AWS Security 101:

함께 만들어봐요. 안전한 서비스

1화

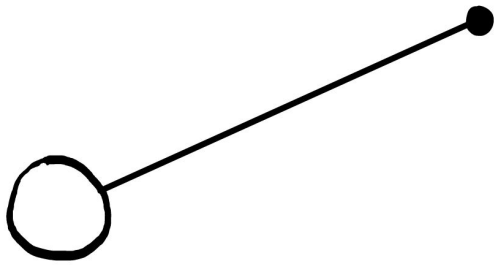
홍성진

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 …



??? :

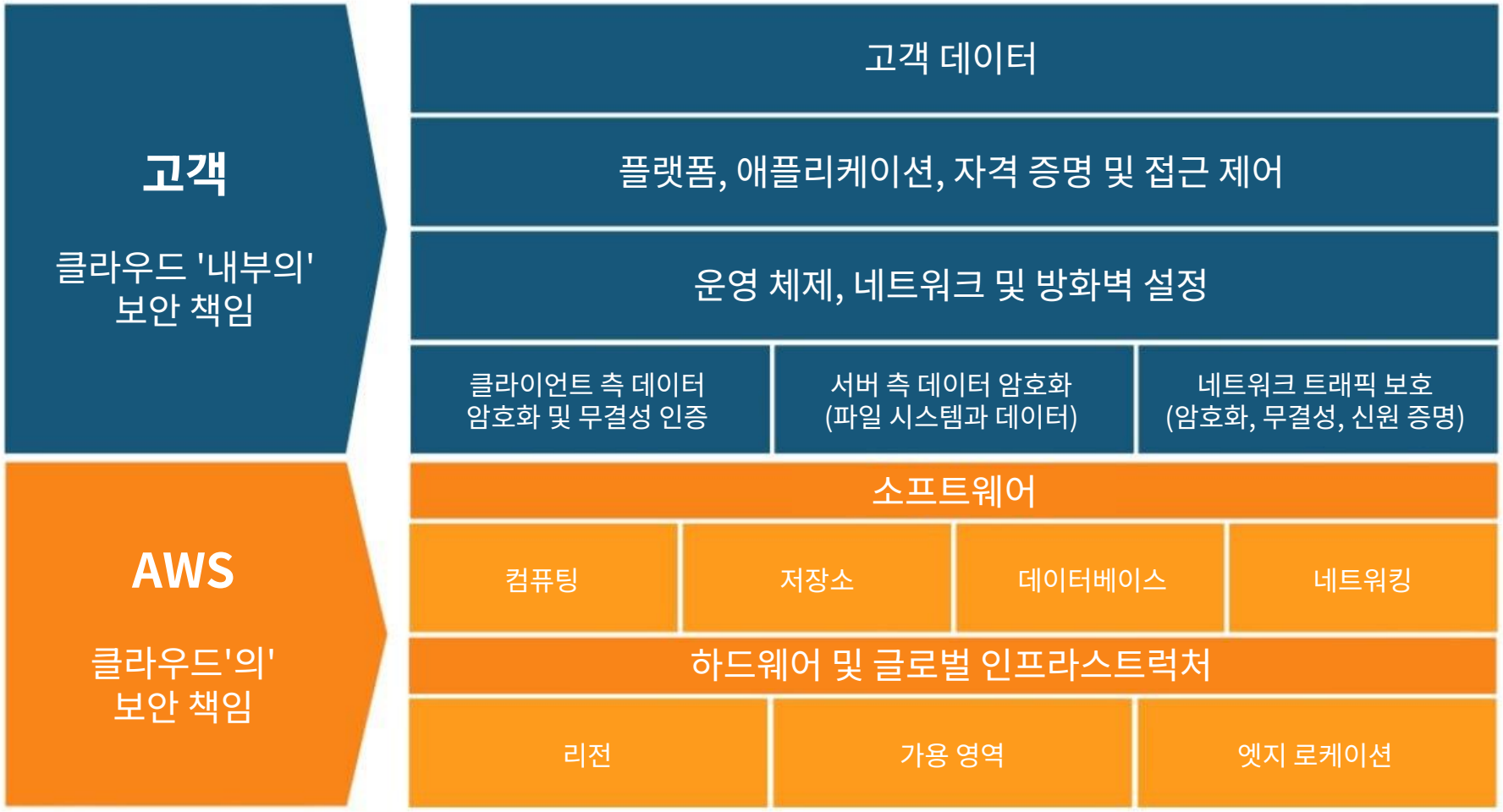
성진 씨 우리 기존 서비스 AWS에 올릴거예요.
내일까지 AWS 계정 만들어서 **안전**하게 설정 해주세요!

성진 :

네? 저 AWS 안 써봤는데요?

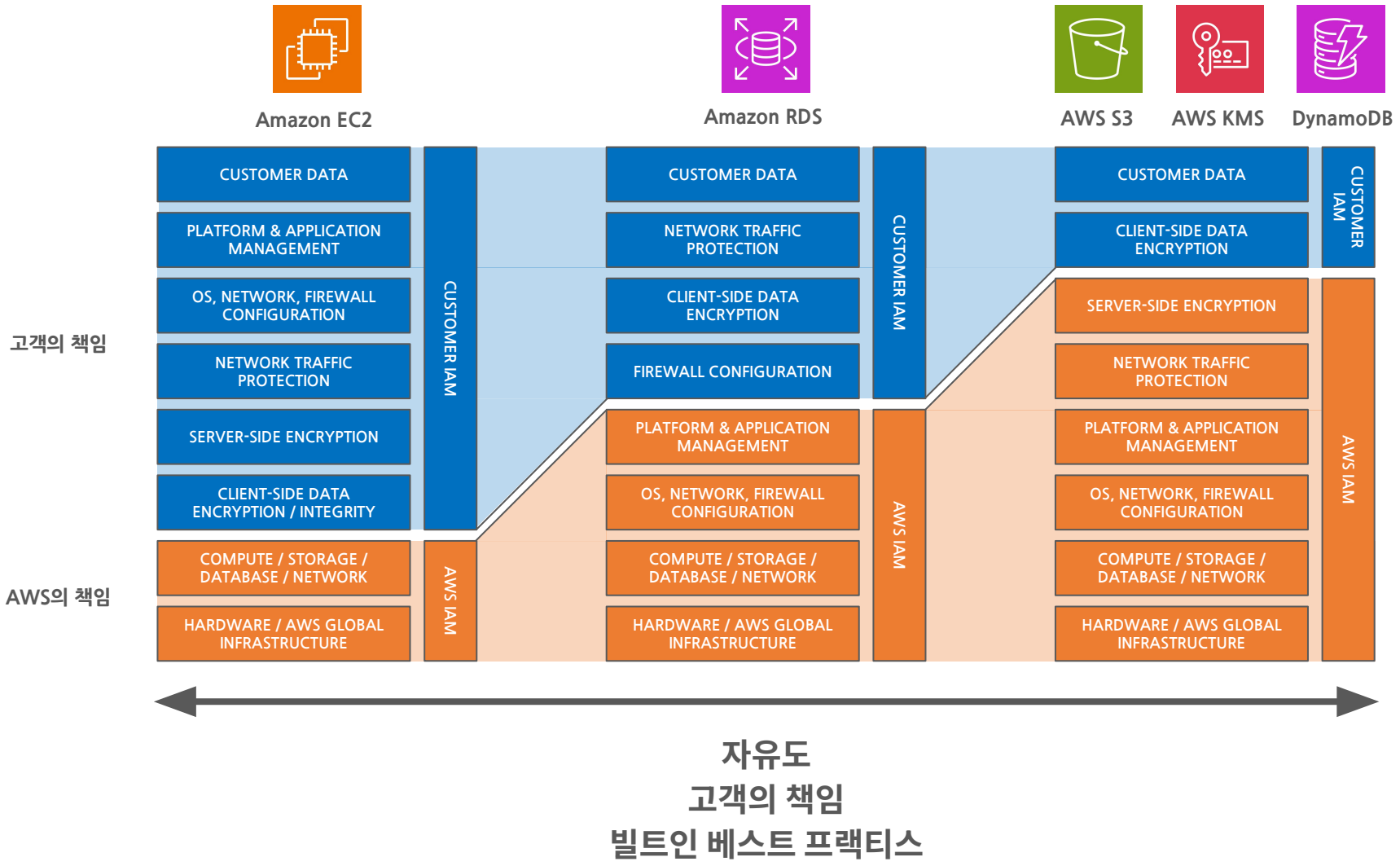
1. 클라우드 보안의 이해

공동 책임 모델


고객
클라우드 '내부의'
보안 책임
고객 데이터
플랫폼, 애플리케이션, 자격 증명 및 접근 제어
운영 체제, 네트워크 및 방화벽 설정
클라이언트 측 데이터
암호화 및 무결성 인증
서버 측 데이터 암호화
(파일 시스템과 데이터)
네트워크 트래픽 보호
(암호화, 무결성, 신원 증명)
AWS
클라우드'의'
보안 책임
소프트웨어
컴퓨팅
저장소
데이터베이스
네트워킹
하드웨어 및 글로벌 인프라스트럭처
리전
가용 영역
엣지 로케이션

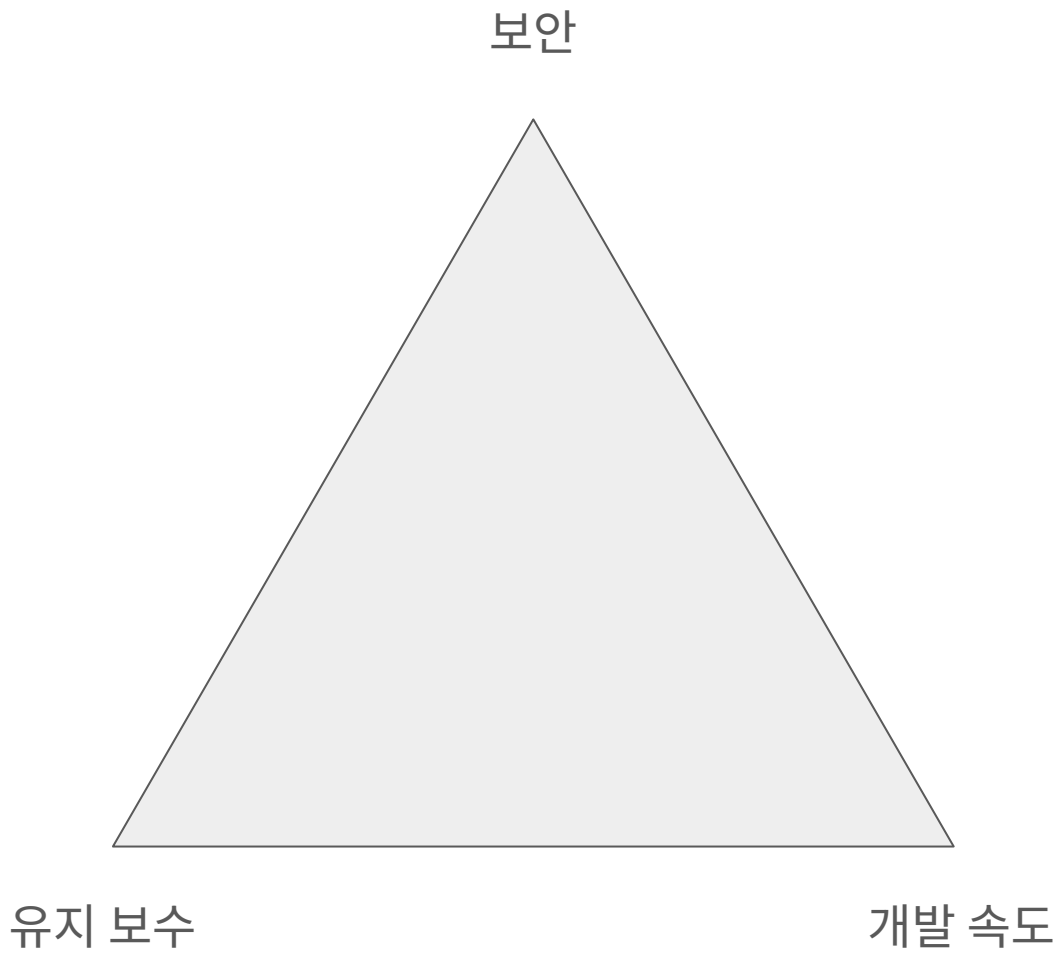

어떻게 길거리로
나오시게 되셨나요?
도박? 마약?
EC2 서버를 실수로
안 껐어요…

공유 책임 모델 - 서비스 별 차이



Misconfiguration

보안 딜레마



우리가 점을 하나 찍는다면 어디다 둬야 하는가…

2. 계정 및 접근 권한 관리

성진 :

AWS 계정을 만들라고 하니까 우선 만들어보자!

