

# AWS Security 101: 함께 만들어봐요. 안전한 서비스

1화

홍성진



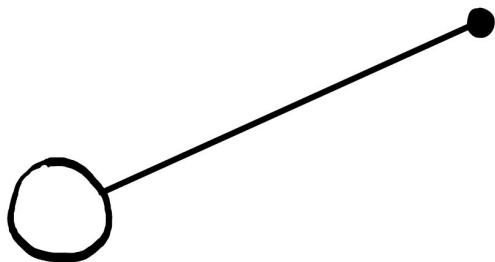
# 홍성진 aka. nisam

- 센드버드 Staff Security Engineer
- AWS 한국 사용자모임 보안 소모임 운영진
- 前 네이버 Security Engineer
- 비오비 4기

#AppSec #CloudSec #DevSecOps #ThreatModeling #BugBounty #SecureCoding  
#☕️ #🎾 #🏋️‍♂️ #💪



여러분들은 이제 ...





??? :

성진 씨 우리 기존 서비스 AWS에 올릴거예요.  
내일까지 AWS 계정 만들어서 안전하게 설정 해주세요!



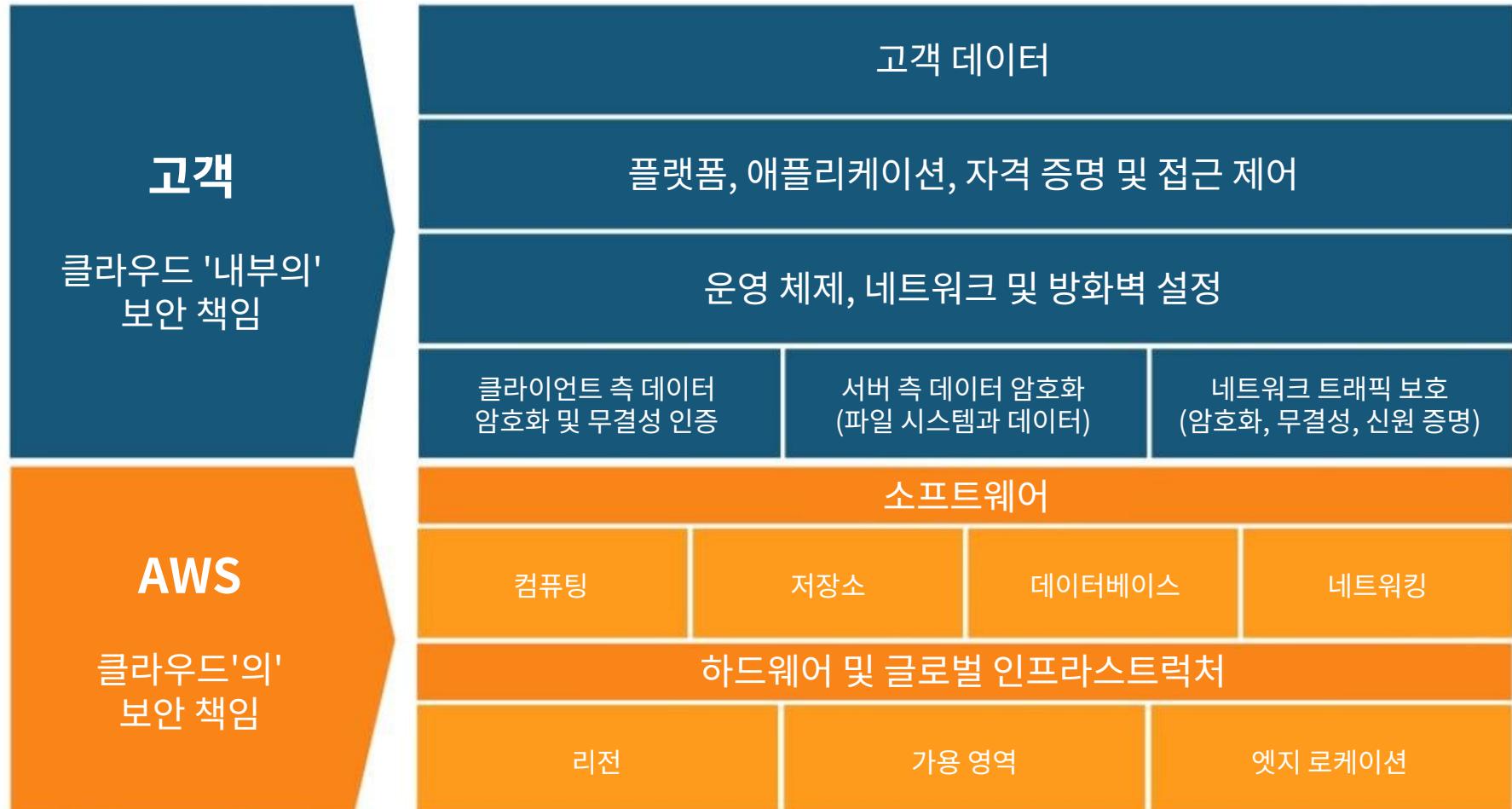
성진 :

네? 저 AWS 안 써봤는데요?



# 1. 클라우드 보안의 이해

# 공동 책임 모델

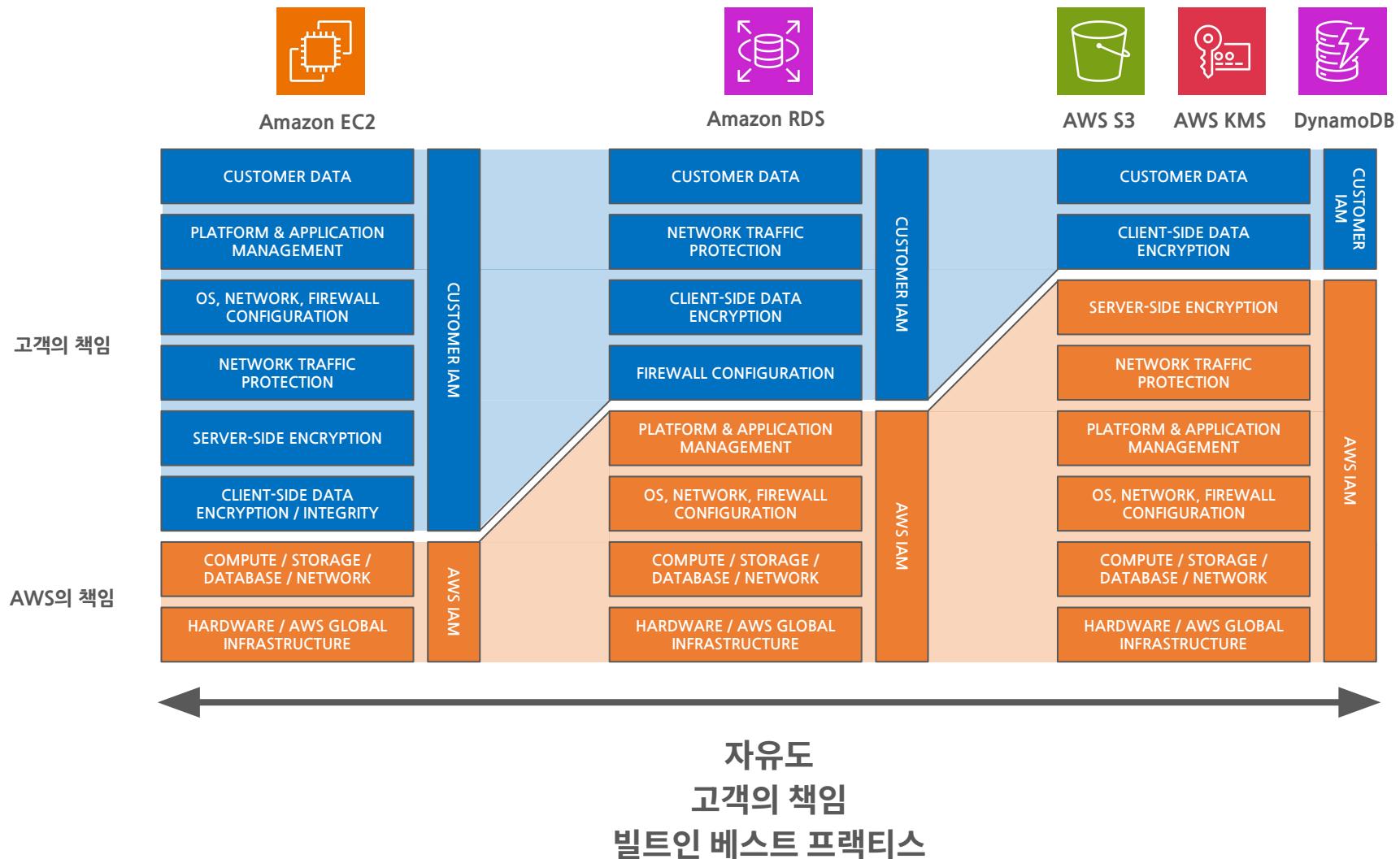


어떻게 길거리로  
나오시게 되셨나요?  
도박? 마약?

