****



**클라우드 취약점진단 결과보고서**

2025. 08. 25.



**Confidentiality Agreements**

본 보고서는 시스템 정보와 관련한 비공개 사항이 포함되어 있으므로, 열람권한은 우선적으로 정보보안 책임자로 제한되며, 이외의 열람자격은 정보보안 책임자가 허락한 최소한의 인원으로 제한하여 주시기 바랍니다.

본 보고서는 양사간의 사전 협의 없이 어떠한 목적으로도 외부로 유출되거나 무단 복제, 무단 사용될 수 없으며, 기밀성을 유지한다는 전제하에 사용이 엄격하게 제한됩니다.

본 보고서는 SK쉴더스에서 작성하였으며, 정보보호 서약에 대한 사항을 준수합니다.

목 차

[1. 개요 8](#_Toc209086324)

[1.1. 진단 목적 8](#_Toc209086325)

[1.2. 진단 대상 8](#_Toc209086326)

[1.3. 진단 일정 8](#_Toc209086327)

[1.4. 진단 인력 8](#_Toc209086328)

[2. 진단 항목 9](#_Toc209086329)

[2.1. 진단 항목 9](#_Toc209086330)

[3. 취약점진단 결과 요약 11](#_Toc209086331)

[3.1. 총평 11](#_Toc209086335)

[3.2. 취약점 요약 12](#_Toc209086336)

[4. 취약점진단 상세 결과 13](#_Toc209086337)

[4.1. 계정 관리 13](#_Toc209086338)

[(1) IAM 사용자 계정 식별 관리 13](#_Toc209086339)

[(2) Key Pair 보관 관리 14](#_Toc209086340)

[(3) MFA (Multi-Factor Authentication) 설정 16](#_Toc209086341)

[(4) AWS 계정 패스워드 정책 관리 17](#_Toc209086342)

[4.2. 권한 관리 20](#_Toc209086343)

[(1) 인스턴스 서비스 정책 관리 20](#_Toc209086344)

[(2) 네트워크 서비스 정책 관리 21](#_Toc209086345)

[(3) 기타 서비스 정책 관리 23](#_Toc209086346)

[4.3. 가상 리소스 관리 24](#_Toc209086347)

[(1) 보안 그룹 인/아웃바운드 ANY 설정 관리 24](#_Toc209086348)

[(2) 보안 그룹 인/아웃바운드 불필요 정책 관리 27](#_Toc209086349)

[(3) 네트워크 ACL 인/아웃바운드 트래픽 정책 관리 29](#_Toc209086350)

[(4) 라우팅 테이블 정책 관리 31](#_Toc209086351)

[4.4. 운영 관리 32](#_Toc209086352)

[(1) EBS 및 볼륨 암호화 설정 32](#_Toc209086353)

[(2) 통신구간 암호화 설정 34](#_Toc209086354)

[(3) AWS 사용자 계정 로깅 설정 35](#_Toc209086355)

[(4) 인스턴스 로깅 설정 36](#_Toc209086356)

[(5) VPC 플로우 로깅 설정 37](#_Toc209086357)

[(6) 백업 사용 여부 38](#_Toc209086358)

그림 목차

[[그림] 1. IAM 사용자 화면 13](#_Toc209086359)

[[그림] 2. team3 계정의 태그 현황 13](#_Toc209086360)

[[그림] 3. EC2 인스턴스 화면 14](#_Toc209086361)

[[그림] 4. WEB-EC2의 세부 정보 14](#_Toc209086362)

[[그림] 5. WAS-EC2의 세부 정보 15](#_Toc209086363)

[[그림] 6. DB-EC2의 세부 정보 15](#_Toc209086364)

[[그림] 7. Key Pair 목록과 운영자 오픈채팅방에 공개된 Key Pair 15](#_Toc209086365)

[[그림] 8. IAM 사용자 화면 16](#_Toc209086366)

[[그림] 9. team3의 MFA 16](#_Toc209086367)

[[그림] 10. IAM 계정 설정 18](#_Toc209086368)

[[그림] 11. IAM 암호 정책 편집 18](#_Toc209086369)

[[그림] 12. IAM 사용자 화면 20](#_Toc209086370)

[[그림] 13. team3 사용자의 권한 20](#_Toc209086371)

[[그림] 14. IAM 사용자 화면 21](#_Toc209086372)

[[그림] 15. team3 사용자의 권한 22](#_Toc209086373)

[[그림] 16. IAM 사용자 화면 23](#_Toc209086374)

[[그림] 17. team3 사용자의 권한 23](#_Toc209086375)

[[그림] 18. EC2 보안그룹 24](#_Toc209086376)

[[그림] 19. WEB-EC2 보안그룹 인바운드 24](#_Toc209086377)

[[그림] 20. WEB-EC2 보안그룹 아웃바운드 25](#_Toc209086378)

[[그림] 21. WAS-EC2 보안그룹 인바운드 25](#_Toc209086379)

[[그림] 22. WAS-EC2 보안그룹 아웃바운드 25](#_Toc209086380)

[[그림] 23. DB-EC2 보안그룹 인바운드 26](#_Toc209086381)

[[그림] 24. DB-EC2 보안그룹 아웃바운드 26](#_Toc209086382)

[[그림] 25. EC2 보안그룹 27](#_Toc209086383)

[[그림] 26. WEB-EC2 보안그룹 인바운드 27](#_Toc209086384)

[[그림] 27. WEB-EC2 보안그룹 아웃바운드 27](#_Toc209086385)

[[그림] 28. WAS-EC2 보안그룹 인바운드 28](#_Toc209086386)

[[그림] 29. WAS-EC2 보안그룹 아웃바운드 28](#_Toc209086387)

[[그림] 30. DB-EC2 보안그룹 인바운드 28](#_Toc209086388)

[[그림] 31. DB-EC2 보안그룹 아웃바운드 29](#_Toc209086389)

[[그림] 32. VPC 네트워크 ACL 29](#_Toc209086390)

[[그림] 33. NACL 인바운드 규칙 30](#_Toc209086391)

[[그림] 34. NACL 아웃바운드 규칙 30](#_Toc209086392)

[[그림] 35. VPC 라우팅 테이블 31](#_Toc209086393)

[[그림] 36. 퍼블릭 라우팅 테이블의 서브넷 설정 31](#_Toc209086394)

[[그림] 37. 프라이빗 라우팅 테이블의 서브넷 설정 31](#_Toc209086395)

[[그림] 38. EC2 볼륨 화면 32](#_Toc209086396)

[[그림] 39. WEB-EC2 EBS 볼륨 화면 32](#_Toc209086397)

[[그림] 40. WAS-EC2 EBS 볼륨 화면 33](#_Toc209086398)

[[그림] 41. DB-EC2 EBS 볼륨 화면 33](#_Toc209086399)

[[그림] 42. 사용되지 않는 HTTPS 인증서 34](#_Toc209086400)

[[그림] 43. CloudTrail 추적 화면 35](#_Toc209086401)

[[그림] 44. S3 버킷 화면 35](#_Toc209086402)

[[그림] 45. CloudWatch 화면 36](#_Toc209086403)

[[그림] 46. VPC 화면 37](#_Toc209086404)

[[그림] 47. VPC 플로우 로그 화면 37](#_Toc209086405)

표 목차

[[표] 1. 진단대상 8](#_Toc209086406)

[[표] 2. 진단 일정 8](#_Toc209086407)

[[표] 3. 진단 인력 8](#_Toc209086408)

[[표] 4. 진단 항목 10](#_Toc209086409)

[[표] 5. 취약점 요약 12](#_Toc209086410)

[[표] 6. 패스워드 설정 기준 18](#_Toc209086411)

개요

* 1. 진단 목적

본 클라우드 진단은 **“J.W.P. MagicShop”**의 서비스가 동작하는 클라우드 환경에 대해서 취약점 진단을 수행하고, 발견된 취약점이 시스템에 미치는 영향을 파악하여 보안대책을 제시함으로써, 침해사고 예방 및 서비스의 안정성을 확보하는데 그 목적이 있습니다.

* 1. 진단 대상

|  |  |  |
| --- | --- | --- |
| No | 계정 | 비고 |
| 1 | team3 | 관리자 |

[표] . 진단대상

* 1. 진단 일정

|  |  |
| --- | --- |
| 업무 수행 내역 | 일정 |
| 사전준비 및 대상 관련 자료 수령 | 2025.08.01 ~ 2025.08.09 |
| 취약점 점검 | 2025.08.11 ~ 2025.08.24 |
| 결과 분석 및 결과 보고서 작성 | 2025.08.24 ~ 2025.08.25 |
| 보고서 최종 수정 및 완료 | 2025.08.25 (종료) |

[표] . 진단 일정

* 1. 진단 인력

|  |  |  |  |
| --- | --- | --- | --- |
| 이름 | 수행업무 | 연락처 | E-Mail |
| 박종우 | 취약점진단 | 010-2257-7957 | qtawhwatp@gmail.com |
| 가하늘 | 취약점진단 | 010-4184-7323 | qufgpsmsqka0@gmail.com |
| 김유림 | 취약점진단 | 010-8319-2263 | dyb0256@gmail.com |
| 김태훈 | 취약점진단 | 010-9060-2556 | pobpob2556@gmail.com |
| 문서영 | 취약점진단 | 010-6740-3346 | msy042195@gmail.com |
| 박민지 | 취약점진단 | 010-8651-8921 | ming9ree@swu.ac.kr |
| 유승민 | 취약점진단 | 010-2851-6547 | ysm001223@gmail.com |
| 이승연 | 취약점진단 | 010-5630-6215 | dltmddus9082@gmail.com |
| 장형순 | 취약점진단 | 010-9209-4535 | gudtns4535@gmail.com |
| 정유민 | 취약점진단 | 010-9565-5279 | jeongym349@gmail.com |