Language
English

aws

Explore Free Tier products with a new AWS account.

To learn more, visit 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?

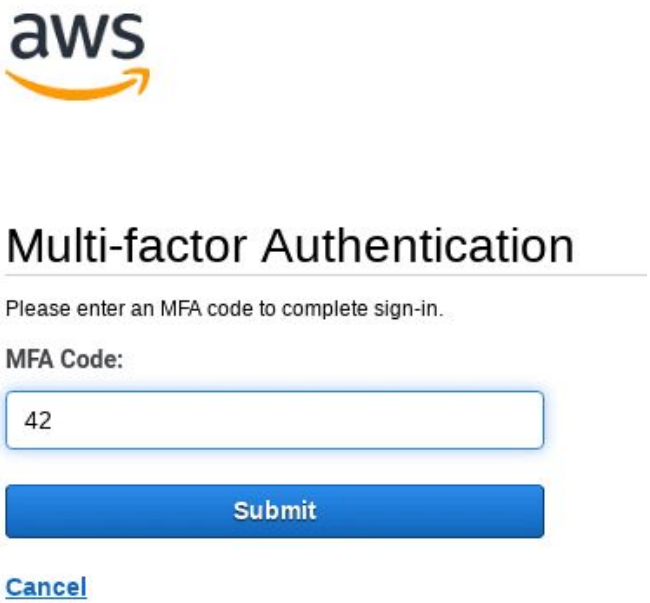
성진 :

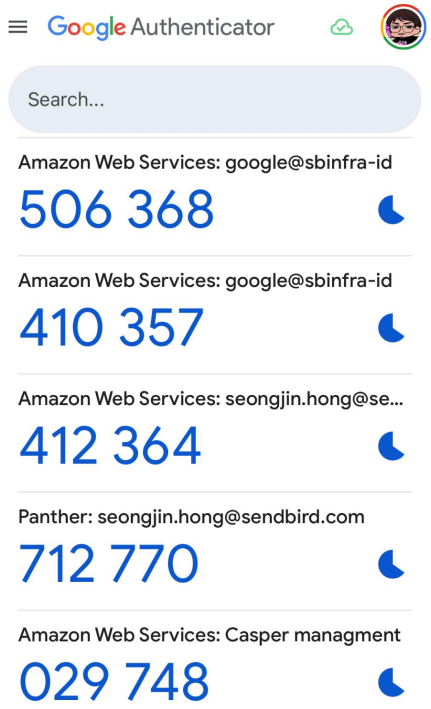
아.. AWS 계정은 만들었고 이제 뭐해야하지?

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.





Multi Factor Authentication - 지원 장치

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

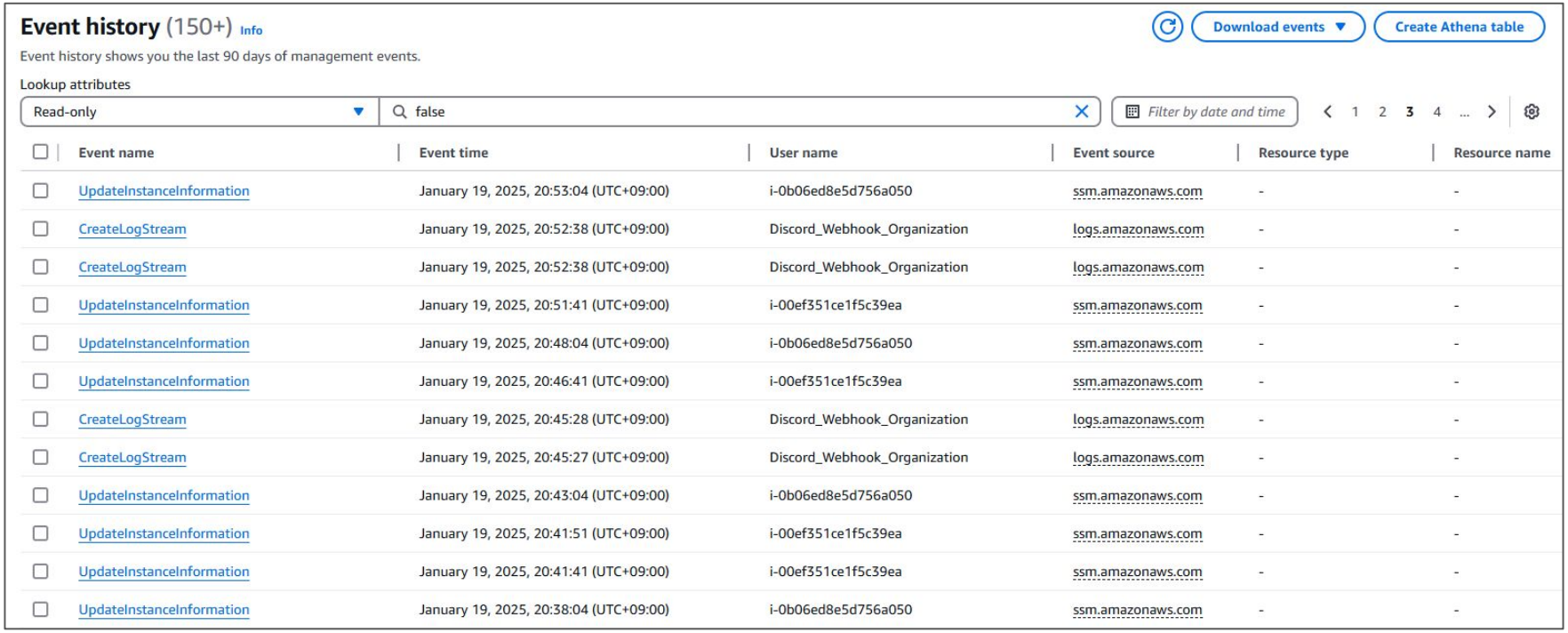
오른쪽 상단 메뉴 > 내 보안 자격 증명

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+) Info

Event history shows you the last 90 days of management events.

Download events | Create Athena table

Lookup attributes

Read-only | false | Filter by date and time | 1 2 3 4 ... |

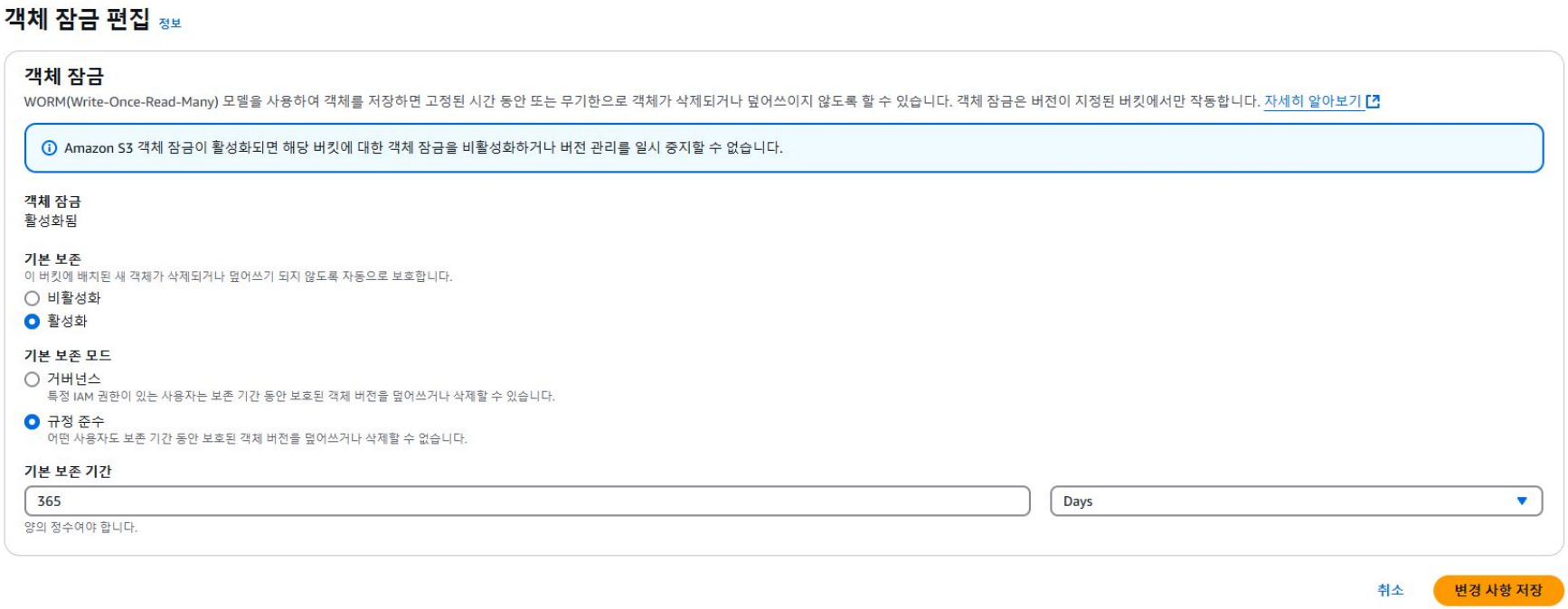
Event name	Event time	User name	Event source	Resource type	Resource name
UpdateInstanceInformation	January 19, 2025, 20:53:04 (UTC+09:00)	i-0b06ed8e5d756a050	ssm.amazonaws.com	-	-
CreateLogStream	January 19, 2025, 20:52:38 (UTC+09:00)	Discord_Webhook_Organization	logs.amazonaws.com	-	-
CreateLogStream	January 19, 2025, 20:52:38 (UTC+09:00)	Discord_Webhook_Organization	logs.amazonaws.com	-	-
UpdateInstanceInformation	January 19, 2025, 20:51:41 (UTC+09:00)	i-00ef351ce1f5c39ea	ssm.amazonaws.com	-	-
UpdateInstanceInformation	January 19, 2025, 20:48:04 (UTC+09:00)	i-0b06ed8e5d756a050	ssm.amazonaws.com	-	-
UpdateInstanceInformation	January 19, 2025, 20:46:41 (UTC+09:00)	i-00ef351ce1f5c39ea	ssm.amazonaws.com	-	-
CreateLogStream	January 19, 2025, 20:45:28 (UTC+09:00)	Discord_Webhook_Organization	logs.amazonaws.com	-	-
CreateLogStream	January 19, 2025, 20:45:27 (UTC+09:00)	Discord_Webhook_Organization	logs.amazonaws.com	-	-
UpdateInstanceInformation	January 19, 2025, 20:43:04 (UTC+09:00)	i-0b06ed8e5d756a050	ssm.amazonaws.com	-	-
UpdateInstanceInformation	January 19, 2025, 20:41:51 (UTC+09:00)	i-00ef351ce1f5c39ea	ssm.amazonaws.com	-	-
UpdateInstanceInformation	January 19, 2025, 20:41:41 (UTC+09:00)	i-00ef351ce1f5c39ea	ssm.amazonaws.com	-	-
UpdateInstanceInformation	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.

