

아마존 웹 서비스

AWS

클라우드 컴퓨팅

1.1 클라우드 컴퓨팅

- 클라우드 컴퓨팅(Cloud Computing)

네트워크를 통해 다양한 **IT리소스**와 어플리케이션을 **온디맨드**로 제공하는 서비스

- **IT리소스** : 서버, 스토리지, 네트워크와 같은 IT의 기반자원
- **온디맨드**: 요구사항에 따라 즉시 제공/공급 하는 방식(주문형)

구분	대상	대표플랫폼
Public	일반 사용자	AWS, Azure, GCP
Private	내부 사용자	Openstack, Cloudstack

1.2 클라우드 컴퓨팅의 분류

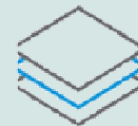
Infrastructure As A Service

- Hardware
- Server
- Storage
- NetworkCard



Platform As A Service

- MiddleWare/Runtime
- Database
- JAVA
- 인증서비스

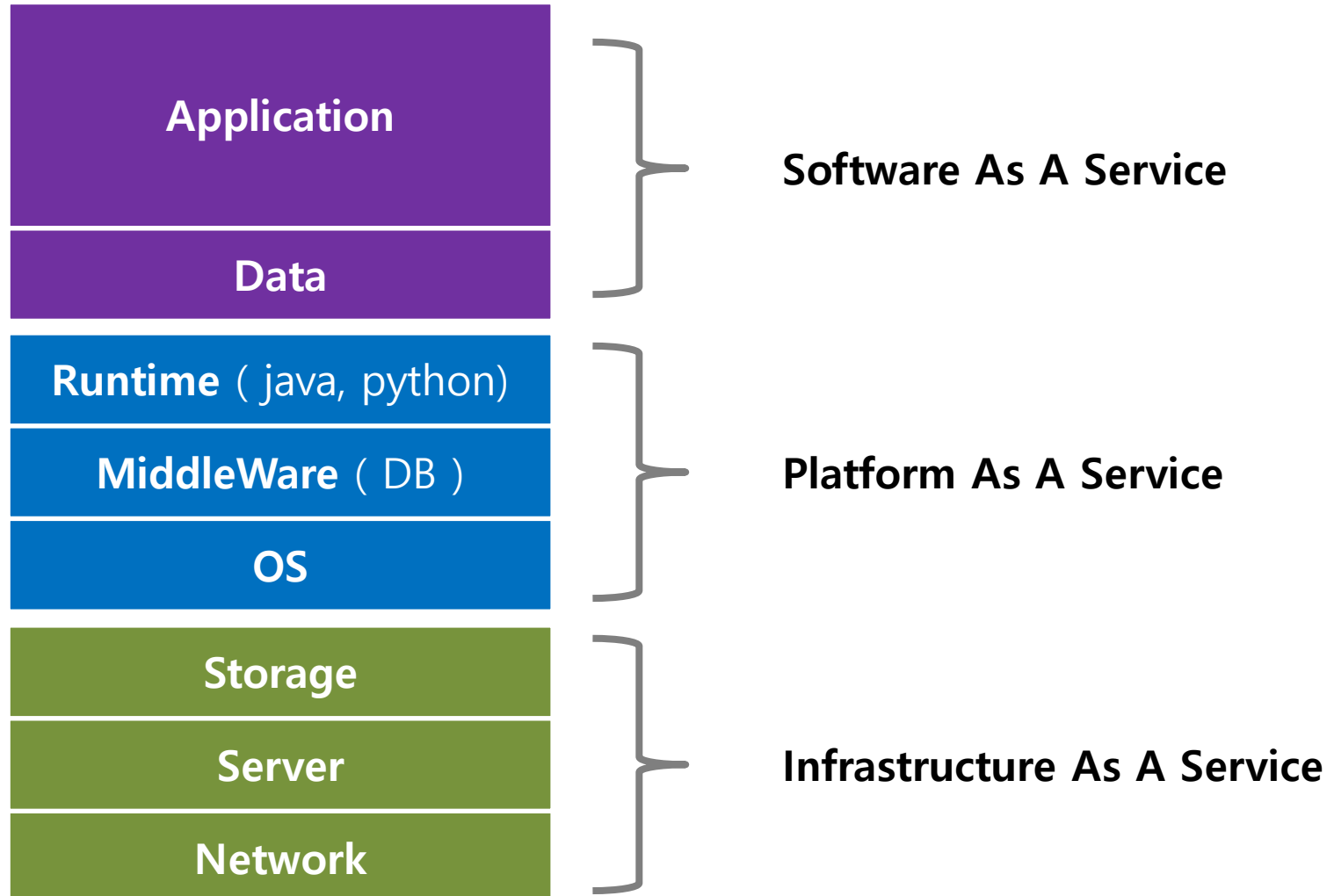


Software As A Service

- Application



1.2 클라우드 컴퓨팅의 분류



1.3 클라우드 컴퓨팅의 특징

- 온디맨드한 접근성
- 종량제 과금정책
- 대규모의 확장성
- 관리의 편리성

1.4 클라우드 컴퓨팅의 이점

- 비즈니스적인 측면

1. 초기 인프라 자원 투자에 대한 부담 감소
2. 사용한 양에 따른 비용(종량제)구조
3. 즉각적인 인프라 자원 제공
4. 효율적인 자원 할당 및 관리
5. Time to Market 시간 절감

1.4 클라우드 컴퓨팅의 이점

- 기술적인 측면

1. 자동화(프로그래밍 가능한 인프라자원)
2. Auto-Scaling, 탄력적인 확장
3. 개발 lifecycle 단축
4. 검증 절차 향상 (QA환경)
5. 대규모의 트래픽 수용 가능 (LB)
6. 비즈니스 연속성과 재해 복구

1.5 클라우드 컴퓨팅의 고려사항

- 고려사항

1. 개인정보 보호
2. 요구된 보안수준 확보
3. 서비스 가용성 확보
4. 제한사항에 따른 요구사항 파악

AWS

2.1 AWS 서비스

- Amazon Web Services

AWS는 높은 신뢰성과 확장성을 바탕으로 **웹스케일**의 솔루션을 제공하며 IT 자원들을 탄력적이며 효율적으로 비용을 관리할 수 있는 대표적인 **클라우드 제공자**이다.

- 웹스케일

글로벌 수준의 대규모의 환경에서도 높은 품질의 서비스를 영속적으로 제공하며 비즈니스의 요구사항에 맞춰 신속하고 안정적으로 IT 자원을 설계, 구축 및 관리하는 패턴

- 기타 클라우드 제공자

- Azure
- Google cloud Platform

2.1 AWS 서비스

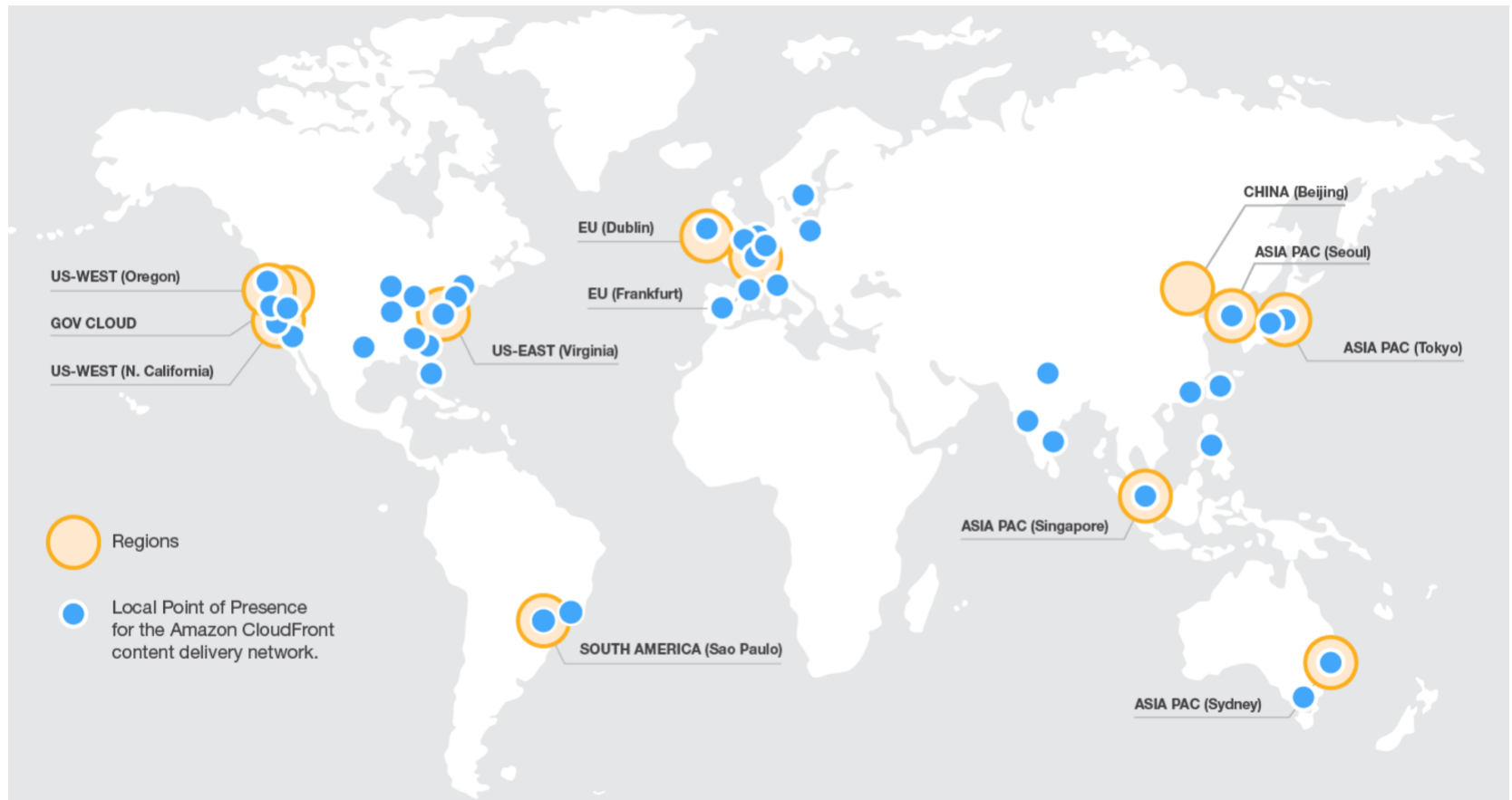
- AWS 서비스 이점
 - 민첩성과 즉각적인 탄력성
 - 비용 절감 효과
 - 개방성 및 유연성
 - 보안
 - 높은 기술 노하우

2.1 AWS 서비스

- AWS의 대표 솔루션
 - 어플리케이션 호스팅
 - 웹 사이트
 - 백업 및 스토리지
 - 데이터베이스
 - 엔터프라이즈 IT

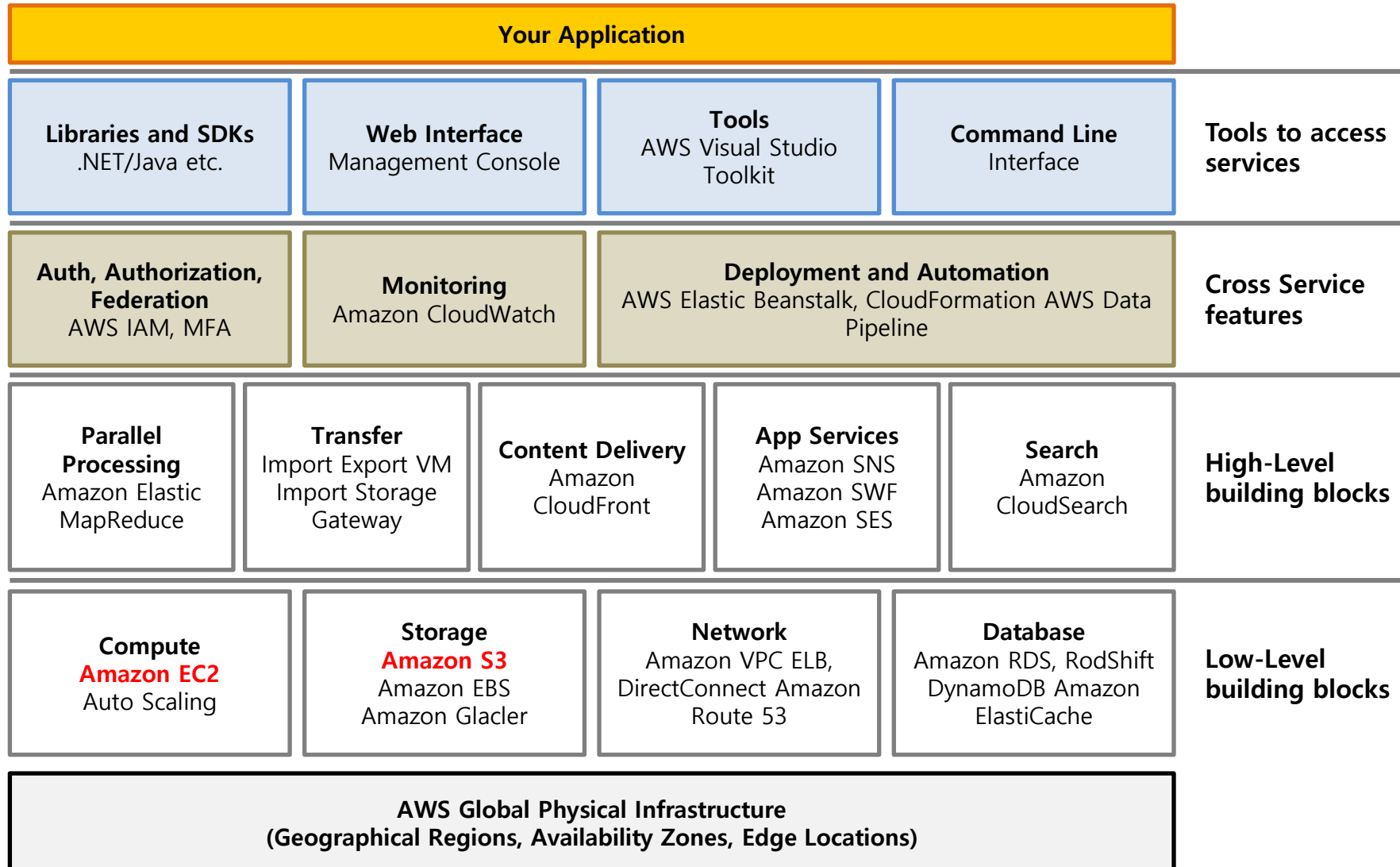
2.1 AWS 서비스

- AWS 글로벌 인프라



2.2 AWS 서비스 레이어

● 빌딩 블록



2.2 AWS 서비스 레이어

- 빌딩 블록



클라우드 디자인

4.1 AWS 지역, 가용영역 및 엣지

- 지역 및 가용영역

- AWS는 다양한 클라우드 서비스들을 세계 각지에서 제공하고 있으며 지리적인 위치를 바탕으로 **Region(지역)**을 구성한다.
- Region(지역)은 **Availability Zone(가용 영역)**이라고 불리는 **물리적으로 격리된 데이터 센터들의 집합**이며 이 가용영역에서 인스턴스와 데이터를 배치/저장/구성할 수 있도록 지원한다.

4.1 AWS 지역, 가용영역 및 엣지

● 지역(Region)

- 10개 이상 지리적인 곳에서 서비스가 되고 있으며 미국 서부, 미국 동부, 유럽, 남미, 중앙 아시아, 극동 아시아 및 호주 등에 위치



4.1 AWS 지역, 가용영역 및 엣지

- 가용영역(Availability Zone)

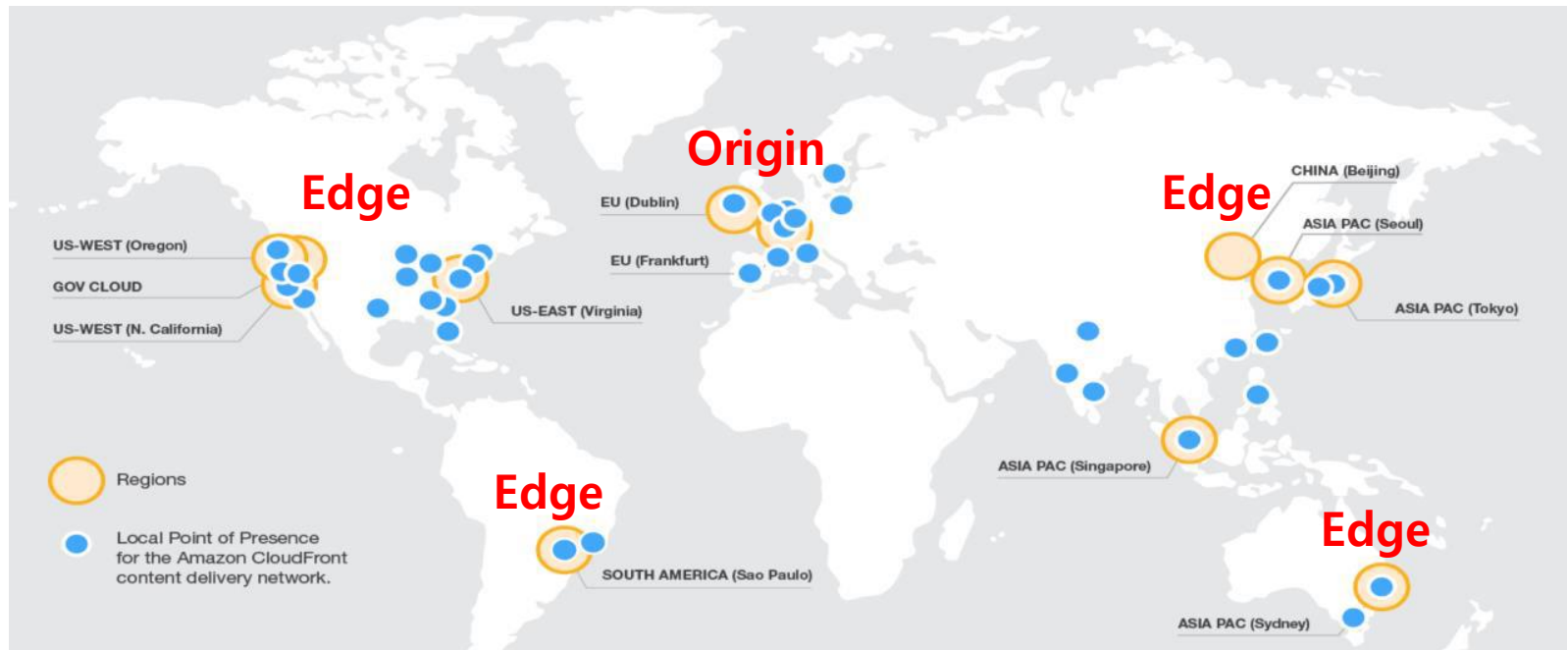
- 가용영역은 하나의 지역 안에 속하여 기본적인 서비스를 구성 가능하도록 IT 자원 등을 제공한다.
- 사용자가 직접 가용 영역을 선택 및 여러 가용영역에 복수개의 인스턴스들을 배치하여 서비스의 가용성을 높인다.
- 높은 가용성을 위해 하나의 지역에는 다수개의 AZ가 존재하며 해당 AZ간은 전용 사설 네트워크를 통해 낮은 네트워크 응답시간을 보장한다.