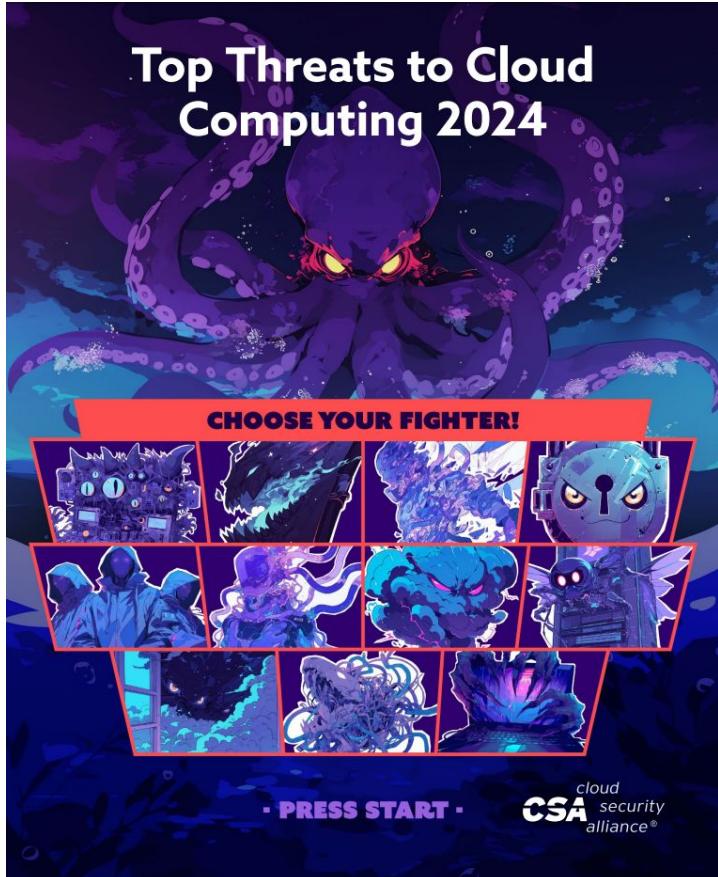
EC2 서버를 실수로  
안 껐어요…



# 공유 책임 모델 - 서비스 별 차이



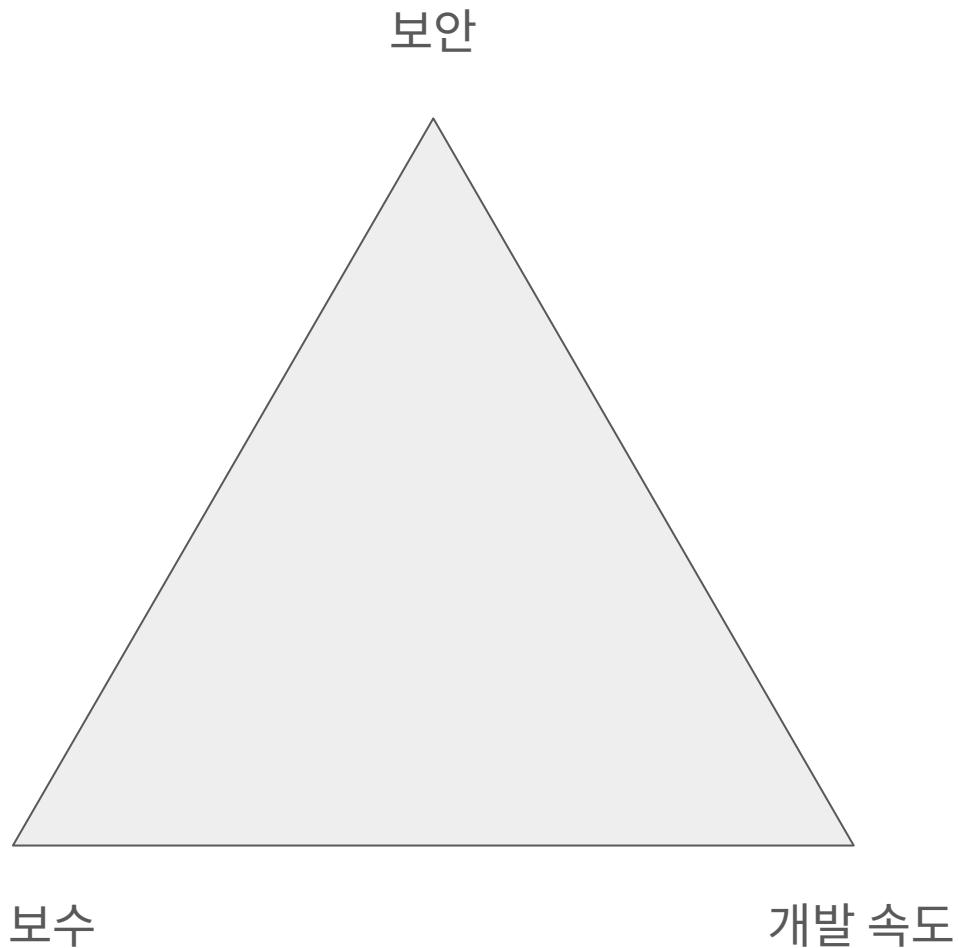
# Misconfiguration



A slide from a presentation about misconfiguration. The background is a dark, futuristic cityscape at night. On the left, a red circular icon contains a white graphic of three vertical bars with a triangle pointing upwards. To the right of the icon, the text "Security Issue 1" is written in white. Below it, the title "MISCONFIGURATION &amp; INADEQUATE CHANGE CONTROL" is displayed in large, bold, red capital letters. To the right of the text, there is a detailed illustration of a complex, multi-eyed machine with many buttons, screens, and mechanical components, all in shades of purple and blue. At the bottom of the slide, a block of text provides a definition and some common examples of misconfigurations.

Misconfigurations are the incorrect or sub-optimal setup of cloud computing assets that can leave them vulnerable to unintended damage or external/internal malicious activity. Lack of cloud system knowledge or understanding of cloud security settings and nefarious intentions can result in misconfigurations. [Some common misconfigurations \[1\]](#) are: 1. secrets management, 2. disabled monitoring and logging, 3. ICMP left open, 4. insecure automated backups, 5. storage access, 6. lack of validation, 7. unlimited access to non-HTTPS/HTTP ports, 8. overly permissive access to virtual machines, containers, and hosts, 9. enabling too many cloud access permissions (least privilege), 10. subdomain hijacking (aka dangling DNS), 11. misconfigurations specific to your cloud provider(s) like AWS S3 buckets. [Misconfiguration of cloud resources is a leading cause of security issues in the cloud](#) that can result in severe damage, as shown in the Business Impact section below. [2]

# 보안 딜레마



우리가 점을 하나 찍는다면 어디다 둬야 하는가…

## 2. 계정 및 접근 권한 관리



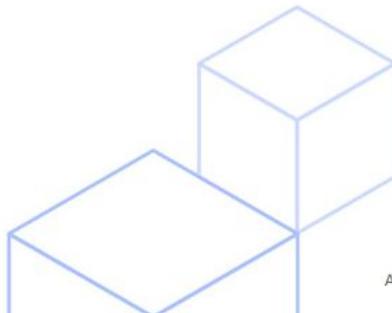
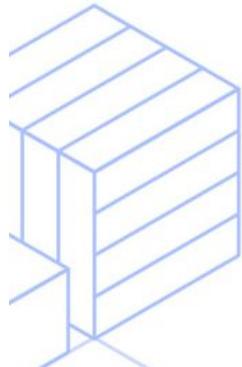
성진 :

AWS 계정을 만들라고 하니까 우선 만들어보자!



**Explore Free Tier products with a new AWS account.**

To learn more, visit [aws.amazon.com/free](https://aws.amazon.com/free).



## Sign up for AWS

### Root user email address

Used for account recovery and some administrative functions

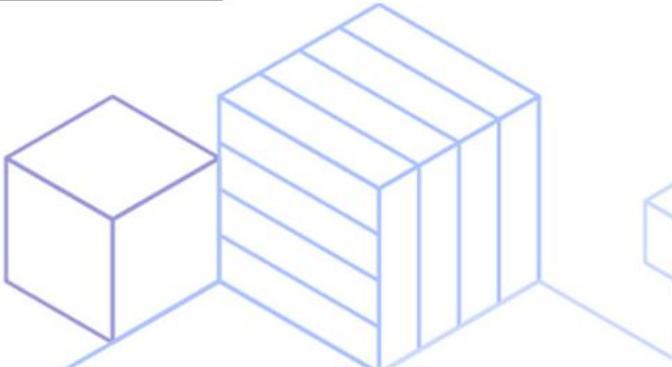
### AWS account name

Choose a name for your account. You can change this name in your account settings after you sign up.

**Verify email address**

OR

**Sign in to an existing AWS account**





# Congratulations!

Thank you for signing up with AWS.

We are activating your account, which should take a few minutes. You will receive an email when this is complete.

[Go to the AWS Management Console](#)

[Sign up for another account](#) or [Contact Sales](#)



성진 :

아.. AWS 계정은 만들었고 이제 뭐해야하지?



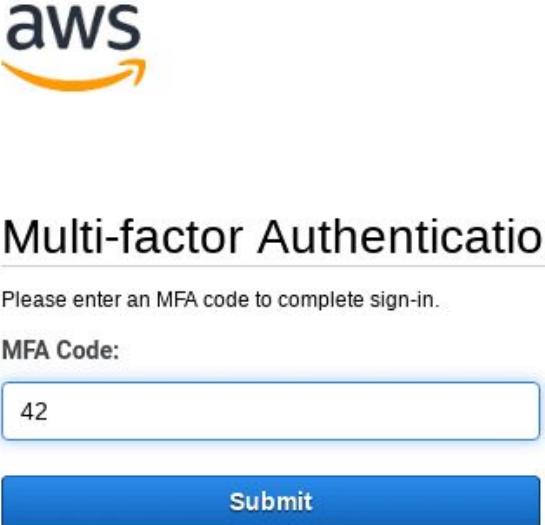
성진 :

아.. AWS 계정은 만들었고 이제 뭐해야하지?

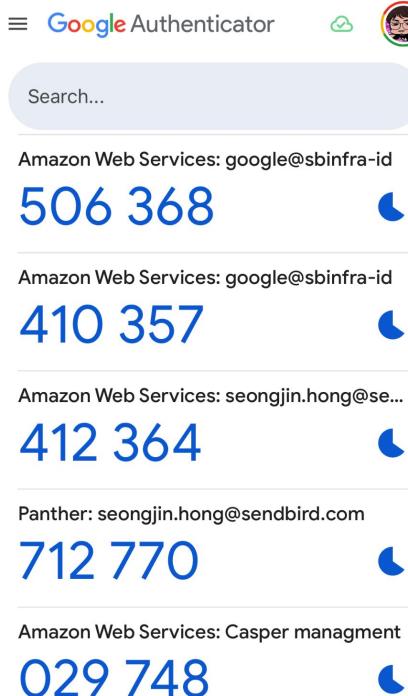
여러분들의 선택은...!?

# Multi Factor Authentication

AWS 다중 인증(MFA)은 사용자 이름 및 암호 로그인 자격 증명 외에 **두 번째 인증 요소**를 추가하는 기능입니다. 생성한 **IAM 사용자** 및 **루트**의 AWS 계정 수준에서 MFA를 활성화할 수 있습니다.



The screenshot shows the AWS Multi-factor Authentication sign-in page. It features the AWS logo at the top left. Below it, the title "Multi-factor Authentication" is displayed. A sub-instruction "Please enter an MFA code to complete sign-in." follows. An input field labeled "MFA Code:" contains the value "42". A large blue "Submit" button is positioned below the input field. At the bottom left, there is a "Cancel" link.



The screenshot shows the Google Authenticator mobile application interface. At the top, it displays the text "≡ Google Authenticator" and icons for account settings and a QR code. Below this is a search bar with the placeholder "Search...". The main area lists several MFA codes, each associated with a user identifier and a blue circular icon:

Amazon Web Services: google@sbinfra-id	506 368	🕒
Amazon Web Services: google@sbinfra-id	410 357	🕒
Amazon Web Services: seongjin.hong@se...	412 364	🕒
Panther: seongjin.hong@sendbird.com	712 770	🕒
Amazon Web Services: Casper managment	029 748	🕒

# Multi Factor Authentication - 지원 장치

지원하는 MFA 방식은 패스키와 보안 키, 가상 인증 앱, 하드웨어 TOTP 토큰을 지원합니다.