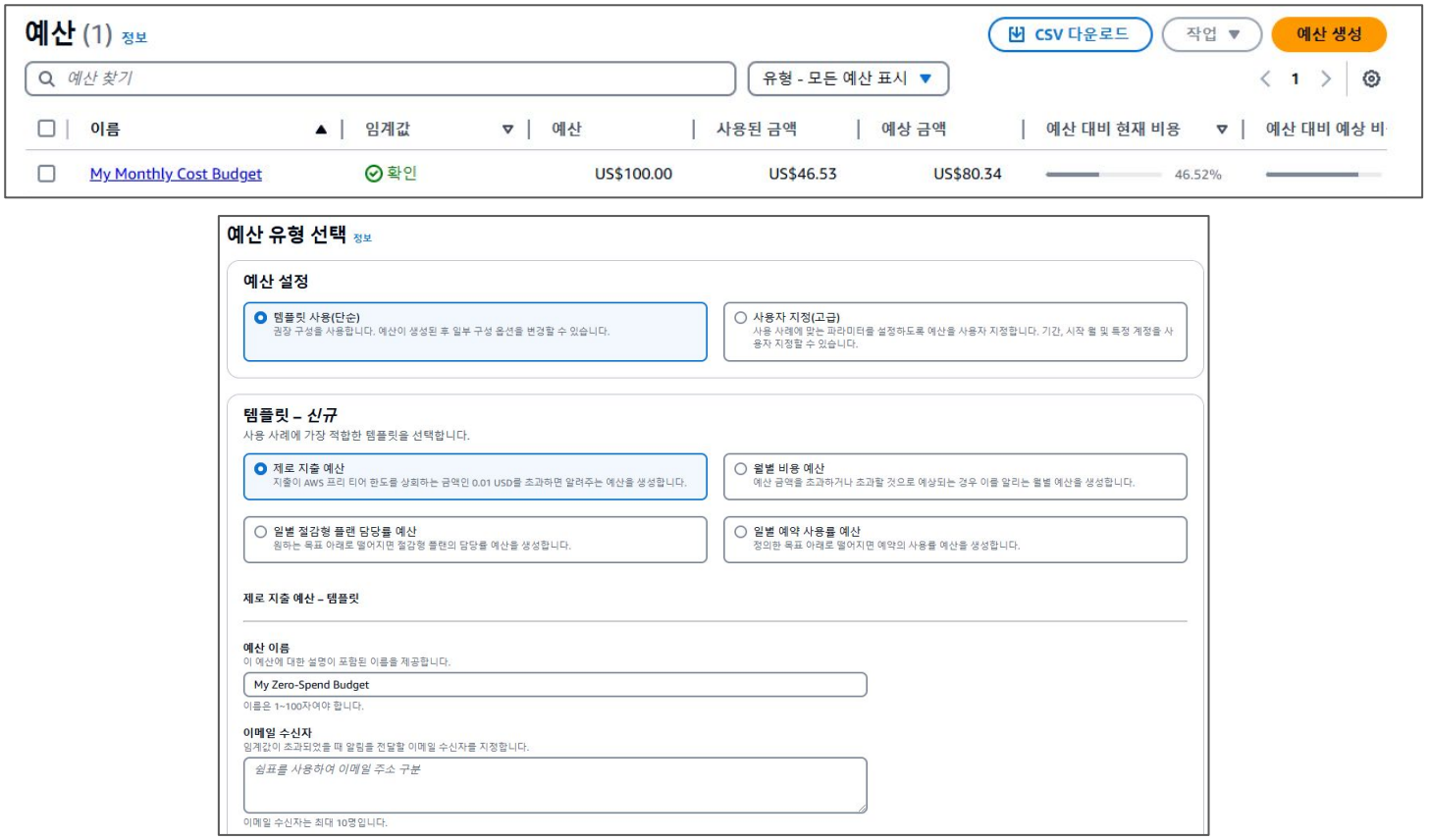
CloudTrail - 추가 보관 객체 잠금 설정

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



예산 설정

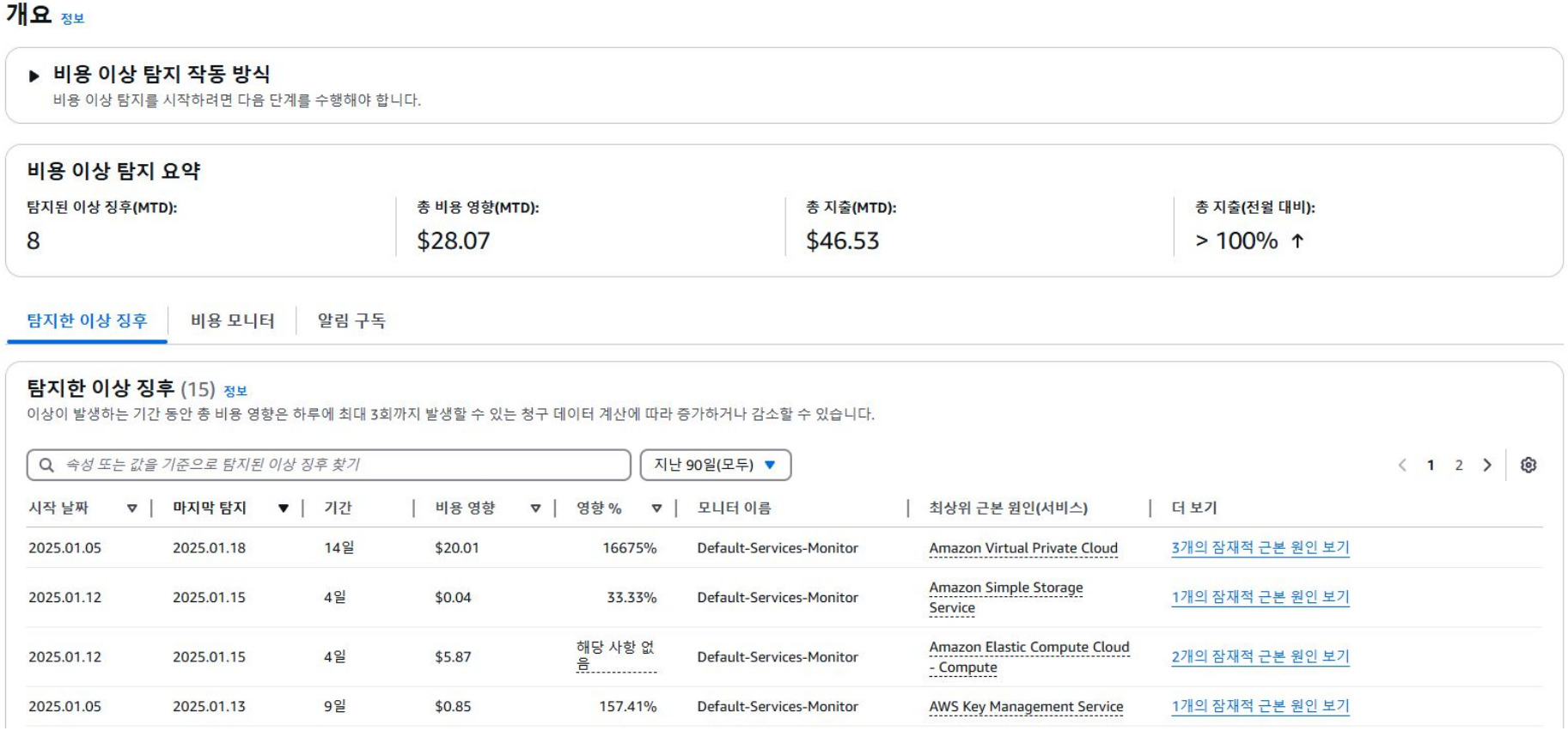
예상외의 금액이 지출되지 않도록 예산 리포트를 생성합니다. 이는 비이상적인 행위 탐지에도 활용 될 수 있습니다.