4.1 AWS 지역, 가용영역 및 엣지

- 엣지(Edge)

컨텐츠 전송 네트워크이며 웹 사이트, API, 동영상 콘텐츠 또는 기타 웹 자산의 전송을 가속화 하는 서비스이다.

- HTTP 또는 HTTPS 프로토콜을 사용하여 콘텐츠를 다운로드 하거나 RTMP 프로토콜로 콘텐츠를 스트리밍하여 배포할 수 있게 지원한다.



4.2 AWS 컴퓨트 서비스

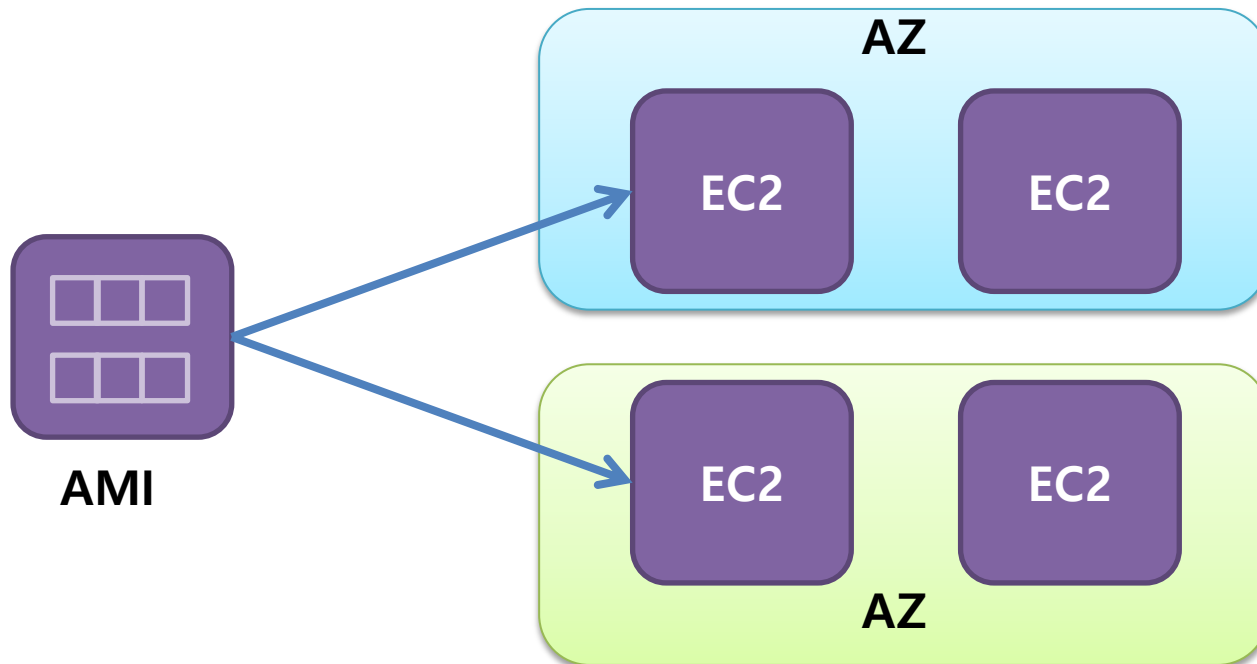
- AWS 컴퓨트 서비스 개념

- AWS는 어플리케이션의 요구사항에 맞게 다양한 컴퓨팅 서비스를 제공하고 있다.
- 예를 들어, **가상 컴퓨팅 자원(EC2)**을 할당하여 탄력적인 **웹스케일의 컴퓨팅**이나 **병렬작업 처리**를 가능하게 한다.
- 컴퓨팅 자원들은 가용영역 안에서 서비스 되며 시스템의 가장 기본적인 구성자원이 된다.

4.2 AWS 컴퓨트 서비스

- Elastic Compute Cloud(EC2)

EC2는 AWS에서 가장 기본이 되는 **Low-Level 빌딩 블록**에 속하는 컴퓨팅 서비스이며, EC2를 통해 원하는 만큼 **가상 서버를 구축하고 보안 및 네트워크 구성과 스토리지 관리가 가능하다.**



4.2 AWS 컴퓨터 서비스

● Amazon EC2란

- Amazon Elastic Compute Cloud(Amazon EC2)는 Amazon Web Services(AWS) 클라우드에서 확장식 컴퓨팅을 제공
- Amazon EC2를 사용하면 하드웨어에 선 투자할 필요가 없어 더 빠르게 애플리케이션을 개발하고 배포
- Amazon EC2를 통해 원하는 만큼 가상 서버를 구축하고 보안 및 네트워크 구성과 스토리지 관리가 가능
- Amazon EC2는 요건이나 갑작스러운 인기 증대 등 변동사항에 따라 확장하거나 축소할 수 있어 트래픽 예측 필요성이 줄어듦

4.2 AWS 컴퓨터 서비스

● Amazon EC2의 기능

- 인스턴스 : 가상 컴퓨팅 환경
- **Amazon 머신 이미지(AMI)** : 서버에 필요한 운영체제와 여러 소프트웨어들이 적절히 구성된 상태로 제공되는 템플릿으로 인스턴스를 쉽게 만들 수 있다.
- **인스턴스 유형** : 인스턴스를 위한 CPU, 메모리, 스토리지, 네트워킹 용량의 여러 가지 구성 제공
- 키 쌍을 사용해 인스턴스 로그인 정보 보호(AWS는 공용키를 저장하고 사용자는 개인 키를 안전한 장소에 보관하는 방식)
- **인스턴스 스토어 볼륨** : 임시 데이터를 저장하는 스토리지 볼륨으로 인스턴스 종료 시 삭제됨
- **Amazon Elastic Block Store(Amazon EBS)**, 즉 Amazon EBS 볼륨을 사용해 영구 스토리지 볼륨에 데이터 저장

4.2 AWS 컴퓨터 서비스

● Amazon EC2의 기능

- 인스턴스와 Amazon EBS 볼륨 등의 리소스를 다른 물리적 장소에서 액세스할 수 있는 리전 및 가용 영역
- 보안 그룹을 사용해 인스턴스에 연결할 수 있는 프로토콜, 포트, 소스 IP 범위를 지정하는 방화벽 기능
- **탄력적 IP 주소(EIP)** : 동적 클라우드 컴퓨팅을 위한 고정 IPv4 주소
- 태그 : 사용자가 생성하여 Amazon EC2 리소스에 할당할 수 있는 메타데이터
- AWS 클라우드에는 논리적으로 격리되어 있지만, 원할 때 마다 고객님의 네트워크와 간편히 연결할 수 있는 가상 네트워크, Virtual Private Clouds(VPC)

4.2 AWS 컴퓨터 서비스

- Elastic Compute Cloud(EC2)

- EC2 구성요소

인스턴스 : 가상 컴퓨팅 환경

AMI : Amazon 머신이미지, 인스턴스에 필요한 OS와 소프트웨어가 구성된 템플릿(골드 이미지)

인스턴스 타입 : 가상 서버의 CPU, Memory 사이즈 용량

EIP(Elastic IP) : 가상의 컴퓨팅 서버에 할당되는 고정 공인 IP

VPC : 가상의 컴퓨팅 서버가 속하는 독립된 네트워크 블록

4.2 AWS 컴퓨터 서비스

- Amazon EC2로 설정

1. [AWS에 가입](#)
2. [IAM 사용자 생성](#)
3. [키 페어 생성](#)
4. [Virtual Private Cloud\(VPC\) 생성](#)
5. [보안 그룹 생성](#)

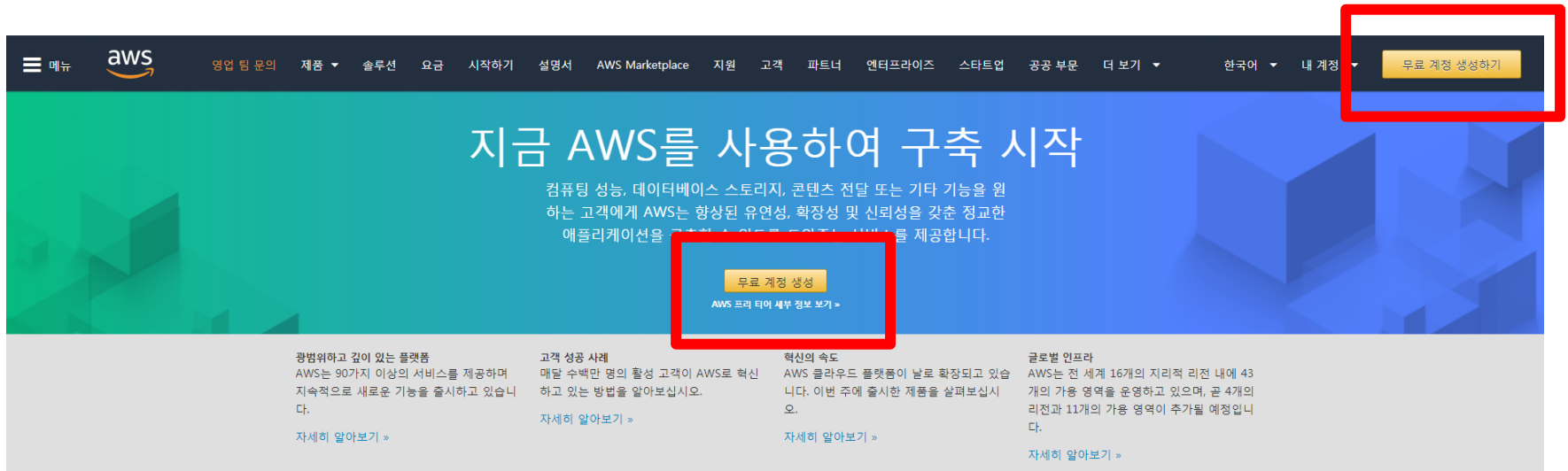
1. [AWS에 가입](#)
2. [키 페어 생성](#)
3. [보안 그룹 생성](#) (선택 : 기본 설정됨)

4.2 AWS 컴퓨트 서비스

1. AWS에 가입

<https://aws.amazon.com/ko/free/>

1. <https://aws.amazon.com/ko/free/>을 열고 [Create an AWS Account]를 선택



AWS 계정에 가입
AWS 프리 티어에 즉시 액세스할 수 있습니다.



10분 자습서로 배우기
간단한 자습서를 통해 자세히 알아보십시오.




AWS를 사용하여 구축 시작
AWS 프로젝트를 시작하는 데 도움이 되는 단계별 안내서를 통해 빌드를 시작하십시오.

AWS 제품 살펴보기



4.2 AWS 컴퓨터 서비스

1. AWS에 가입

한국어 ▾

AWS 계정 생성

12개월 프리 티어 액세스 포함
AWS 계정

Amazon EC2, Amazon S3 및 Amazon DynamoDB 사용 포함
제안 약관 전문은 aws.amazon.com/free 참조

이메일 주소

* 이메일은 필수 항목입니다

암호

암호 확인

AWS 계정 이름 ⓘ

계속

[기존의 AWS 계정으로 로그인](#)

© 2019 Amazon Web Services, Inc. 또는 자회사.
All rights reserved.
[개인 정보 보호 정책](#) | [이용 약관](#)

4.2 AWS 컴퓨터 서비스

1. AWS에 가입



한국어 ▾

결제 정보

결제 정보를 입력해야 자격 증명을 확인할 수 있습니다. 사용량이 [AWS 프리 티어 한도](#)를 초과하지 않는 한 요금을 청구하지 않습니다. 자세한 정보는 [FAQ](#)를 참조하십시오.

신용/직불 카드 번호

XXXXXXXXXXXXXXXXXXXX

카드 만료일

MM/YY - MM/YY

카드 소유자 이름

XXXXXXXXXXXXXXXXXXXX

청구지 주소

☒ 내 연락처 주소 사용

XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXX
XXXX

☐ 새 주소 사용

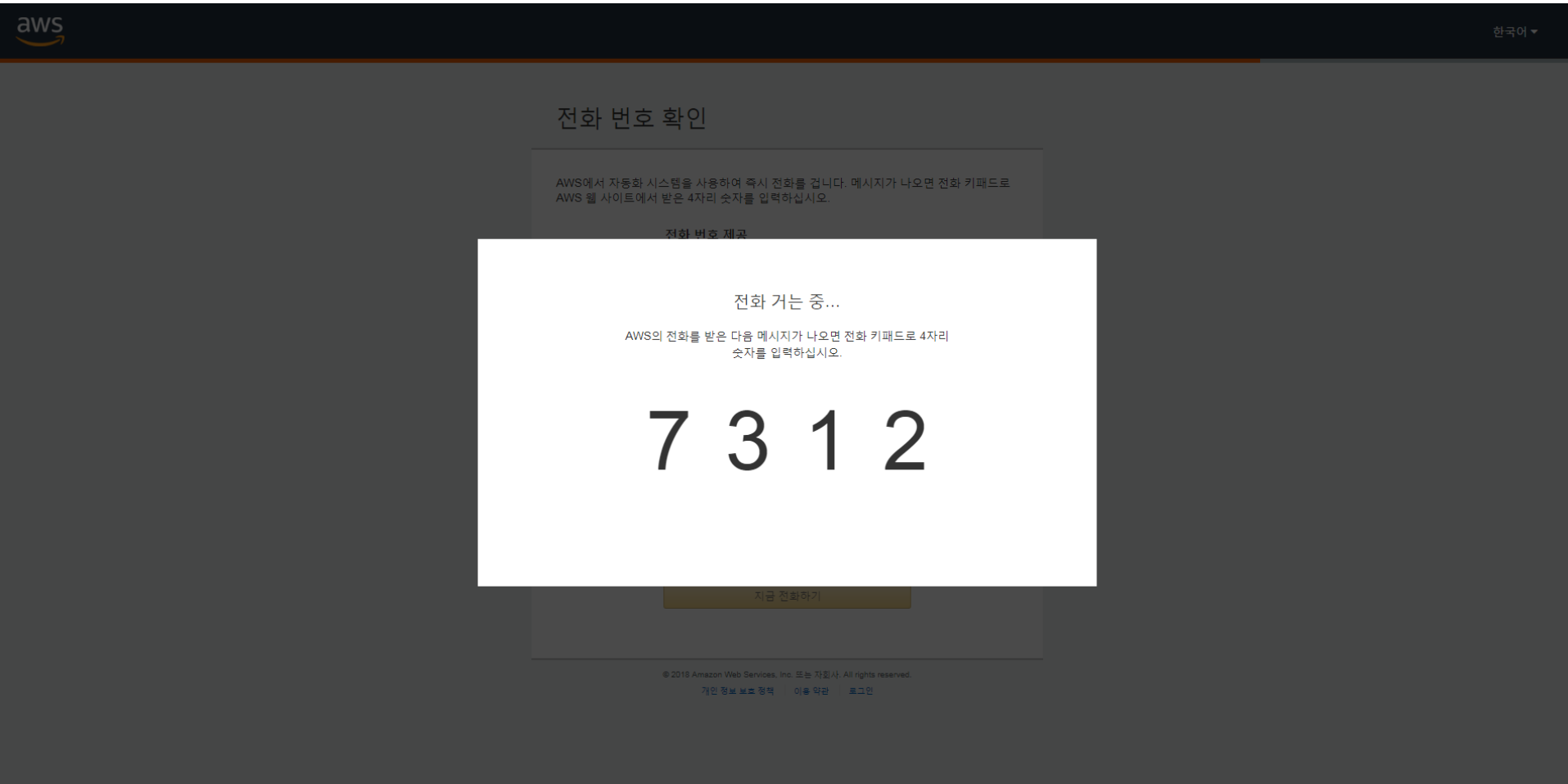
보안 전송

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

[개인 정보 보호 정책](#) | [이용 약관](#) | [로그인](#)

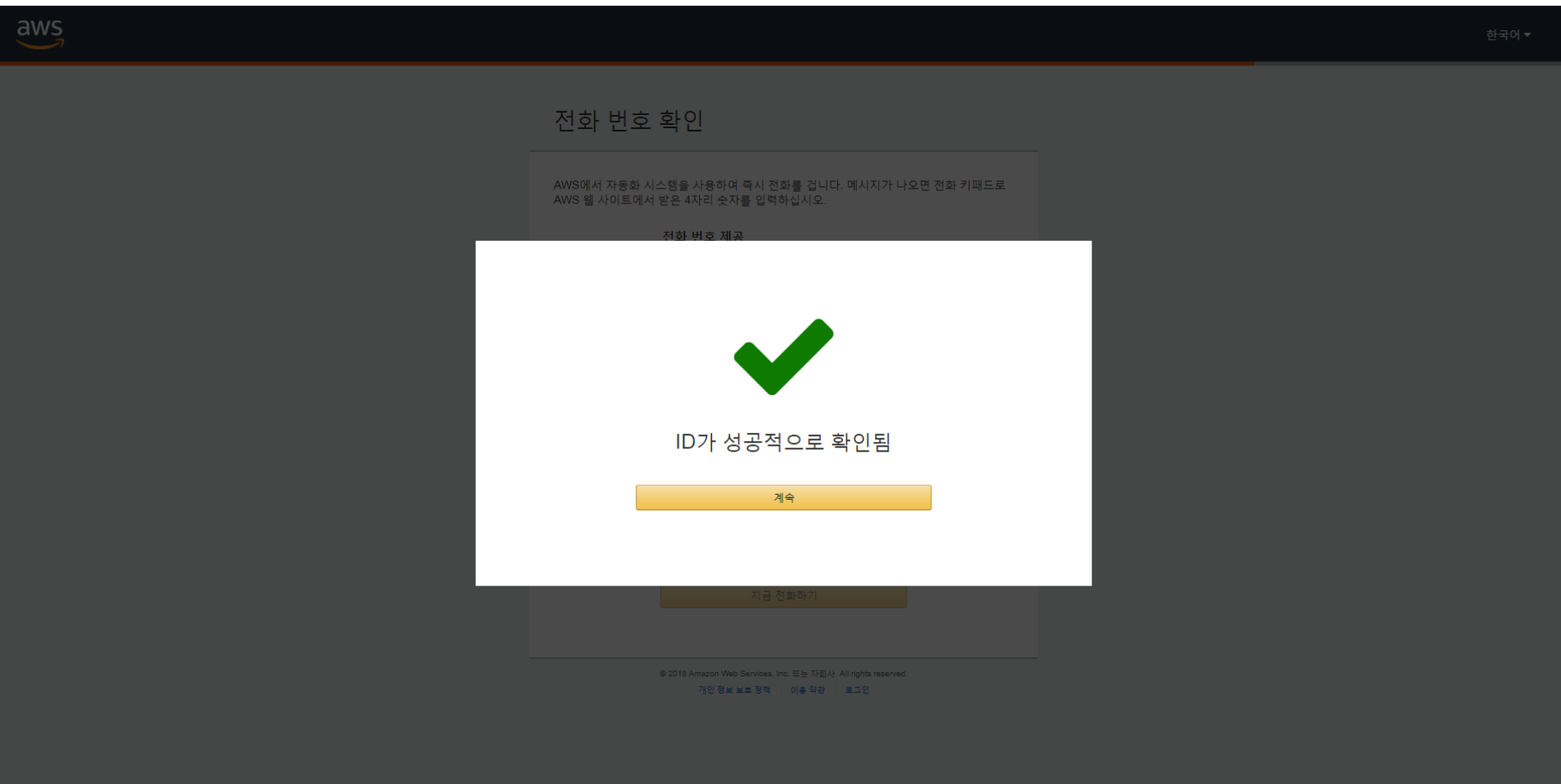
4.2 AWS 컴퓨터 서비스

1. AWS에 가입



4.2 AWS 컴퓨터 서비스

1. AWS에 가입



4.2 AWS 컴퓨터 서비스

1. AWS에 가입



한국어 ▾

지원 플랜 선택

AWS는 귀하의 요구를 충족할 수 있는 선별된 지원 플랜을 제공합니다. 귀하의 AWS 사용량에 맞는 지원 플랜을 선택하십시오. [자세히 알아보기](#)



기본 플랜

무료

- 모든 계정에 포함됨
- 포럼 및 리소스에 대한 상시 셀프 서비스 액세스
- 보안 및 성능 개선을 돕는 모범 사례 확인
- 상태 확인 및 알림에 대한 액세스



개발자 플랜

월 \$29부터

- 이론 채택, 테스트 및 개발을 위해 사용됨
- 업무 시간 중 AWS Support로의 이메일 액세스
- 하나의 기본 연락처로 무제한의 지원 사례를 열 수 있음
- 비 프로덕션 시스템에 대한 12시간 이내 응답



비즈니스 플랜

월 \$100부터

- 프로덕션 워크로드 및 비즈니스 크리티컬 의존성에 사용됨
- 채팅, 전화 및 이메일을 통한 AWS Support로의 상시 액세스
- 무제한의 연락처로 무제한의 지원 사례를 열 수 있음
- 프로덕션 시스템에 대한 1시간 이내 응답

엔터프라이즈 수준의 지원이 필요하십니까?