[표] . 진단 인력

진단 항목

* 1. 진단 항목

진단에 사용될 체크리스트는 SK쉴더스에서 제공하는 “2024 클라우드 보안 가이드(AWS)”를 기반으로 작성되었습니다. AWS 보안가이드라인에서의 영역은 계정 관리(13개 항목), 권한 관리(3개 항목), 가상 리소스 관리(10개 항목), 운영 관리(15개 항목)으로 총 4개 영역에서 41개 항목으로 구성하였습니다.

| **분류** | **취약점 번호** | **세부 진단 항목** | **준수기준** |
| --- | --- | --- | --- |
| **1.****계정 관리** | 1-1 | 사용자 계정 관리 | **상** |
| 1-2 | IAM 사용자 계정 단일화 관리 | **상** |
| 1-3 | IAM 사용자 계정 식별 관리 | **중** |
| 1-4 | IAM 그룹 사용자 계정 관리 | **중** |
| 1-5 | Key Pair 접근 관리 | **상** |
| 1-6 | Key Pair 보관 관리 | **상** |
| 1-7 | Admin Console 관리자 정책 관리 | **중** |
| 1-8 | Admin Console 계정 Access Key 활성화 및 사용주기 관리 | **상** |
| 1-9 | MFA (Multi-Factor Authentication) 설정 | **중** |
| 1-10 | AWS 계정 패스워드 정책 관리 | **중** |
| 1-11 | EKS 사용자 관리 | **상** |
| 1-12 | EKS 서비스 어카운트 관리 | **중** |
| 1-13 | EKS 불필요한 익명 접근 관리 | **상** |
| **2.권한 관리** | 2-1 | 인스턴스 서비스 정책 관리 | **상** |
| 2-2 | 네트워크 서비스 정책 관리 | **상** |
| 2-3 | 기타 서비스 정책 관리 | **상** |
| **3.가상 리소스**  **관리** | 3-1 | 보안 그룹 인/아웃바운드 ANY 설정 관리 | **상** |
| 3-2 | 보안 그룹 인/아웃바운드 불필요 정책 관리 | **상** |
| 3-3 | 네트워크 ACL 인/아웃바운드 트래픽 정책 관리 | **상** |
| 3-4 | 라우팅 테이블 정책 관리 | **중** |
| 3-5 | 인터넷 게이트웨이 연결 관리 | **하** |
| 3-6 | NAT 게이트웨이 연결 관리 | **중** |
| 3-7 | S3 버킷/객체 접근 관리 | **중** |
| 3-8 | RDS 서브넷 가용 영역 관리 | **중** |
| 3-9 | EKS Pod 보안 정책 관리 | **상** |
| 3-10 | ELB(Elastic Load Balancing) 연결 관리 | **중** |
| **4.운영 관리** | 4-1 | EBS 및 볼륨 암호화 설정 | **중** |
| 4-2 | RDS 암호화 설정 | **중** |
| 4-3 | S3 암호화 설정 | **중** |
| 4-4 | 통신구간 암호화 설정 | **중** |
| 4-5 | CloudTrail 암호화 설정 | **중** |
| 4-6 | CloudWatch 암호화 설정 | **중** |
| 4-7 | AWS 사용자 계정 로깅 설정 | **상** |
| 4-8 | 인스턴스 로깅 설정 | **중** |
| 4-9 | RDS 로깅 설정 | **중** |
| 4-10 | S3 버킷 로깅 설정 | **중** |
| 4-11 | VPC 플로우 로깅 설정 | **중** |
| 4-12 | 로그 보관 기간 설정 | **중** |
| 4-13 | 백업 사용 여부 | **중** |
| 4-14 | EKS Cluster 제어 플레인 로깅 설정 | **중** |
| 4-15 | EKS Cluster 암호화 설정 | **중** |

[표] . 진단 항목

취약점진단 결과 요약

3. 1. 총평

**“J.W.P. MagicShop”**의 총 1개의 클라우드 기반 웹사이트(43.203.87.232)를 대상으로 클라우드 취약점 진단을 수행한 결과, 총 17건의 보안 취약점이 확인되었습니다.

주요 취약점은 IAM 계정의 최소 권한 원칙 위반 및 과도한 리소스 접근 권한, Key Pair 관리 부실, 보안 그룹과 네트워크 ACL의 무분별한 ANY 허용, CloudTrail, CloudWatch, VPC Flow Logs 등 핵심 로깅 기능 미구현 등이었습니다. 이는 계정 탈취, 무단 접근, 데이터 유출, 서비스 마비 등으로 직결될 수 있는 고위험 요인으로 평가됩니다.

특히, 계정 관리 영역에서는 단일 관리자 계정에 과도한 권한이 집중되어 있으며, MFA와 암호 정책 등 기본 보안 통제가 부족하여 계정 기반 침해 사고 발생 시 피해가 클 수 있습니다. 또한, 권한 관리 영역에서는 인스턴스, 네트워크, 기타 서비스 권한이 모두 단일 계정(team3)에 집중되어 있어, 서비스별 최소 권한 원칙이 적용되지 않고 있었습니다. 이로 인해 특정 계정 탈취 시 전체 클라우드 자원에 대한 무단 접근 가능성이 존재하며, 서비스별 IAM 그룹과 역할을 분리하고 권한을 최소화하여 각 담당자에게 재분배해야 합니다.

가상 리소스 관리 영역에서는 보안 그룹과 NACL 설정이 부적절하게 열려 있어 외부 공격자에 의한 불법 접근 가능성이 존재합니다.

운영 관리 영역에서는 로그 수집과 보관 체계가 미비해 사고 발생 시 원인 분석이 어렵고, 백업 미도입으로 서비스 연속성에도 심각한 위협이 됩니다.

종합적으로 볼 때, 현재 환경은 서비스 운영은 가능하나 보안 통제가 전반적으로 미흡하여 침해사고 발생 가능성이 높으며, 발견된 취약점의 다수가 계정과 권한 관리 및 네트워크 보안과 같은 기초적 영역에 집중되어 있습니다. 특히 많은 리소스가 존재하지 않아 진단 항목 중 논외인 것이 많았습니다.

따라서 단기적으로는 MFA 활성화, Key Pair 재관리, 보안 그룹 최소화, 로깅과 백업 활성화 등 기본 보안 통제 조치를 우선 시행해야 합니다. 중장기적으로는 IAM Role 기반 권한 분리, 네트워크 세분화, 암호화 정책 전면 적용, 백업 및 복구 체계 확립, 그리고 관련 보안 규정 및 표준 준수를 통해 관리 수준을 체계적으로 높여야 합니다.

자세한 사항은 아래 진단 결과 상세 내역을 확인해 주시고, 본 결과보고서와 함께 제공드리는 「2024 클라우드 보안가이드(AWS)」를 참고하여 적절한 보안 대책을 수립하고 조치하실 것을 권고드립니다.

**※ 본 진단은 실 서비스 환경(상용 클라우드 인프라)에서 수행되었으며, 시스템 안정성을 고려하여 전체 구성 요소에 대한 정밀 진단이 아닌, 제한된 범위 내 샘플링 방식으로 진행되었습니다. 이에 따라 일부 취약점이 누락되었을 가능성이 있으며, 유사 구성에 대해서는 담당 부서에서 직접 점검 및 추가 조치가 필요합니다.**

**※ J.W.P. MagicShop(대표홈페이지)에서 1개의 계정만 제공되어 본래 있던 관리자 계정들은 진단에서 제외하고, 운영 담당자 계정(team3)에서만 진단을 진행하였습니다.**

**※ 진단항목 기준 “3-3. 네트워크 ACL 인/아웃바운드 트래픽 정책 관리”가 보안 그룹의 포트 및 소스의 정책이 ANY로 허용되어 있어, 중요도가 상으로 변경되었습니다.**

**※ 실제 운영 환경에서 사용 중인 서비스 항목을 대상으로 진단을 수행하였으며, 사용하지 않는 서비스는 진단 범위에서 제외(N/A 처리)하였습니다. 제외된 항목은 Admin Console 2개, EKS 6개, RDS 3개, S3 버킷 3개, CloudTrail 1개, CloudWatch 1개로 총 16개 항목이 N/A 처리되었습니다.**

* 1. 취약점 요약

| 대상(도메인) | 취약점  심각도 | 취약점 명칭 | 개수 |
| --- | --- | --- | --- |
| **J.W.P. MagicShop (http://43.203.87.232)** | **상** | **계정 및 인증 관리 미흡** | **3** |
| **상** | **권한 관리 정책 부재** | **3** |
| **상** | **네트워크 접근 제어 미흡** | **4** |
| **상** | **데이터 보호 미흡** | **2** |
| **상** | **로그 및 모니터링 미흡** | **3** |
| 중 | 키 관리 취약 | 1 |
| 중 | 백업 정책 미흡 | 1 |