**내 보안 자격 증명** Root user 정보

루트 사용자는 이 계정의 모든 AWS 리소스에 액세스할 수 있으며 다음 모범 사례 [\[?\]을\(를\)](#) 수행하는 것이 좋습니다.

**계정 세부 정보**

계정 이름  
admin

AWS 계정 ID  
 2343551

**멀티 팩터 인증(MFA) (1)**

MFA를 사용하여 AWS 환경의 보안을 강화합니다. MFA로 로그인하려면 MFA 디바이스의 인증 코드가 필요합니다.

유형	식별자
<input type="radio"/> 가상	arn:aws:iam::234355188026:mfa/google

**MFA device**

디바이스 옵션  
사용자 이름과 암호 외에도 이 디바이스를 사용하여 계정에 인증합니다.

**패스키 또는 보안 키**  
지문, 얼굴 또는 화면 잠금을 사용하여 인증합니다. 이 디바이스에서 패스키를 생성하거나 FIDO2 보안 키와 같은 다른 디바이스를 사용하세요.

**인증 관리자 앱**  
모바일 디바이스 또는 컴퓨터에 설치된 앱에서 생성된 코드를 사용하여 인증합니다.

**하드웨어 TOTP 토큰**  
하드웨어 TOTP 토큰 또는 기타 하드웨어 디바이스에서 생성된 코드를 사용하여 인증합니다.

오른쪽 상단 메뉴 > 내 보안 자격 증명

# CloudTrail



CloudTrail은 AWS 계정의 운영 및 위험 감사, 거버넌스, 그리고 규정 준수를 가능하게 해주는 AWS 서비스입니다. 사용자, 역할 또는 AWS 서비스에 의해 수행된 작업들이 CloudTrail에 이벤트로 기록됩니다.

# CloudTrail - 기본 로그 보관 시간

CloudTrail은 특별한 설정 없이 기본적으로 **90일 동안** 로그를 보관합니다.

Event history (150+)							<a href="#">Info</a>	<a href="#">C</a>	<a href="#">Download events</a>	<a href="#">Create Athena table</a>
Event history shows you the last 90 days of management events.										
Lookup attributes										
Read-only	▼	<input type="text"/> Q false	X	<a href="#">Filter by date and time</a>	<	1	2	3	4	...
<input type="checkbox"/>	Event name	Event time	User name	Event source	Resource type	Resource name				
<input type="checkbox"/>	<a href="#">UpdateInstanceInformation</a>	January 19, 2025, 20:53:04 (UTC+09:00)	i-0b06ed8e5d756a050	ssm.amazonaws.com	-	-				
<input type="checkbox"/>	<a href="#">CreateLogStream</a>	January 19, 2025, 20:52:38 (UTC+09:00)	Discord_Webhook_Organization	logs.amazonaws.com	-	-				
<input type="checkbox"/>	<a href="#">CreateLogStream</a>	January 19, 2025, 20:52:38 (UTC+09:00)	Discord_Webhook_Organization	logs.amazonaws.com	-	-				
<input type="checkbox"/>	<a href="#">UpdateInstanceInformation</a>	January 19, 2025, 20:51:41 (UTC+09:00)	i-00ef351ce1f5c39ea	ssm.amazonaws.com	-	-				
<input type="checkbox"/>	<a href="#">UpdateInstanceInformation</a>	January 19, 2025, 20:48:04 (UTC+09:00)	i-0b06ed8e5d756a050	ssm.amazonaws.com	-	-				
<input type="checkbox"/>	<a href="#">UpdateInstanceInformation</a>	January 19, 2025, 20:46:41 (UTC+09:00)	i-00ef351ce1f5c39ea	ssm.amazonaws.com	-	-				
<input type="checkbox"/>	<a href="#">CreateLogStream</a>	January 19, 2025, 20:45:28 (UTC+09:00)	Discord_Webhook_Organization	logs.amazonaws.com	-	-				
<input type="checkbox"/>	<a href="#">CreateLogStream</a>	January 19, 2025, 20:45:27 (UTC+09:00)	Discord_Webhook_Organization	logs.amazonaws.com	-	-				
<input type="checkbox"/>	<a href="#">UpdateInstanceInformation</a>	January 19, 2025, 20:43:04 (UTC+09:00)	i-0b06ed8e5d756a050	ssm.amazonaws.com	-	-				
<input type="checkbox"/>	<a href="#">UpdateInstanceInformation</a>	January 19, 2025, 20:41:51 (UTC+09:00)	i-00ef351ce1f5c39ea	ssm.amazonaws.com	-	-				
<input type="checkbox"/>	<a href="#">UpdateInstanceInformation</a>	January 19, 2025, 20:41:41 (UTC+09:00)	i-00ef351ce1f5c39ea	ssm.amazonaws.com	-	-				
<input type="checkbox"/>	<a href="#">UpdateInstanceInformation</a>	January 19, 2025, 20:38:04 (UTC+09:00)	i-0b06ed8e5d756a050	ssm.amazonaws.com	-	-				

# CloudTrail - 추가 보관

90일 이상의 로그를 저장하려면 스토리지 서비스인 Simple Storage Service(S3)에 추가적으로 저장해야합니다. 트레일 로그는 리전 별로 생성해야 합니다.

단계 1  
 주적 속성 선택

단계 2  
 로그 이벤트 선택

단계 3  
 검토 및 생성

### 추적 속성 선택

**일반 세부 정보**  
콘솔에서 생성된 주적은 다중 리전 주적입니다. 자세히 알아보기 [\[i\]](#)

**주적 이름**  
주적의 표시 이름을 입력합니다.

**3~128자입니다. 문자, 숫자, 마침표, 밑줄 및 대시만 허용됩니다.**

조직의 모든 계정에 대해 활성화  
조직의 계정을 검토하려면 AWS Organizations를 엽니다. 모든 계정 보기 [\[i\]](#)

**스토리지 위치 | 정보**

새 S3 버킷 생성  
주적에 대한 로그를 저장할 버킷을 생성합니다.

기존 S3 버킷 사용  
이 주적에 대한 로그를 저장할 기존 버킷을 선택합니다.

**주적 로그 버킷 및 폴더**  
로그를 저장할 새 S3 버킷 이름 및 폴더(접두사)를 입력합니다. 버킷 이름은 전역적으로 고유해야 합니다.

로그는 aws-cloudtrail-logs-234355188026-aec85370/AWSLogs/234355188026에 저장됨

**로그 파일 SSE-KMS 암호화 | 정보**  
 활성화됨

**고객 관리형 AWS KMS 키**  
 신규  
 기존

**AWS KMS 별칭**

KMS 키와 S3 버킷이 동일한 리전에 있어야 합니다.

# CloudTrail - 추가 보관 객체 잠금 설정

로그를 저장하는 S3 스토리지에 객체 잠금 기능을 활용하여 로그의 삭제를 예방할 수 있습니다.

## 객체 잠금 편집 정보

### 객체 잠금

WORM(Write-Once-Read-Many) 모델을 사용하여 객체를 저장하면 고정된 시간 동안 또는 무기한으로 객체가 삭제되거나 덮어쓰이지 않도록 할 수 있습니다. 객체 잠금은 버전이 지정된 버킷에서만 작동합니다. [자세히 알아보기](#)

① Amazon S3 객체 잠금이 활성화되면 해당 버킷에 대한 객체 잠금을 비활성화하거나 버전 관리를 일시 중지할 수 없습니다.

#### 객체 잠금

활성화됨

#### 기본 보존

이 버킷에 배치된 새 객체가 삭제되거나 덮어쓰기 되지 않도록 자동으로 보호합니다.

비활성화

활성화

#### 기본 보존 모드

거버넌스

특정 IAM 권한이 있는 사용자는 보존 기간 동안 보호된 객체 버전을 덮어쓰거나 삭제할 수 있습니다.

규정 준수

어떤 사용자도 보존 기간 동안 보호된 객체 버전을 덮어쓰거나 삭제할 수 없습니다.

#### 기본 보존 기간

365

Days

양의 정수여야 합니다.

취소

변경 사항 저장

# 예산 설정

예상외의 금액이 지출되지 않도록 예산 리포트를 생성합니다. 이는 비이상적인 행위 탐지에도 활용 될 수 있습니다.

예산 (1) 정보

CSV 다운로드 작업 예산 생성

유형 - 모든 예산 표시 ▾

□   이름	▲   임계값	▼   예산	사용된 금액	예상 금액	예산 대비 현재 비용	▼   예산 대비 예상 비
□ My Monthly Cost Budget	확인	US\$100.00	US\$46.53	US\$80.34	46.52%	

My Monthly Cost Budget 확인 US\$100.00 US\$46.53 US\$80.34 46.52%

예산 유형 선택 정보

예산 설정

템플릿 사용(단순)  
권장 구성을 사용합니다. 예산이 생성된 후 일부 구성 옵션을 변경할 수 있습니다.

사용자 지정(고급)  
사용 사례에 맞는 파라미터를 설정하도록 예산을 사용자 지정합니다. 기간, 시작 흘 및 특정 계정을 사용자 지정할 수 있습니다.

템플릿 - 신규

사용 사례에 가장 적합한 템플릿을 선택합니다.

제로 지출 예산  
지출이 AWS 프리 티어 한도를 상회하는 금액인 0.01 USD를 초과하면 알려주는 예산을 생성합니다.

월별 비용 예산  
예산 금액을 초과하거나 초과할 것으로 예상되는 경우 이를 알리는 월별 예산을 생성합니다.

일별 절감형 플랜 담당 예산  
원하는 목표 아래로 떨어지면 절감형 플랜의 담당을 예산을 생성합니다.

일별 예약 사용률 예산  
정의한 목표 아래로 떨어지면 예약의 사용률을 예산을 생성합니다.

제로 지출 예산 - 템플릿

예산 이름  
이 예산에 대한 설명이 포함된 이름을 제공합니다.  
My Zero-Spend Budget

이메일 수신자  
임계값이 초과되었을 때 알림을 전달할 이메일 수신자를 지정합니다.  
쉼표를 사용하여 이메일 주소 구분

이메일 수신자는 최대 10명입니다.

# 비용 이상 정후 탐지

AWS 비용 이상 탐지는 기계 학습 모델을 사용하여 이상 지출 패턴을 탐지하고 경고하는 기능입니다.

## 개요 정보

### ▶ 비용 이상 탐지 작동 방식

비용 이상 탐지를 시작하려면 다음 단계를 수행해야 합니다.

### 비용 이상 탐지 요약

탐지된 이상 정후(MTD):

8

총 비용 영향(MTD):

\$28.07

총 지출(MTD):

\$46.53

총 지출(전월 대비):

> 100% ↑

탐지한 이상 정후

비용 모니터

알림 구독

### 탐지한 이상 정후 (15) 정보

이상이 발생하는 기간 동안 총 비용 영향은 하루에 최대 3회까지 발생할 수 있는 청구 데이터 계산에 따라 증가하거나 감소할 수 있습니다.