AWS에서 비즈니스와 미션 크리티컬 워크로드 실행(월 15,000 USD부터 시작됨)에 관한 추가 정보는 계정 관리자에게 문의하십시오. [자세히 알아보기](#)

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

[개인 정보 보호 정책](#) | [이용 약관](#) | [로그인](#)

4.2 AWS 컴퓨터 서비스

1. AWS에 가입

☰ 메뉴

aws

영업 팀 문의

제품 ▾

솔루션

요금

시작하기

설명서

AWS Marketplace

지원

고객

파트너

엔터프라이즈

스타트업

공공 부문

더 보기 ▾

한국어 ▾

내 계정 ▾

콘솔에 로그인

Amazon Web Services 사용을 환영합니다.

Amazon Web Services 계정을 만들어 주셔서 감사합니다. 지금 계정을 활성화하고 있으며 몇 분 이내에 완료됩니다. 활성화가 완료되면 이메일이 전송됩니다.

콘솔에 로그인

영업 팀 문의

귀하의 경험을 개인화하십시오.

아래 양식을 작성하면 귀하의 역할과 사용 사례에 따라 맞춤형 추천을 해드립니다.

말은 역할:


역할 선택 ▾

관심 분야:


사용 사례 선택 ▾

제출


10분 자습서로 AWS 시작하기




Linux 가상 머신 시작



파일을 클라우드에 저장



WordPress 웹사이트 시작



웹 애플리케이션 시작

모든 자습서 보기 >>

4.2 AWS 컴퓨터 서비스

2. IAM 사용자 생성

- Amazon EC2 등의 AWS 서비스에 액세스하려면 자격 증명을 제공해야 합니다.
- 리소스에 대한 액세스 권한이 있는지 여부를 파악해야 하기 때문입니다.
- 콘솔은 암호를 요구합니다.
- AWS 계정에 대한 액세스 키를 생성하면 명령줄 인터페이스 또는 API에 액세스할 수 있습니다. 그러나 AWS 계정에 자격 증명을 사용하여 AWS에 액세스하지 말고, AWS Identity and Access Management(IAM)를 사용하는 것이 좋습니다.
- IAM 사용자를 생성하여 관리자 권한과 함께 IAM 그룹에 추가하거나, 이 사용자에게 관리자 권한을 부여하면 IAM 사용자의 특정 URL이나 자격 증명을 사용하여 AWS에 액세스할 수 있습니다.

4.2 AWS 컴퓨터 서비스

2. IAM 사용자 생성

IAM 사용자를 직접 생성하여 Administrators 그룹에 추가하기

1. <https://console.aws.amazon.com/iam/>에서 AWS 계정 루트 사용자 이메일 주소 및 암호를 사용하여 IAM 콘솔에 [AWS 계정 루트 사용자](#) 로그인
2. 콘솔의 탐색 창에서 [Users]를 선택한 다음 [Add user]를 선택
3. [User name]에 Administrator를 입력
4. AWS Management 콘솔 access 옆의 확인란을 선택하고 Custom password를 선택한 다음 텍스트 상자에 새 사용자의 암호를 입력. 선택적으로 Require password reset을 선택하여 다음에 사용자가 로그인할 때 의무적으로 새 암호를 선택하도록 설정할 수 있다.
5. Next: Permissions를 선택.
6. Set permissions for user 페이지에서 Add user to group을 선택.

4.2 AWS 컴퓨터 서비스

7. **Create group**을 선택합니다.
8. [**Create group**] 대화 상자에 **Administrators**를 입력합니다.
9. **Filter**로 **Job function**을 선택합니다.
10. 정책 목록에서 **AdministratorAccess** 옆의 확인란을 선택합니다. 그런 다음 **Create group**을 선택합니다.
11. 그룹 목록으로 돌아가 새로 만든 그룹 옆의 확인란을 선택합니다. 목록에서 그룹을 확인하기 위해 필요한 경우 **Refresh**를 선택합니다.
12. **Next: Review**를 선택하여 새 사용자에게 추가될 그룹 멤버십의 목록을 확인합니다. 계속 진행할 준비가 되었으면 **Create user**를 선택합니다.

4.2 AWS 컴퓨터 서비스

● IAM 사용자 생성

1. <https://console.aws.amazon.com/iam/>에서 AWS 계정 루트 사용자 이메일 주소 및 암호를 사용하여 IAM 콘솔에 AWS 계정 루트 사용자 로그인



로그인 ⓘ

AWS 계정의 이메일 주소

IAM 사용자로 로그인하려면 계정 ID 또는
계정 별칭 을 입력하십시오.

weovercom

다음

————— AWS를 처음 사용하십니까? —————

AWS 계정 새로 만들기



AWS 계정에는 12개월 동안
프리 티어가 제공됩니다

Amazon EC2, Amazon S3 및
Amazon RDS 사용 포함

전체 제안 약관은 aws.amazon.com/free 참조

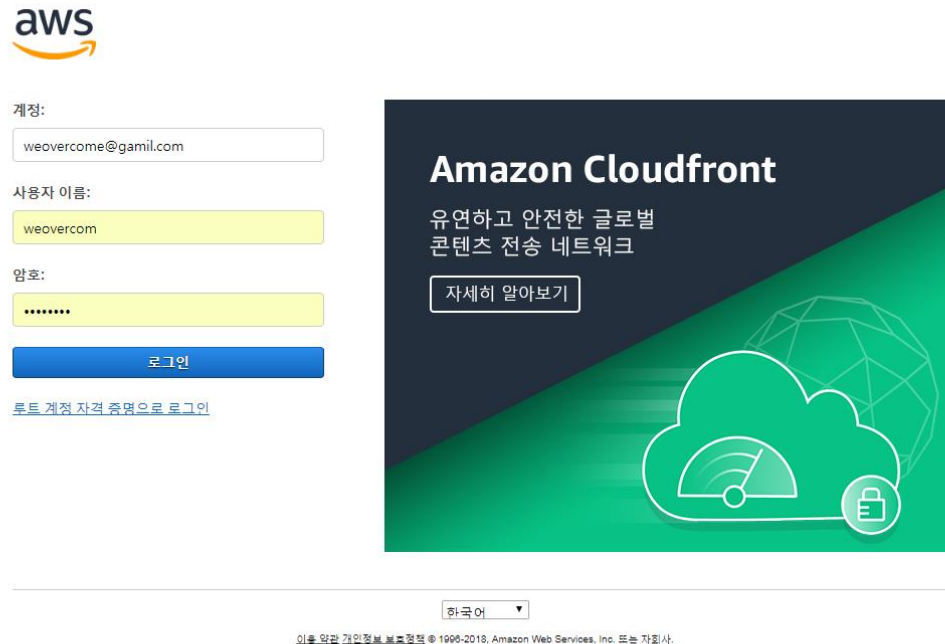
Amazon.com 로그인 정보

Amazon Web Services는 귀하의 Amazon.com 계정의 정보를 사용하여 귀하의 신원을 확인하고 Amazon Web Services에 대한 액세스를 허용합니다. 이 사이트 이용 시 아래에 링크된 당사 이용 약관 및 개인정보보호 정책이 적용됩니다. Amazon Web Services 제품 및 서비스 사용 시 귀하가 Amazon Web Services 또는 이러한 제품과 서비스를 판매하는 AWS VAR(Value Added Reseller)과 별도의 계약을 체결하지 않은 한, 아래 링크된 AWS 고객 계약이 적용됩니다. AWS 고객 계약은 2017년 3월 31일에 업데이트되었습니다. 이러한 업데이트에 대한 자세한 내용은 [최근 변경 사항](#)을 참조하십시오.

4.2 AWS 컴퓨터 서비스

2. IAM 사용자 생성

1. <https://console.aws.amazon.com/iam/>에서 AWS 계정 루트 사용자 이메일 주소 및 암호를 사용하여 IAM 콘솔에 [AWS 계정 루트 사용자](#) 로그인



aws

계정:
weovercome@gamil.com

사용자 이름:
weovercom

암호:

로그인

[루트 계정 자격 증명으로 로그인](#)

Amazon Cloudfront
유연하고 안전한 글로벌
콘텐츠 전송 네트워크
[자세히 알아보기](#)

한국어 ▼

이용 약관 개인정보 보호정책 © 1996-2018, Amazon Web Services, Inc. 또는 자회사.

4.2 AWS 컴퓨터 서비스

2. IAM 사용자 생성

1. <https://console.aws.amazon.com/iam/>에서 AWS 계정 루트 사용자 이메일 주소 및 암호를 사용하여 IAM 콘솔에 AWS 계정 루트 사용자 로그인

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with options like 'IAM 검색', '대시보드', '그룹', '사용자', '역할', '정책', '자격 증명 공급자', '계정 설정', '자격 증명 보고서', and '암호화 키'. The main content area is titled 'Identity and Access Management 소개'. It includes an 'IAM 사용자 로그인 링크:' section with a URL and a link icon. Below that, it shows 'IAM 리소스' with counts for '사용자: 0', '역할: 0', '그룹: 0', and '정책: 0'. A '보안 상태' (Security State) section shows a progress bar at 1/5 and a list of security checks: '루트 액세스 키 삭제' (checked), '루트 계정에서 MFA 활성화' (warning), '개별 IAM 사용자 생성' (warning), '그룹을 사용하여 권한 할당' (warning), and 'IAM 비밀번호 정책 적용' (warning). On the right, there's a '주요 기능' (Key Features) section with a video player titled 'Introduction to AWS IAM' and a '추가 정보' (Additional Information) section with links to 'IAM 모범 사례', 'IAM 설명서', 'Web Identity Federation Playground', '정책 시뮬레이터', and '비디오, IAM 릴리스 기록 및 추가 리소스'.

4.2 AWS 컴퓨터 서비스

2. IAM 사용자 생성

2. 콘솔의 탐색 창에서 [Users]를 선택한 다음 [Add user]를 선택

The screenshot shows the AWS IAM console interface. On the left, the navigation pane has '사용자' (Users) highlighted with a red box. The main content area is titled 'Identity and Access Management 소개'. It includes a link to the IAM user login page: <https://978124574942.signin.aws.amazon.com/console>. Below this, it shows statistics: '사용자: 0' (Users: 0), '그룹: 0' (Groups: 0), and '역할: 0' (Roles: 0). There is also a section for '고객 관리형 정책: 0' (Customer managed policies: 0). A '보안 상태' (Security state) section shows a progress bar at 1/5 완료 (1/5 complete) and a list of security checks, including '루트 액세스 키 삭제' (Delete root access keys), '루트 계정에서 MFA 활성화' (Enable MFA on root account), '개별 IAM 사용자 생성' (Create individual IAM users), '그룹을 사용하여 권한 할당' (Assign permissions using groups), and 'IAM 비밀번호 정책 적용' (Apply IAM password policy).

주요 기능

Introduction to AWS IAM

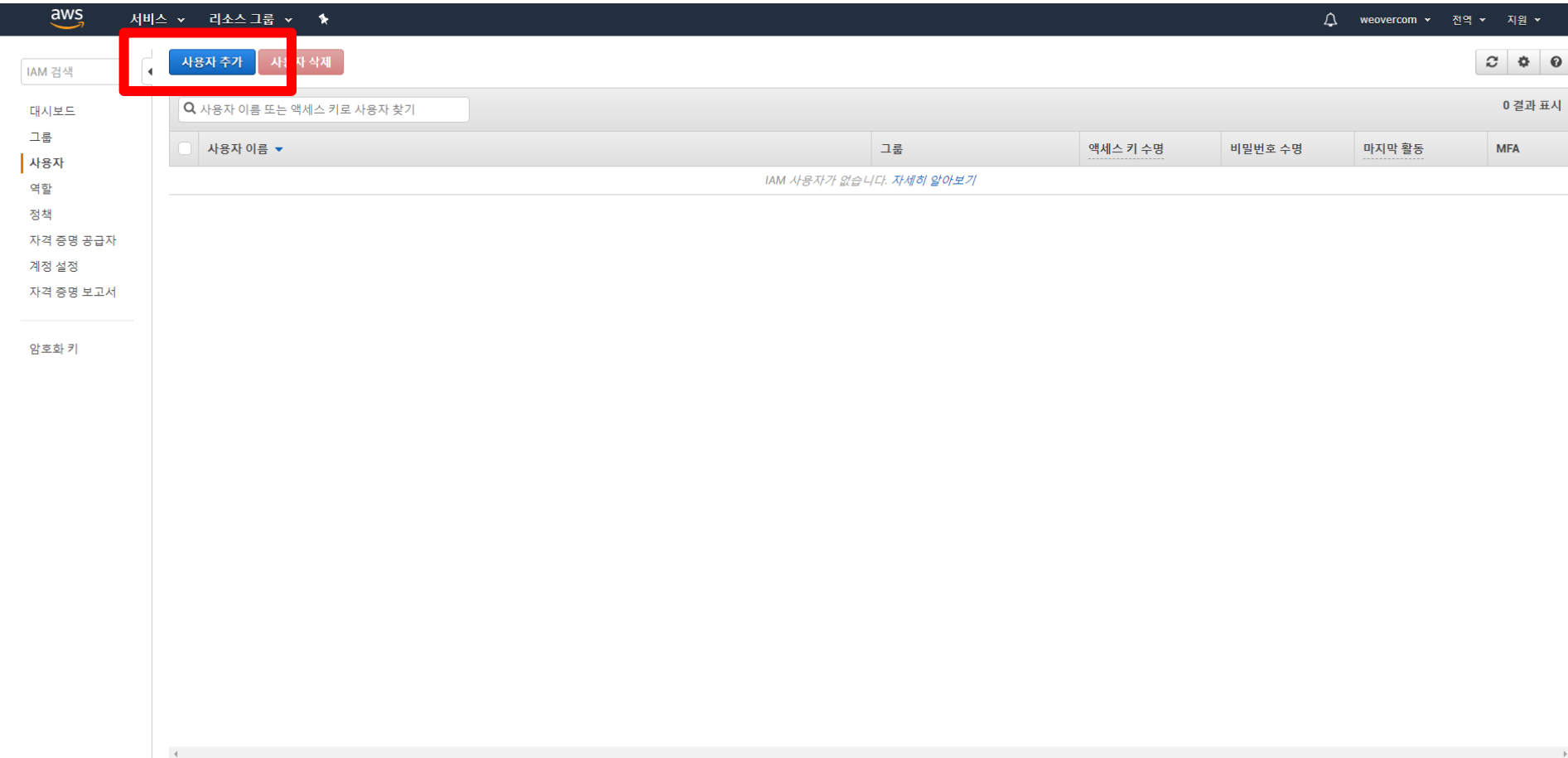
추가 정보

- [IAM 모범 사례](#)
- [IAM 설명서](#)
- [Web Identity Federation Playground](#)
- [정책 시뮬레이터](#)
- [비디오, IAM 릴리스 기록 및 추가 리소스](#)

4.2 AWS 컴퓨터 서비스

2. IAM 사용자 생성

2. 콘솔의 탐색 창에서 [Users]를 선택한 다음 [Add user]를 선택



4.2 AWS 컴퓨터 서비스

2. IAM 사용자 생성

3. [User name]에 Administrator를 입력

aws

서비스 ▾ 리소스 그룹 ▾ ★

🔔 weovercom ▾ 전역 ▾ 자원 ▾

사용자 추가

1234

사용자 세부 정보 설정

동일한 액세스 유형 및 권한을 사용하여 한 번에 여러 사용자를 추가할 수 있습니다. 자세히 알아보기

사용자 이름*

administrator

➕ 다른 사용자 추가

AWS 액세스 유형 선택

해당 사용자가 AWS에 액세스하는 방법을 선택합니다. 마지막 단계에서는 액세스 키와 자동 생성된 비밀번호가 제공됩니다. 자세히 알아보기

액세스 유형*

☐ 프로그래밍 방식 액세스

AWS API, CLI, SDK 및 기타 개발 도구에 대해 액세스 키 ID 및 비밀 액세스 키 을(를) 활성화합니다.

☐ AWS Management Console 액세스

사용자가 AWS Management Console에 로그인할 수 있도록 허용하는 비밀번호 을(를) 활성화합니다.