결제 및 비용 관리 > 예산

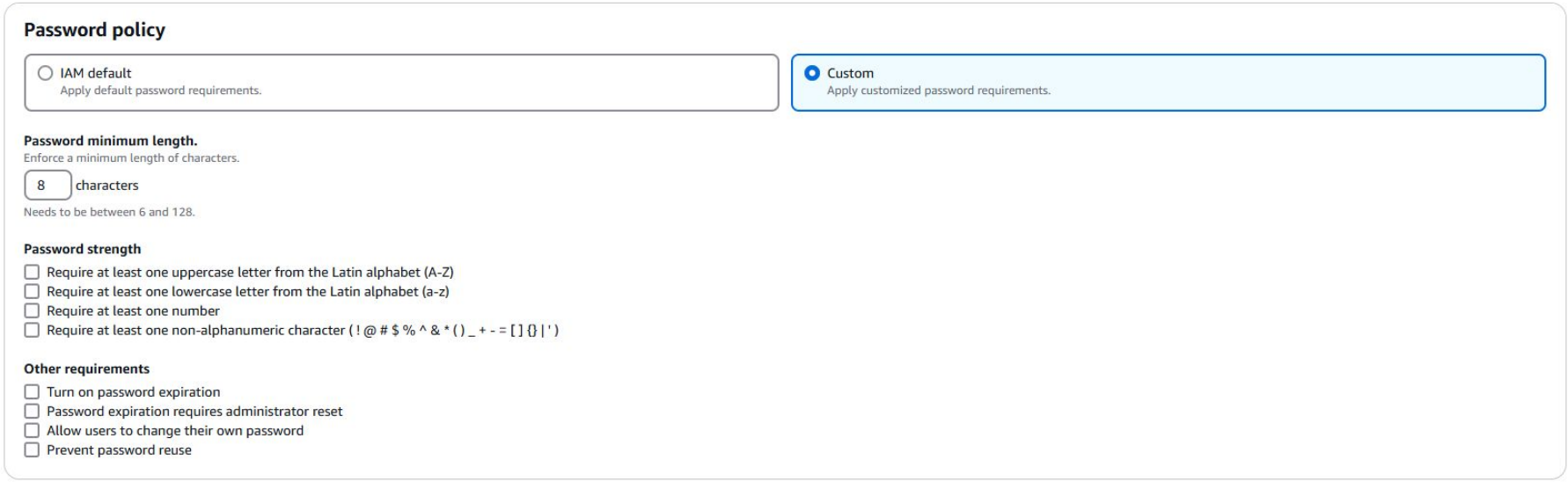
비용 이상 징후 탐지

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



패스워드 정책 변경

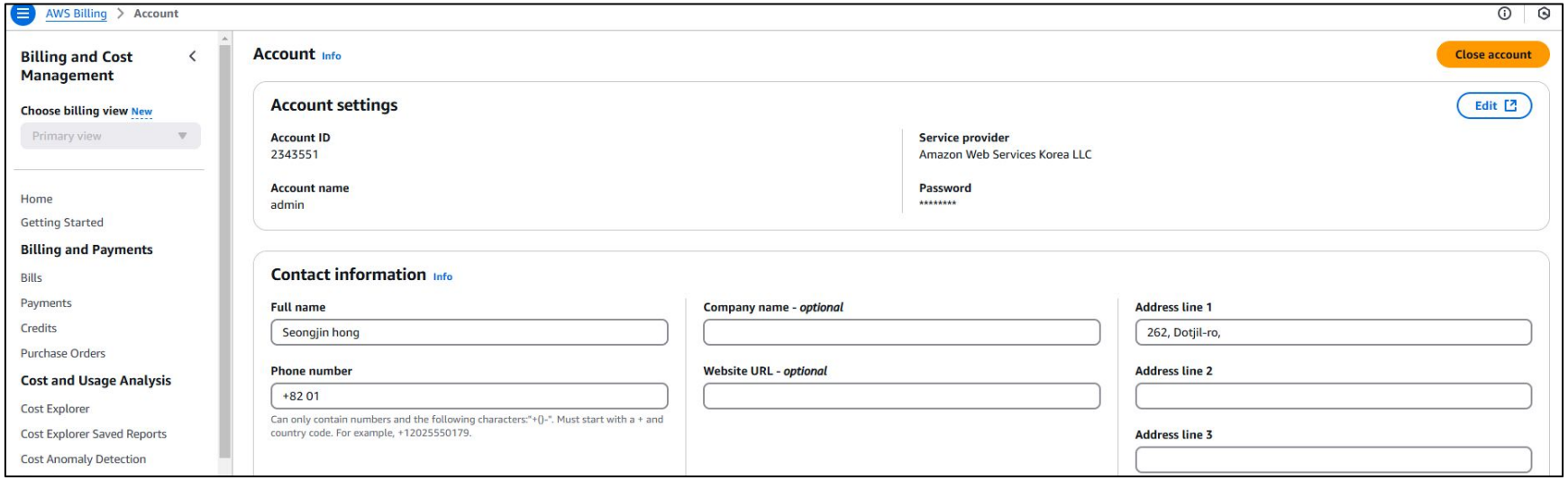
기본으로 제공하는 패스워드 정책을 업데이트하여 높은 비밀번호 복잡도를 적용할 수 있습니다.

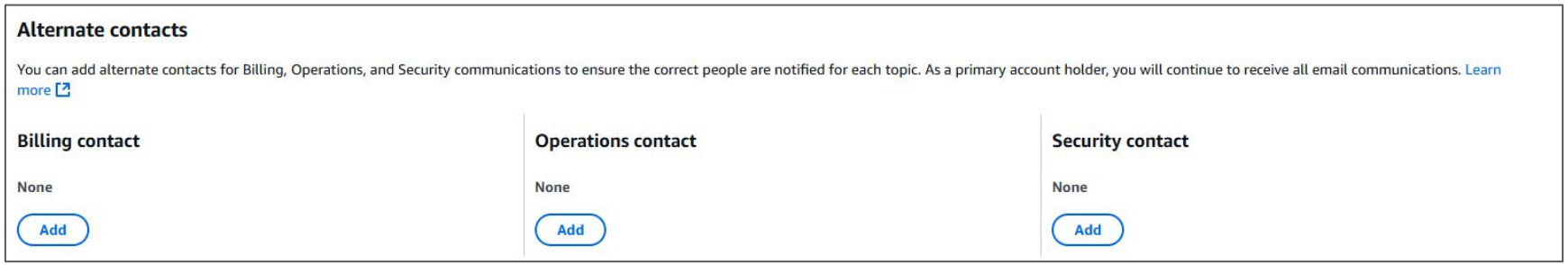


IAM 콘솔 > 계정 설정 > 비밀번호 정책

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.



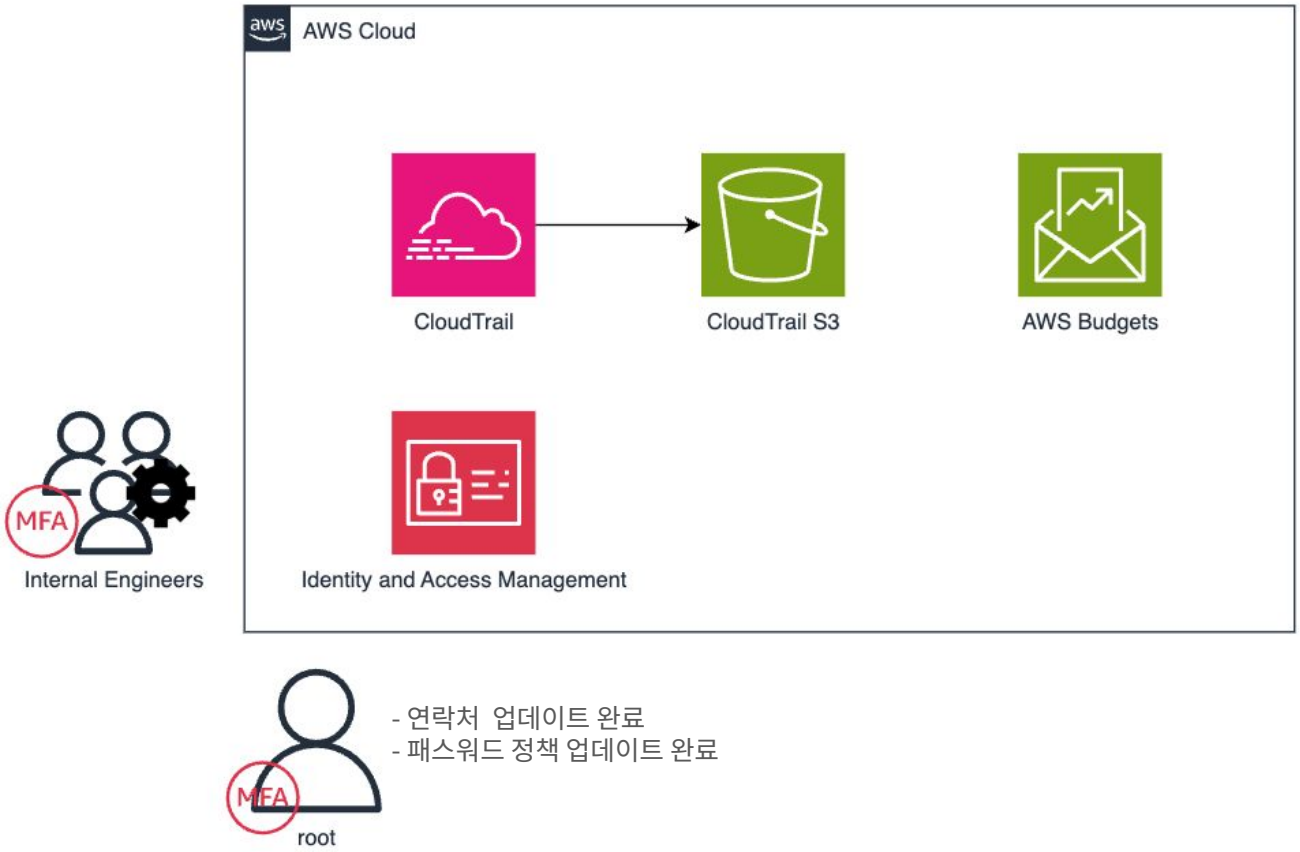


Root 계정 보안 베스트 프랙티스

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

??? :

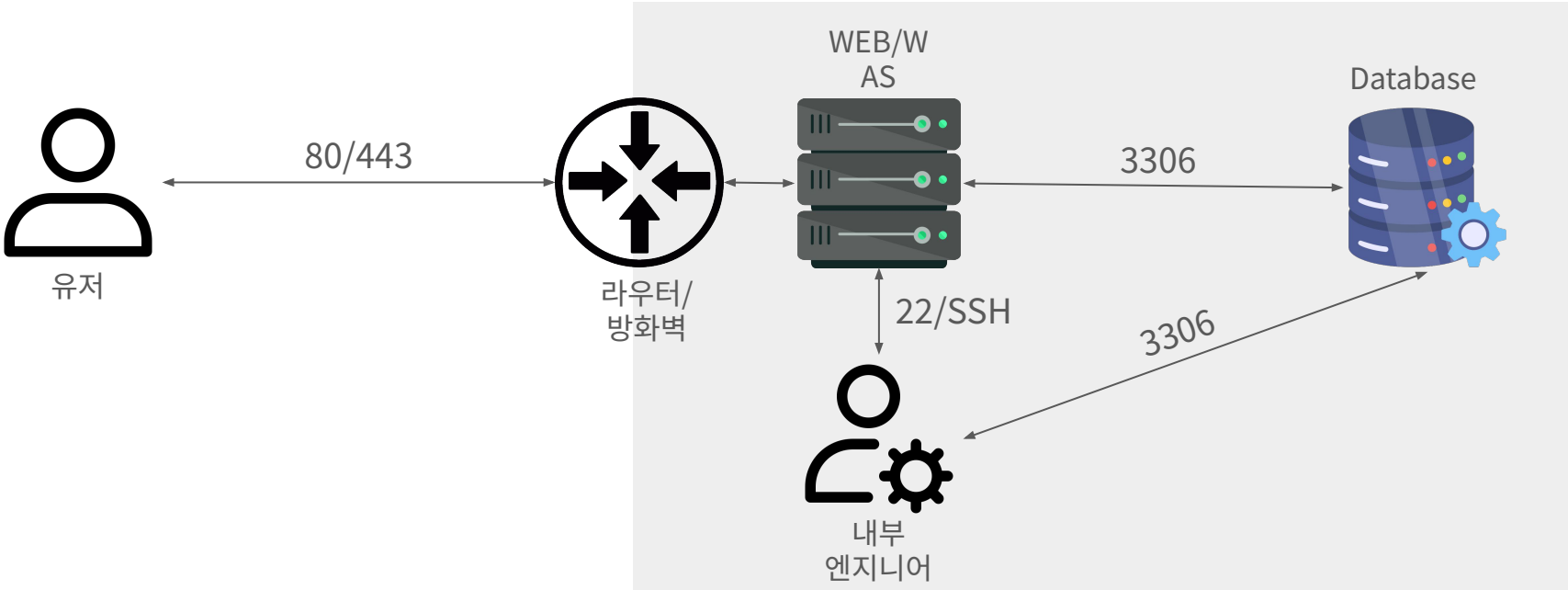
성진씨 계정 만든거 잘 확인했어요.
이제 저희 회사 서버 서비스 **안전하게 AWS로** 옮겨주세요.