Q 속성 또는 값을 기준으로 탐지된 이상 정후 찾기						지난 90일(모두) ▾	◀	1	2	▶	⚙️		
시작 날짜	▼	마지막 탐지	▼	기간	▼	비용 영향	▼	영향 %	▼	모니터 이름	▼	최상위 근본 원인(서비스)	더 보기
2025.01.05		2025.01.18		14일		\$20.01		16675%		Default-Services-Monitor		Amazon Virtual Private Cloud	<a href="#">3개의 잠재적 근본 원인 보기</a>
2025.01.12		2025.01.15		4일		\$0.04		33.33%		Default-Services-Monitor		Amazon Simple Storage Service	<a href="#">1개의 잠재적 근본 원인 보기</a>
2025.01.12		2025.01.15		4일		\$5.87		해당 사항 없음		Default-Services-Monitor		Amazon Elastic Compute Cloud - Compute	<a href="#">2개의 잠재적 근본 원인 보기</a>
2025.01.05		2025.01.13		9일		\$0.85		157.41%		Default-Services-Monitor		AWS Key Management Service	<a href="#">1개의 잠재적 근본 원인 보기</a>

# 패스워드 정책 변경

기본으로 제공하는 패스워드 정책을 업데이트하여 높은 비밀번호 복잡도를 적용할 수 있습니다.

## Password policy

### IAM default

Apply default password requirements.

### Custom

Apply customized password requirements.

#### Password minimum length.

Enforce a minimum length of characters.

8 characters

Needs to be between 6 and 128.

#### Password strength

- Require at least one uppercase letter from the Latin alphabet (A-Z)
- Require at least one lowercase letter from the Latin alphabet (a-z)
- Require at least one number
- Require at least one non-alphanumeric character (! @ # \$ % ^ & \* () \_ + - = [ ] { } | ' )

#### Other requirements

- Turn on password expiration
- Password expiration requires administrator reset
- Allow users to change their own password
- Prevent password reuse

IAM 콘솔 > 계정 설정 > 비밀번호 정책

# 연락처 정보 업데이트

관리자 계정 탈취와 같은 긴급 상황에서 사용자 인증을 위하여 정확한 연락처 정보를 사용해야합니다. 이메일을 회사의 그룹 메일을 활용하여 관리포인트를 분산할 수 있습니다.

The screenshot shows the AWS Billing & Cost Management interface under the 'Account' section. On the left sidebar, there are links for 'Billing and Cost Management', 'Choose billing view', 'Home', 'Getting Started', 'Billing and Payments' (with sub-links for Bills, Payments, Credits, Purchase Orders), 'Cost and Usage Analysis' (with sub-links for Cost Explorer, Cost Explorer Saved Reports, Cost Anomaly Detection), and 'Alternate contacts'. The main content area is titled 'Account Info' and contains two sections: 'Account settings' and 'Contact information'. In 'Account settings', fields include 'Account ID' (2343551), 'Account name' (admin), 'Service provider' (Amazon Web Services Korea LLC), and 'Password' (\*\*\*\*\*). In 'Contact information', fields include 'Full name' (Seongjin hong), 'Company name - optional' (empty), 'Address line 1' (262, Dotjil-ro, empty), 'Phone number' (+82 01), 'Website URL - optional' (empty), 'Address line 2' (empty), and 'Address line 3' (empty).

## Alternate contacts

You can add alternate contacts for Billing, Operations, and Security communications to ensure the correct people are notified for each topic. As a primary account holder, you will continue to receive all email communications. [Learn more](#)

### Billing contact

None

Add

### Operations contact

None

Add

### Security contact

None

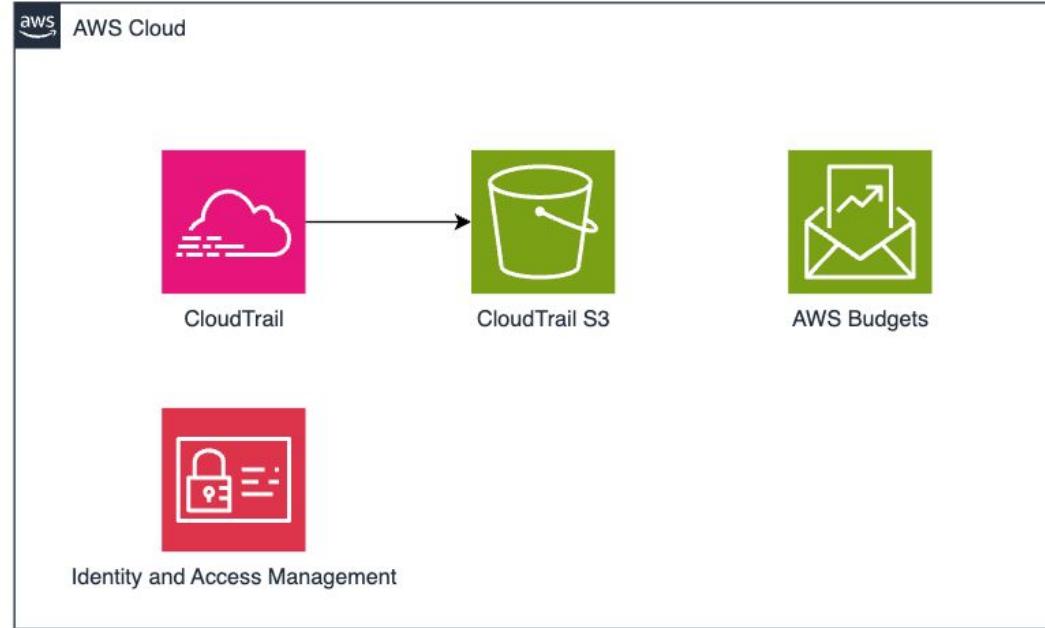
Add

# Root 계정 보안 베스트 프랙티스

root 사용자는 IAM 사용자보다 높은 권한을 가지게 됩니다. 꼭 필요하지 않는 경우 사용을 금지하고 아래의 베스트 프랙티스를 따릅니다.

- MFA 설정
- 관리용 IAM 생성
  - IAM 사용자 MFA 강제 활성
  - 최소권한
- 액세스키 생성 금지
- root 사용자 비밀번호, MFA 관리주체 분리
- root 계정 사용 알림

# 아키텍처 v0.1



- 연락처 업데이트 완료
- 패스워드 정책 업데이트 완료



성진 :

아.. 계정 보안은 우선 이 정도면 충분한 것 같아.  
루트는 내가 관리하고, IAM 유저 정보 전달드려야겠다.

### 3. 인프라 보안



??? :

성진씨 계정 만든거 잘 확인했어요.

이제 저희 회사 서버 서비스 **안전하게 AWS로 옮겨주세요.**

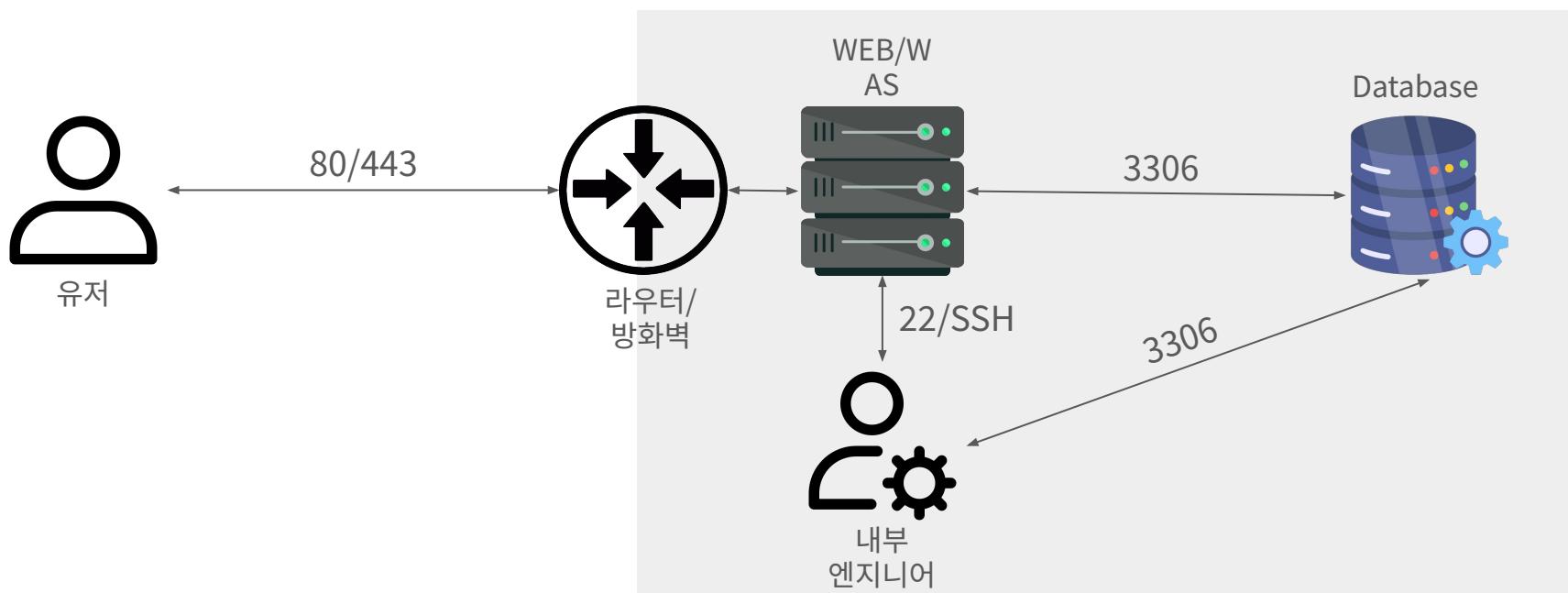


**성진 :**

네? 저 이제 AWS 계정 생성했는데…

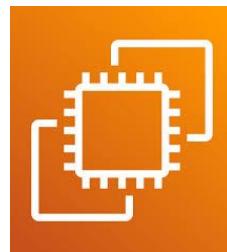
# 기존 현황 및 인프라 구성도

- 스타트업
- 커뮤니티 앱을 운영하는 회사, 간단한 이미지 파일들을 업로드 가능함
- 유저 하루 100명
- 직원수 3명
- 온프레미스 WEB/WAS 서버, Database



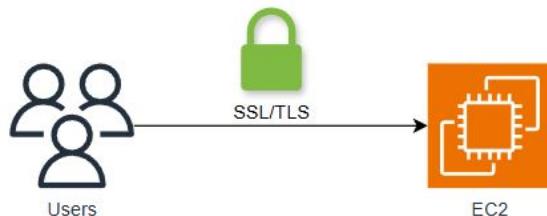
# 여러분들의 선택은..!?