[표] . 취약점 요약

※ 취약점심각도

상 : 시스템 직접 장악이나 데이터 유출로 이어질 수 있는 치명적 취약점

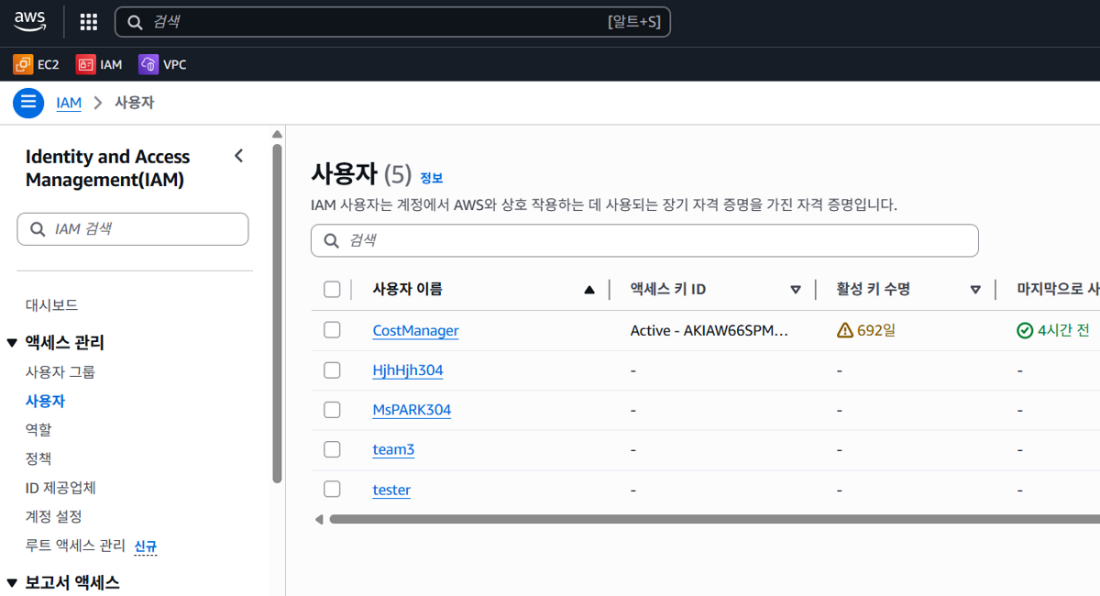
중 : 보안성은 낮추지만 단독으로 치명적이지 않은 취약점

하 : 운영적 보완이 필요한 부분

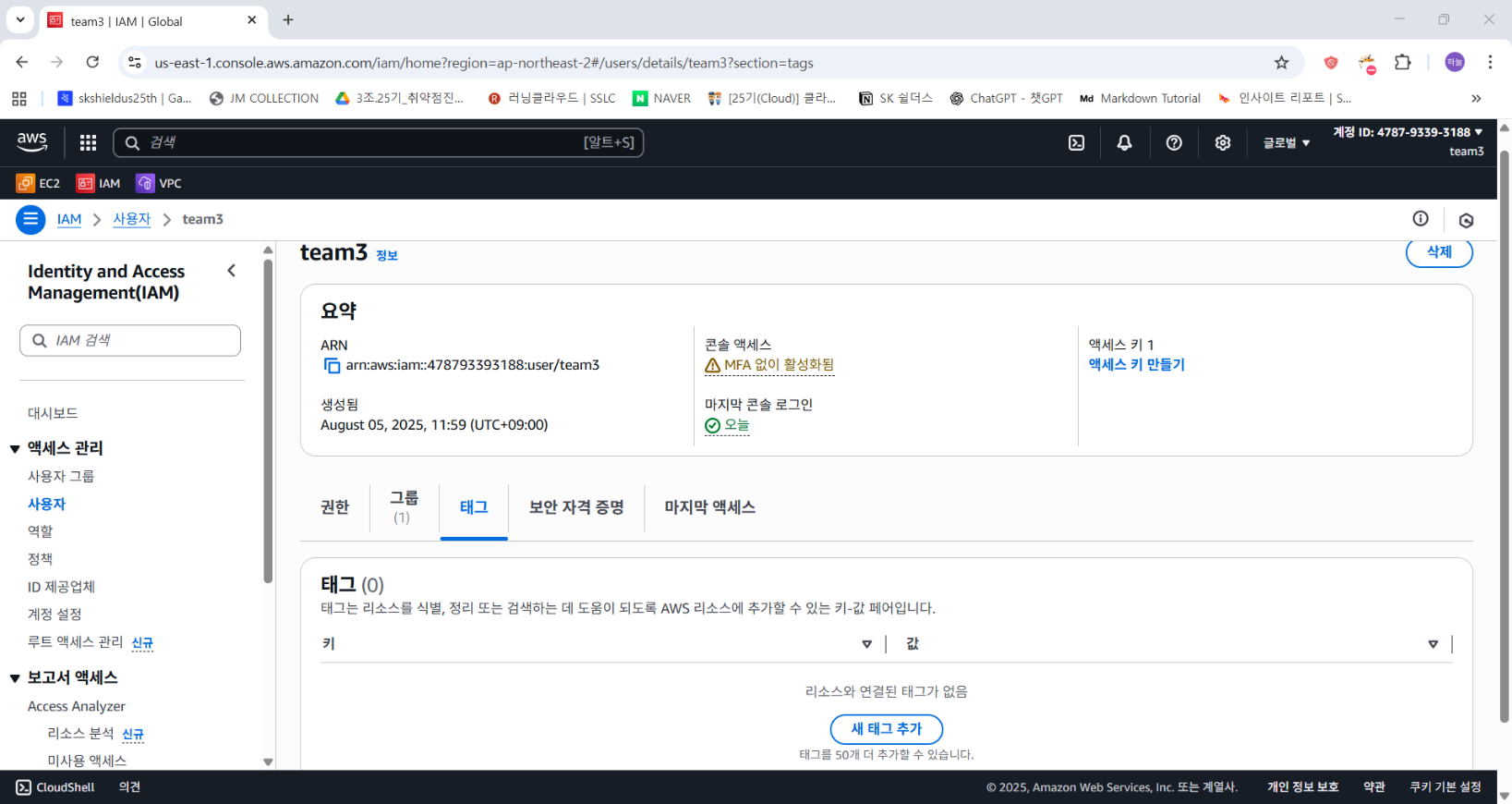
취약점진단 상세 결과

* 1. 계정 관리
     1. IAM 사용자 계정 식별 관리
        1. **문제점**

IAM 사용자 계정은 태그를 추가할 수 있으며, 태그는 IAM 사용자에 대한 액세스 구성, 추정 또는 제어가 가능합니다. 하지만 현재 사용자 team3의 태그를 확인한 결과 태그가 설정되어 있지 않습니다.



[그림] . IAM 사용자 화면



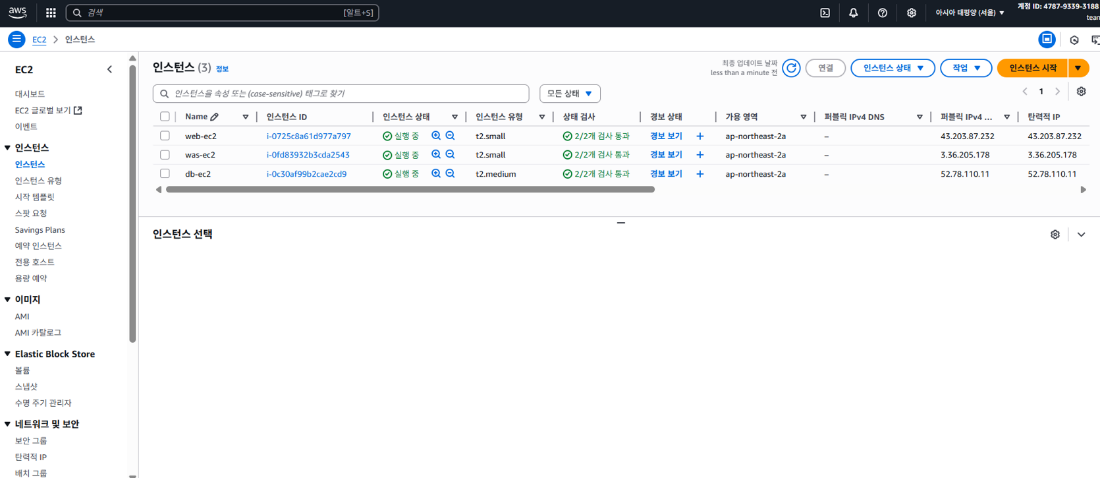
[그림] . team3 계정의 태그 현황

* + - 1. **해결 방안**

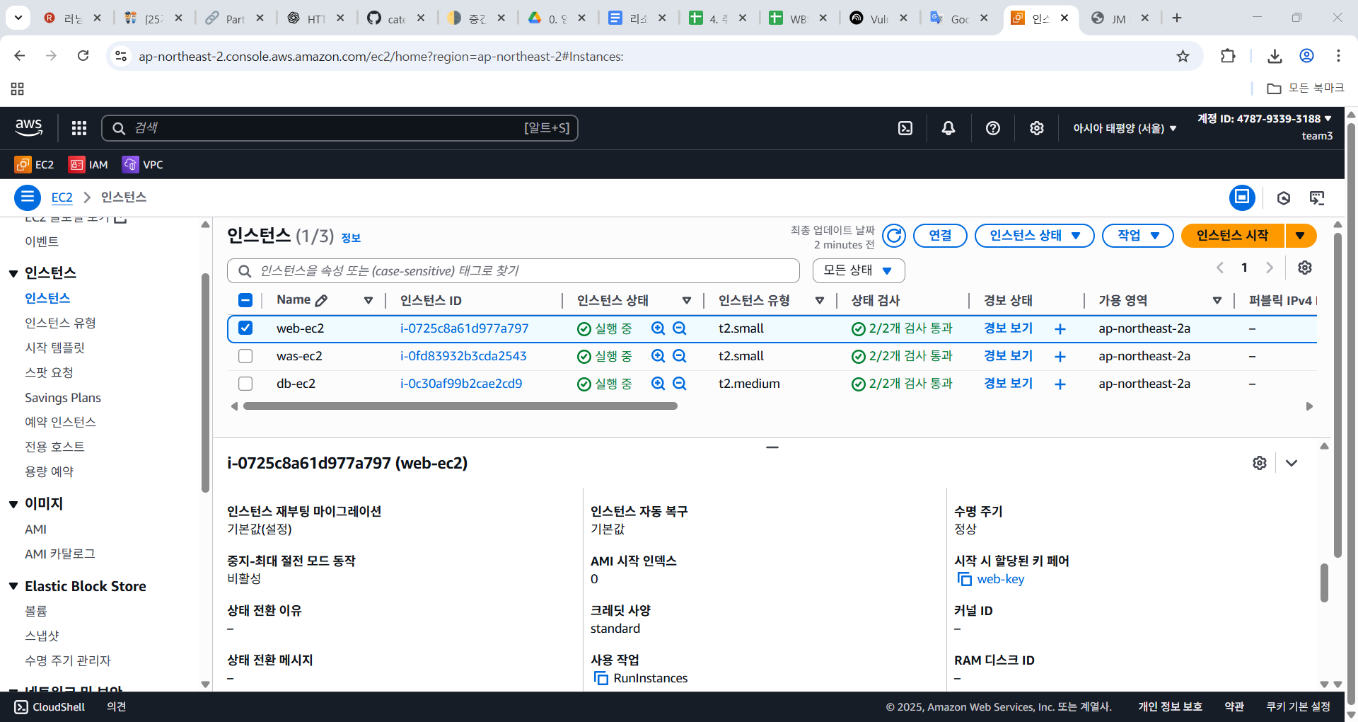
IAM 사용자 계정에 부서, 직책, 사용 목적 등 표준화된 태그를 부여하여 계정 식별과 관리 효율성을 강화해야 합니다. 또한, AWS Config 규칙이나 정책을 활용하여 태그 누락을 자동 탐지 및 통제하고, 퇴사자나 직무 변경자의 계정은 즉시 비활성화 및 삭제하여 불필요한 계정이 남지 않도록 관리해야 합니다.