성진 :

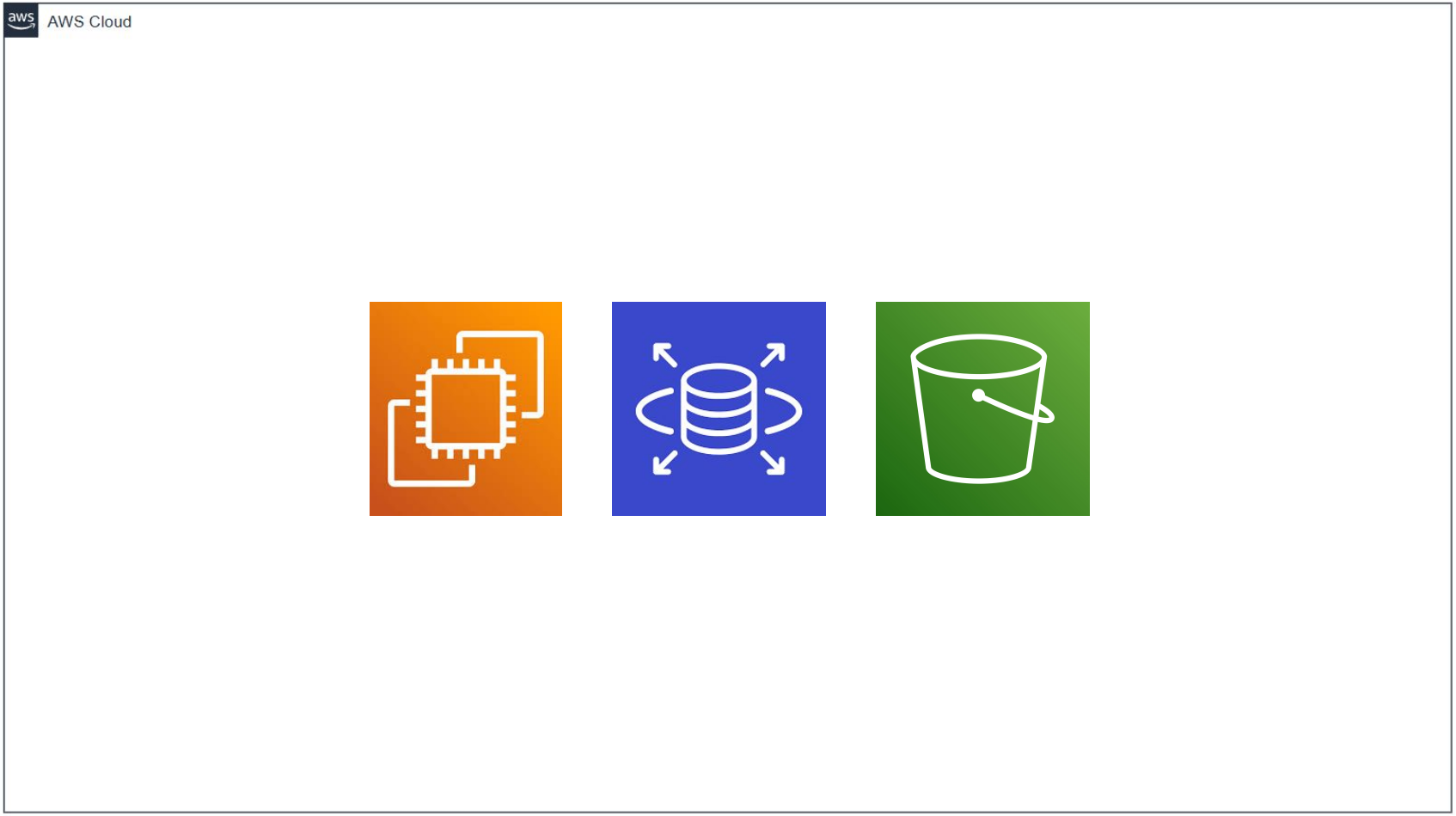
네? 저 이제 AWS 계정 생성했는데…

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

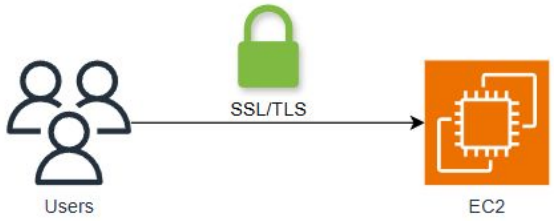


여러분들의 선택은..!?

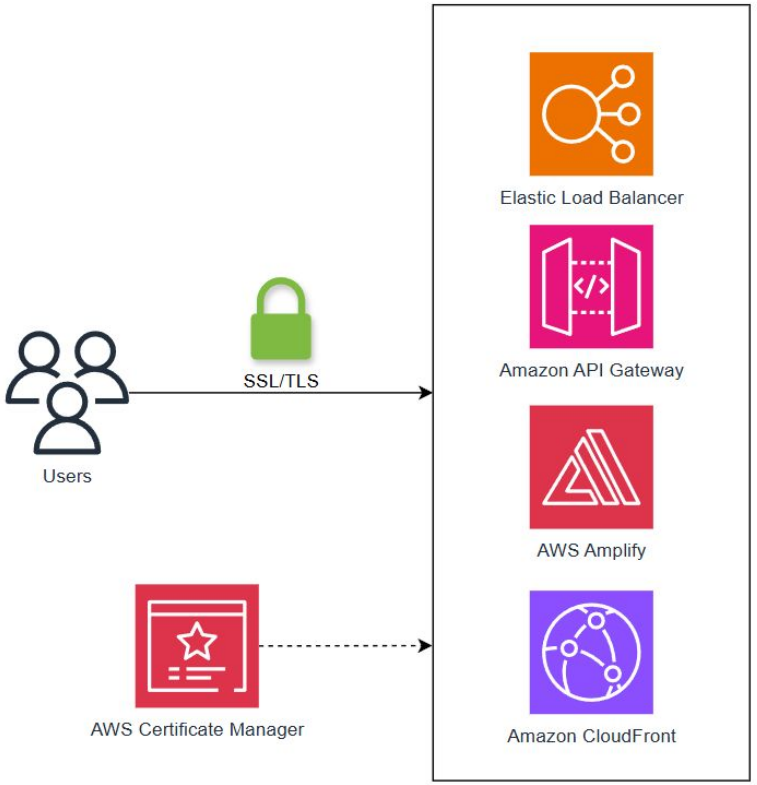


네트워크 보안 - 암호화 통신

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.

