, MariaDB, PostgreSQL, Microsoft SQL Server)에 Secure Socket Layer(**SSL**) 연결 사용.
- ▣ RDS 암호화를 사용하여 저장된 RDS 인스턴스와 스냅샷을 보호.
- ▣ Oracle DB and Microsoft SQL Server 인스턴스에 네트워크 암호화와 Transparent Data Encryption(**TDE**) 사용.
- ▣ DB 엔진의 보안 기능을 사용하여 DB 인스턴스에 대한 액세스를 제어.

© 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved.

10

DB 인스턴스에서 Amazon RDS 리소스 및 데이터베이스에 대한 액세스를 관리할 수 있습니다. 액세스 관리 방법은 사용자가 Amazon RDS를 사용하여 수행해야 하는 작업 유형에 따라 다릅니다.

- 네트워크 액세스 제어를 최대한 강화하려면 Amazon Virtual Private Cloud(Amazon VPC)에서 DB 인스턴스를 실행합니다.
- AWS Identity and Access Management (IAM) 정책을 사용하여, RDS 리소스를 관리할 수 있는 사용자를 결정하는 권한을 지정합니다. 예를 들면, AWS IAM을 사용하여 DB 인스턴스를 생성, 설명, 수정 및 삭제하고, 리소스에 태그를 지정하거나, DB 보안 그룹을 수정할 수 있는 사용자를 결정할 수 있습니다.
- 보안 그룹을 사용하여 어떤 IP 주소 또는 EC2 인스턴스가 DB 인스턴스에 있는 데이터베이스에 연결할 수 있는지 제어합니다. DB 인스턴스를 처음 생성하면, DB 인스턴스 방화벽이 연결된 보안 그룹에서 지정한 규칙 이외의 데이터베이스 액세스를 차단합니다.
- MySQL, MariaDB, PostgreSQL 또는 Microsoft SQL Server 데이터베이스 엔진을 실행하는 DB 인스턴스에 Secure Socket Layer(SSL) 연결을 사용합니다.
- Amazon RDS 암호화를 사용하여 저장된 RDS 인스턴스와 스냅샷을 보안합니다. Amazon RDS 암호화는 업계 표준 AES-256 암호화 알고리즘을 사용하여 RDS DB

인스턴스를 호스팅하는 서버의 데이터를 암호화합니다.

- Oracle DB 인스턴스에 네트워크 암호화와 Transparent Data Encryption(TDE)을 사용합니다.
- 데이터베이스가 로컬 네트워크에 있을 때처럼 DB 엔진의 보안 기능을 사용하여 DB 인스턴스에 있는 데이터베이스에 누가 로그인할 수 있는지 제어합니다.

자세한 내용은 다음을 참조하십시오.

- Virtual Private Cloud(VPC)와 Amazon RDS -
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.html
- IAM 사용자 생성 -
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_SettingUp.html#CHAP_SettingUp.IAM
- SSL을 사용하여 DB 인스턴스에 대한 연결 암호화 -
<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html>
- Amazon RDS 리소스 암호화 -
<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>
- Oracle NNE -
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.NetworkEncryption.html>
- Oracle TDE -
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.AdvSecurity.html>



이 슬라이드는 Amazon RDS 데이터베이스 인스턴스에서 실행되는 마스터 데이터베이스가 지원하는 Amazon EC2 인스턴스에서 실행 중인 애플리케이션의 간단한 애플리케이션 스택을 보여줍니다. 탄력적 로드 밸런서 뒤에 애플리케이션을 배치함으로써 나중에 Auto Scaling 및 Elastic Load Balancing 그룹과 같은 확장 기능과 컴퓨팅 복원력을 사용할 수 있습니다.