* + 1. Key Pair 보관 관리
       1. **문제점**

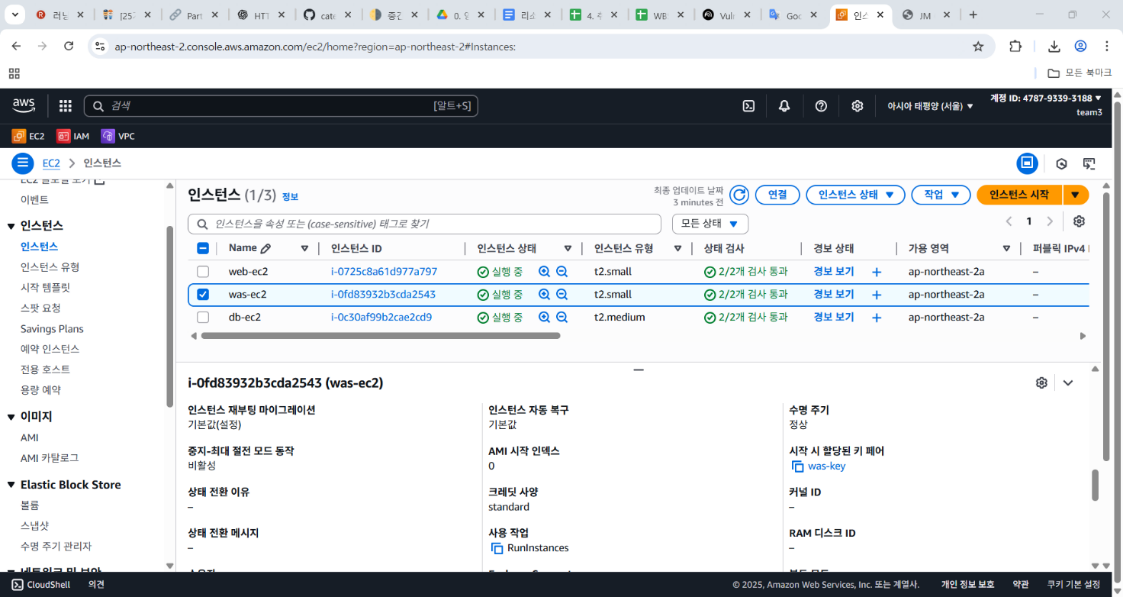
Key Pair는 타 사용자가 확인이 가능한 공개된 위치에 보관하게 될 경우 EC2 인스턴스에 무단으로 접근이 가능해지므로 비인가자가 쉽게 유추 및 접근 불가능한 장소에 보관해야 합니다.