* 필수

취소 다음: 권한

4.2 AWS 컴퓨터 서비스

2. IAM 사용자 생성

4. AWS Management 콘솔 access 옆의 확인란을 선택하고 Custom password를 선택한 다음 텍스트 상자에 새 사용자의 암호를 입력

aws

서비스 ▾ 리소스 그룹 ▾ ☆

🔔 weovercom ▾ 전역 ▾ 자원 ▾

사용자 추가

1 2 3 4

사용자 세부 정보 설정

동일한 액세스 유형 및 권한을 사용하여 한 번에 여러 사용자를 추가할 수 있습니다. 자세히 알아보기

사용자 이름* administrator

+ 다른 사용자 추가

AWS 액세스 유형 선택

해당 사용자가 AWS에 액세스하는 방법을 선택합니다. 마지막 단계에서는 액세스 키와 자동 생성된 비밀번호가 제공됩니다. 자세히 알아보기

액세스 유형* ☐ 프로그래밍 방식 액세스
AWS API, CLI, SDK 및 기타 개발 도구에 대해 액세스 키 ID 및 비밀 액세스 키 을(를) 활성화합니다.

☒ AWS Management Console 액세스
사용자가 AWS Management Console에 로그인할 수 있도록 허용하는 비밀번호 을(를) 활성화합니다.

콘솔 비밀번호* ☐ 자동 생성된 비밀번호

☒ 사용자 지정 비밀번호

☐ 비밀번호 표시

비밀번호 재설정 필요 ☒ 사용자가 다음에 로그인할 때 새 비밀번호 생성 요청
사용자가 비밀번호를 변경할 수 있도록 허용하는 IAMUserChangePassword 정책을 자동으로 가져옵니다.

* 필수

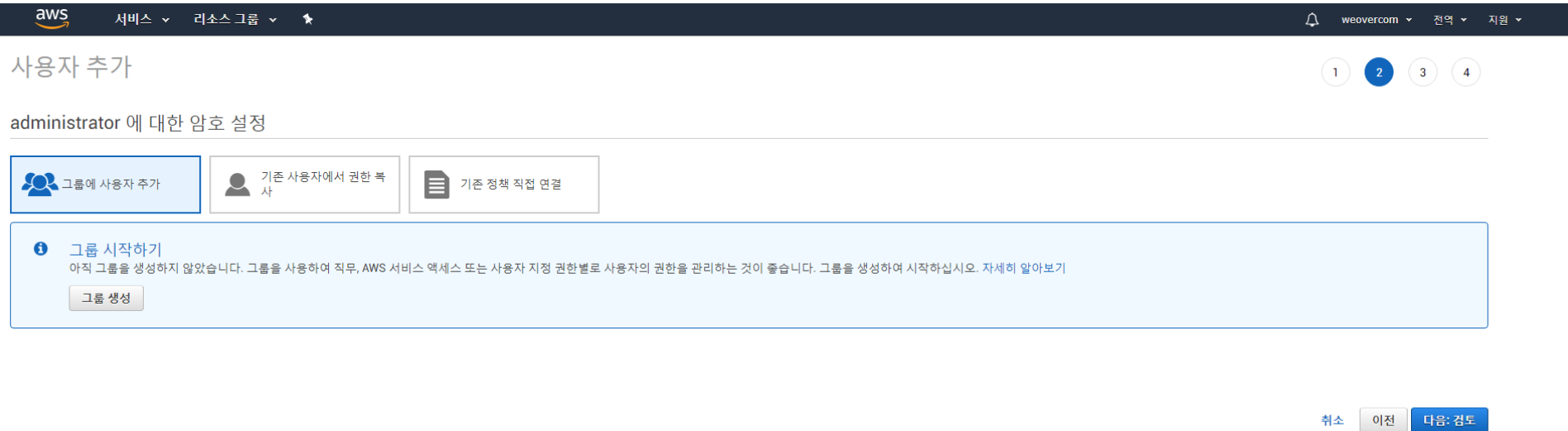
취소 다음: 권한

4.2 AWS 컴퓨터 서비스

2. IAM 사용자 생성

6. Set permissions for user 페이지에서 **Add user to group**을 선택.

7. **Create group**을 선택합니다.



aws 서비스 리소스 그룹

사용자 추가

1 2 3 4

administrator에 대한 암호 설정

그룹에 사용자 추가 | 기존 사용자에서 권한 복사 | 기존 정책 직접 연결

그룹 시작하기
아직 그룹을 생성하지 않았습니다. 그룹을 사용하여 직무, AWS 서비스 액세스 또는 사용자 지정 권한별로 사용자의 권한을 관리하는 것이 좋습니다. 그룹을 생성하여 시작하십시오. [자세히 알아보기](#)

그룹 생성

취소 이전 다음: 검토

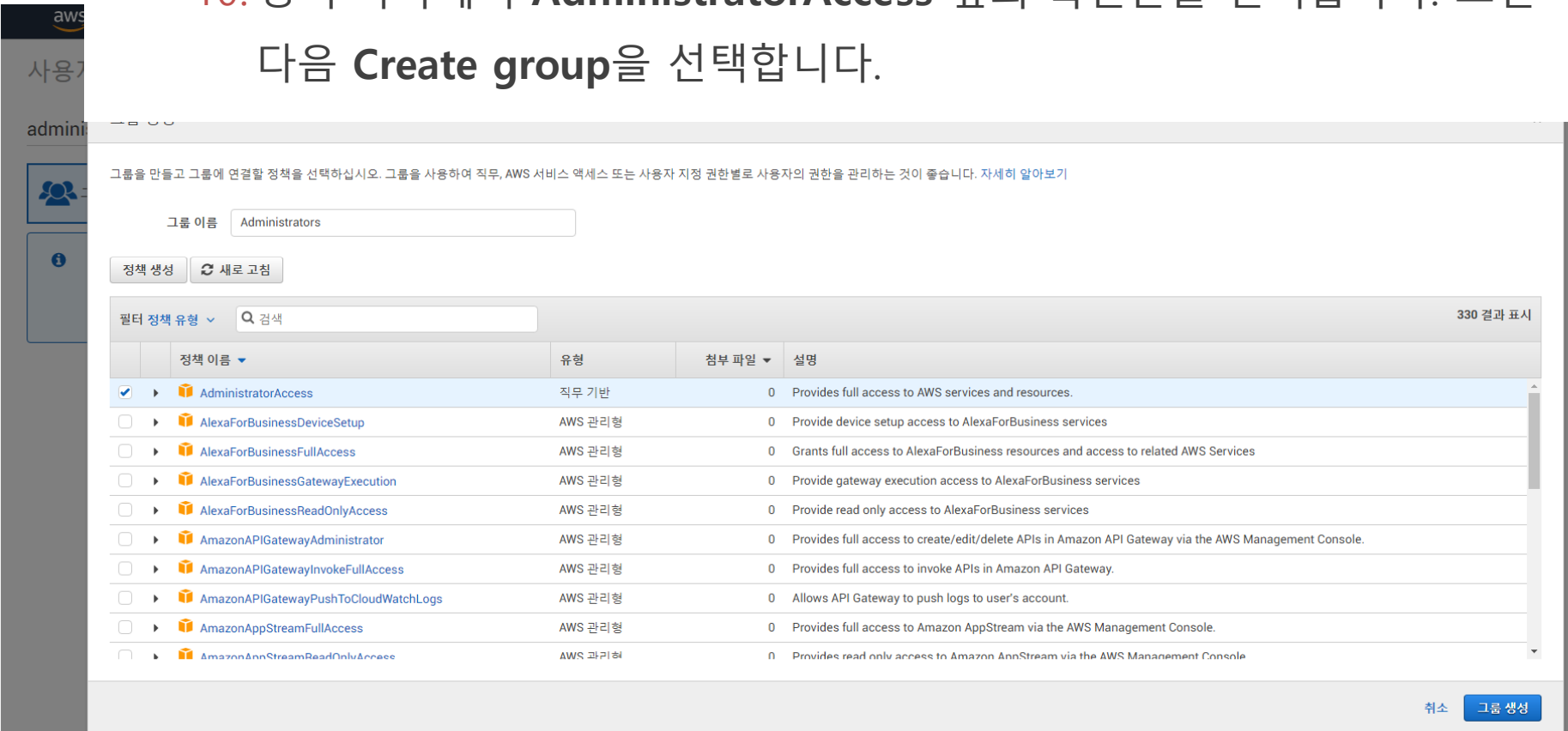
4.2 AWS 컴퓨터 서비스

2. IAM 사용자 생성

8. [Create group] 대화 상자에 **Administrators**를 입력합니다.

9. **Filter**로 **Job function**을 선택합니다.

10. 정책 목록에서 **AdministratorAccess** 옆의 확인란을 선택합니다. 그런 다음 **Create group**을 선택합니다.



그룹을 만들고 그룹에 연결할 정책을 선택하십시오. 그룹을 사용하여 직무, AWS 서비스 액세스 또는 사용자 지정 권한별로 사용자의 권한을 관리하는 것이 좋습니다. [자세히 알아보기](#)

그룹 이름: Administrators

정책 생성 새로 고침

필터 정책 유형 검색 330 결과 표시

	정책 이름	유형	첨부 파일	설명
<input checked="" type="checkbox"/>	AdministratorAccess	직무 기반	0	Provides full access to AWS services and resources.
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS 관리형	0	Provide device setup access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS 관리형	0	Grants full access to AlexaForBusiness resources and access to related AWS Services
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS 관리형	0	Provide gateway execution access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	AWS 관리형	0	Provide read only access to AlexaForBusiness services
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	AWS 관리형	0	Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Management Console.
<input type="checkbox"/>	AmazonAPIGatewayInvokeFullAccess	AWS 관리형	0	Provides full access to invoke APIs in Amazon API Gateway.
<input type="checkbox"/>	AmazonAPIGatewayPushToCloudWatchLogs	AWS 관리형	0	Allows API Gateway to push logs to user's account.
<input type="checkbox"/>	AmazonAppStreamFullAccess	AWS 관리형	0	Provides full access to Amazon AppStream via the AWS Management Console.
<input type="checkbox"/>	AmazonAppStreamReadOnlyAccess	AWS 관리형	0	Provides read only access to Amazon AppStream via the AWS Management Console.

취소 그룹 생성

4.2 AWS 컴퓨터 서비스

2. IAM 사용자 생성

11. 그룹 목록으로 돌아가 새로 만든 그룹 옆의 확인란을 선택합니다.

aws

서비스 ▾ 리소스 그룹 ▾ ★

🔔 weovercom ▾ 전역 ▾ 자원 ▾

사용자 추가


1


2


3

4

administrator 에 대한 암호 설정

 그룹에 사용자 추가

 기존 사용자에서 권한 복사

 기존 정책 직접 연결

기존 그룹에 사용자를 추가하거나 새 그룹을 생성합니다. 그룹을 사용하여 직무별로 사용자의 권한을 관리하는 것이 좋습니다. [자세히 알아보기](#)

그룹에 사용자 추가

그룹 생성

🔄 새로 고침

🔍 검색

1 결과 표시

그룹 ▾	연결된 정책
<input checked="" type="checkbox"/> Administrators	AdministratorAccess

취소

이전

다음: 검토

의견

한국어

© 2008 - 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved. [개인 정보 보호 정책](#) [이용 약관](#)

4.2 AWS 컴퓨터 서비스

2. IAM 사용자 생성

12. **Next: Review**를 선택하여 새 사용자에게 추가될 그룹 멤버십의 목록을 확인합니다. 계속 진행할 준비가 되었으면 **Create user**를 선택합니다.

aws

서비스 ▾ 리소스 그룹 ▾

weavercom ▾ 전역 ▾ 지원 ▾

사용자 추가

1234

검토

선택 항목을 검토합니다. 사용자를 생성한 후 자동으로 생성된 비밀번호와 액세스 키를 보고 다운로드할 수 있습니다.

사용자 세부 정보

사용자 이름	administrator
AWS 액세스 유형	AWS Management Console 액세스 - 비밀번호 사용
콘솔 비밀번호 유형	사용자 지정
비밀번호 재설정 필요	예

권한 요약

위에 표시된 사용자를 다음 그룹에 추가합니다.

유형	이름
그룹	Administrators
관리형 정책	IAMUserChangePassword

취소

이전

사용자 만들기

4.2 AWS 컴퓨터 서비스

2. IAM 사용자 생성

사용자 추가 완료

aws

서비스 ▾ 리소스 그룹 ▾

🔔 weovercom ▾ 전역 ▾ 지원 ▾

사용자 추가

1

2

3

4

✓ 성공

아래에 표시된 사용자를 생성했습니다. 사용자 보안 자격 증명을 보고 다운로드할 수 있습니다. AWS Management Console 로그인을 위한 사용자 지침을 이메일로 보낼 수도 있습니다. 지금이 이 자격 증명을 다운로드할 수 있는 마지막 기회입니다. 하지만 언제든지 새 자격 증명을 생성할 수 있습니다.

AWS Management Console 액세스 권한이 있는 사용자가 <https://978124574942.signin.aws.amazon.com/console>에 로그인할 수 있습니다.

📄 .csv 다운로드

	사용자	이메일 로그인 지침
▶ ✓	administrator	이메일 전송

닫기

4.2 AWS 컴퓨터 서비스

2. IAM 사용자 생성 로그인



계정:

사용자 이름:

암호:

로그인

[루트 계정 자격 증명으로 로그인](#)

Amazon Lightsail

AWS를 사용해 가상 프라이빗
서버를 손쉽게 시작 및 관리

자세히 알아보기



한국어 ▼

이용 약관 개인정보 보호정책 © 1996-2018, Amazon Web Services, Inc. 또는 자회사.

4.2 AWS 컴퓨터 서비스

3. 키 페어 생성

- AWS에서는 퍼블릭 키 암호화를 사용하여 인스턴스에 대한 로그인 정보를 보호.
- Linux 인스턴스에는 암호가 없으므로 인스턴스에 안전하게 로그인하기 위해 키 페어를 사용.
- 인스턴스를 시작할 때 키 페어의 이름을 지정한 다음 프라이빗 키를 제공하여 SSH를 사용하여 로그인할 때 키 페어를 아직 생성하지 않은 경우 Amazon EC2 콘솔을 사용하여 생성할 수 있다.
- 여러 리전에서 인스턴스를 시작하려면 각 리전에서 키 페어를 생성.

4.2 AWS 컴퓨터 서비스

3. 키 페어 생성 순서

1. 이전 섹션에서 생성한 URL을 사용하여 AWS에 로그인.
2. AWS 대시보드에서 [EC2]를 선택하여 Amazon EC2 콘솔 열기.
3. 탐색 모음에서 키 페어를 만들 리전을 선택. 현재 위치와 관계없이 사용자가 고를 수 있는 리전을 임의로 선택. 그러나 키 페어는 리전에 고유합니다. 예를 들어, 미국 동부(오하이오) 리전에서 인스턴스를 시작하려면 미국 동부(오하이오) 리전에서 인스턴스에 대한 키 페어를 생성해야 합니다.
4. 탐색 창의 **NETWORK & SECURITY**에서 **Key Pairs**를 선택합니다. 탐색 창은 콘솔의 왼쪽에 있습니다. 창이 보이지 않는 경우 창이 최소화되었을 수 있으니 화살표를 선택해 확대하십시오. [Key Pairs] 링크가 보이려면 아래로 스크롤해야 할 수 있습니다.

4.2 AWS 컴퓨터 서비스

5. **Create Key Pair**를 선택합니다.
6. **Create Key Pair** 대화 상자의 **Key pair name** 필드에 새 키 페어의 이름을 입력하고 **Create**를 선택. 기억하기 쉬운 이름(예: IAM 사용자 이름)을 사용하고, 뒤에 **-key-pair** 및 리전 이름을 추가합니다. 예를 들어, *me-key-pair-useast2*로 지정할 수 있습니다.
7. 브라우저에서 프라이빗 키 파일이 자동으로 다운로드됩니다. 기본 파일 이름은 키 페어의 이름으로 지정된 이름이며, 파일 이름 확장명은 **.pem**입니다. 안전한 장소에 프라이빗 키 파일을 저장합니다.

중요 !!!!!!!

이때가 사용자가 프라이빗 키 파일을 저장할 수 있는 유일한 기회입니다. 인스턴스를 시작할 때 키 페어의 이름을 제공하고, 인스턴스에 연결할 때마다 해당 프라이빗 키를 제공해야 합니다.

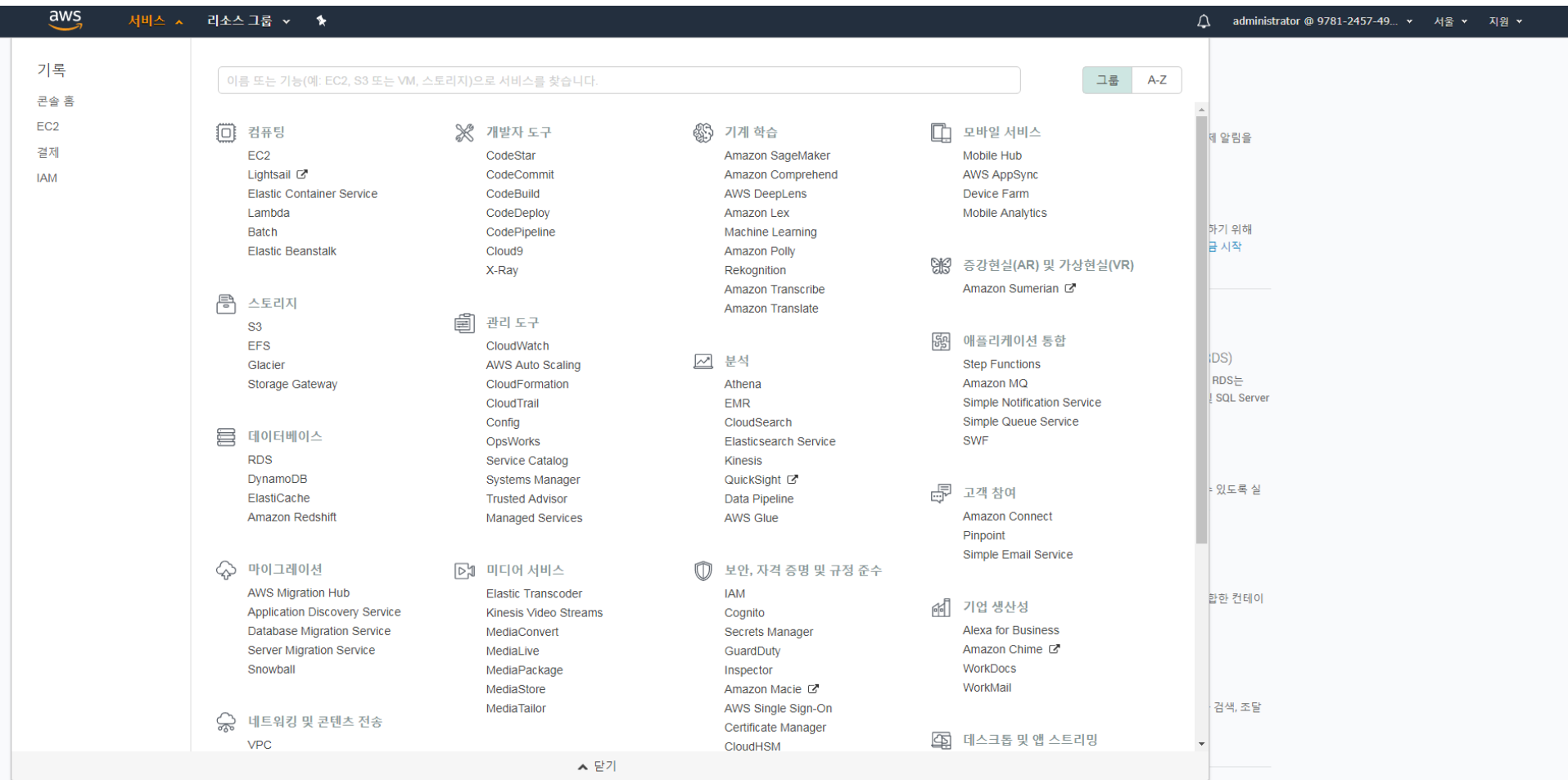
4.2 AWS 컴퓨트 서비스

8. Mac 또는 Linux 컴퓨터에서 SSH 클라이언트를 사용하여 Linux 인스턴스에 연결하려면 사용자만 프라이빗 키 파일을 읽을 수 있도록 다음 명령으로 해당 권한을 설정합니다.

4.2 AWS 컴퓨터 서비스

3. 키 페어 생성 순서

2. AWS 대시보드에서 [EC2]를 선택하여 Amazon EC2 콘솔 열기.



4.2 AWS 컴퓨터 서비스

3. 키 페어 생성 순서

3. 탐색 모음에서 키 페어를 만들 리전을 선택.
현재 위치와 관계없이 사용자가 고를 수 있는 리전을 임의로 선택. 그러나 키 페어는 리전에 고유합니다. 예를 들어, 미국 동부(오하이오) 리전에서 인스턴스를 시작하려면 미국 동부(오하이오) 리전에서 인스턴스에 대한 키 페어를 생성해야 합니다.