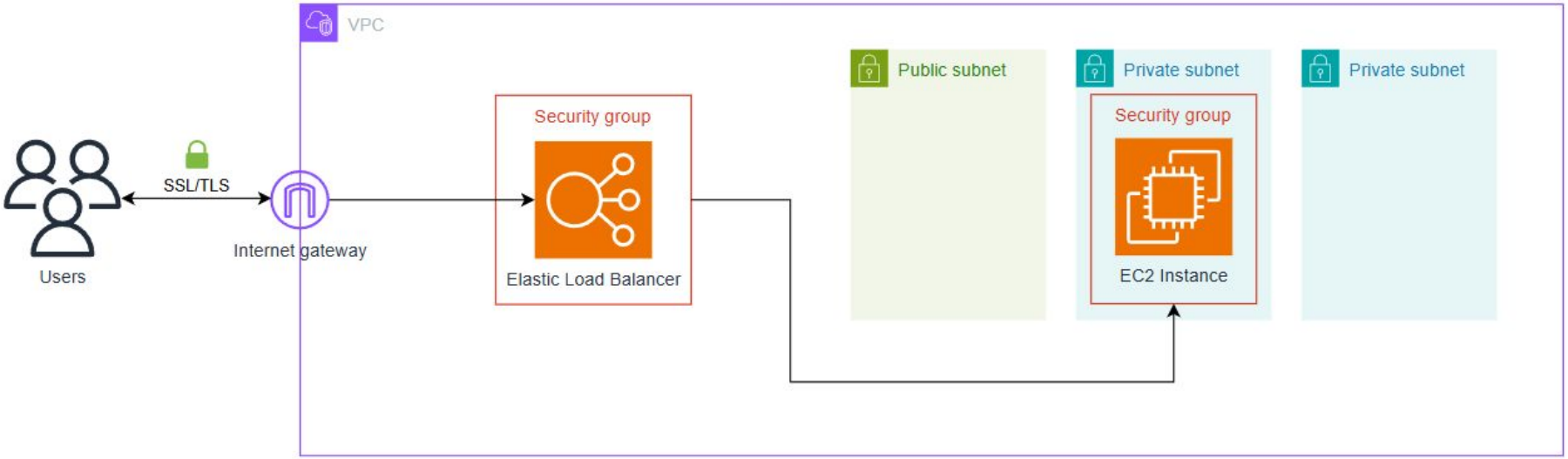


암호화 통신을 위한 인증서 직접관리



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

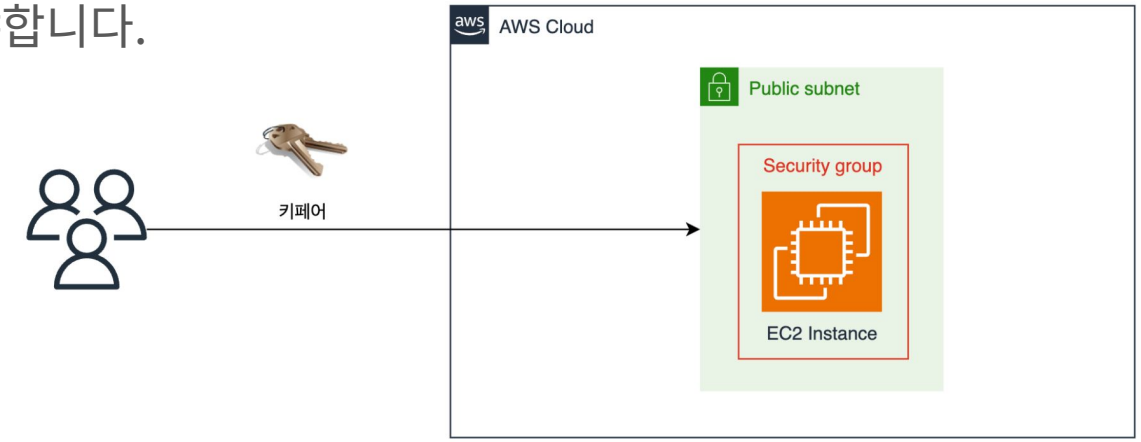
EC2 서버 접근 제어 - SSH 직접 접속

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

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

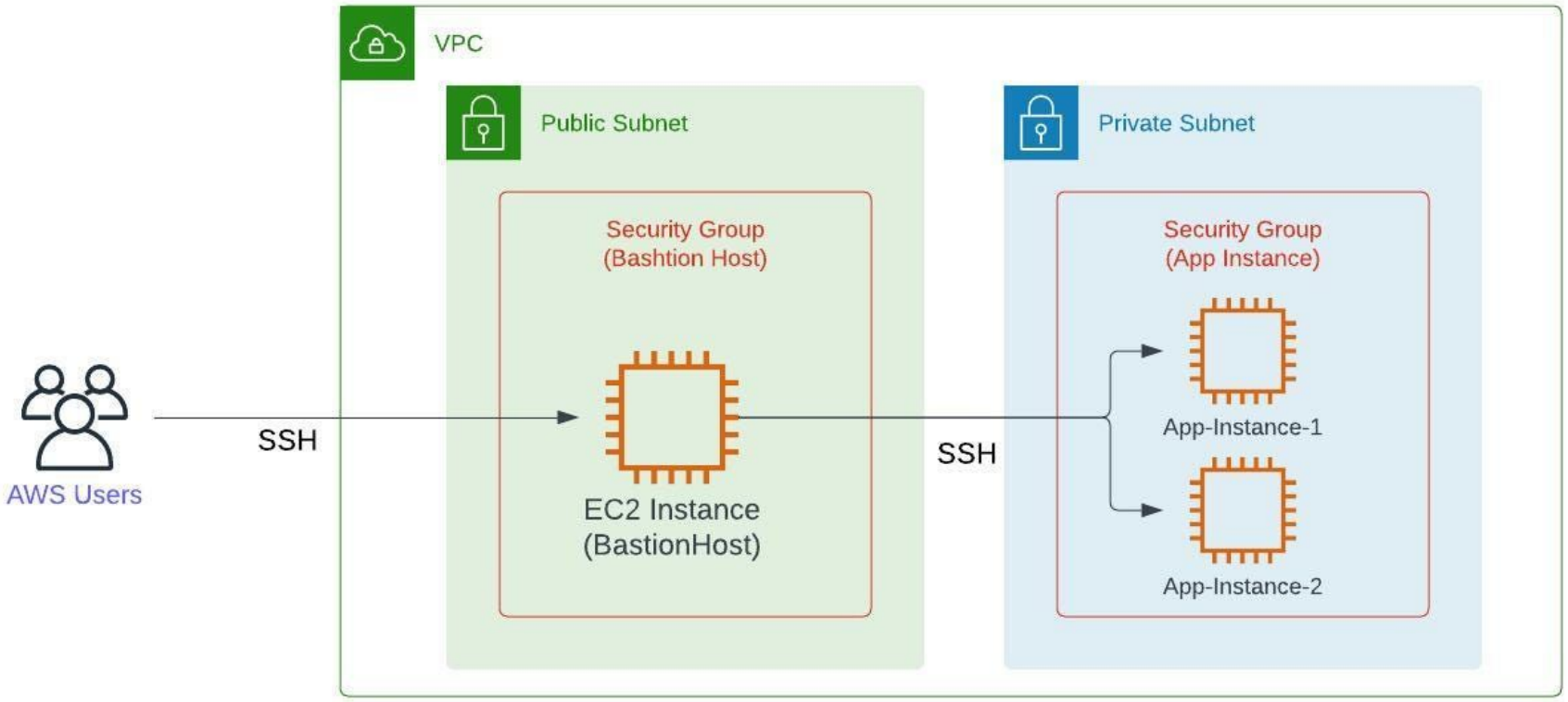
단점

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



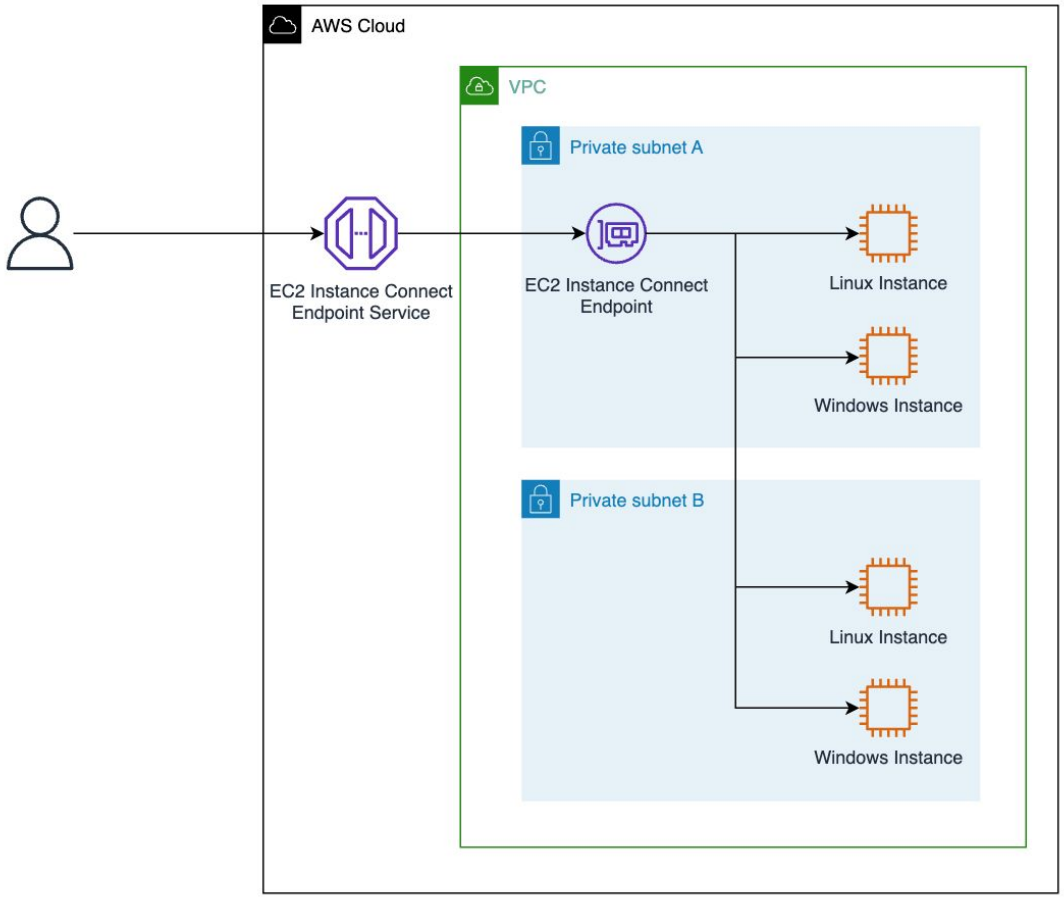
EC2 서버 접근 제어 - Bastion host

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.

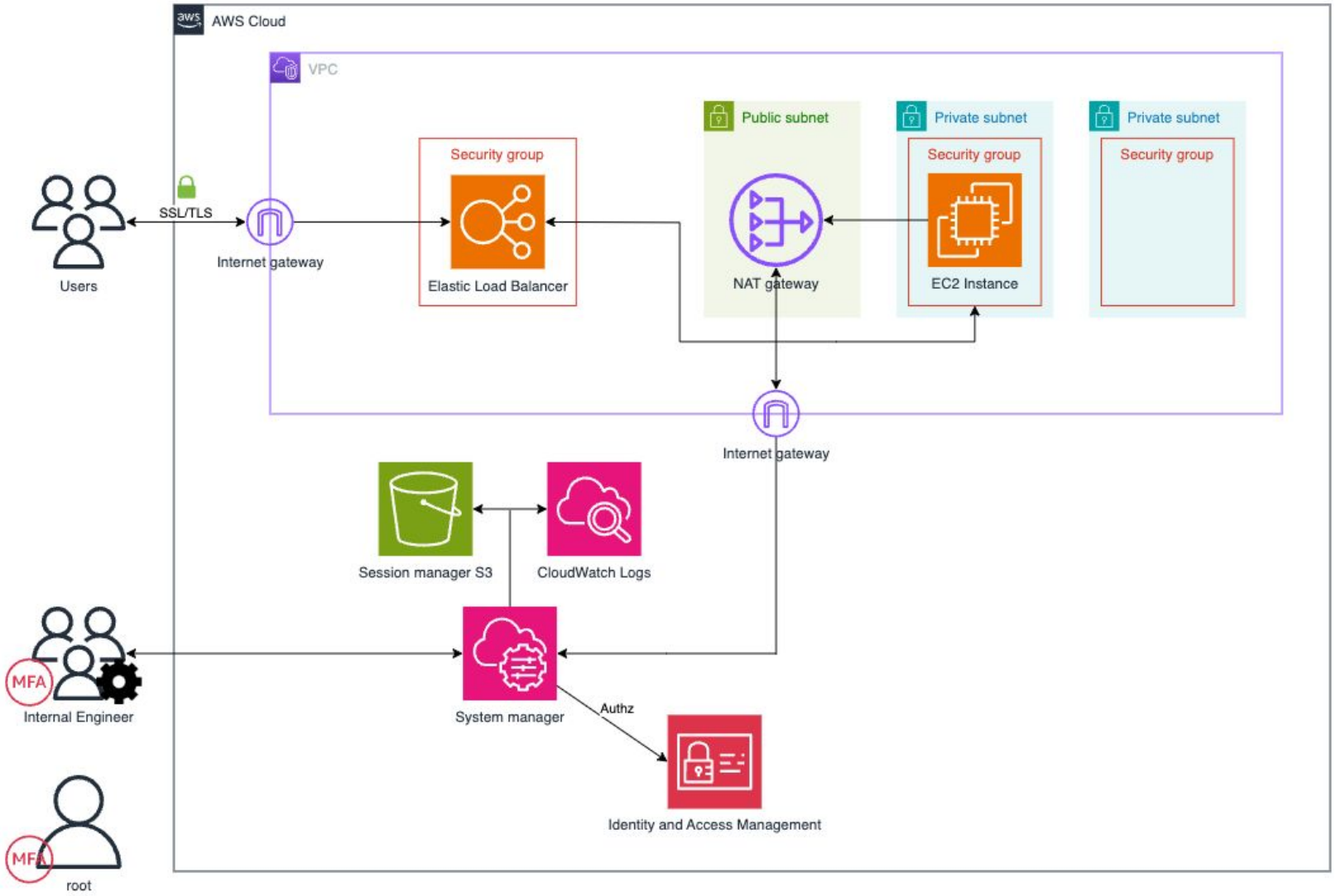


EC2 서버 접근 제어 - AWS System manager

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)