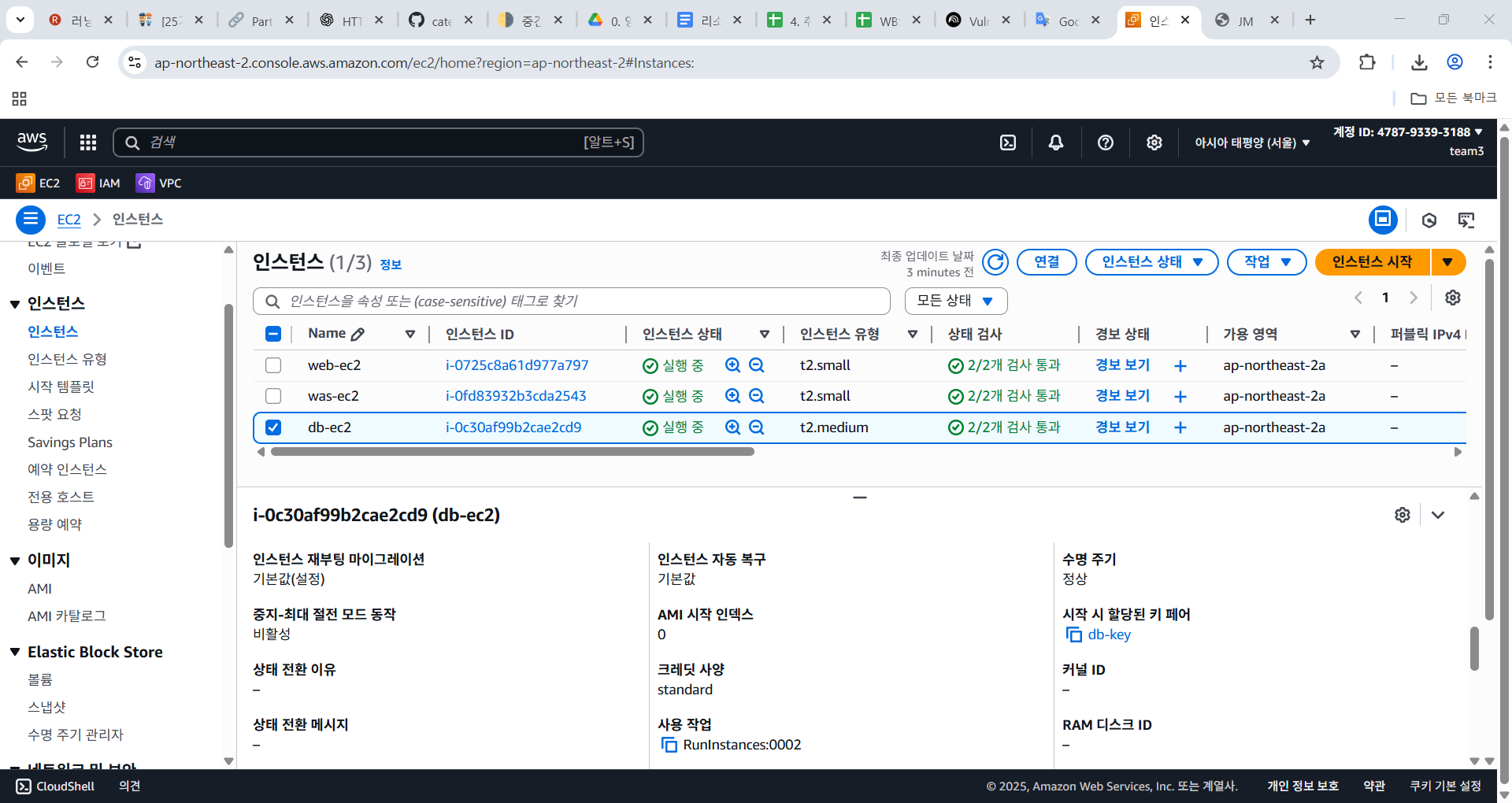
[그림] . EC2 인스턴스 화면



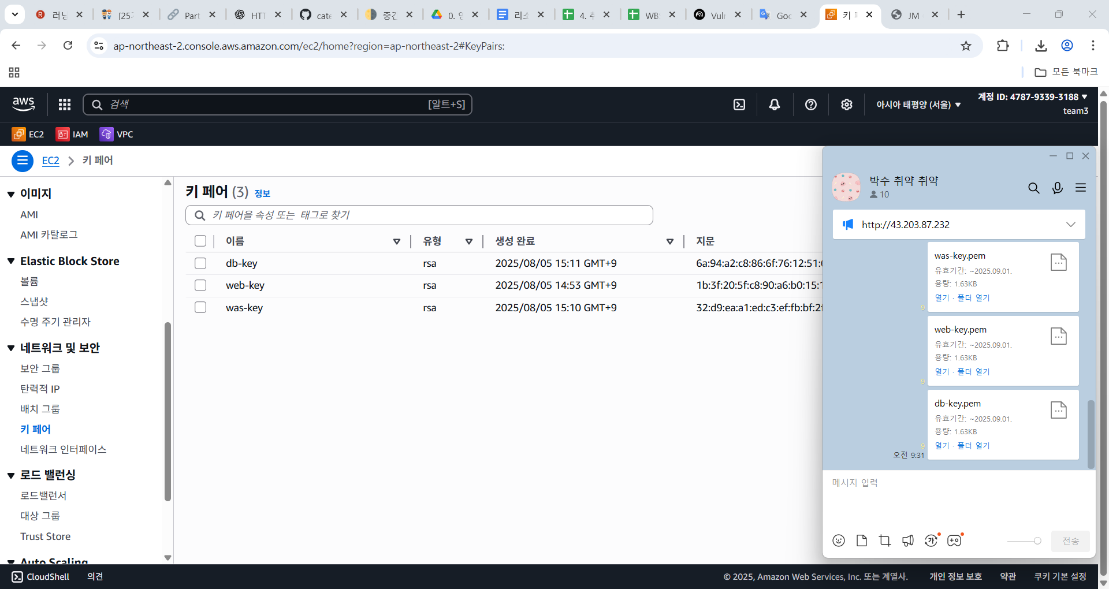
[그림] . WEB-EC2의 세부 정보



[그림] . WAS-EC2의 세부 정보



[그림] . DB-EC2의 세부 정보



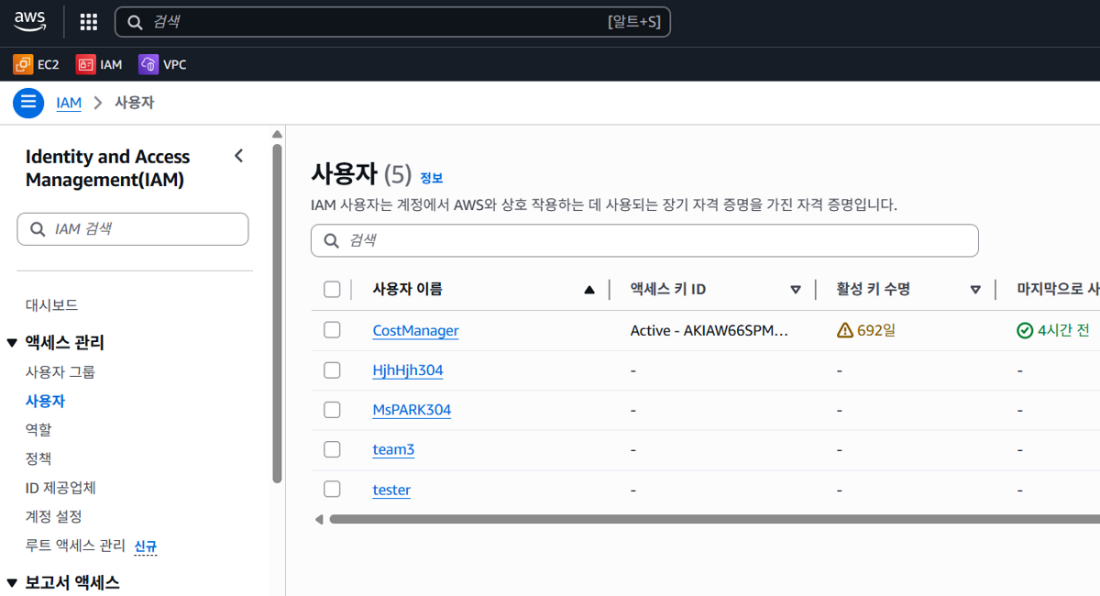
[그림] . Key Pair 목록과 운영자 오픈채팅방에 공개된 Key Pair

* + - 1. **해결 방안**

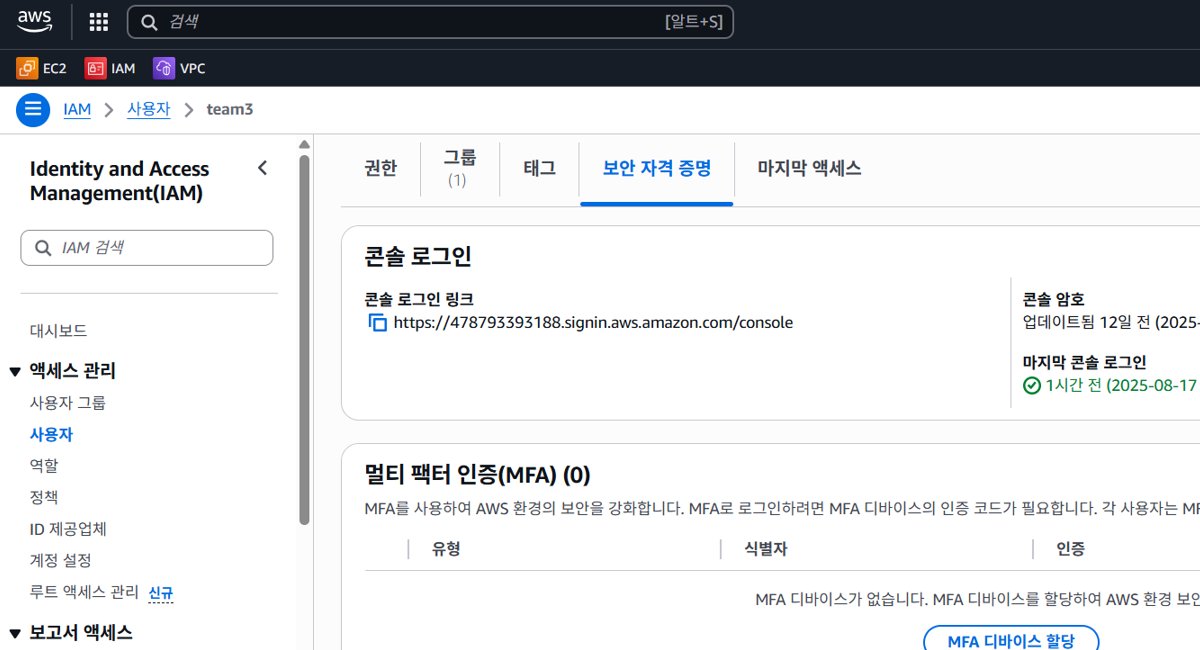
AWS에서 Key Pair는 발급 직후 프라이빗 S3 버킷을 생성하여 Key Pair를 저장하거나 보관 위치를 쉽게 유추할 수 없는 위치에 보관해야 합니다. 또한, 개인 컴퓨터에 보관은 자제하고, 사용하지 않는 Key Pair는 즉시 삭제하여 관리 위험을 최소화해야 합니다.

* + 1. MFA (Multi-Factor Authentication) 설정
       1. **문제점**

AWS MFA(Multi-Factor Authentication)는 사용자 이름과 암호 외에 추가로 보안을 강화할 수 있는 방법으로 MFA를 활성화하면 사용자가 AWS 웹 사이트에 로그인할 때 사용자 이름과 암호와 함께 AWS MFA 디바이스에서 생성된 인증 코드를 함께 입력해야 합니다. 이러한 다중 인증 절차를 통해 AWS 계정 설정 및 리소스에 대한 보안을 높일 수 있습니다.



[그림] . IAM 사용자 화면



[그림] . team3의 MFA

* + - 1. **해결 방안**

AWS 계정 및 IAM 사용자 계정에 MFA를 활성화하여 계정 로그인 시 MFA 인증을 하도록 해야 합니다. 또한, IAM 정책이나 AWS Organizations의 서비스 제어 정책(SCP)을 활용해 MFA가 설정되지 않은 계정의 콘솔 로그인이나 특정 작업을 제한하여 보안성을 강화할 수 있습니다.

* + 1. AWS 계정 패스워드 정책 관리
       1. **문제점**

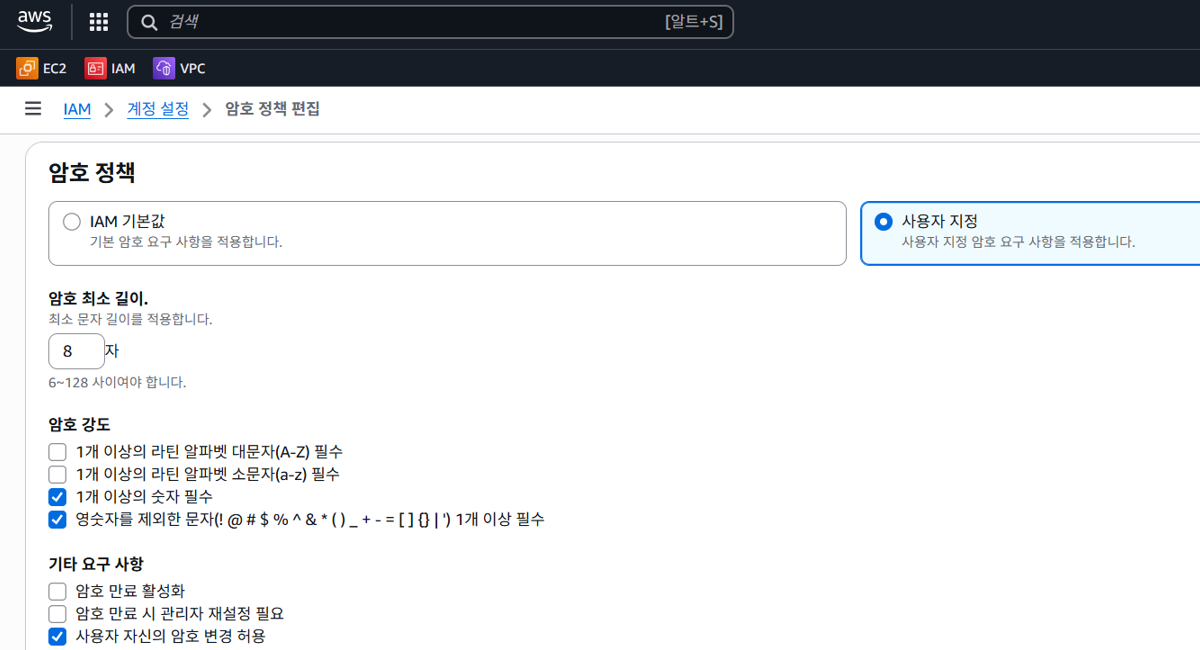
AWS Admin Console 계정 및 IAM 사용자 계정의 암호는 패스워드 설정 기준에 따라 일반적으로 유추하기 어려운 형태로 설정하여, 비인가 사용자의 접근을 방지해야 합니다.