4.2 AWS 컴퓨터 서비스

3. 키 페어 생성 순서

4. 탐색 창의 NETWORK & SECURITY에서 Key Pairs를 선택.

The screenshot displays the AWS Management Console interface. On the left, the navigation sidebar lists various services, with '키 페어' (Key Pairs) under '네트워크 및 보안' (Network & Security) highlighted with a red box. The main content area is titled '리소스' (Resources) and shows a summary of EC2 resources in the Asia Pacific (Seoul) region. It includes counts for running instances, dedicated hosts, volumes, key pairs, and placement groups. A blue notification bar indicates that EC2 Spot instances are available with up to 90% discount. Below this, there are sections for '인스턴스 생성' (Create Instance) with a button to start, and '서비스 상태' (Service Status) showing that the EC2 service is operating normally in the ap-northeast-2 region. On the right, there is a section for '예약된 이벤트' (Reserved Events) which currently shows no events.

aws 서비스 리소스 그룹

EC2 대시보드

이벤트

태그

보고서

제한

인스턴스

인스턴스

시작 템플릿

스팟 요청

예약 인스턴스

전용 호스트

이미지

AMI

번들 작업

ELASTIC BLOCK STORE

볼륨

스냅샷

네트워크 및 보안

보안 그룹

탄력적 IP

키 페어

리소스

아시아 태평양(서울) 리전에서 다음 Amazon EC2 리소스를 사용하고 있습니다.

0 실행 중인 인스턴스

0 전용 호스트

0 볼륨

0 키 페어

0 배치 그룹

0 탄력적 IP

0 스냅샷

0 로드 밸런서

1 보안 그룹

EC2 스팟입니다. 온디맨드 가격 대비 최대 90%가 절약됩니다. 워크로드에 날개를 달아 보십시오. [Amazon EC2 스팟 인스턴스 시작하기](#).

인스턴스 생성

Amazon EC2 사용을 시작하려면 Amazon EC2 인스턴스라고 하는 가상 서버를 시작해야 합니다.

인스턴스 시작

참고: 인스턴스는 아시아 태평양(서울) 리전에서 시작됩니다.

서비스 상태

서비스 상태:

아시아 태평양(서울):
This service is operating normally

가용 영역 상태:

ap-northeast-2a:
가용 영역이 정상 작동 중입니다.

예약된 이벤트

아시아 태평양(서울):
이벤트 없음

4.2 AWS 컴퓨터 서비스

3. 키 페어 생성 순서

5. Create Key Pair를 선택합니다.

The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, service categories, the user's account name 'administrator @ 9781-2457-49...', and the region '서울'. The left-hand navigation pane lists various AWS services, with '키 페어' (Key Pair) highlighted under the 'EC2' category. The main content area displays a message in Korean: '현재 리전에 키 페어가 없습니다.' (There are no key pairs in the current region.) and '키 페어 생성' (Create Key Pair) 버튼을 클릭하여 첫 번째 키 페어를 생성합니다. (Click the 'Create Key Pair' button to create the first key pair.) Below this message is a prominent blue button labeled '키 페어 생성' (Create Key Pair). At the bottom of the console, there is a footer with copyright information and links to the privacy policy and terms of service.

aws 서비스 리소스 그룹

administrator @ 9781-2457-49... 서울 지원

EC2 대시보드
이벤트
태그
보고서
제한

인스턴스
인스턴스
시작 템플릿
스팟 요청
예약 인스턴스
전용 호스트

이미지
AMI
변환 작업

ELASTIC BLOCK STORE
볼륨
스냅샷

네트워크 및 보안
보안 그룹
탄력적 IP
배치 그룹

키 페어
네트워크 인터페이스

로드 밸런싱
로드밸런서
대상 그룹

AUTO SCALING
시작 구성
Auto Scaling 그룹

SYSTEMS MANAGER

키 페어 생성 키 페어 가져오기 삭제

속성별 필터 또는 키워드별 검색

현재 리전에 키 페어가 없습니다.

"키 페어 생성" 버튼을 클릭하여 첫 번째 키 페어를 생성합니다.

키 페어 생성

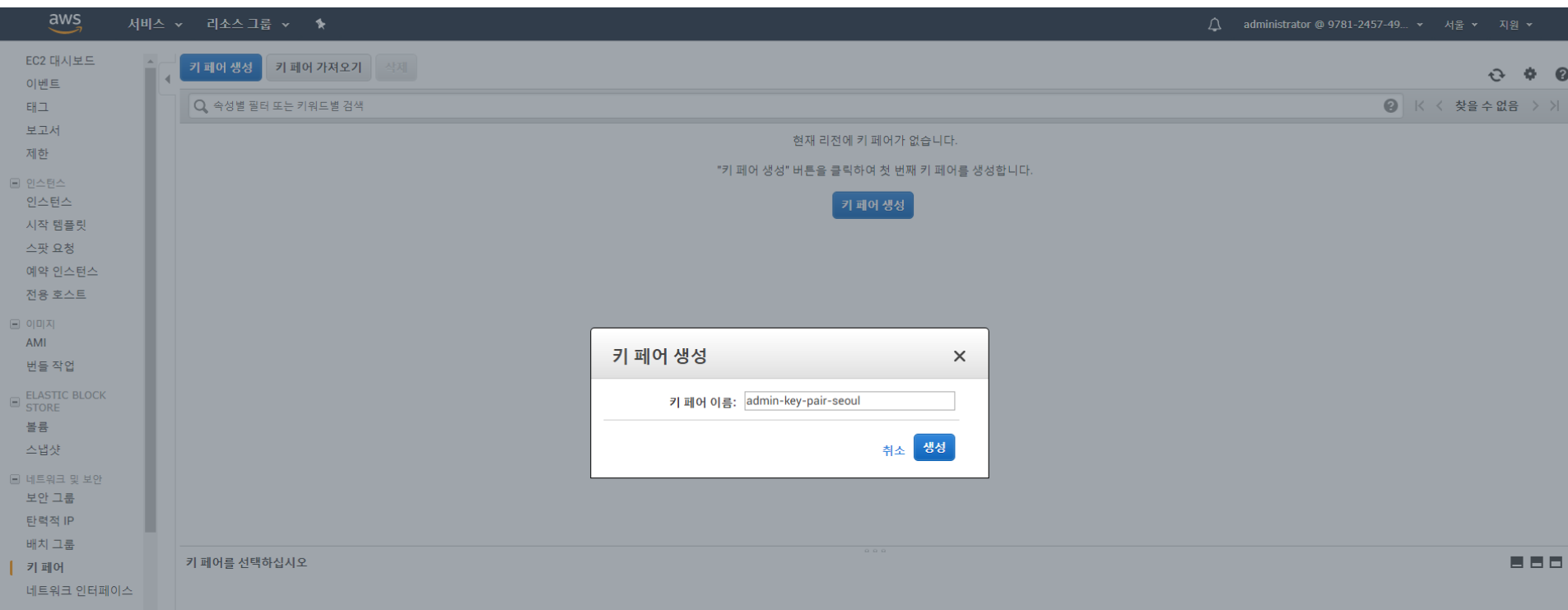
키 페어를 선택하십시오

© 2008 - 2018, Amazon Web Services, Inc. 또는 자회사. All rights reserved. 개인 정보 보호 정책 이용 약관

4.2 AWS 컴퓨터 서비스

3. 키 페어 생성 순서

6. Create Key Pair 대화 상자의 **Key pair name** 필드에 새 키 페어의 이름을 입력하고 **Create**를 선택.

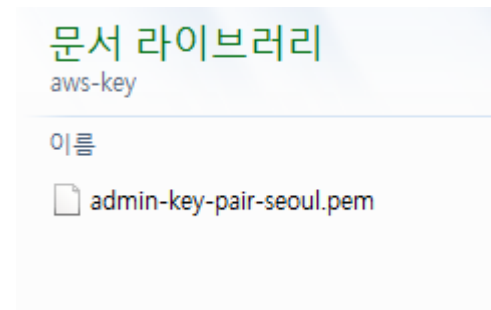
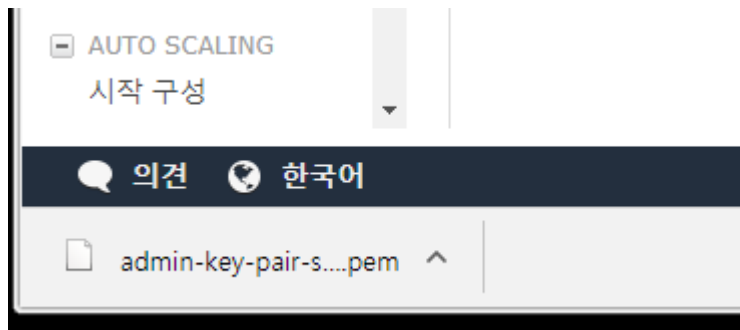


기억하기 쉬운 이름(예: IAM 사용자 이름)을 사용하고, 뒤에 -key-pair 및 리전 이름을 추가합니다. 예를 들어, *me-key-pair-useast2*로 지정할 수 있습니다.

4.2 AWS 컴퓨터 서비스

3. 키 페어 생성 순서

7. 브라우저에서 프라이빗 키 파일이 자동으로 다운로드됩니다. 기본 파일 이름은 키 페어의 이름으로 지정된 이름이며, 파일 이름 확장명은 .pem입니다. 안전한 장소에 프라이빗 키 파일을 저장합니다.



4.2 AWS 컴퓨터 서비스

3. 키 페어를 사용하여 인스턴스에 연결

Mac 또는 Linux를 실행 중인 컴퓨터에서 Linux 인스턴스에 연결하려면 `-i` 옵션과 프라이빗 키 경로를 사용하여 SSH 클라이언트에 `.pem` 파일을 지정합니다. Windows를 실행 중인 컴퓨터에서 Linux 인스턴스에 연결하려면 MindTerm 또는 PuTTY를 사용합니다. PuTTY를 사용하려면 먼저 설치하고 다음 절차에 따라 `.pem` 파일을 `.ppk` 파일로 변환해야 합니다.

4.2 AWS 컴퓨터 서비스

3. 키 페어를 사용하여 인스턴스에 연결

- PuTTY를 사용하여 Windows에서 Linux 인스턴스에 연결

1. <http://www.chiark.greenend.org.uk/~sgtatham/putty/>에서 PuTTY를 다운로드하여 설치합니다. 전체 제품군을 설치해야 합니다.
2. PuTTYgen을 시작.
3. **Type of key to generate**에서 **RSA**를 선택합니다.
4. **Load**를 선택. 기본적으로 PuTTYgen에는 확장명이 .ppk인 파일만 표시. .pem 파일을 찾으려면 모든 유형의 파일을 표시하는 옵션을 선택.
5. 이전 절차에서 생성한 프라이빗 키 파일을 선택하고 **Open**을 선택. **OK**를 선택하여 확인 대화 상자를 닫는다.
6. **Save private key**를 선택. PuTTYgen에서 암호 없이 키 저장에 대한 경고가 표시. **Yes**를 선택.
7. 키 페어에 사용한 키와 동일한 이름을 지정. PuTTY가 자동으로 .ppk 파일 확장자를 추가.

4.2 AWS 컴퓨터 서비스

3. 키 페어를 사용하여 인스턴스에 연결

- PuTTY를 사용하여 Windows에서 Linux 인스턴스에 연결

1. <http://www.chiark.greenend.org.uk/~sgtatham/putty/>에서

PuTTY를 다운로드하여 설치합니다. 전체 제품군을 설치해야 합니다.

PuTTY: a free SSH and Telnet client

Home | [FAQ](#) | [Feedback](#) | [Licence](#) | [Updates](#) | [Mirrors](#) | [Keys](#) | [Links](#) | [Team](#)
Download: [Stable](#) · [Snapshot](#) | [Docs](#) | [Changes](#) | [Wishlist](#)

PuTTY is a free implementation of SSH and Telnet for Windows and Unix platforms, along with an xterm terminal emulator. It is written and maintained primarily by [Simon Tatham](#).

The latest version is 0.70. [Download it here](#).

LEGAL WARNING: Use of PuTTY, PSCP, PSFTP and Plink is illegal in countries where encryption is outlawed. We believe it is legal to use PuTTY, PSCP, PSFTP and Plink in England and Wales and in many other countries, but we are not lawyers, and so if in doubt you should seek legal advice before downloading it. You may find useful information at cryptolaw.org, which collects information on cryptography laws in many countries, but we can't vouch for its correctness.

Use of the Telnet-only binary (PuTTYtel) is unrestricted by any cryptography laws.

Latest news

2017-07-08 PuTTY 0.70 released, containing security and bug fixes

PuTTY 0.70, released today, fixes further problems with Windows DLL hijacking, and also fixes a small number of bugs in 0.69, including broken printing support and Unicode keyboard input on Windows.

2017-04-29 PuTTY 0.69 released, containing security and bug fixes

64-bit:	pageant.exe	(or by FTP)
	(signature)	
puttygen.exe (a RSA and DSA key generation utility)		
32-bit:	puttygen.exe	(or by FTP)
	(signature)	
64-bit:	puttygen.exe	(or by FTP)
	(signature)	
putty.zip (a .ZIP archive of all the above)		
32-bit:	putty.zip	(or by FTP)
	(signature)	
64-bit:	putty.zip	(or by FTP)
	(signature)	

Documentation

Browse the documentation on the web

HTML: [Contents page](#)

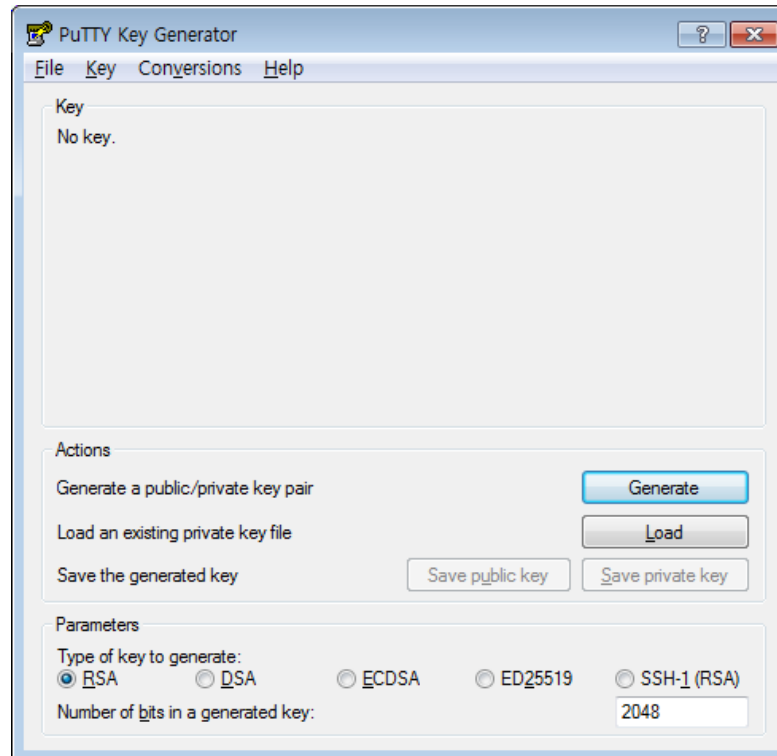
4.2 AWS 컴퓨터 서비스

3. 키 페어를 사용하여 인스턴스에 연결

- PuTTY를 사용하여 Windows에서 Linux 인스턴스에 연결

2. PuTTYgen을 시작.

3. Type of key to generate에서 RSA를 선택합니다.

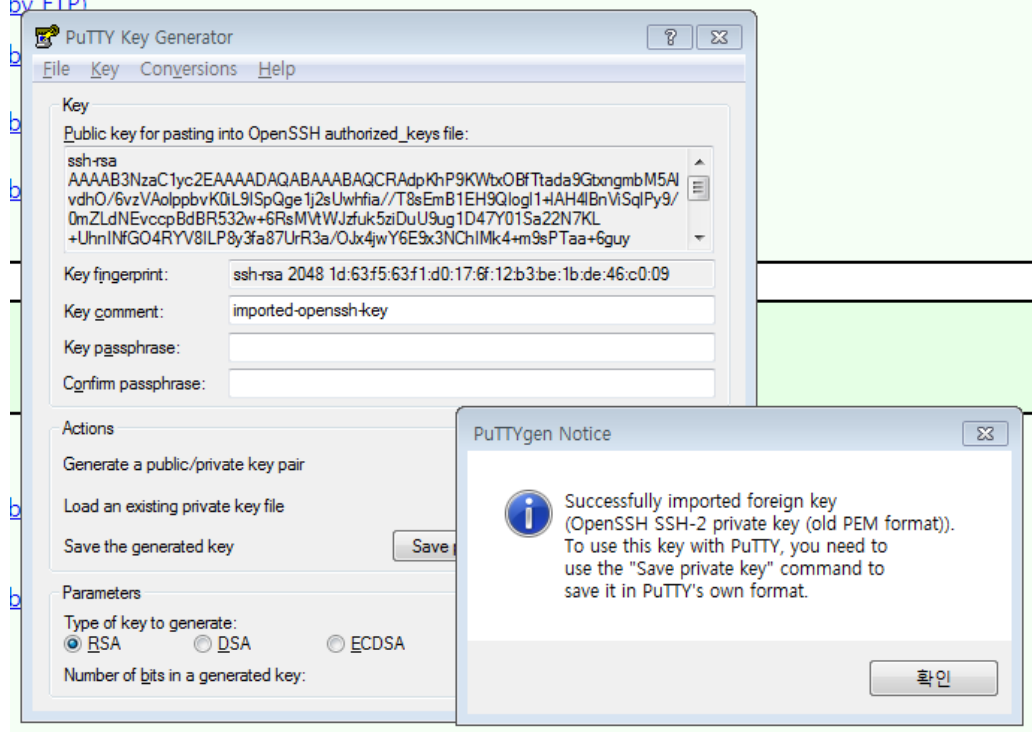


4.2 AWS 컴퓨터 서비스

3. 키 페어를 사용하여 인스턴스에 연결

- PuTTY를 사용하여 Windows에서 Linux 인스턴스에 연결

4. **Load**를 선택. 기본적으로 PuTTYgen에는 확장명이 .ppk인 파일만 표시. .pem 파일을 찾으려면 모든 유형의 파일을 표시하는 옵션을 선택.
5. 이전 절차에서 생성한 프라이빗 키 파일을 선택하고 **Open**을 선택. **OK**를 선택하여 확인 대화 상자를 닫는다.