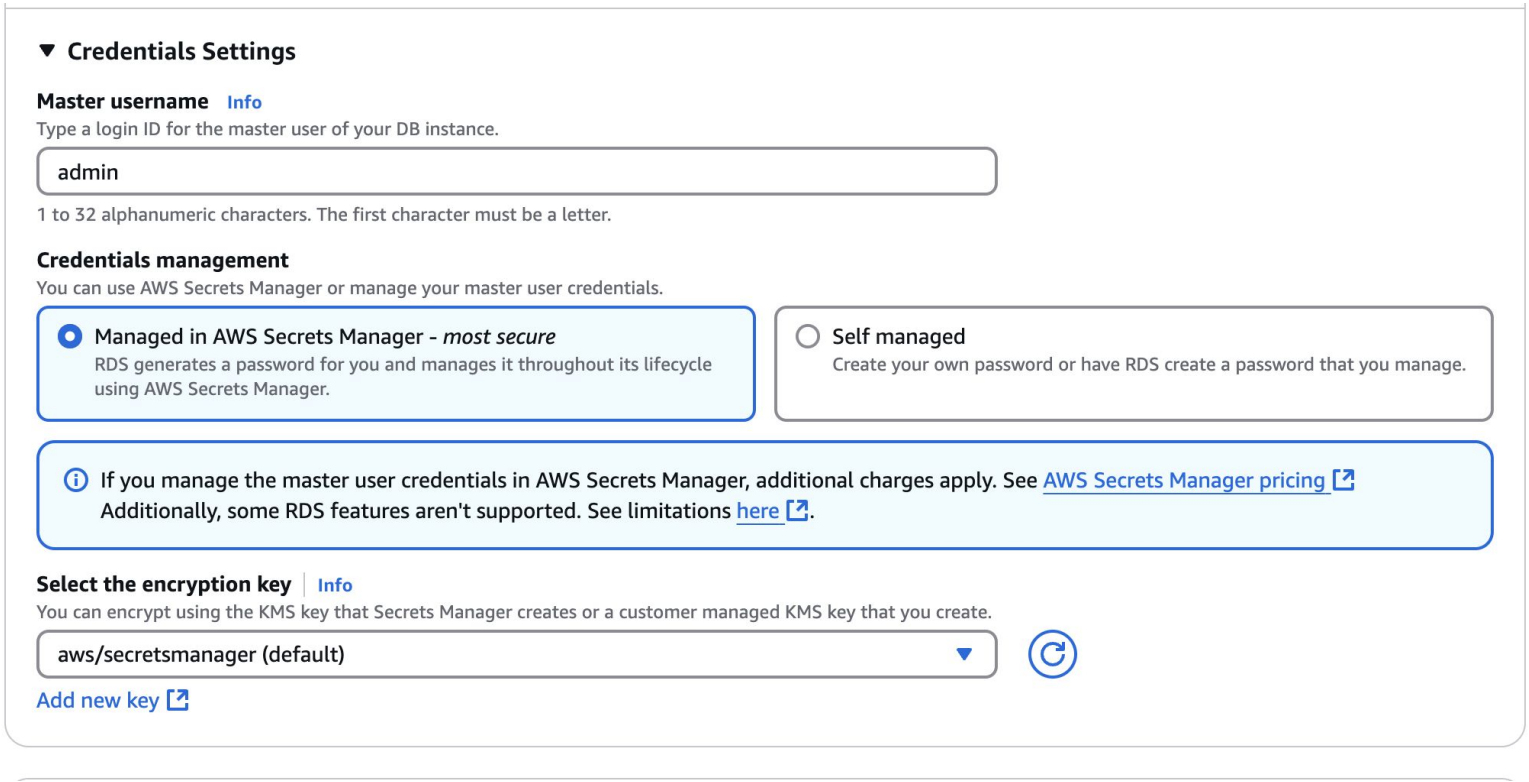
Amazon Relational Database Service 보안

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

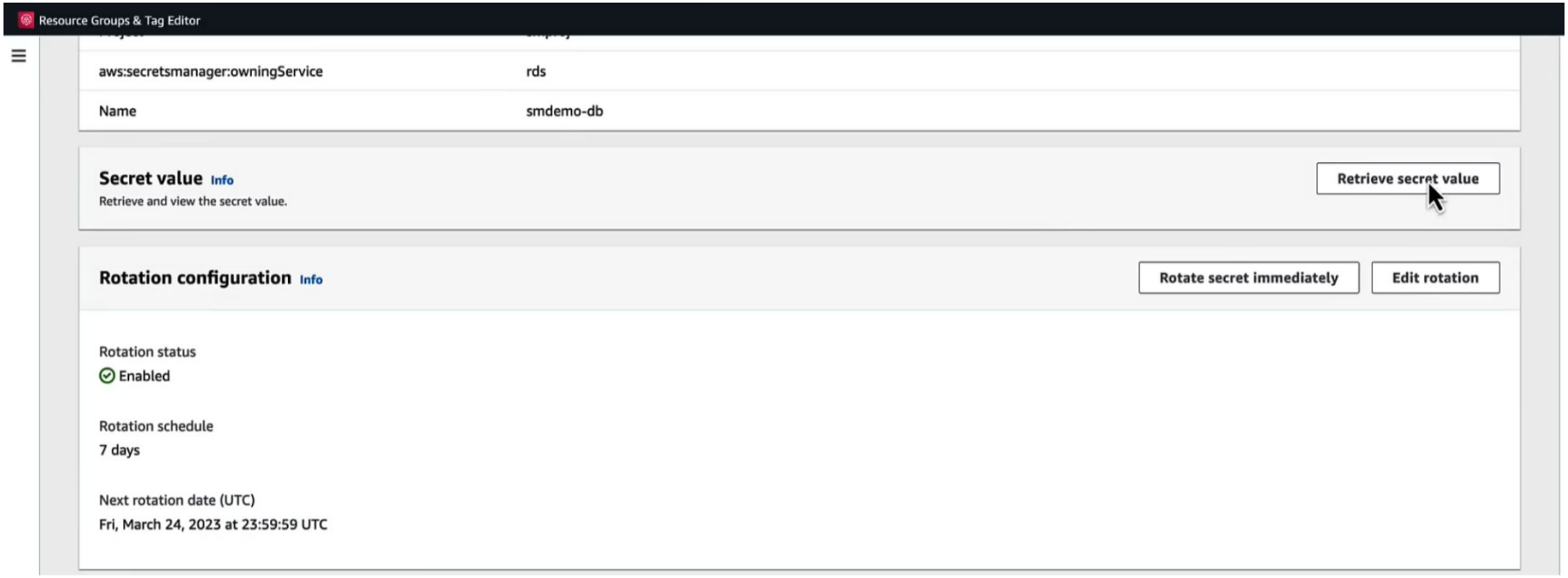
RDS 보안 - 패스워드 관리

패스워드 관리는 직접 관리와 시크릿 매니저에 저장하는 두가지 기능을 제공합니다.



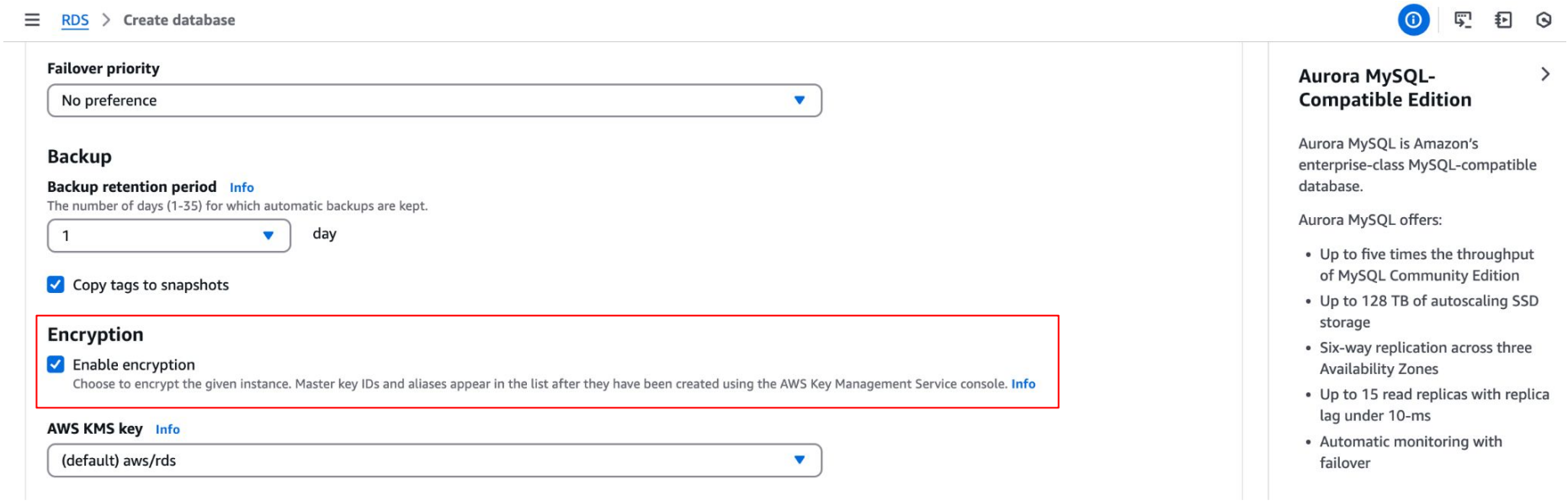
RDS 보안 - 패스워드 관리 (시크릿 매니저)