|  |
| --- |
| <패스워드 설정 기준> |
| 1) 패스워드는 4가지 문자 종류 중 2종류 이상을 사용하여 최소 10자리 이상, 또는 3종류 이상을 조합하여 최소 8자리 이상으로 구성  \* 영문 대문자(26개), 영문 소문자(26개), 숫자(10개), 특수문자(32개) |
|  |
| <패스워드는 비인가자에 의한 추측이 어렵도록 다음의 사항을 반영하여 설계해야 함> |
| 1) Null 패스워드 사용 금지  2) 문자 또는 숫자만으로 구성 금지  3) 사용자 ID와 동일한 패스워드 금지  4) 연속적인 문자 및 숫자 사용 금지  5) 주기성 패스워드 사용 금지  6) 전화번호, 생일, 계정 명, hostname과 같이 추측하기 쉬운 패스워드 사용 금지 |
|  |
| 1) 패스워드 최소 길이  패스워드 추측 공격을 피하기 위해 패스워드 최소 길이가 설정되어 있는지 점검함  패스워드 최소 길이가 설정되어 있지 않거나 짧게 설정되어 있을 경우 취약한 패스워드를  사용함으로 인해 악의적인 사용자가 패스워드를 쉽게 유추할 수 있음    2) 패스워드 최대 사용 기간  패스워드가 임의의 경로로 유출되었을 때, 임의로 접속한 사용자가 언제든 다시 접속할 수 있는 환경을 방지하기 위해 패스워드 날짜 제한을 점검함  3) 패스워드 최소 사용 기간  패스워드가 임의의 경로로 유출되었을 때, 임의로 접속한 사용자가 언제든 다시 접속할 수 있는 환경을 방지하기 위하여 패스워드 날짜 제한을 점검함  4) 이전 패스워드 기억  이전에 사용한 패스워드를 기억하여 패스워드 변경 시 기존에 사용했던 패스워드 재사용 금지  - 패스워드 길이는 8자 이상 설정하는 것을 권고  - 패스워드 최대 사용 기간을 60일 이하로 설정할 것을 권고  - 패스워드 최소 사용 기간을 1일 이상으로 설정할 것을 권고  5) 암호 만료 활성화 및 재사용 제한  - 암호 만료 활성화, 암호 만료일은 90일 이하여야 함  - 암호 재사용 제한 최소 1개 이상이어야 함 |

[표] 6. 패스워드 설정 기준



[그림] . IAM 계정 설정



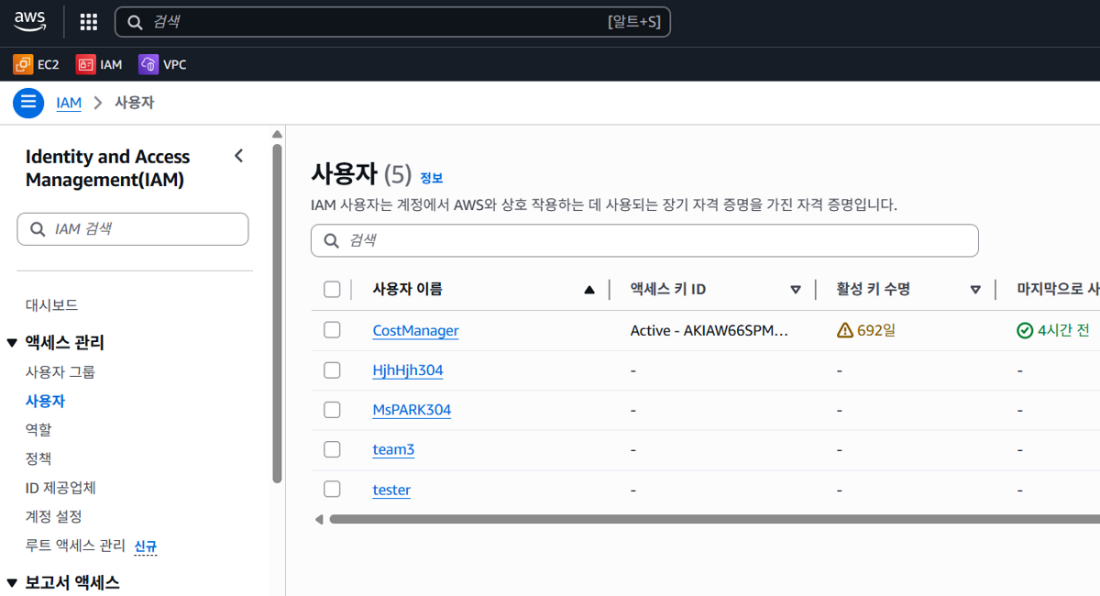
[그림] . IAM 암호 정책 편집

* + - 1. **해결 방안**

IAM의 계정 암호 정책의 편집을 통해 현재 암호 정책에서 1개 이상의 라틴 알파벳 소문자(a-z) 필수 체크, 암호 만료 활성화를 90일 이하 그리고 암호 재사용 제한을 설정하여 암호 정책을 강화해야 합니다. 또한, MFA를 병행 적용하고 정책 준수 여부를 주기적으로 점검해야 합니다.

* 1. 권한 관리
     1. 인스턴스 서비스 정책 관리
        1. **문제점**

AWS 인스턴스 서비스(EC2, RDS, S3 등)의 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다. 하지만 하나의 계정으로 모든 서비스를 관리하고 있기 때문에 보안에 취약합니다.



[그림] . IAM 사용자 화면



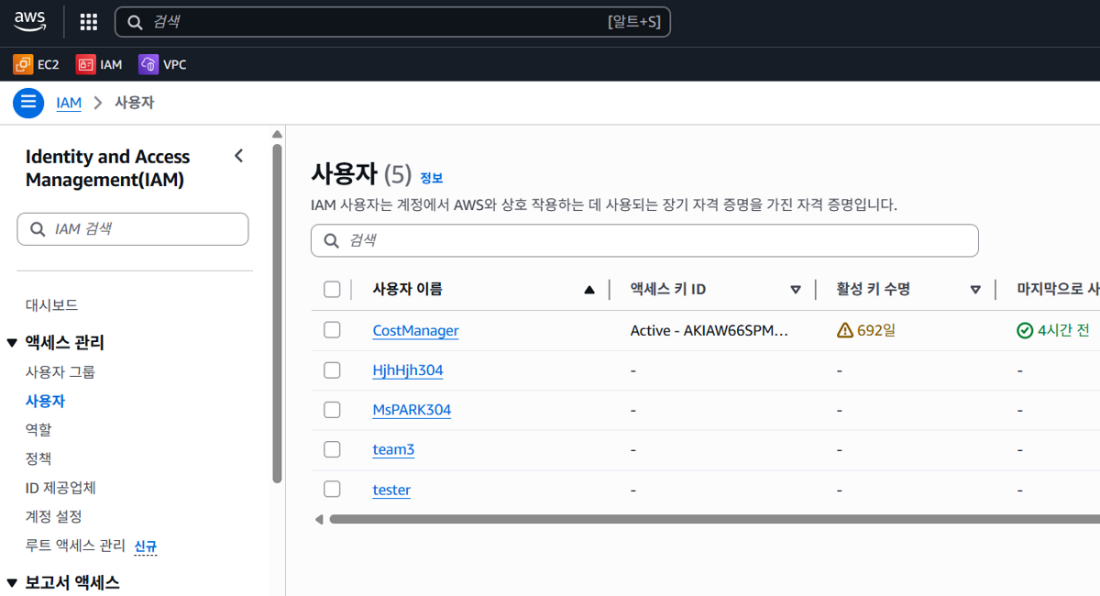
[그림] . team3 사용자의 권한

* + - 1. **해결 방안**

AWS 인스턴스 서비스(EC2, RDS, S3 등)의 리소스 생성 및 접근 권한은 전용 IAM 그룹을 통해 관리해야 하며, 반드시 해당 그룹에 속한 특정 IAM 계정으로 로그인하여 서비스 관리 및 운영해야 합니다. 이를 통해 권한 관리와 책임 소재를 명확히 할 수 있으며, 계정별로 접근 통제가 가능합니다.

* + 1. 네트워크 서비스 정책 관리
       1. **문제점**

AWS 네트워크 서비스(VPC, Route 53, Direct Connect 등)의 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다. 하지만, 네트워크 서비스 별로 관리자 계정이 생성되지 않고 권한이 부여되지 않았기 때문에 보안에 취약합니다.