 AWS Cloud

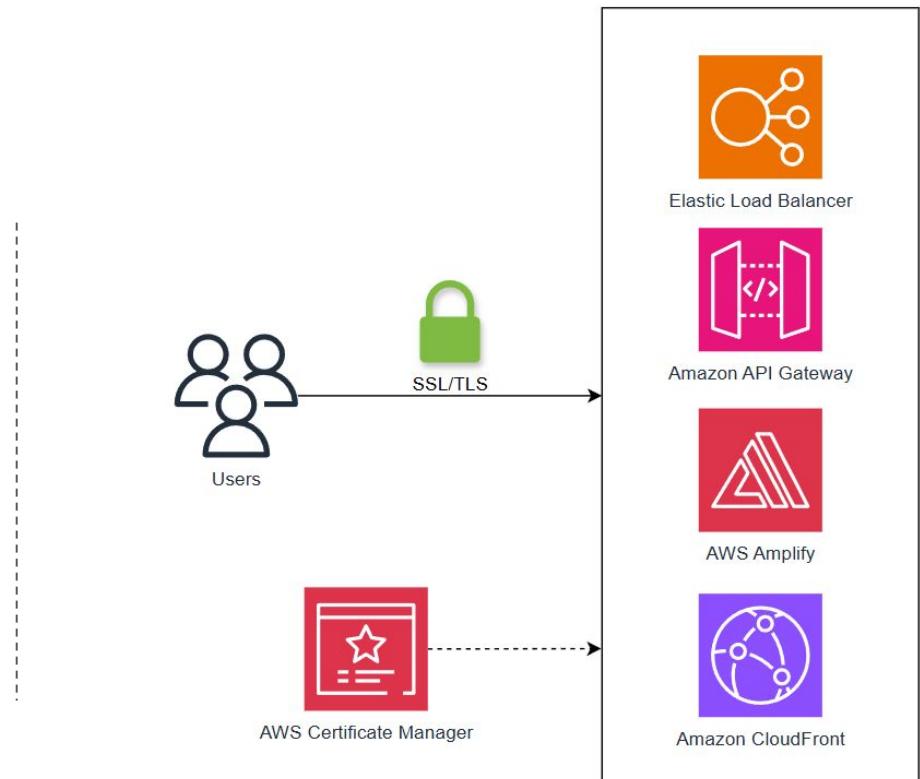


# 네트워크 보안 - 암호화 통신

암호화 통신은 서비스 제공에 필수적이며 각종 법, 컴플라이언스의 요구 조건입니다. 기존의 방식대로 직접 인증서를 유지하는 방법과 AWS에서 제공하는 두 가지 방법 중 하나를 활용할 수 있습니다.

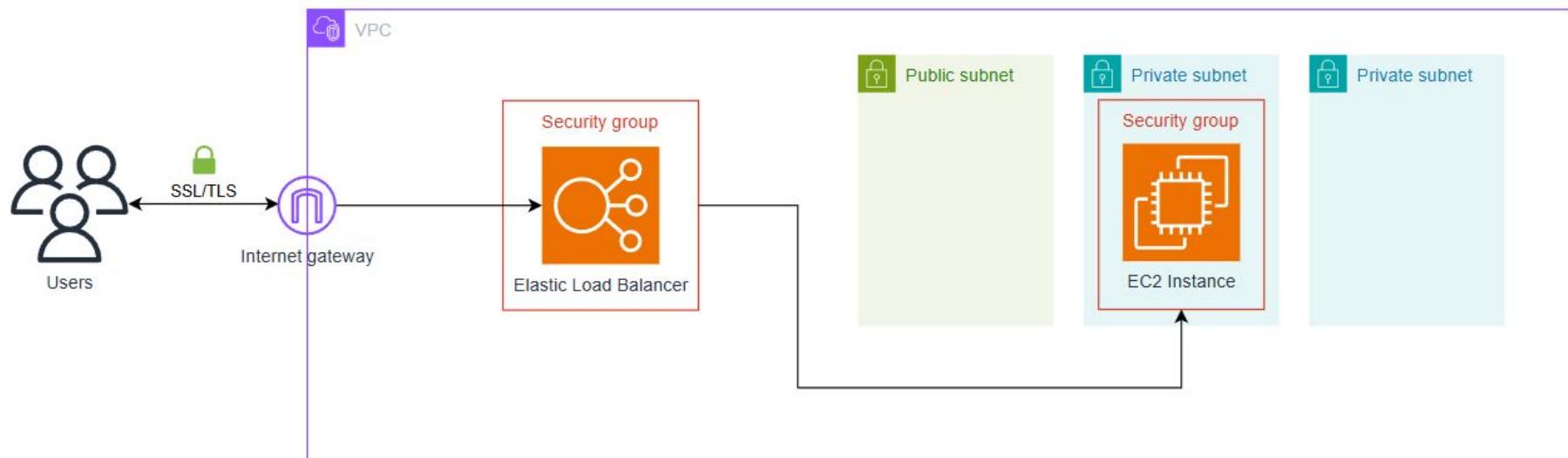


암호화 통신을 위한 인증서 직접관리



AWS가 제공하는 기능을 활용하여 통신  
암호화 제공

# 아키텍처 v0.2 (암호화 통신 적용)



# EC2 서버 접근 제어 - 서버 접근 제어

서버 관리를 위해 서버에 접근할 때 선택할 수 있는 방법 중 하나를 적용합니다.

1. SSH 직접 접속
2. Bastion host
3. EC2 Instance Connect
4. AWS Systems Manager - Session Manager
5. 서드파티 솔루션

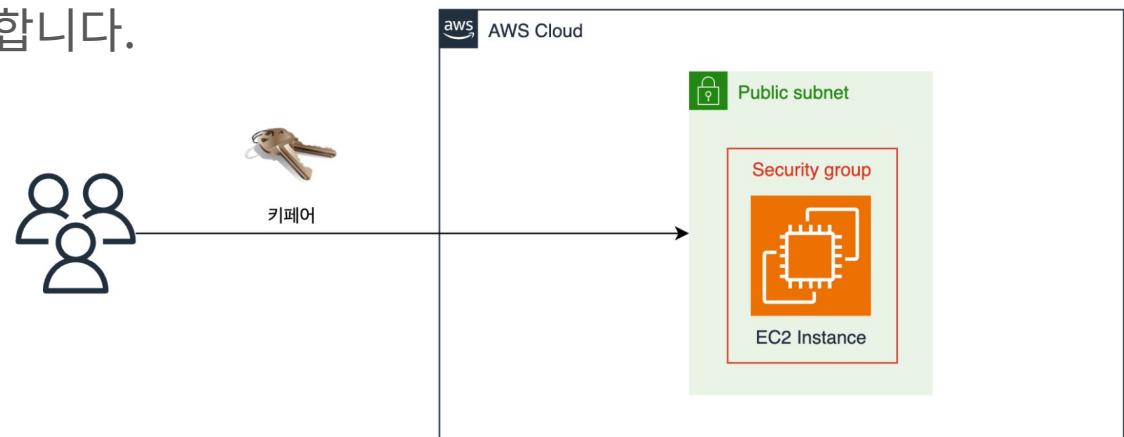
# EC2 서버 접근 제어 - SSH 직접 접속

기존 방식대로 SSH 직접 접속을 하고싶다면 SSH를 통해 직접 접속이 가능합니다.

- 퍼블릭 서브넷에 위치해야합니다.
- 22번 포트로 외부에서 접속이 가능해야 합니다.

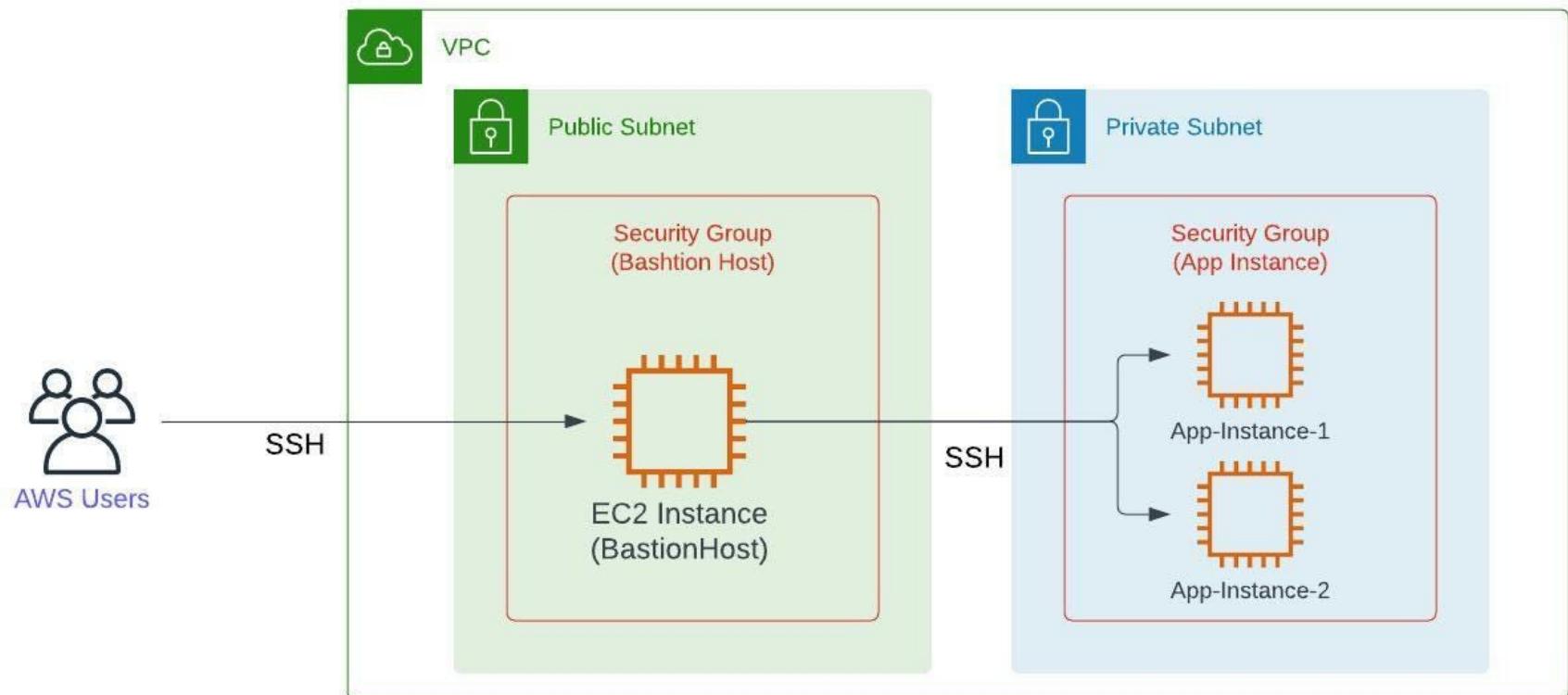
단점

- 외부 공격의 대상이 될 수 있습니다.
- 키페어 관리에 유의해야합니다.