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



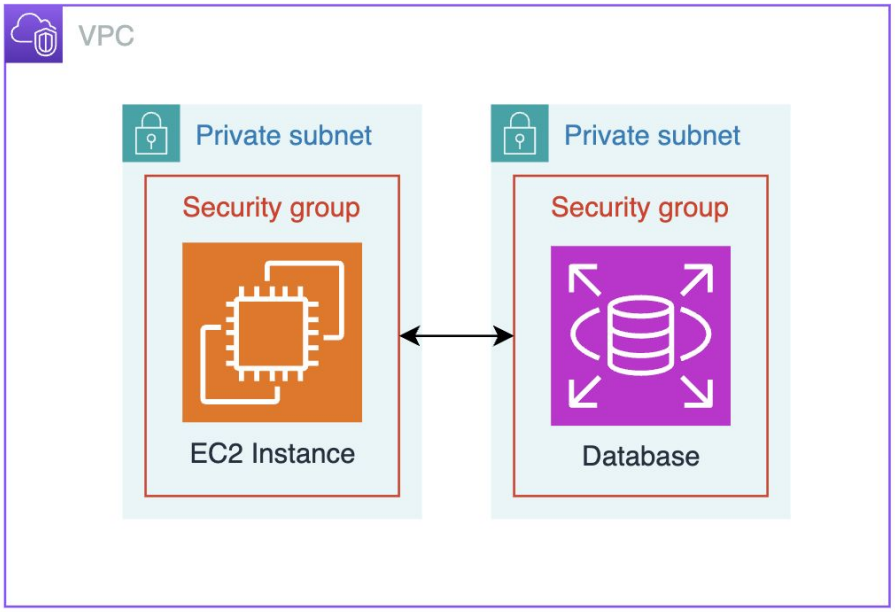
RDS 보안 - 리소스 암호화

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



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

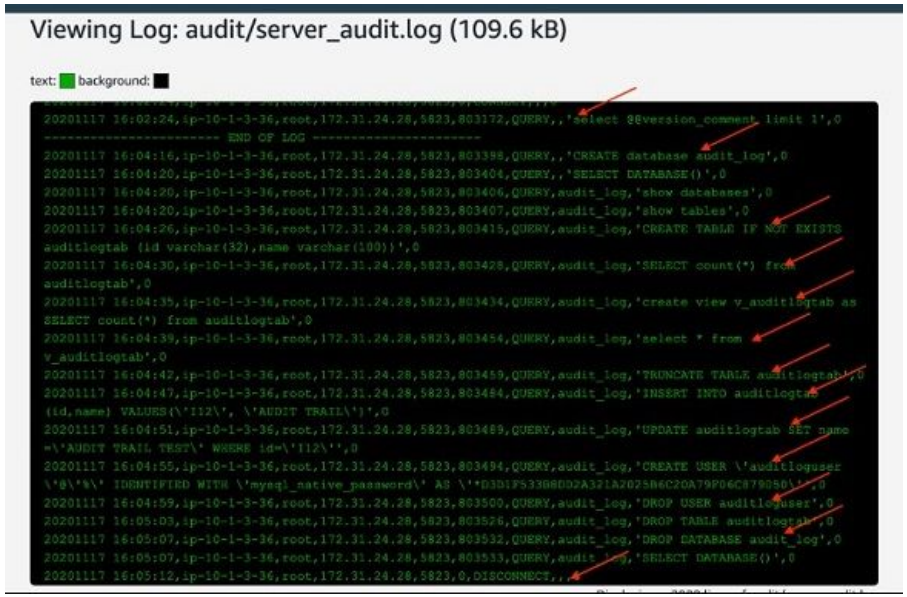
default

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

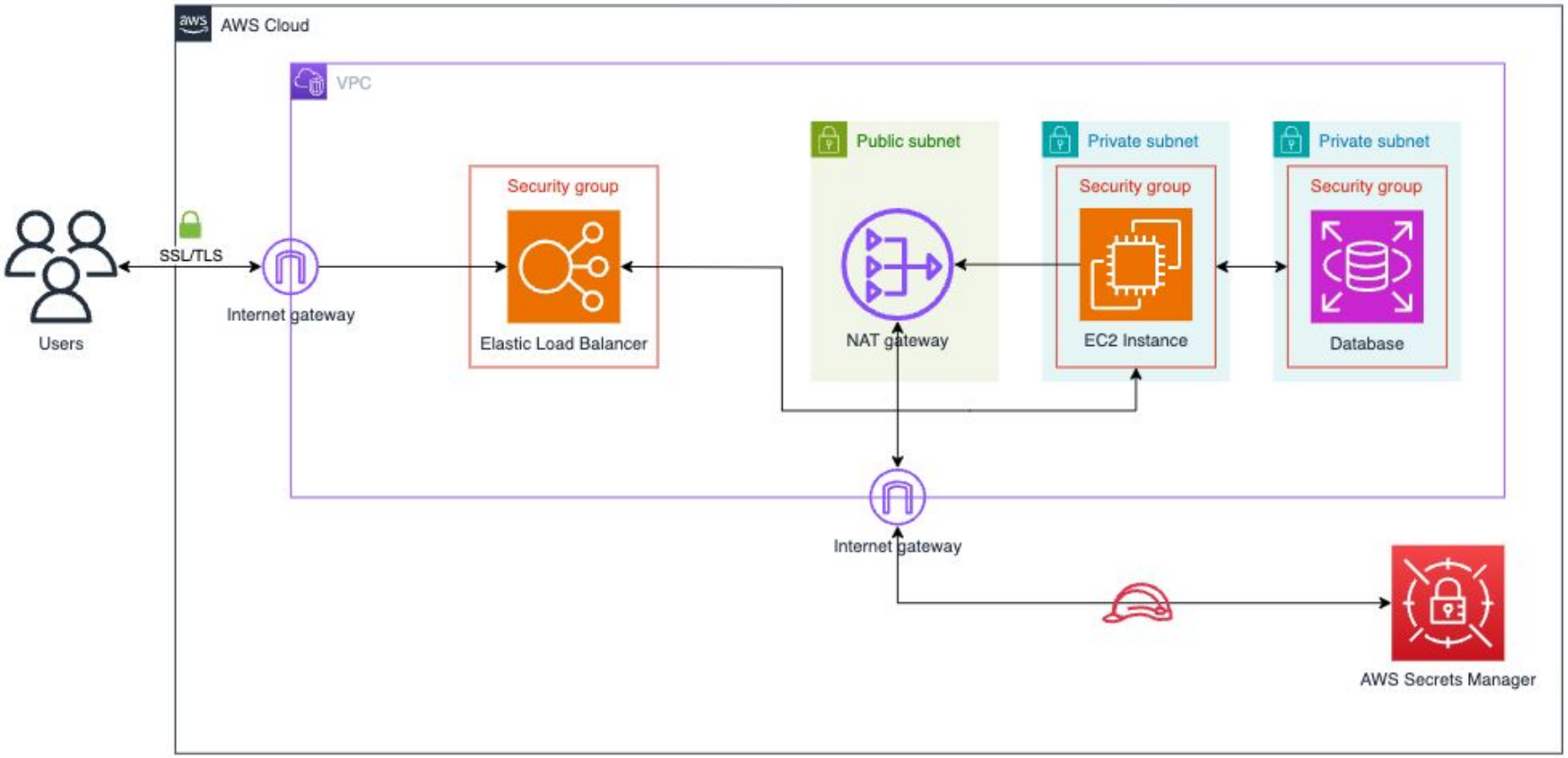
Log exports

Select the log types to publish to Amazon CloudWatch Logs

- [x] Audit log
- [ ] Error log
- [ ] General log
- [ ] iam-db-auth-error log
- [ ] Slow query log



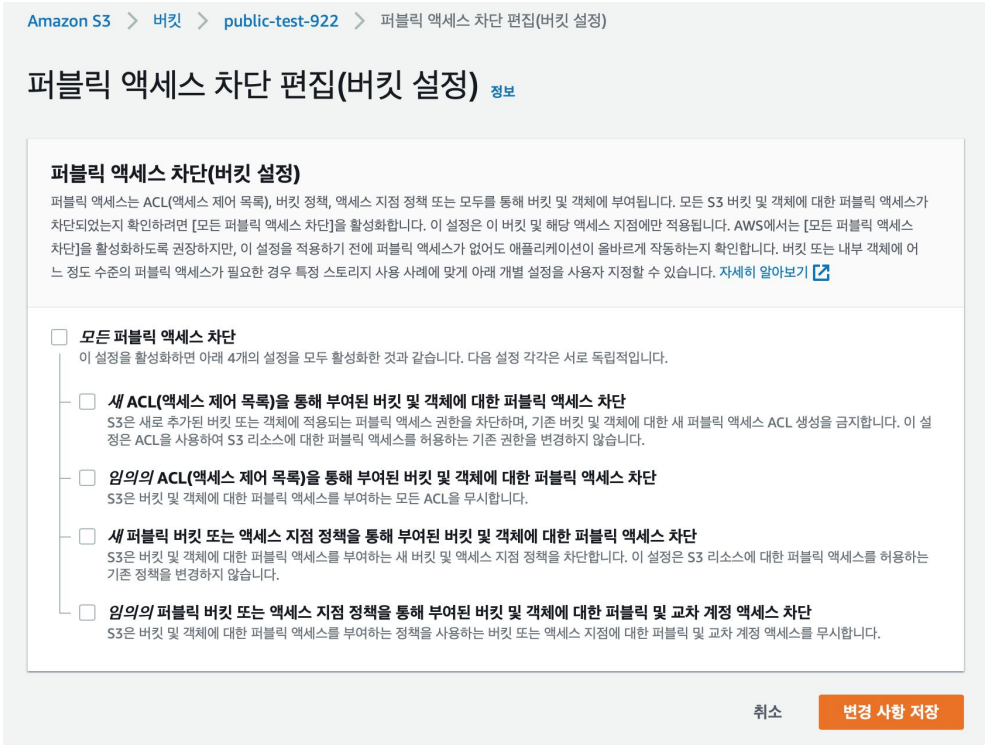
아키텍처 v0.4 (데이터 베이스)



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.

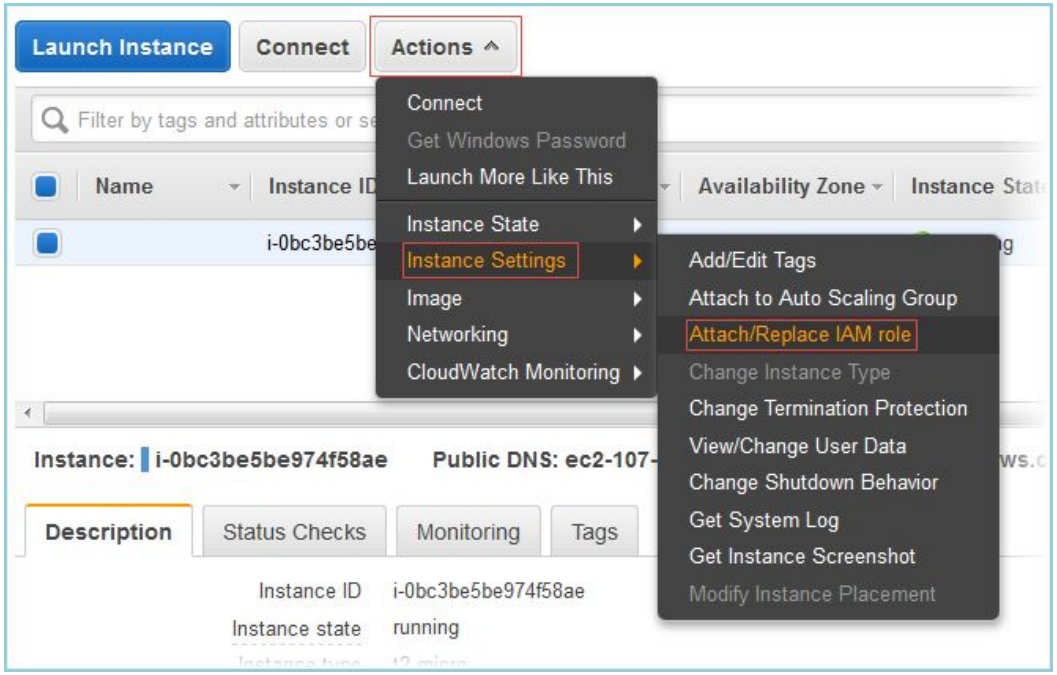
- 객체 암호화 (디폴트)
- 퍼블릭 액세스 차단
- 파일 공유 필요시 서명 URL 사용



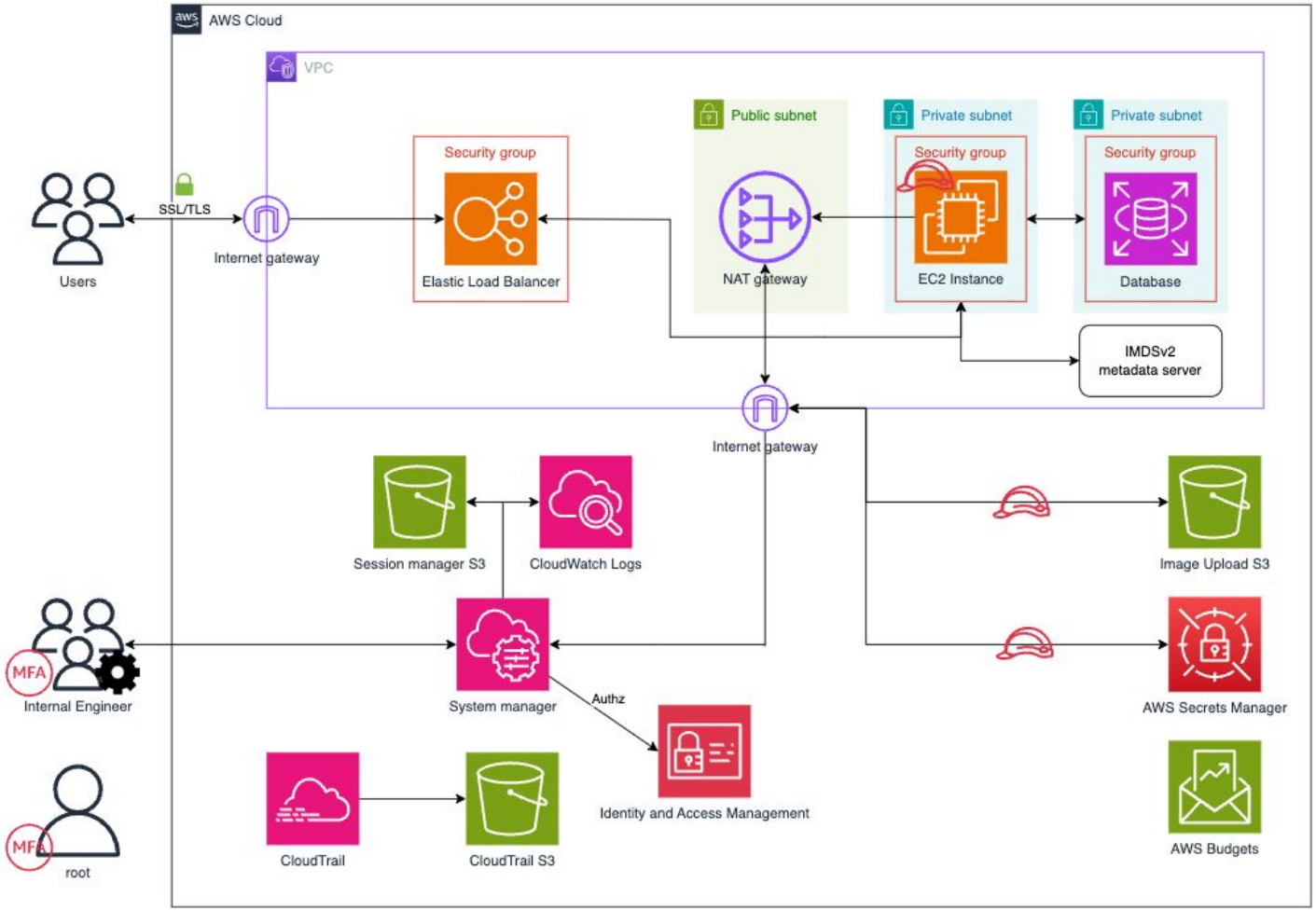
EC2 IAM role 부여

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