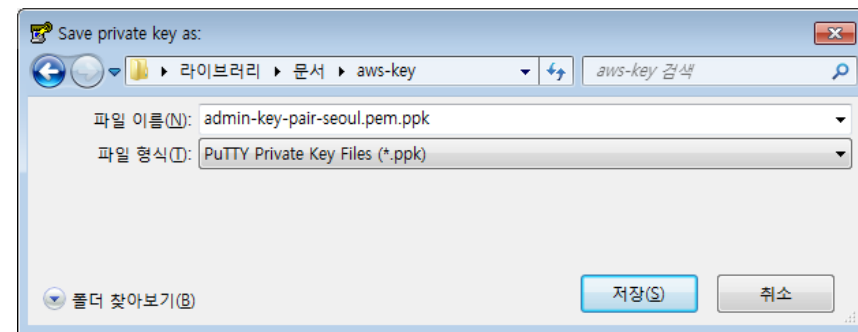
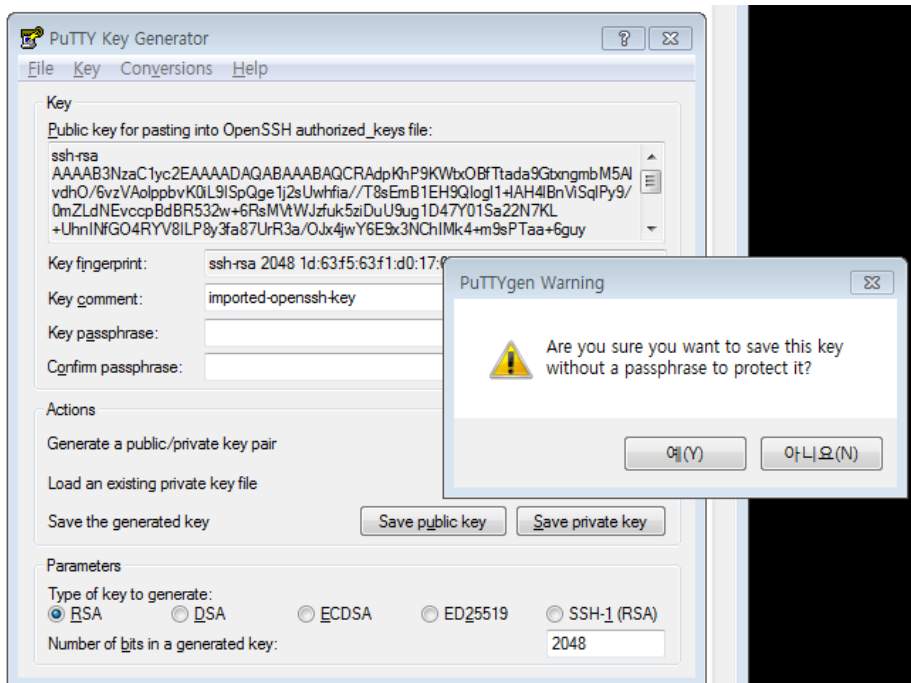
4.2 AWS 컴퓨터 서비스

3. 키 페어를 사용하여 인스턴스에 연결

- PuTTY를 사용하여 Windows에서 Linux 인스턴스에 연결

6. **Save private key**를 선택. PuTTYgen에서 암호 없이 키 저장에 대한 경고가 표시. **Yes**를 선택.

7. 키 페어에 사용한 키와 동일한 이름을 지정. PuTTY가 자동으로 .ppk 파일 확장자를 추가.



4.2 AWS 컴퓨터 서비스

4. Virtual Private Cloud(VPC) 생성

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 모음에서 VPC를 생성할 리전을 선택. VPC는 리전에 고유하므로 키 페어를 생성한 리전과 동일한 리전을 선택.
3. VPC 대시보드에서 **[Start VPC Wizard]**를 선택.

The screenshot shows the AWS VPC console interface. The top navigation bar includes the AWS logo, service categories, resource groups, and user information. The left sidebar contains a 'VPC 대시보드' (VPC Dashboard) section with a search bar and a list of VPCs. The main content area is titled '서비스 상태' (Service Status) and '추가 정보' (Additional Information). The '서비스 상태' section shows the status of Amazon VPC and Amazon EC2 services, both of which are 'operating normally'. The '추가 정보' section includes links to VPC documentation, all VPC resources, and a '문제 보고' (Report Problem) link. A red box highlights the 'VPC 마법사 시작' (Start VPC Wizard) button in the left sidebar.

aws 서비스 리소스 그룹

administrator @ 9781-2457-49... 서울 지원

VPC 대시보드

VPC로 필터링:

Q VPC 선택

VPC 마법사 시작

참고: 인스턴스는 아시아 태평양(서울) 리전에서 시작됩니다.

가상 프라이빗 클라우드

가상 프라이빗 클라우드 (VPC)는 가상화된 네트워크 환경을 제공합니다. VPC는 가상화된 네트워크 환경을 제공합니다.

VPCs

서브넷

라우팅 테이블

인터넷 게이트웨이

외부 전용 인터넷 게이트웨이

DHCP 옵션 세트

탄력적 IP

엔드포인트

엔드포인트 서비스

NAT 게이트웨이

피어링 연결

보안

네트워크 ACL

보안 그룹

1 VPC

0 외부 전용 인터넷 게이트웨이

1 라우팅 테이블

0 탄력적 IP

0 엔드포인트

1 보안 그룹

0 VPN 연결

0 고객 게이트웨이

1 인터넷 게이트웨이

2 서브넷

1 네트워크 ACL

0 VPC 피어링 연결

0 NAT 게이트웨이

0 실행 중인 인스턴스

0 가상 프라이빗 게이트웨이

1 DHCP 옵션 세트

VPN 연결

Amazon VPC를 통해 AWS 클라우드 내에서 자신만의 격리된 리소스를 사용한 다음 업계 표준 암호화 방식의 IPsec VPN 연결을 사용하여 이러한 리소스를 자신의 데이터 센터에 직접 연결할 수 있습니다.

VPN 연결 생성

현재 상태

세부 정보

Amazon VPC - Asia Pacific (Seoul) Service is operating normally

Amazon EC2 - Asia Pacific (Seoul) Service is operating normally

전체 서비스 상태 세부 정보 보기

추가 정보

VPC 설명서

모든 VPC 리소스

도움

문제 보고

4.2 AWS 컴퓨터 서비스

4. Virtual Private Cloud(VPC) 생성

4. [Step 1: Select a VPC Configuration] 페이지에서 [VPC with a Single Public Subnet]이 선택되어 있는지 확인하고 [Select]를 선택.

aws 서비스 리소스 그룹

1단계: VPC 구성 선택

단일 퍼블릭 서브넷이 있는 VPC

퍼블릭 및 프라이빗 서브넷이 있는 VPC

퍼블릭 및 프라이빗 서브넷이 있고 하드웨어 VPN 액세스를 제공하는 VPC

프라이빗 서브넷만 있고 하드웨어 VPN 액세스를 제공하는 VPC

고객의 인스턴스는 AWS 클라우드의 프라이빗 격리 섹션에서 실행되며 인터넷에 직접 액세스합니다. 네트워크 액세스 제어 목록 및 보안 그룹을 사용하여 인스턴스를 드나드는 인바운드 및 아웃바운드 네트워크 트래픽을 엄격히 제어할 수 있습니다.

생성:

/24 서브넷이 있는 /16 네트워크. 퍼블릭 서브넷 인스턴스는 인터넷을 액세스하기 위해 탄력적 IP 또는 퍼블릭 IP를 사용합니다.

선택

Internet, S3, DynamoDB, SNS, SQS, etc.

Public Subnet

Amazon Virtual Private Cloud

4.2 AWS 컴퓨터 서비스

4. Virtual Private Cloud(VPC) 생성

5. [Step 2: VPC with a Single Public Subnet] 페이지의 [VPC name] 필드에 VPC의 이름을 입력. 다른 기본 구성 설정은 그대로 두고 [Create VPC]를 선택. 확인 페이지에서 [OK]를 선택.

 서비스 ▾ 리소스 그룹 ▾ ✨

administrator @ 9781-2457-49... ▾ 서울 ▾ 지원 ▾

2단계: 단일 퍼블릭 서브넷이 있는 VPC

IPv4 CIDR 블록: 10.0.0.0/16 (65531 IP 주소 사용 가능)

IPv6 CIDR 블록: ☒ IPv6 CIDR 블록 없음
☐ Amazon에서 IPv6 CIDR 블록 제공

VPC 이름: a-m-vpc

퍼블릭 서브넷의 IPv4 CIDR: 10.0.0.0/24 (251 IP 주소 사용 가능)

가용 영역: 기본 설정 없음 ▾

서브넷 이름: 퍼블릭 서브넷

AWS가 VPC를 생성한 후 더 많은 서브넷을 추가할 수 있습니다.

서비스 엔드포인트

엔드포인트 추가

DNS 호스트 이름 활성화: ☒ 예 ☐ 아니요

하드웨어 태넌시: 기본값 ▾

취소 및 종료 뒤로 VPC 만들기

4.2 AWS 컴퓨터 서비스

5. 보안 그룹 생성

- 보안 그룹은 연결된 인스턴스에 대한 방화벽 역할을 하여 인스턴스 수준에서 인바운드 트래픽과 아웃바운드 트래픽을 모두 제어합니다.
- SSH를 사용하여 IP 주소에서 인스턴스에 연결할 수 있게 하는 규칙을 보안 그룹에 추가해야 합니다.
- 어디서나 인바운드 및 아웃바운드 HTTP/HTTPS 액세스를 허용하는 규칙을 추가할 수도 있습니다.
- **사전 조건**
 - 로컬 컴퓨터의 퍼블릭 IPv4 주소가 필요합니다. Amazon EC2 콘솔의 보안 그룹 편집기는 퍼블릭 IPv4 주소를 자동으로 검색할 수 있습니다. 또는 인터넷 브라우저에서 "내 IP 주소"와 같은 검색 구문을 사용하거나 [Check IP](#) 서비스를 사용할 수도 있습니다. 고정 IP 주소가 없는 방화벽 뒤나 ISP(인터넷 서비스 공급자)를 통해 연결되어 있는 경우 클라이언트 컴퓨터가 사용하는 IP 주소의 범위를 찾아야 합니다.

4.2 AWS 컴퓨터 서비스

5. 보안 그룹 생성

1. <https://console.aws.amazon.com/ec2/>에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 모음에서 보안 그룹을 생성할 리전을 선택합니다. 보안 그룹은 리전에 고유하므로 키 페어를 생성한 리전과 동일한 리전을 선택해야 합니다.
3. 탐색 창에서 [**Security Groups**]를 선택합니다.
4. [**Create Security Group**]을 선택합니다.
5. 새 보안 그룹의 이름과 설명을 입력합니다. 기억하기 쉬운 이름(예: IAM 사용자 이름)을 사용하고, 뒤에 `_SG_` 및 리전 이름을 추가합니다. 예를 들어, `me_SG_uswest2`로 지정할 수 있습니다.
6. [**VPC**] 목록에서 VPC를 선택합니다. 기본 VPC가 있는 경우 별표(*)가 표시되어 있습니다.

4.2 AWS 컴퓨터 서비스

7. [Inbound] 탭에서 다음 규칙을 생성한 다음(각 새 규칙에 대해 [Add Rule] 선택) [Create]를 선택합니다.

- [Type] 목록에서 [HTTP]를 선택하고 [Source]가 [Anywhere](0.0.0.0/0)로 설정되어 있는지 확인합니다.
- [Type] 목록에서 [HTTPS]를 선택하고 [Source]가 [Anywhere](0.0.0.0/0)로 설정되어 있는지 확인합니다.
- [Type] 목록에서 [SSH], []를 선택합니다. 필드를 로컬 컴퓨터의 퍼블릭 IPv4 주소로 자동으로 채우려면 [Source] 상자에서 [My IP]를 선택하면 됩니다. 또는 [Custom]을 선택하고 컴퓨터 또는 네트워크의 퍼블릭 IPv4 주소를 CIDR 표기법으로 지정해도 됩니다. 개별 IP 주소를 CIDR 표기법으로 지정하려면 라우팅 접미사 /32를 추가합니다(예: 203.0.113.25/32). 회사에서 주소를 범위로 할당하는 경우 전체 범위(예: 203.0.113.0/24)를 지정합니다.

4.2 AWS 컴퓨트 서비스

5. 보안 그룹 생성


1. <https://console.aws.amazon.com/ec2/>에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 모음에서 보안 그룹을 생성할 리전을 선택합니다. 보안 그룹은 리전에 고유하므로 키 페어를 생성한 리전과 동일한 리전을 선택해야 합니다.
3. 탐색 창에서 [Security Groups]를 선택합니다.

The screenshot displays the AWS Management Console for the '아시아 태평양(서울)' (Asia Pacific (Seoul)) region. The left-hand navigation pane includes sections for 'EC2 대시보드' (EC2 Dashboard) with links to 이벤트, 태그, 보고서, 제한, 인스턴스, 인스턴스 시작 템플릿, 스팟 요청, 예약 인스턴스, 전용 호스트, 이미지, AMI, 변형 작업, ELASTIC BLOCK STORE, 볼륨, 스냅샷, 네트워크 및 보안, 보안 그룹, 탄력적 IP, 배치 그룹, 키 페어, and 네트워크 인터페이스. The main content area is titled '리소스' (Resources) and states that the following Amazon EC2 resources are being used in the '아시아 태평양(서울)' region. A summary table shows: 0 실행 중인 인스턴스 (Running Instances), 0 전용 호스트 (Dedicated Hosts), 0 볼륨 (Volumes), 1 키 페어 (Key Pairs), 0 배치 그룹 (Placement Groups), 0 탄력적 IP (Elastic IPs), 0 스냅샷 (Snapshots), 0 로드 밸런서 (Load Balancers), and 2 보안 그룹 (Security Groups). A blue notification box indicates that EC2 Spot instances can save up to 90% compared to on-demand prices. Below this, the '인스턴스 생성' (Create Instance) section provides instructions and a button to '인스턴스 시작' (Start Instance). The '서비스 상태' (Service Status) section shows that the '아시아 태평양(서울)' service is operating normally. The '예약된 이벤트' (Reserved Events) section shows no events. The right-hand sidebar contains '계정 속성' (Account Attributes) such as '지원 가능 플랫폼' (Supported Platforms) and '기본 VPC' (Default VPC), '추가 정보' (Additional Information) like '시작 안내서' (Getting Started) and '설명서' (Documentation), and 'AWS Marketplace' information.

4.2 AWS 컴퓨터 서비스

5. 보안 그룹 생성

4. [Create Security Group]을 선택합니다.



The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, a '서비스' (Services) dropdown, a '리소스 그룹' (Resource Groups) dropdown, and a user profile 'administrator @ 9781-2457-49...'. The left sidebar lists navigation options: EC2 대시보드, 이벤트, 태그, 보고서, 제한, 인스턴스, 인스턴스 시작 템플릿, 스냅 요청, 예약 인스턴스, and 전용 호스트. The main content area is titled '보안 그룹 생성' (Create Security Group) and includes a search bar and a table of existing security groups.

<input type="checkbox"/>	Name	그룹 ID	그룹 이름	VPC ID	설명
<input type="checkbox"/>		sg-0a939fba13d5715f6	default	vpc-01547098d18169e42	default VPC security group
<input type="checkbox"/>		sg-6dc93307	default	vpc-6219410a	default VPC security group

4.2 AWS 컴퓨터 서비스

5. 보안 그룹 생성

5. 새 보안 그룹의 이름과 설명을 입력합니다. 기억하기 쉬운 이름(예: IAM 사용자 이름)을 사용하고, 뒤에 `_SG_` 및 리전 이름을 추가합니다. 예를 들어, `me_SG_uswest2`로 지정할 수 있습니다.
6. **[VPC]** 목록에서 VPC를 선택합니다.

The screenshot shows the '보안 그룹 생성' (Create Security Group) dialog box in the AWS Management Console. The dialog has a title bar with a close button (X). Inside, there are three input fields: '보안 그룹 이름' (Security Group Name) with the value 'admin_SG_Seoul', '설명' (Description) with the value '사용자 그룹', and 'VPC' (VPC) with a dropdown menu showing 'vpc-6219410a (기본값)'. Below these fields, there are two tabs: '인바운드' (Inbound) and '아웃바운드' (Outbound). Under the '인바운드' tab, there is a table with columns: '유형' (Type), '프로토콜' (Protocol), '포트 범위' (Port Range), '소스' (Source), and '설명' (Description). The table is currently empty, and a message below it says '이 보안 그룹에 규칙이 없습니다.' (There are no rules for this security group). At the bottom left of the dialog is a button labeled '규칙 추가' (Add Rule). At the bottom right are two buttons: '취소' (Cancel) and '생성' (Create).