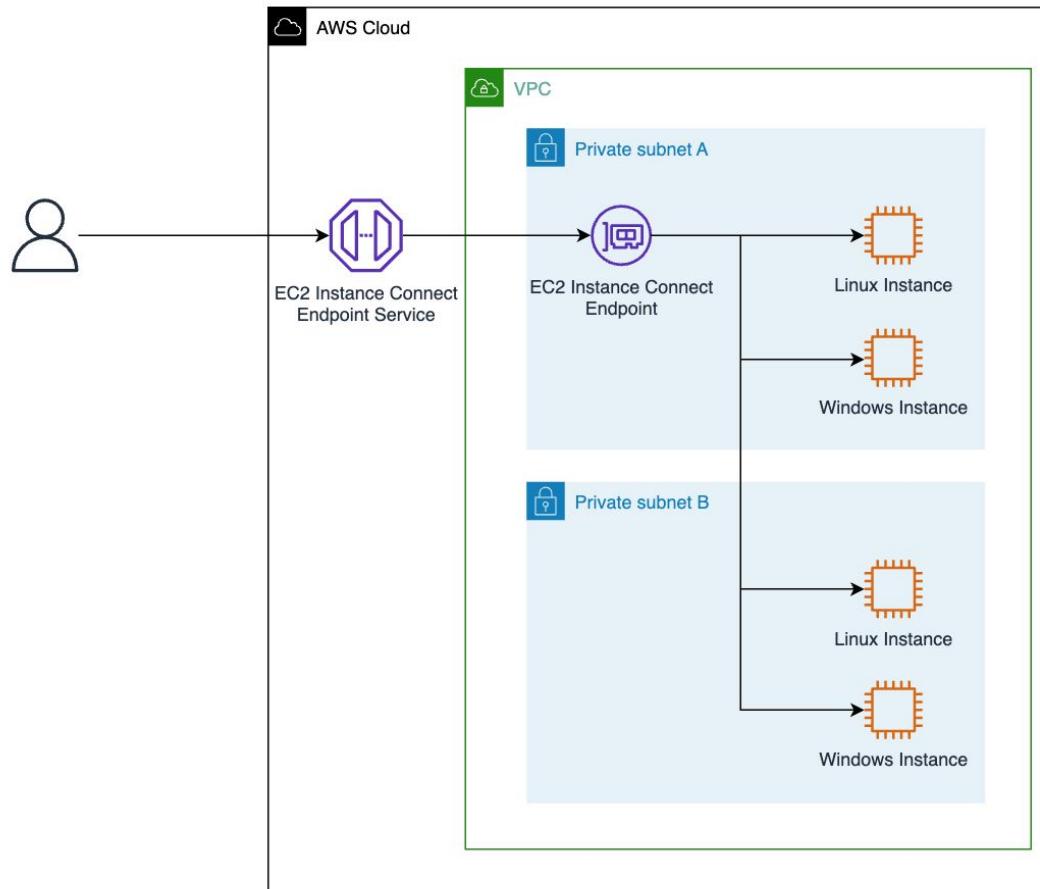
# EC2 서버 접근 제어 - Bastion host

베스천 호스트는 별도의 인스턴스를 두어 서버의 직접적인 노출을 막아 공격 표면을 최소화 시킬 수 있습니다. 여전히 키페어 관리에 유의해야합니다.



# EC2 서버 접근 제어 - EC2 Instance Connect

별도의 키페어를 사용하지 않으나 IAM 권한이 필요합니다. VPC endpoint를 이용해 프라이빗 서브넷에도 접근이 가능합니다.

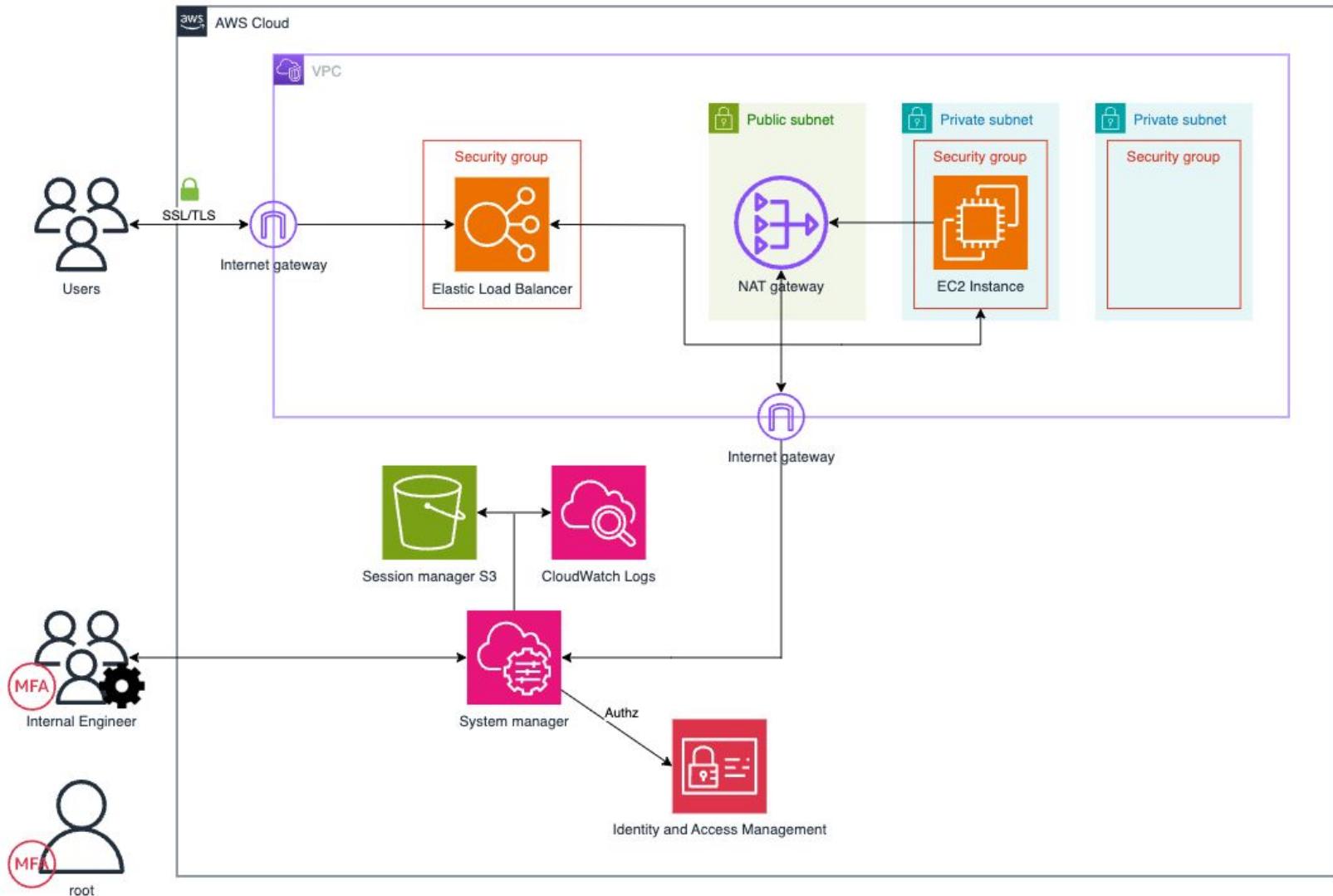


# EC2 서버 접근 제어 - AWS System manager

에이전트 기반의 서버 관리 도구로 SSH를 사용하지 않으며 443 포트를 사용합니다. 서버 명령어 전송, 세션 연결, 세션 로깅 등의 기능을 제공합니다.

- IAM 권한 필요
- VPC 엔드포인트를 이용해 프라이빗 서브넷 접근 가능
- 별도의 에이전트 설치 필요(Amazon linux 기본 탑재)
- CloudWatch, S3 버킷에 세션 로깅 가능

# 아키텍처 v0.3 (서버 접근 제어 적용)



# Amazon Relational Database Service 보안

Amazon Relational Database Service(Amazon RDS)는 AWS 클라우드에서 관계형 데이터베이스를 더 쉽게 설치, 운영 및 확장할 수 있는 서비스입니다.

- 패스워드 관리
- 리소스 암호화
- 네트워크 트래픽 제어
- Audit 로그 활성화

# RDS 보안 - 패스워드 관리

패스워드 관리는 직접 관리와 시크릿 매니저에 저장하는 두 가지 기능을 제공합니다.

▼ Credentials Settings

**Master username** [Info](#)  
Type a login ID for the master user of your DB instance.  
  
1 to 32 alphanumeric characters. The first character must be a letter.

**Credentials management**  
You can use AWS Secrets Manager or manage your master user credentials.

**Managed in AWS Secrets Manager - most secure**  
RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.

**Self managed**  
Create your own password or have RDS create a password that you manage.

**ⓘ** If you manage the master user credentials in AWS Secrets Manager, additional charges apply. See [AWS Secrets Manager pricing](#). Additionally, some RDS features aren't supported. See limitations [here](#).

**Select the encryption key** [Info](#)  
You can encrypt using the KMS key that Secrets Manager creates or a customer managed KMS key that you create.  
    
[Add new key](#)

# RDS 보안 - 패스워드 관리 (시크릿 매니저)

AWS Secrets Manager 시크릿 정보를 저장하는 서비스로 수명 주기 동안 자격 증명 등을 손쉽게 교체, 관리 및 검색할 수 있습니다.

The screenshot shows the AWS Secrets Manager console interface. At the top, there's a header bar with the title "Resource Groups & Tag Editor". Below the header, a table displays the following information:

aws:secretsmanager:owningService	rds
Name	smdemo-db

Below the table, there are two main sections:

- Secret value**: Contains a link "Info" and a button labeled "Retrieve secret value" with a cursor icon pointing to it.
- Rotation configuration**: Contains a link "Info", a "Rotate secret immediately" button, and an "Edit rotation" button.

Under the "Rotation configuration" section, there are three settings:

- Rotation status: A checked checkbox labeled "Enabled".
- Rotation schedule: A dropdown menu showing "7 days".
- Next rotation date (UTC): A text field showing "Fri, March 24, 2023 at 23:59:59 UTC".

# RDS 보안 - 리소스 암호화

RDS에서는 디스크 전체를 암호화하는 기능을 제공합니다. 업계 표준 AES-256 암호화 알고리즘을 사용하여 성능 저하를 최소화 합니다.