[그림] . IAM 사용자 화면



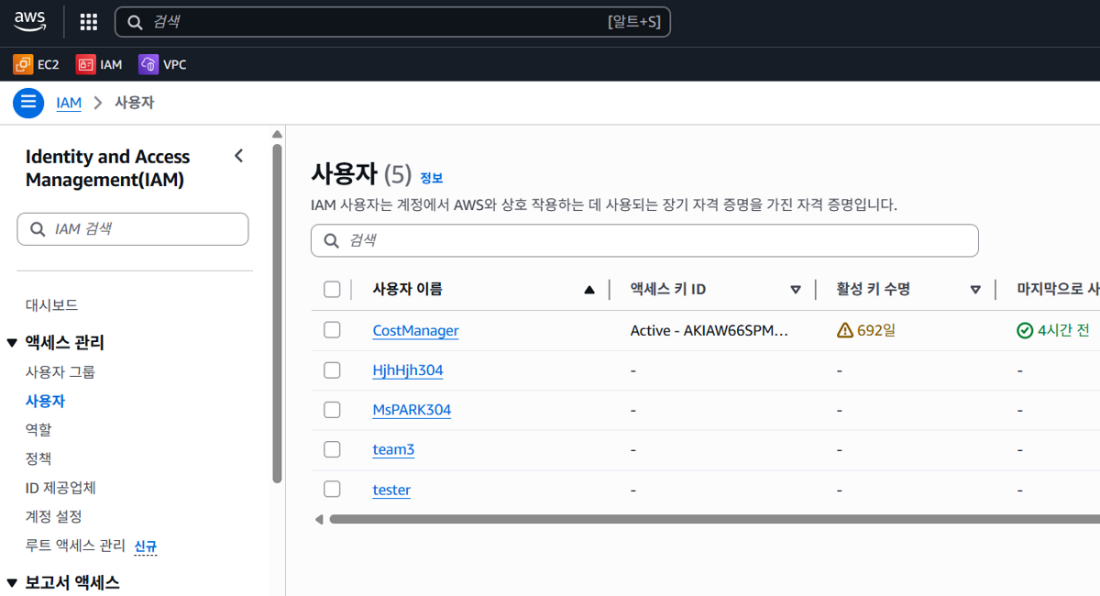
[그림] . team3 사용자의 권한

* + - 1. **해결 방안**

AWS 네트워크 서비스(VPC, Route 53, Direct Connect 등)의 리소스 생성 또는 접근 권한을 가진 새로운 그룹을 생성하고, 네트워크 관리를 위한 별도 IAM 계정을 추가 생성해야 합니다. 네트워크 서비스의 운영 및 관리 시에는 반드시 해당 IAM 계정을 통해 로그인하도록 하여, 권한 관리와 책임 소재를 명확히 하고 계정 별 접근 통제를 구현할 수 있습니다.

* + 1. 기타 서비스 정책 관리
       1. **문제점**

AWS 기타 서비스(CloudWatch, CloudTrail, KMS 등)의 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다. 그러나 서비스별로 관리자 계정이 생성되어 있지 않아 보안에 취약합니다.



[그림] . IAM 사용자 화면



[그림] . team3 사용자의 권한

* + - 1. **해결 방안**

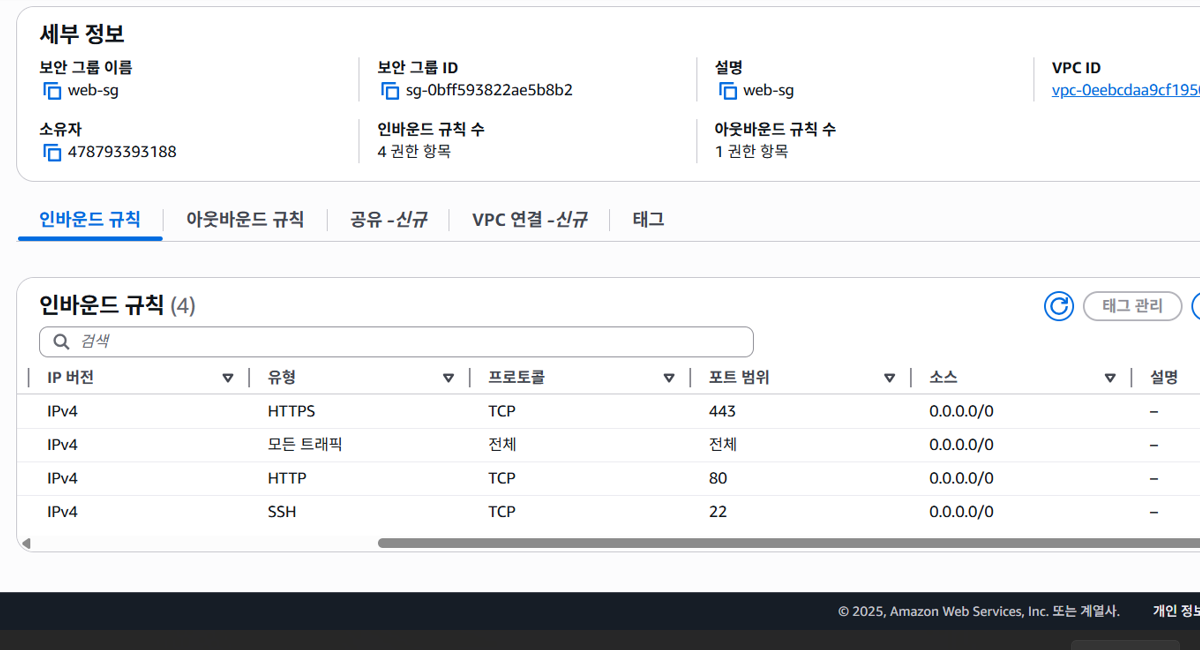
AWS 기타 서비스(CloudWatch, CloudTrail, KMS 등)의 리소스 생성 및 액세스 권한을 가진 그룹을 생성하고, 새로 생성한 IAM 계정을 해당 그룹에 추가해야 합니다. 기타 서비스의 운영 및 관리를 수행할 때는 반드시 해당 IAM 계정으로 로그인하도록 하여, 권한 관리와 책임 소재를 명확히 하고 계정별로 서비스 접근 통제를 구현할 수 있습니다.

* 1. 가상 리소스 관리
     1. 보안 그룹 인/아웃바운드 ANY 설정 관리
        1. **문제점**

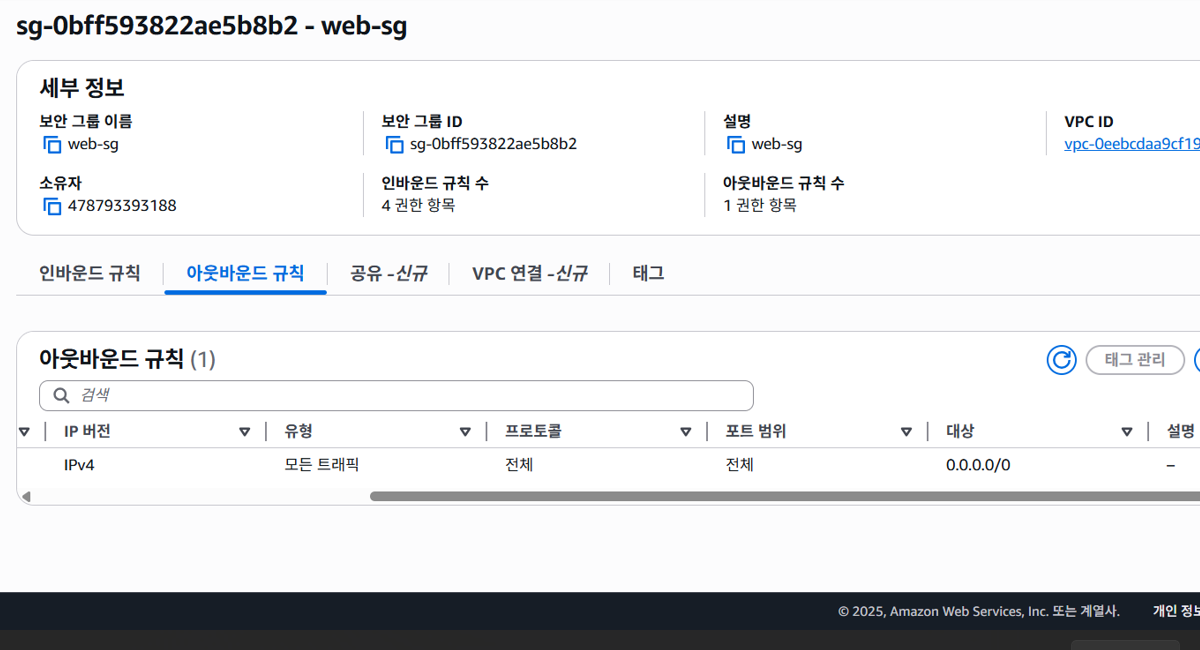
VPC에서의 보안 그룹은 EC2 인스턴스에 대한 인/아웃바운드 트래픽을 제어하는 가상 방화벽 역할을 합니다. 현재 설정이 ANY(모든 포트 및 IP)로 열려 있어 불필요한 접근을 허용하고 있어 보안에 취약한 상태입니다.