4.2 AWS 컴퓨터 서비스

5. 보안 그룹 생성

7. [Inbound] 탭에서 다음 규칙을 생성한 다음(각 새 규칙에 대해 [Add Rule] 선택) [Create]를 선택합니다.

보안 그룹 생성

보안 그룹 이름 ⓘ

admin_SG_Seoul

설명 ⓘ

사용자 그룹

VPC ⓘ

vpc-6219410a (기본값)

보안 그룹 규칙:

인바운드

아웃바운드

유형 ⓘ	프로토콜 ⓘ	포트 범위 ⓘ	소스 ⓘ	설명 ⓘ	
HTTP ▾	TCP	80	위치 무관 ▾	0.0.0.0/0, ::/0	예: 관리자 데스크톱용 SSH ×
HTTPS ▾	TCP	443	위치 무관 ▾	0.0.0.0/0, ::/0	예: 관리자 데스크톱용 SSH ×
SSH ▾	TCP	22	내 IP ▾	49.175.156.79/32	예: 관리자 데스크톱용 SSH ×

규칙 추가

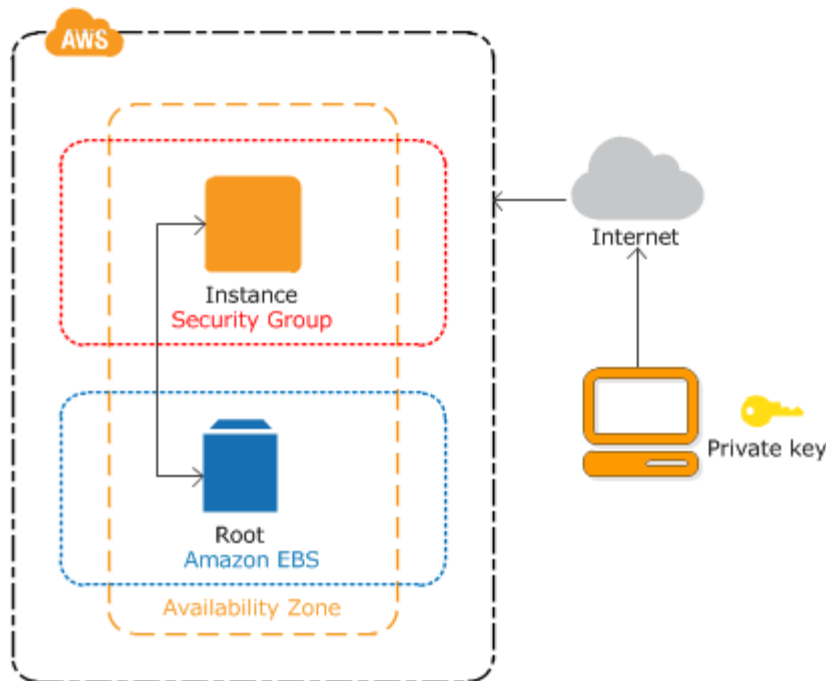
취소

생성

4.2 AWS 컴퓨터 서비스

● Amazon EC2 Linux 인스턴스

이 인스턴스는 Amazon EBS 지원 인스턴스(루트 볼륨이 EBS 볼륨임을 의미)입니다. 인스턴스가 실행되는 가용 영역을 지정하거나 적합한 가용 영역이 Amazon EC2에서 자동으로 선택할 수 있습니다. 인스턴스를 시작할 때 키 페어와 보안 그룹을 지정하여 인스턴스 보안을 설정합니다. 인스턴스에 연결할 때는 인스턴스 시작 시 지정한 키 페어의 프라이빗 키를 지정해야 합니다.



인스턴스 실행 단계

1. 인스턴스 시작
2. 인스턴스에 연결
3. 인스턴스 정리

4.2 AWS 컴퓨터 서비스

- 1단계: 인스턴스 시작

1. <https://console.aws.amazon.com/ec2/>에서 Amazon EC2 콘솔을 엽니다.
2. 콘솔 대시보드에서 **[Launch Instance]**를 선택합니다.
3. **[Choose an Amazon Machine Image (AMI)]** 페이지에 인스턴스에 대한 템플릿 역할을 하는 *[Amazon Machine Images (AMIs)]*라는 기본 구성 목록이 표시됩니다. Amazon Linux AMI의 HVM 버전을 선택합니다. 이 AMI는 "Free tier eligible"로 표시됩니다.
4. **[Choose an Instance Type]** 페이지에서 인스턴스의 하드웨어 구성을 선택할 수 있습니다. 기본적으로 선택된 t2.micro 유형을 선택합니다. 이 인스턴스 유형은 프리 티어에 적격입니다.
5. **[Review and Launch]**를 선택하여 마법사가 다른 구성 설정을 완료하게 합니다.

4.2 AWS 컴퓨터 서비스

6. **[Review Instance Launch]** 페이지의 **[Security Groups]** 아래에서 마법사가 보안 그룹을 만들고 선택했음을 확인합니다. 이 보안 그룹을 사용하거나, 다음 단계를 이용하여 설정을 시작할 때 만든 보안 그룹을 선택합니다.
 1. **[Edit security groups]**를 선택합니다.
 2. **[Configure Security Group]** 페이지에서 **[Select an existing security group]**이 선택되어 있는지 확인합니다.
 3. 기존 보안 그룹 목록에서 보안 그룹을 선택한 다음 **[Review and Launch]**를 선택합니다.
7. **[Review Instance Launch]** 페이지에서 **[Launch]**를 선택합니다.

4.2 AWS 컴퓨터 서비스

8. 키 페어에 대한 메시지가 나타나면 [**Choose an existing key pair**]를 선택한 다음 설치할 때 생성한 키 페어를 선택합니다.
또는 키 페어를 새로 만들 수 있습니다. [**Create a new key pair**]를 선택하고 키 페어 이름을 입력한 다음 [**Download Key Pair**]를 선택합니다.
이때가 사용자가 프라이빗 키 파일을 저장할 수 있는 유일한 기회이므로 반드시 다운로드하십시오. 프라이빗 키 파일은 안전한 장소에 저장합니다. 인스턴스를 시작할 때 키 페어의 이름을 제공하고, 인스턴스에 연결할 때마다 해당 프라이빗 키를 제공해야 합니다.
주의 - [**Proceed without a key pair**] 옵션을 선택하지 마십시오. 키 쌍 없이 인스턴스를 시작하면 인스턴스에 연결할 수 없습니다.
9. 준비되면 승인 확인란을 선택한 다음, [**Launch Instances**]를 선택합니다.
10. 확인 페이지에서 인스턴스가 실행 중인지 확인할 수 있습니다. **View Instances**를 선택하여 확인 페이지를 닫고 콘솔로 돌아갑니다.

4.2 AWS 컴퓨터 서비스

11. **[Instances]** 화면에서 시작 상태를 볼 수 있습니다. 인스턴스를 시작하는데 약간 시간이 걸립니다. 인스턴스를 시작할 때 초기 상태는 pending입니다. 인스턴스가 시작된 후에는 상태가 **[running]**으로 바뀌고 퍼블릭 DNS 이름을 받습니다. (**[Public DNS (IPv4)]** 열이 숨겨져 있는 경우 페이지 오른쪽 상단 모서리에 있는 **[Show/Hide Columns]**(기어 모양 아이콘)를 선택한 다음 **[Public DNS (IPv4)]**를 선택합니다.)
12. 연결할 수 있도록 인스턴스가 준비될 때까지 몇 분 정도 걸릴 수 있습니다. 인스턴스가 상태 확인을 통과했는지 확인하십시오. **[Status Checks]** 열에서 이 정보를 볼 수 있습니다.

4.2 AWS 컴퓨트 서비스

● 1단계: 인스턴스 시작

1. <https://console.aws.amazon.com/ec2/>에서 Amazon EC2 콘솔을 엽니다.
2. 콘솔 대시보드에서 [Launch Instance]를 선택합니다.

The screenshot displays the AWS Management Console for the EC2 service. The top navigation bar includes the AWS logo, service categories, and user information. The left-hand navigation pane lists various EC2-related features. The main area is divided into several sections: 'Resources' (showing a summary of EC2 resources), a highlighted 'EC2 Spot Instance' message, 'Instances' (with a table of running instances), 'Service Status' (indicating that services are operating normally), and 'Reserved Events' (showing no events). The right-hand pane provides links to account settings, support, and AWS Marketplace.

Resource	Count
Running Instance	0
Spot Instance	0
Reserved Instance	0
Dedicated Host	1
Key Pair	0
Network Interface	0
Elastic Network Adapter	0
Elastic IP Address	0
Elastic Network Interface	0
Elastic Network Adapter	0
Elastic Network Interface	0
Elastic Network Adapter	0

Service	Status
Amazon EC2	Operating normally
Amazon EC2 Instance Profiles	Operating normally
Amazon EC2 Spot Fleet	Operating normally
Amazon EC2 Reserved Instances	Operating normally
Amazon EC2 Dedicated Hosts	Operating normally
Amazon EC2 Images	Operating normally
Amazon EC2 AMIs	Operating normally
Amazon EC2 Instance Profiles	Operating normally
Amazon EC2 Spot Fleet	Operating normally
Amazon EC2 Reserved Instances	Operating normally
Amazon EC2 Dedicated Hosts	Operating normally
Amazon EC2 Images	Operating normally
Amazon EC2 AMIs	Operating normally

Event	Event Type
Amazon EC2	Operating normally
Amazon EC2 Instance Profiles	Operating normally
Amazon EC2 Spot Fleet	Operating normally
Amazon EC2 Reserved Instances	Operating normally
Amazon EC2 Dedicated Hosts	Operating normally
Amazon EC2 Images	Operating normally
Amazon EC2 AMIs	Operating normally
Amazon EC2 Instance Profiles	Operating normally
Amazon EC2 Spot Fleet	Operating normally
Amazon EC2 Reserved Instances	Operating normally
Amazon EC2 Dedicated Hosts	Operating normally
Amazon EC2 Images	Operating normally
Amazon EC2 AMIs	Operating normally

4.2 AWS 컴퓨터 서비스

● 1단계: 인스턴스 시작

3. [Choose an Amazon Machine Image (AMI)] 페이지에 인스턴스에 대한 템플릿 역할을 하는 [Amazon Machine Images (AMIs)]라는 기본 구성 목록이 표시됩니다. Amazon Linux AMI의 HVM 버전을 선택합니다. 이 AMI는 "Free tier eligible"로 표시됩니다.

The screenshot shows the AWS console interface for selecting an Amazon Machine Image (AMI). The top navigation bar includes the AWS logo, service dropdowns, and user information. The main content area is titled '단계 1: Amazon Machine Image(AMI) 선택' and includes a description of AMIs. A red box highlights the 'Amazon Linux 2 LTS Candidate 2 AMI (HVM), SSD Volume Type' option, which is marked as '프리 티어 사용 가능' (Free tier eligible). The left sidebar shows navigation options like 'AMI 선택', '인스턴스 유형 선택', etc. The right sidebar shows the 'AMI 1~35/35' pagination and a '선택' (Select) button.

AMI Name	AMI ID	Architecture	Platform	Free Tier Eligible
Amazon Linux AMI 2017.09.1 (HVM), SSD Volume Type	ami-5e1ab730	x86_64	Linux	Yes
Amazon Linux 2 LTS Candidate 2 AMI (HVM), SSD Volume Type	ami-96b916f8	x86_64	Linux	Yes
SUSE Linux Enterprise Server 12 SP3 (HVM), SSD Volume Type	ami-e22b898c	x86_64	Linux	No

4.2 AWS 컴퓨트 서비스

● 1단계: 인스턴스 시작

4. [Choose an Instance Type] 페이지에서 인스턴스의 하드웨어 구성을 선택할 수 있습니다. 기본적으로 선택된 t2.micro 유형을 선택합니다. 이 인스턴스 유형은 프리 티어에 적격입니다.

 서비스 ▾ 리소스 그룹 ▾ ★

1. AMI 선택 2. 인스턴스 유형 선택 3. 인스턴스 구성 4. 스토리지 추가 5. 태그 추가 6. 보안 그룹 구성 7. 검토

단계 2: 인스턴스 유형 선택

Amazon EC2는 각 사용 사례에 맞게 최적화된 다양한 인스턴스 유형을 제공합니다. 인스턴스는 애플리케이션을 실행할 수 있는 가상 서버입니다. 이러한 인스턴스에는 CPU, 메모리, 스토리지 및 네트워킹 용량이 다양하게 조합되어 있으며, 애플리케이션에 사용할 적절한 리소스 조합을 유연하게 선택할 수 있습니다. 인스턴스 유형과 이러한 인스턴스 유형이 컴퓨팅 요건을 충족하는 방식에 대해 자세히 알아보기

필터링 기준: 모든 인스턴스 유형 ▾ 현재 세대 ▾ 열 표시/숨기기

현재 선택된 항목: t2.micro (Variable ECU, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB 메모리, EBS 전용)

	그룹 ▾	유형 ▾	vCPUs ① ▾	메모리 (GiB) ▾	인스턴스 스토리지 (GB) ① ▾	EBS 최적화 사용 가능 ① ▾	네트워크 성능 ① ▾	IPv6 지원 ① ▾
<input checked="" type="checkbox"/>	General purpose	t2.micro 프리 티어 사용 가능	1	1	EBS 전용	-	낮음에서 중간	예
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS 전용	-	낮음에서 중간	예
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS 전용	-	낮음에서 중간	예

	그룹 ▾	유형 ▾	vCPUs ① ▾	메모리 (GiB) ▾	인스턴스 스토리지 (GB) ① ▾	EBS 최적화 사용 가능 ① ▾	네트워크 성능 ① ▾	IPv6 지원 ① ▾
<input checked="" type="checkbox"/>	General purpose	t2.micro 프리 티어 사용 가능	1	1	EBS 전용	-	낮음에서 중간	예
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS 전용	-	낮음에서 중간	예
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS 전용	-	낮음에서 중간	예

4.2 AWS 컴퓨터 서비스

6. **[Review Instance Launch]** 페이지의 **[Security Groups]** 아래에서 마법사가 보안 그룹을 만들고 선택했음을 확인합니다. 이 보안 그룹을 사용하거나, 다음 단계를 이용하여 설정을 시작할 때 만든 보안 그룹을 선택합니다.
 1. **[Edit security groups]**를 선택합니다.
 2. **[Configure Security Group]** 페이지에서 **[Select an existing security group]**이 선택되어 있는지 확인합니다.
 3. 기존 보안 그룹 목록에서 보안 그룹을 선택한 다음 **[Review and Launch]**를 선택합니다.
7. **[Review Instance Launch]** 페이지에서 **[Launch]**를 선택합니다.

4.2 AWS 컴퓨터 서비스

6. [Review Instance Launch] 페이지의 [Security Groups] 아래에서 마법사가 보안 그룹을 만들고 선택했음을 확인합니다. 이 보안 그룹을 사용하거나, 다음 단계를 이용하여 설정을 시작할 때 만든 보안 그룹을 선택.



1. AMI 선택 2. 인스턴스 유형 선택 3. 인스턴스 구성 4. 스토리지 추가 5. 태그 추가 6. 보안 그룹 구성 7. 검토

단계 6: 보안 그룹 구성

보안 그룹은 인스턴스에 대한 트래픽을 제어하는 방화벽 규칙 세트입니다. 이 페이지에서는 특정 트래픽을 인스턴스에 도달하도록 허용할 규칙을 추가할 수 있습니다. 예를 들면 웹 서버를 설정하여 인터넷 트래픽을 인스턴스에 도달하도록 허용하려는 경우 HTTP 및 HTTPS 트래픽에 대한 무제한 액세스를 허용하는 규칙을 추가합니다. 새 보안 그룹을 생성하거나 아래에 나와 있는 기존 보안 그룹 중에서 선택할 수 있습니다. [Amazon EC2 보안 그룹에 대해 자세히 알아보기](#)

보안 그룹 할당: ☐ 새 보안 그룹 생성
☒ 기존 보안 그룹 선택

보안 그룹 ID	이름	설명	작업
<input checked="" type="checkbox"/> sg-0e5e03d3df880d550	admin_SG_Seoul	user	새로 복사
<input type="checkbox"/> sg-6dc93307	default	default VPC security group	새로 복사

경고
소스가 0.0.0.0/0인 규칙은 모든 IP 주소에서 인스턴스에 액세스하도록 허용합니다. 알려진 IP 주소의 액세스만 허용하도록 보안 그룹을 설정하는 것이 좋습니다.

sg-6dc93307에 대한 inbound 규칙 (선택한 보안 그룹: sg-0e5e03d3df880d550)

유형 ⓘ	프로토콜 ⓘ	포트 범위 ⓘ	소스 ⓘ	설명 ⓘ
모든 트래픽	모두	모두	sg-6dc93307 (default)	

4.2 AWS 컴퓨터 서비스

6. [Review Instance Launch] 페이지의 [Security Groups] 아래에서 마법사가 보안 그룹을 만들고 선택했음을 확인합니다. 이 보안 그룹을 사용하거나, 다음 단계를 이용하여 설정을 시작할 때 만든 보안 그룹을 선택.

▼ 보안 그룹

보안 그룹 ID	이름	설명
sg-0e5e03d3df880d550	admin_SG_Seoul	user

선택한 모든 보안 그룹 인바운드 규칙

유형 ⓘ	프로토콜 ⓘ	포트 범위 ⓘ	소스 ⓘ	설명 ⓘ
HTTP	TCP	80	0.0.0.0/0	
HTTP	TCP	80	::/0	
SSH	TCP	22	49.175.156.79/32	
사용자 지정 TCP 규칙	TCP	443	0.0.0.0/0	
사용자 지정 TCP 규칙	TCP	443	::/0	

4.2 AWS 컴퓨터 서비스

- 키 페어에 대한 메시지가 나타나면 [**Choose an existing key pair**]를 선택한 다음 설치할 때 생성한 키 페어를 선택합니다.
- 준비되면 승인 확인란을 선택한 다음, [**Launch Instances**]를 선택합니다.
- 확인 페이지에서 인스턴스가 실행 중인지 확인할 수 있습니다. **View Instances**를 선택하여 확인 페이지를 닫고 콘솔로 돌아갑니다.

기존 키 페어 선택 또는 새 키 페어 생성

키 페어는 AWS에 저장하는 퍼블릭 키와 사용자가 저장하는 프라이빗 키 파일로 구성됩니다. 이 둘을 모두 사용하여 SSH를 통해 인스턴스에 안전하게 접속할 수 있습니다. Windows AMI의 경우 인스턴스에 로그인하는 데 사용되는 암호를 얻으려면 프라이빗 키 파일이 필요합니다. Linux AMI의 경우, 프라이빗 키 파일을 사용하면 인스턴스에 안전하게 SSH로 연결할 수 있습니다.

참고: 선택한 키 페어가 이 인스턴스에 대해 승인된 키 세트에 추가됩니다. 퍼블릭 AMI에서 기존 키 페어 제거에 대해 자세히 알아보십시오.