The screenshot shows the 'Create database' configuration page in the AWS RDS console. The 'Encryption' section is highlighted with a red box. It contains the 'Enable encryption' checkbox, which is checked, and a note: 'Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console.' Below this is the 'AWS KMS key' dropdown, which currently shows '(default) aws/rds'. Other sections visible include 'Failover priority' (set to 'No preference'), 'Backup' (with retention set to 1 day), and 'Aurora MySQL-Compatible Edition' information on the right.

☰ RDS > Create database

Failover priority

No preference

Backup

Backup retention period [Info](#)

The number of days (1-35) for which automatic backups are kept.

1 day

Copy tags to snapshots

Encryption

Enable encryption

Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. [Info](#)

AWS KMS key [Info](#)

(default) aws/rds

Aurora MySQL-Compatible Edition

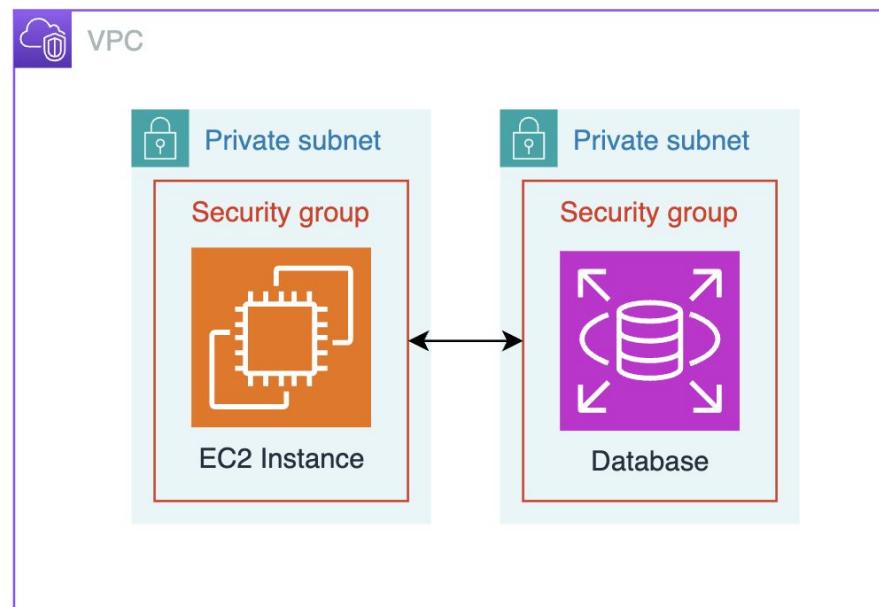
Aurora MySQL is Amazon's enterprise-class MySQL-compatible database.

Aurora MySQL offers:

- Up to five times the throughput of MySQL Community Edition
- Up to 128 TB of autoscaling SSD storage
- Six-way replication across three Availability Zones
- Up to 15 read replicas with replica lag under 10-ms
- Automatic monitoring with failover

# RDS 보안 - 네트워크 트래픽 제어

RDS에는 주로 프라이빗 서브넷에 위치해야 하며, 필요한 소스로 부터만 트래픽을 받아야 합니다.



# RDS 보안 - Audit log 활성화

Audit log를 활성화하여 서버에서 발생한 쿼리들을 조회 할 수 있습니다.

## OS metrics granularity

60 seconds

## Monitoring role for OS metrics

default

Clicking "Create database" will authorize RDS to create the IAM role rds-monitoring-role

## Log exports

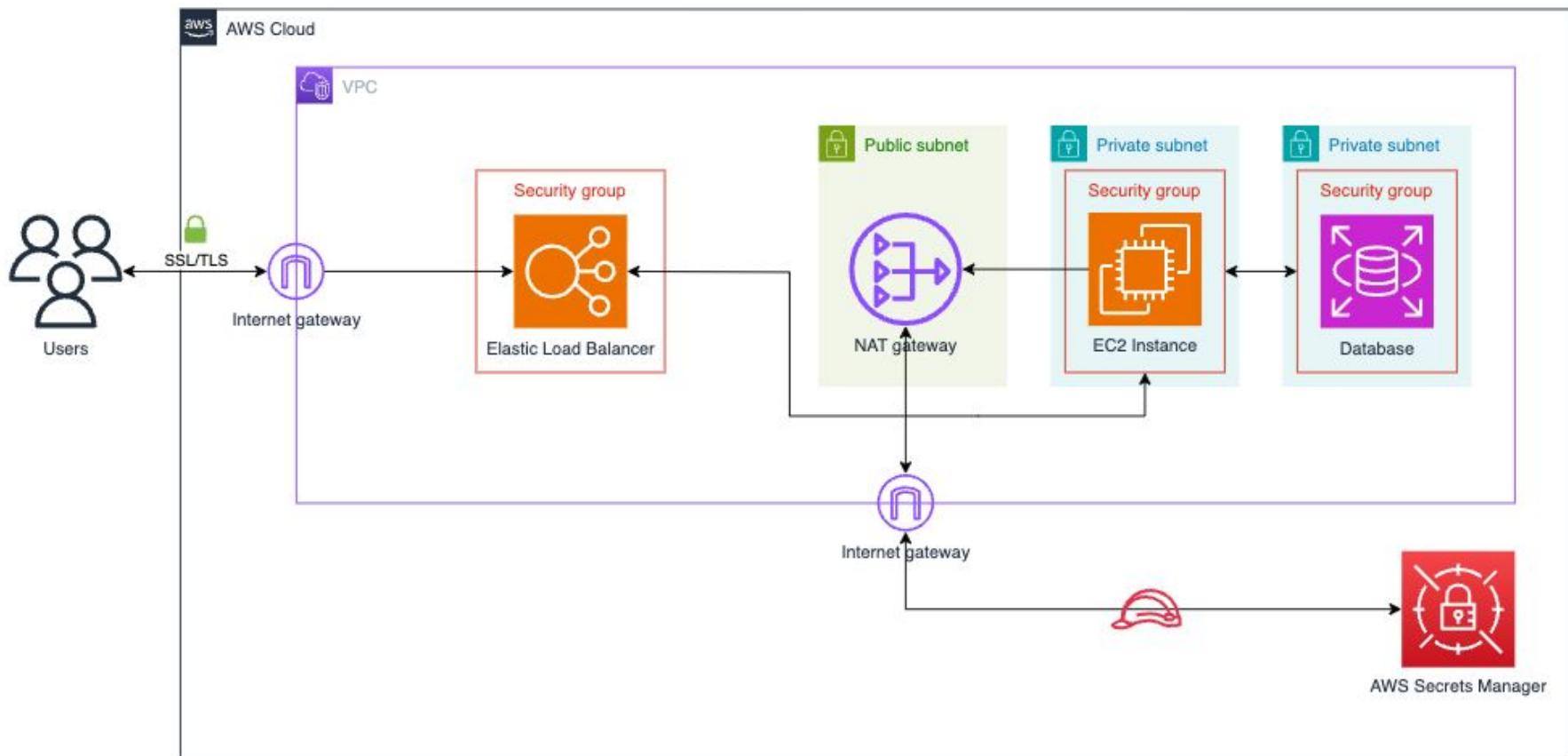
Select the log types to publish to Amazon CloudWatch Logs

- Audit log
- Error log
- General log
- iam-db-auth-error log
- Slow query log

## Viewing Log: audit/server\_audit.log (109.6 kB)

```
text: [background: ]  
----- END OF LOG -----  
20201117 16:03:24,ip=10-1-3-36,root,172.31.24.28,5823,803172,QUERY,, 'select @@version_comment limit 1',0  
20201117 16:04:20,ip=10-1-3-36,root,172.31.24.28,5823,803404,QUERY,, 'SELECT DATABASE()',0  
20201117 16:04:20,ip=10-1-3-36,root,172.31.24.28,5823,803406,QUERY,audit_log,'show databases',0  
20201117 16:04:20,ip=10-1-3-36,root,172.31.24.28,5823,803407,QUERY,audit_log,'show tables',0  
20201117 16:04:26,ip=10-1-3-36,root,172.31.24.28,5823,803415,QUERY,audit_log,'CREATE TABLE IF NOT EXISTS auditlogtab (id varchar(52),name varchar(100))',0  
20201117 16:04:30,ip=10-1-3-36,root,172.31.24.28,5823,803428,QUERY,audit_log,'SELECT count(*) FROM auditlogtab',0  
20201117 16:04:35,ip=10-1-3-36,root,172.31.24.28,5823,803434,QUERY,audit_log,'create view v_auditlogtab as SELECT count(*) from auditlogtab',0  
20201117 16:04:39,ip=10-1-3-36,root,172.31.24.28,5823,803454,QUERY,audit_log,'select * from v_auditlogtab',0  
20201117 16:04:42,ip=10-1-3-36,root,172.31.24.28,5823,803469,QUERY,audit_log,'TRUNCATE TABLE auditlogtab',0  
20201117 16:04:47,ip=10-1-3-36,root,172.31.24.28,5823,803484,QUERY,audit_log,'INSERT INTO auditlogtab (id,name) VALUES ('112','AUDIT TRAIL')',0  
20201117 16:04:51,ip=10-1-3-36,root,172.31.24.28,5823,803489,QUERY,audit_log,'UPDATE auditlogtab SET name = ''AUDIT TRAIL TEST'' WHERE id = ''112''',0  
20201117 16:04:55,ip=10-1-3-36,root,172.31.24.28,5823,803494,QUERY,audit_log,'CREATE USER ''auditloguser''@'%' IDENTIFIED WITH 'mysql_native_password' AS ''E3D0F9330BD02A321A202S96C20A79P06C8790801'',0  
20201117 16:04:59,ip=10-1-3-36,root,172.31.24.28,5823,803500,QUERY,audit_log,'DROP USER auditloguser',0  
20201117 16:05:03,ip=10-1-3-36,root,172.31.24.28,5823,803526,QUERY,audit_log,'DROP TABLE auditlogtab',0  
20201117 16:05:07,ip=10-1-3-36,root,172.31.24.28,5823,803532,QUERY,audit_log,'DROP DATABASE audit_log',0  
20201117 16:05:07,ip=10-1-3-36,root,172.31.24.28,5823,803533,QUERY,audit_log,'SELECT DATABASE()',0  
20201117 16:05:12,ip=10-1-3-36,root,172.31.24.28,5823,0,DISCONNECT,,0
```

# 아키텍처 v0.4 (데이터 베이스)



# S3(Simple Storage Service) 보안

Amazon S3(Simple Storage Service) 확장성, 데이터 가용성, 보안 및 성능을 제공하는 객체 스토리지 서비스입니다. 버킷 정책과 객체의 ACL을 통해 버킷 및 객체의 개별적인 보안설정을 할 수 있습니다.

- 객체 암호화 (디폴트)
- 퍼블릭 액세스 차단
- 파일 공유 필요시 서명 URL 사용

Amazon S3 > 버킷 > public-test-922 > 퍼블릭 액세스 차단 편집(버킷 설정)

## 퍼블릭 액세스 차단 편집(버킷 설정) 정보

### 퍼블릭 액세스 차단(버킷 설정)

퍼블릭 액세스는 ACL(액세스 제어 목록), 버킷 정책, 액세스 지점 정책 또는 모두를 통해 버킷 및 객체에 부여됩니다. 모든 S3 버킷 및 객체에 대한 퍼블릭 액세스가 차단되었거나 확인하려면 [모든 퍼블릭 액세스 차단]을 활성화합니다. 이 설정은 이 버킷 및 해당 액세스 지점에만 적용됩니다. AWS에서는 [모든 퍼블릭 액세스 차단]을 활성화하도록 권장하지만, 이 설정을 적용하기 전에 퍼블릭 액세스가 없어도 애플리케이션이 올바르게 작동하는지 확인합니다. 버킷 또는 내부 객체에 어느 정도 수준의 퍼블릭 액세스가 필요한 경우 특정 스토리지 사용 사례에 맞게 아래 개별 설정을 사용자 지정할 수 있습니다. [자세히 알아보기](#)

#### 모든 퍼블릭 액세스 차단

이 설정을 활성화하면 아래 4개의 설정을 모두 활성화한 것과 같습니다. 다음 설정 각각은 서로 독립적입니다.

#### 새 ACL(액세스 제어 목록)을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단

S3은 새로 추가된 버킷 또는 객체에 적용되는 퍼블릭 액세스 권한을 차단하여, 기존 버킷 및 객체에 대한 새 퍼블릭 액세스 ACL 생성을 금지합니다. 이 설정은 ACL을 사용하여 S3 리소스에 대한 퍼블릭 액세스를 허용하는 기존 권한을 변경하지 않습니다.

#### 임의의 ACL(액세스 제어 목록)을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단

S3은 버킷 및 객체에 대한 퍼블릭 액세스를 부여하는 모든 ACL을 무시합니다.

#### 새 퍼블릭 버킷 또는 액세스 지점 정책을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단

S3은 버킷 및 객체에 대한 퍼블릭 액세스를 부여하는 새 버킷 및 액세스 지점 정책을 차단합니다. 이 설정은 S3 리소스에 대한 퍼블릭 액세스를 허용하는 기존 정책을 변경하지 않습니다.

#### 임의의 퍼블릭 버킷 또는 액세스 지점 정책을 통해 부여된 버킷 및 객체에 대한 퍼블릭 및 교차 계정 액세스 차단

S3은 버킷 및 객체에 대한 퍼블릭 액세스를 부여하는 정책을 사용하는 버킷 또는 액세스 지점에 대한 퍼블릭 및 교차 계정 액세스를 무시합니다.

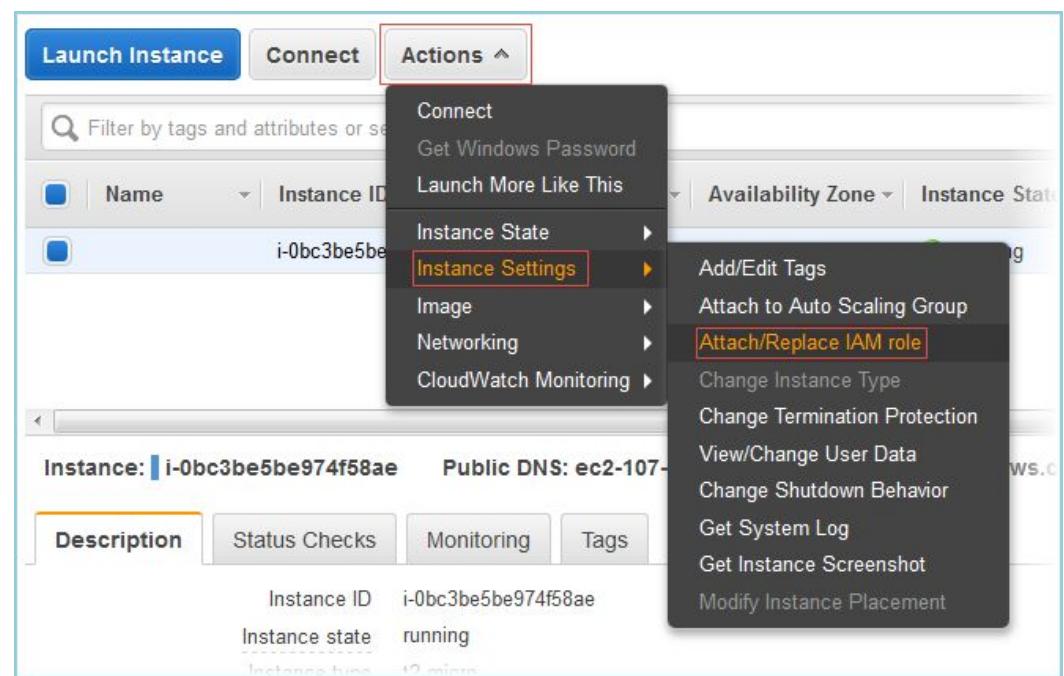
취소

변경 사항 저장

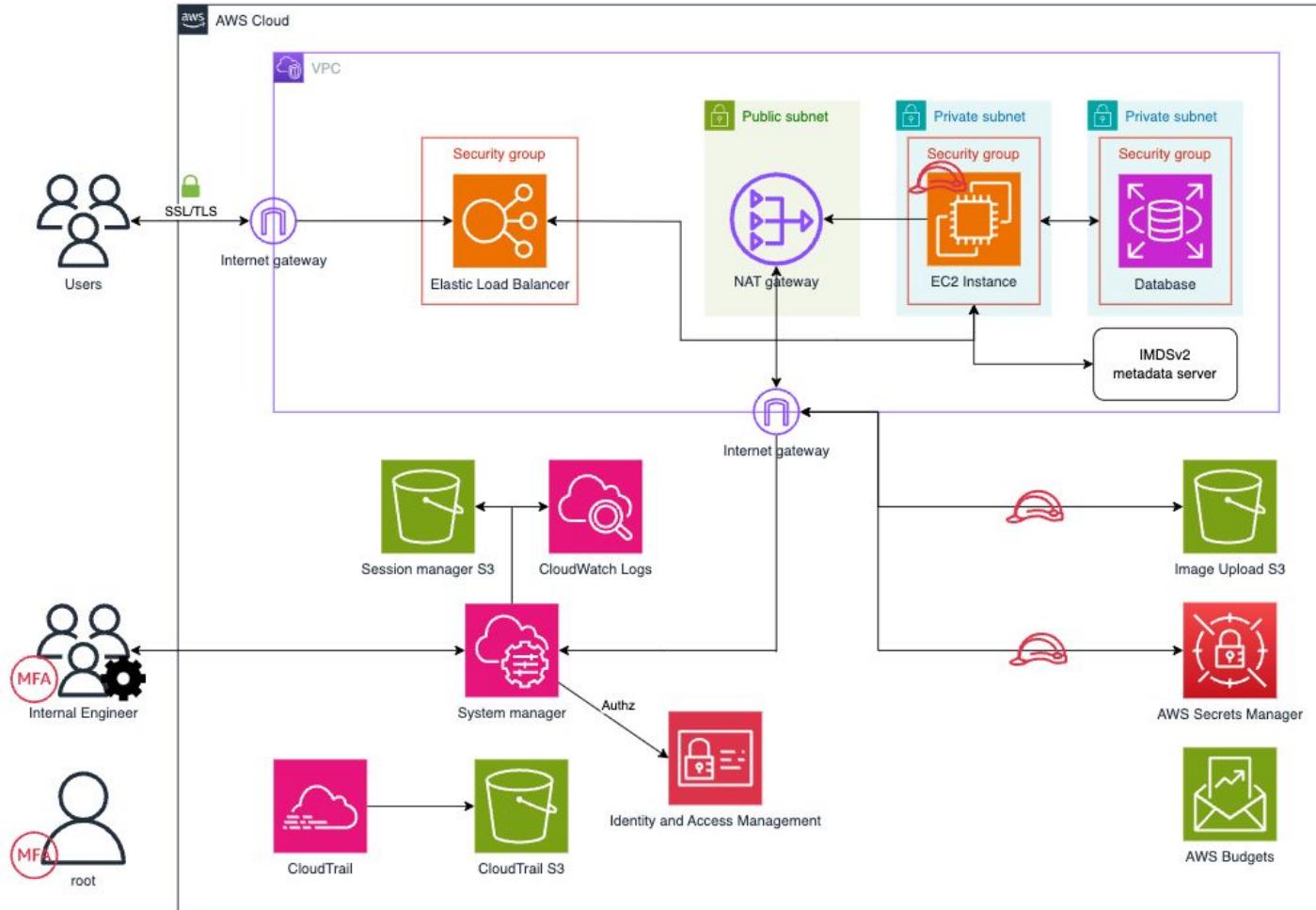
# EC2 IAM role 부여

EC2에서 아마존 서비스에 접근하기 위해서 권한을 부여받기 위해 IAM role을 부여해야합니다.

- Access key 사용 금지
- 최소 권한 원칙
  - AWS IAM Access Analyzer



# 최종 인프라 구성도 v1.0



# 보안 모범 사례 영역

- 클라우드 보안 이해
- 계정 및 접근 권한 관리
- 인프라 보호
- 데이터 보호
- 탐지
- 인시던트 대응



성진 :

우선 이정도면 오늘은 퇴근해도 되겠지…?



성진 :

우선 이정도면 오늘은 퇴근해도 되겠지…?



??? :

성진씨! 잠시 제 자리로 와주시겠어요?



Thank you!

# Q & A

# 참고자료

Applying the AWS Shared Responsibility Model to your GxP Solution  
<https://aws.amazon.com/ko/blogs/industries/applying-the-aws-shared-responsibility-model-to-your-gxp-solution/>

AWS 사용자 필수 기초 보안 가이드 및 서비스 소개  
<https://www.youtube.com/watch?v=c3bRdLXQhxA>

CSA top 10 threats to cloud computing-2024

<https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024>

아이콘 출처

<https://www.flaticon.com/> Freepik, Royyan Wijaya, zafdesign, Ranah Pixel Studio, Roundicons, Vectorslab

AWS 계정에 대한 루트 사용자 모범 사례

[https://docs.aws.amazon.com/ko\\_kr/IAM/latest/UserGuide/root-user-best-practices.html#ru-bp-multi](https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/root-user-best-practices.html#ru-bp-multi)