기존 키 페어 선택

키 페어를 선택하십시오

admin-key-pair-seoul

☐ 선택한 프라이빗 키 파일(admin-key-pair-seoul.pem)에 액세스할 수 있음을 확인합니다. 이 파일이 없으면 내 인스턴스에 로그인할 수 없습니다.

취소

인스턴스 시작

4.2 AWS 컴퓨터 서비스

11. **[Instances]** 화면에서 시작 상태를 볼 수 있습니다. 인스턴스를 시작하는데 약간 시간이 걸립니다. 인스턴스를 시작할 때 초기 상태는 pending입니다. 인스턴스가 시작된 후에는 상태가 **[running]**으로 바뀌고 퍼블릭 DNS 이름을 받습니다. (**[Public DNS (IPv4)]** 열이 숨겨져 있는 경우 페이지 오른쪽 상단 모서리에 있는 **[Show/Hide Columns]**(기어 모양 아이콘)를 선택한 다음 **[Public DNS (IPv4)]**를 선택합니다.)
12. 연결할 수 있도록 인스턴스가 준비될 때까지 몇 분 정도 걸릴 수 있습니다. 인스턴스가 상태 확인을 통과했는지 확인하십시오. **[Status Checks]** 열에서 이 정보를 볼 수 있습니다.

4.2 AWS 컴퓨터 서비스

- 2단계: PuTTY를 사용하여 Windows에서 Linux 인스턴스에 연결
 - PuTTY 설치 : [PuTTY 다운로드 페이지](#)에서 PuTTY 전체 제품군을 설치.
 - 인스턴스의 ID 보기

Amazon EC2 콘솔을 사용하여 인스턴스의 ID를 볼 수 있습니다([**Instance ID**] 열에서). [describe-instances](#)(AWS CLI) 또는 [Get-EC2Instance](#)(Windows PowerShell용 AWS 도구) 명령을 사용할 수도 있습니다.
 - 인스턴스의 퍼블릭 DNS 이름 보기

Amazon EC2 콘솔을 사용해서 사용자의 인스턴스에 대한 퍼블릭 DNS를 얻을 수 있습니다([**Public DNS (IPv4)**] 열 확인. 이 열이 숨겨진 경우는 [**Show/Hide**] 아이콘을 클릭하고 [**Public DNS (IPv4)**]를 선택). [describe-instances](#)(AWS CLI) 또는 [Get-EC2Instance](#)(Windows PowerShell용 AWS 도구) 명령을 사용할 수도 있습니다.

4.2 AWS 컴퓨터 서비스

- **(IPv6 전용) 인스턴스의 IPv6 주소를 얻습니다.**

인스턴스에 IPv6 주소를 할당했다면 퍼블릭 IPv4 주소나 퍼블릭 IPv4 DNS 호스트 이름 대신 IPv6 주소를 사용하여 인스턴스에 연결할 수도 있습니다. 로컬 컴퓨터에 IPv6 주소가 있고 IPv6를 사용하도록 컴퓨터를 구성해야 합니다. Amazon EC2 콘솔을 사용하여 인스턴스의 IPv6 주소를 얻을 수 있습니다([**IPv6 IPs**] 필드 확인). [describe-instances](#)(AWS CLI) 또는 [Get-EC2Instance](#)(Windows PowerShell용 AWS 도구) 명령을 사용할 수도 있습니다.

- **프라이빗 키 찾기**

인스턴스를 시작할 때 지정한 키 페어를 찾기 위해 .pem 파일의 컴퓨터 상 위치에 대한 정규화된 경로를 얻습니다.

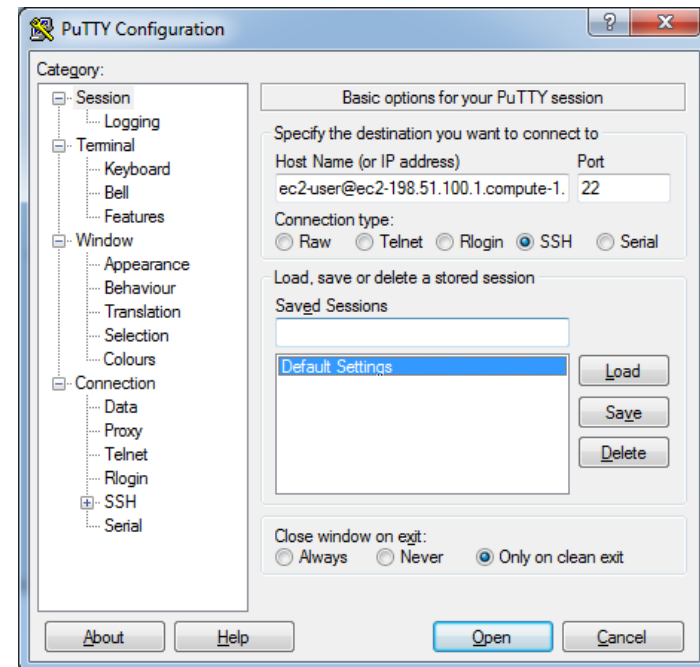
4.2 AWS 컴퓨터 서비스

- 인스턴스를 시작하는 데 사용한 AMI의 기본 사용자 이름을 가져옵니다
 - **Amazon Linux AMI의 경우 사용자 이름은 ec2-user입니다.**
 - Centos AMI의 경우 사용자 이름은 centos입니다.
 - Debian AMI의 경우 사용자 이름은 admin 또는 root입니다.
 - Fedora AMI의 경우 사용자 이름은 ec2-user입니다.
 - RHEL AMI의 경우 사용자 이름은 ec2-user 또는 root입니다.
 - SUSE AMI의 경우 사용자 이름은 ec2-user 또는 root입니다.
 - Ubuntu AMI의 경우 사용자 이름은 ubuntu 또는 root입니다.
 - ec2-user 및 root를 사용할 수 없는 경우 AMI 공급자에게 문의하십시오.
- **IP 주소에서 인스턴스로의 인바운드 SSH 트래픽 활성화**

인스턴스와 연관된 보안 그룹이 IP 주소로부터 들어오는 SSH 트래픽을 허용하는지 확인하십시오. 기본 보안 그룹은 기본적으로 들어오는 SSH 트래픽을 허용하지 않습니다.

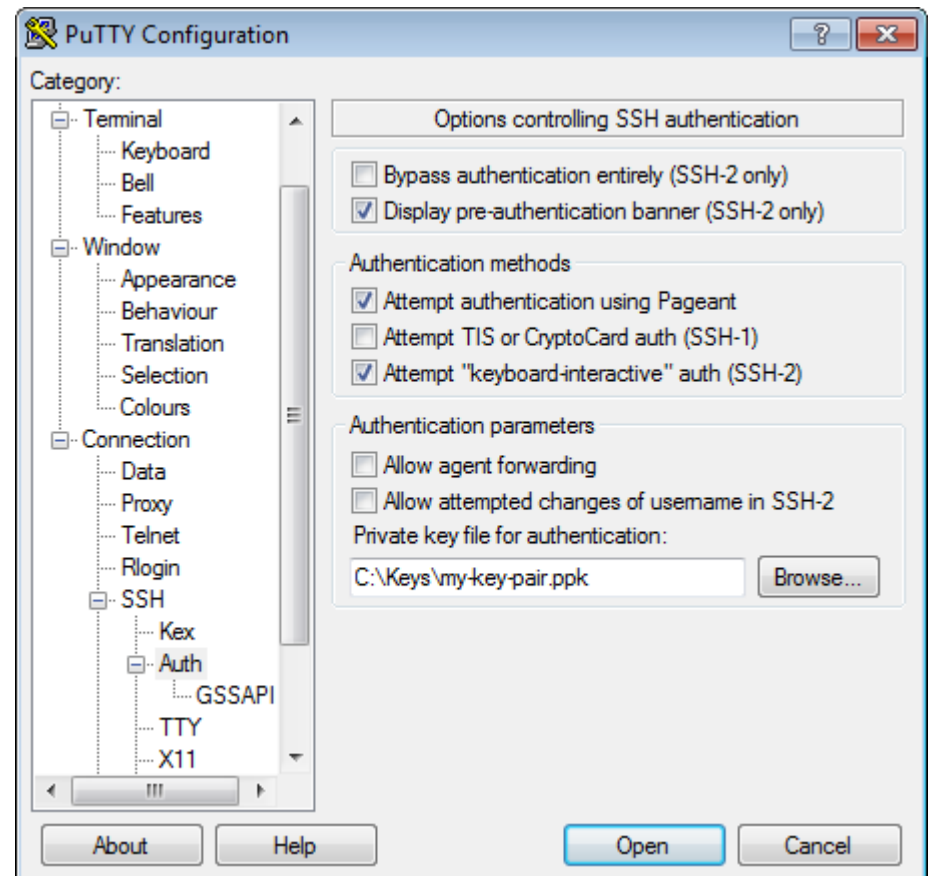
4.2 AWS 컴퓨터 서비스

- 2단계: PuTTY를 사용하여 Windows에서 Linux 인스턴스에 연결
 - PuTTY 세션 시작
 1. PuTTY를 시작합니다.
 2. [Category] 창에서 [Session]를 선택하고 다음 필드를 작성합니다.
 1. [Host Name] 상자에 `user_name@public_dns_name`을 입력합니다. AMI에 적합한 사용자 이름을 지정해야 합니다.
 2. [Connection type] 아래에서 [SSH]를 선택
 3. [Port]가 22인지 확인합니다.



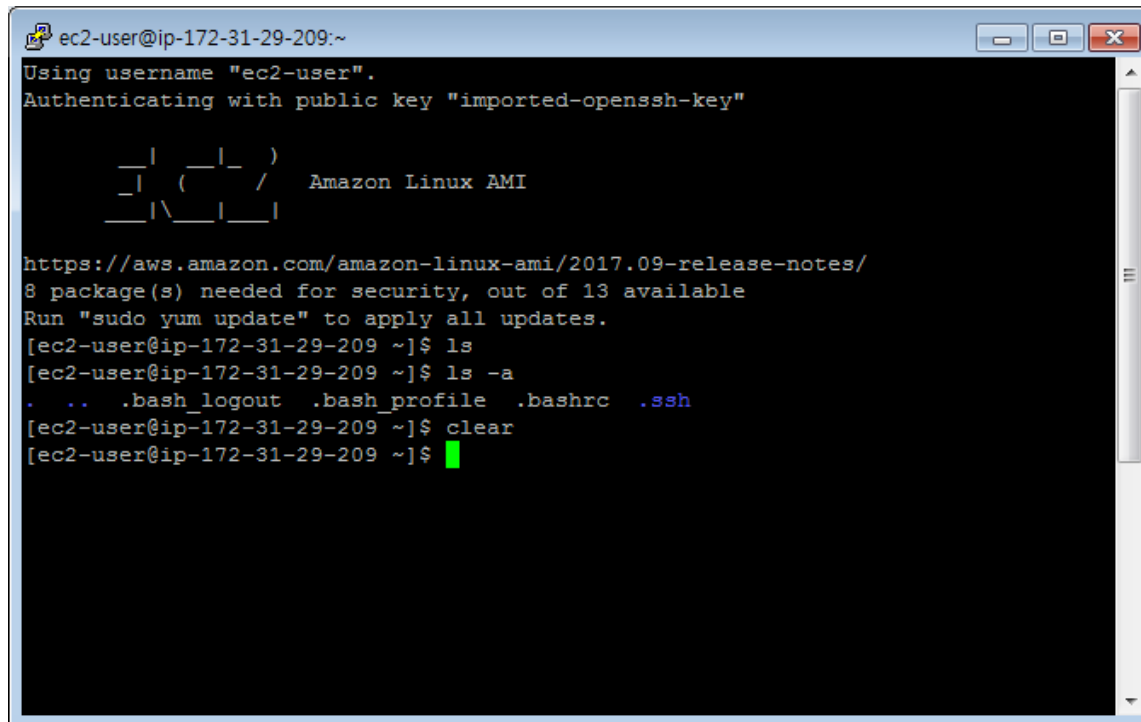
4.2 AWS 컴퓨터 서비스

- 2단계: PuTTY를 사용하여 Windows에서 Linux 인스턴스에 연결
 - PuTTY 세션 시작
- 3. [Category] 창에서 [Connection], [SSH]를 확장한 다음 [Auth]를 선택.
 1. [Browse]를 선택합니다.
 2. 키 페어에 대해 생성한 .ppk 파일을 선택한 다음 [Open]을 선택합니다.
 3. [Open]을 클릭하여 PuTTY 세션을 선택합니다.



4.2 AWS 컴퓨터 서비스

4. 이 인스턴스에 처음 연결한 경우 PuTTY에서 연결하려는 호스트를 신뢰할 수 있는지 묻는 보안 알림 대화 상자가 표시됩니다.
5. (선택 사항) 보안 알림 대화 상자의 지문이 1단계에서 얻은 이전 지문과 일치하는지 확인합니다.
6. [Yes]를 선택합니다. 창이 열리고 인스턴스에 연결됩니다.



```
ec2-user@ip-172-31-29-209:~  
Using username "ec2-user".  
Authenticating with public key "imported-openssh-key"  
  
  _ | _ | _ )  
  _ | ( _ | /   Amazon Linux AMI  
  _ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/  
8 package(s) needed for security, out of 13 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-172-31-29-209 ~]$ ls  
[ec2-user@ip-172-31-29-209 ~]$ ls -a  
.  ..  .bash_logout  .bash_profile  .bashrc  .ssh  
[ec2-user@ip-172-31-29-209 ~]$ clear  
[ec2-user@ip-172-31-29-209 ~]$
```

4.2 AWS 컴퓨터 서비스

- root 로 이동

- `sudo su -`

- Java version 확인하는 방법

- 아래 명령어를 사용하여, 현재 서버에 설치된 자바 버전을 확인.
- `$ java -version`

- Java 1.8 설치하는 방법

- 먼저, `yum list` 명령어를 활용하여, 설치 가능한 java 버전을 확인.
(만약, 최신 버전이 없다면 `yum update`를 실시.)
- `$ yum list java*jdk-devel`
- 설치하고자 하는 버전을 확인하고, `yum install` 명령어를 활용하여 설치합니다.
- `$ yum install -y java-1.8.0-openjdk-devel.x86_64`

- Java version을 변경하는 방법

- 변경 후, 사용하지 않는 이전 버전의 java 1.7을 삭제합니다.
- `$yum remove java-1.7.0-openjdk`

4.2 AWS 컴퓨터 서비스

- 웹서버 설정

```
# sudo yum update -y
```

```
# sudo yum install -y httpd24 php56 php56-mysqlnd
```

```
# sudo service httpd start
```

```
# iptables -t nat -I PREROUTING -p tcp --dport 80 -j REDIRECT --to-port  
8080
```

```
# service iptables save
```

- Tomcat 설정

```
# sudo yum list tomcat8*
```

```
# sudo yum install -y tomcat8
```

```
# sudo yum install tomcat8-admin-webapps
```

```
# sudo yum install tomcat8-webapps
```

4.2 AWS 컴퓨터 서비스

- Mysql 설정

```
# sudo yum install mysql57-server
```

```
# mysql -V
```

```
# sudo service mysqld start
```

```
# mysqladmin -u root password
```

```
# mysql -u root -p
```

AWS EC2 TOMCAT 권한 설정

```
[root@ip-172-31-28-56 tomcat8]# cd /usr/share/tomcat8
[root@ip-172-31-28-56 tomcat8]# chgrp -R tomcat /usr/share/tomcat8
[root@ip-172-31-28-56 tomcat8]# chown -R tomcat webapps/ work/ temp/ logs/
[root@ip-172-31-28-56 tomcat8]# find conf webapps -type d -exec chmod 755 {} +
[root@ip-172-31-28-56 tomcat8]# find conf webapps -type f -exec chmod 644 {} +
[root@ip-172-31-28-56 tomcat8]# find logs temp work -type d -exec chmod 750 {} +
[root@ip-172-31-28-56 tomcat8]# find logs temp work -type f -exec chmod 640 {} +
[root@ip-172-31-28-56 tomcat8]# service tomcat8 restart
```

```
[root@ip-172-31-28-56 tomcat8]# cd /usr/share/tomcat8
[root@ip-172-31-28-56 tomcat8]# ls -l
total 4
drwxr-xr-x 2 tomcat tomcat 4096 Aug  6 07:42 bin
lrwxrwxrwx 1 tomcat tomcat  12 Aug  6 07:42 conf -> /etc/tomcat8
lrwxrwxrwx 1 tomcat tomcat  23 Aug  6 07:42 lib -> /usr/share/java/tomcat8
lrwxrwxrwx 1 tomcat tomcat  16 Aug  6 07:42 logs -> /var/log/tomcat8
lrwxrwxrwx 1 tomcat tomcat  23 Aug  6 07:42 temp -> /var/cache/tomcat8/temp
lrwxrwxrwx 1 tomcat tomcat  24 Aug  6 07:42 webapps -> /var/lib/tomcat8/webapps
lrwxrwxrwx 1 tomcat tomcat  23 Aug  6 07:42 work -> /var/cache/tomcat8/work
```

```
[root@ip-172-31-28-56 tomcat8]# cd chgrp -R tomcat /usr/share/tomcat8
-bash: cd: chgrp: No such file or directory
[root@ip-172-31-28-56 tomcat8]# cd chgrp -R tomcat /usr/share/tomcat8
-bash: cd: chgrp: No such file or directory
```

```
[root@ip-172-31-28-56 tomcat8]# chgrp -R tomcat /usr/share/tomcat8
[root@ip-172-31-28-56 tomcat8]# chown -R tomcat webapps/ work/ temp/ logs/
[root@ip-172-31-28-56 tomcat8]# find conf webapps -type d -exec chmod 755 {} +
[root@ip-172-31-28-56 tomcat8]# find conf webapps -type f -exec chmod 644 {} +
[root@ip-172-31-28-56 tomcat8]# find logs temp work -type d -exec chmod 750 {} +
[root@ip-172-31-28-56 tomcat8]# find logs temp work -type f -exec chmod 640 {} +
[root@ip-172-31-28-56 tomcat8]# service tomcat8 restart
[root@ip-172-31-28-56 tomcat8]#
```

4.2 AWS 컴퓨터 서비스

- 3단계: 인스턴스 정리

1. 탐색 창에서 [**Instances**]를 선택합니다. 인스턴스 목록에서 인스턴스를 선택합니다.
2. [**Actions**], [**Instance State**], [**Terminate**]를 차례로 선택합니다.
3. 확인 메시지가 나타나면 [**Yes, Terminate**]를 선택합니다.
4. Amazon EC2가 인스턴스를 종료합니다. 인스턴스는 종료한 후에도 잠시 동안 콘솔에서 표시된 상태로 유지되며, 그 이후 항목이 삭제됩니다.