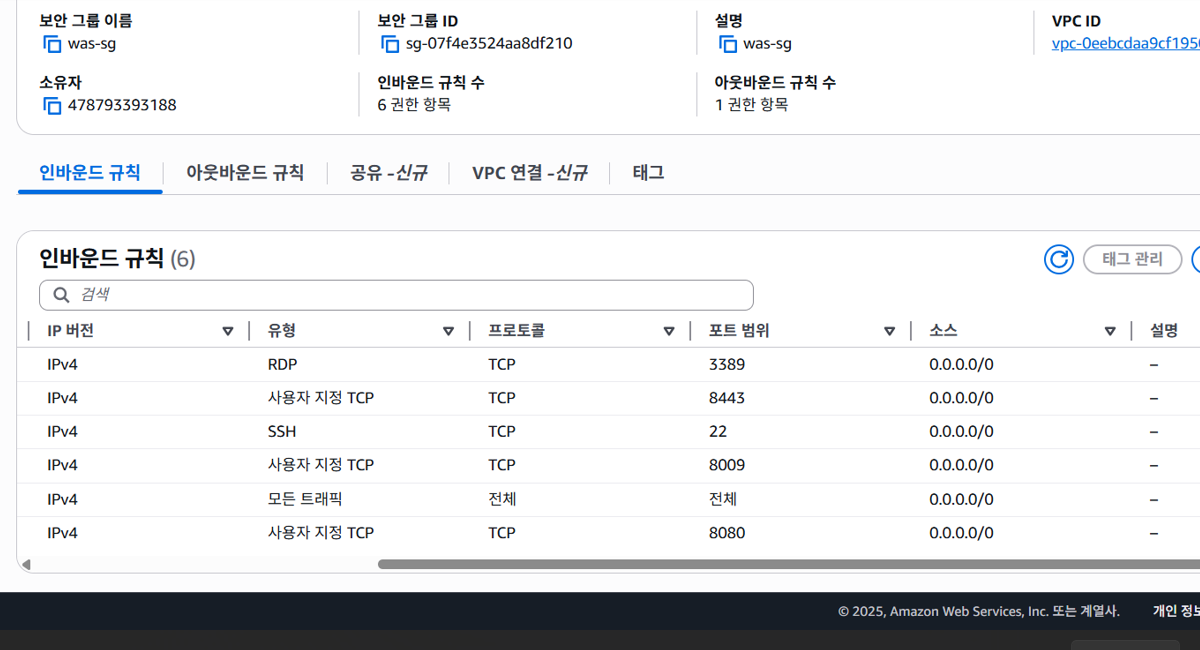
[그림] . EC2 보안그룹



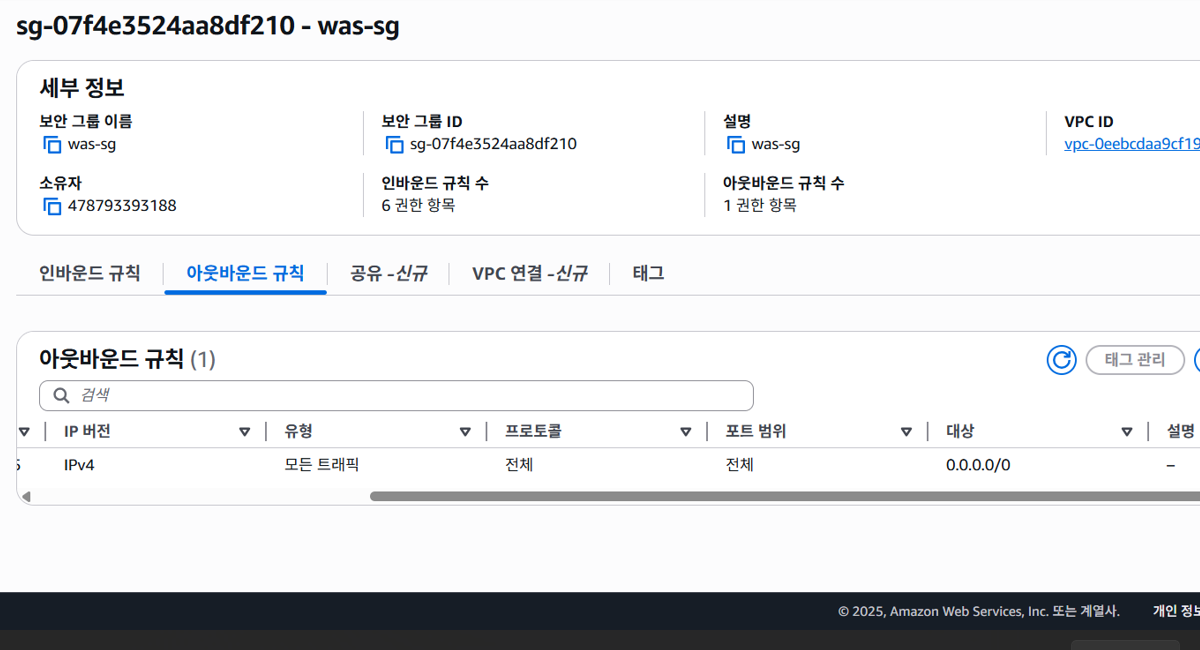
[그림] . WEB-EC2 보안그룹 인바운드



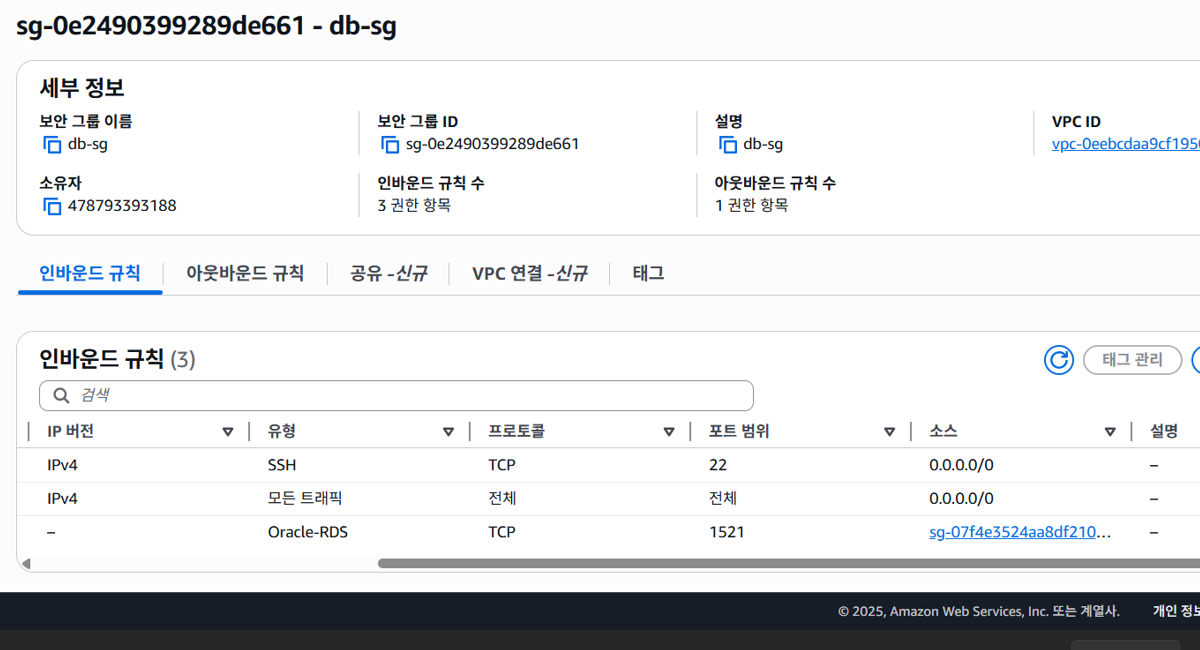
[그림] . WEB-EC2 보안그룹 아웃바운드



[그림] . WAS-EC2 보안그룹 인바운드



[그림] . WAS-EC2 보안그룹 아웃바운드



[그림] . DB-EC2 보안그룹 인바운드



[그림] 24. DB-EC2 보안그룹 아웃바운드

* + - 1. **해결 방안**

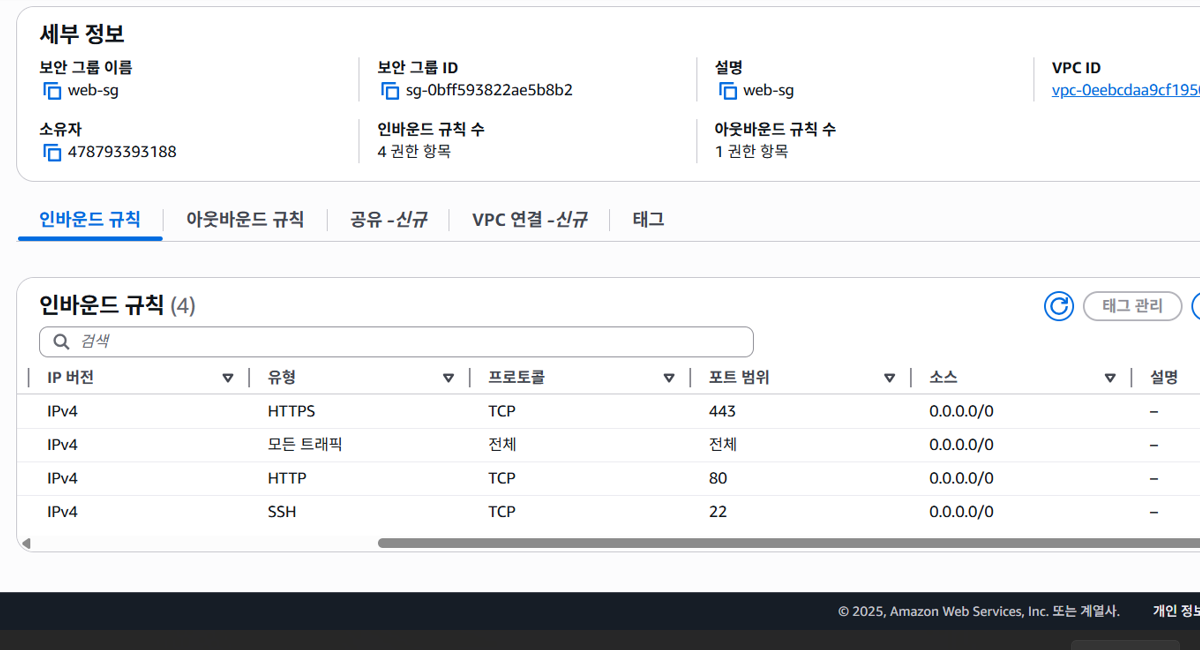
사용 중인 포트들은 허용(Allow)을, 사용 중이지 않은 포트들은 거부(Deny)해야 합니다. 서비스 운영 중 사용이 중단된 포트가 발생할 수 있으므로, 운영 담당자가 인지하지 못한 열린 포트가 없도록 주기적으로 사용 중인 포트를 점검해야 합니다.

* + 1. 보안 그룹 인/아웃바운드 불필요 정책 관리
       1. **문제점**

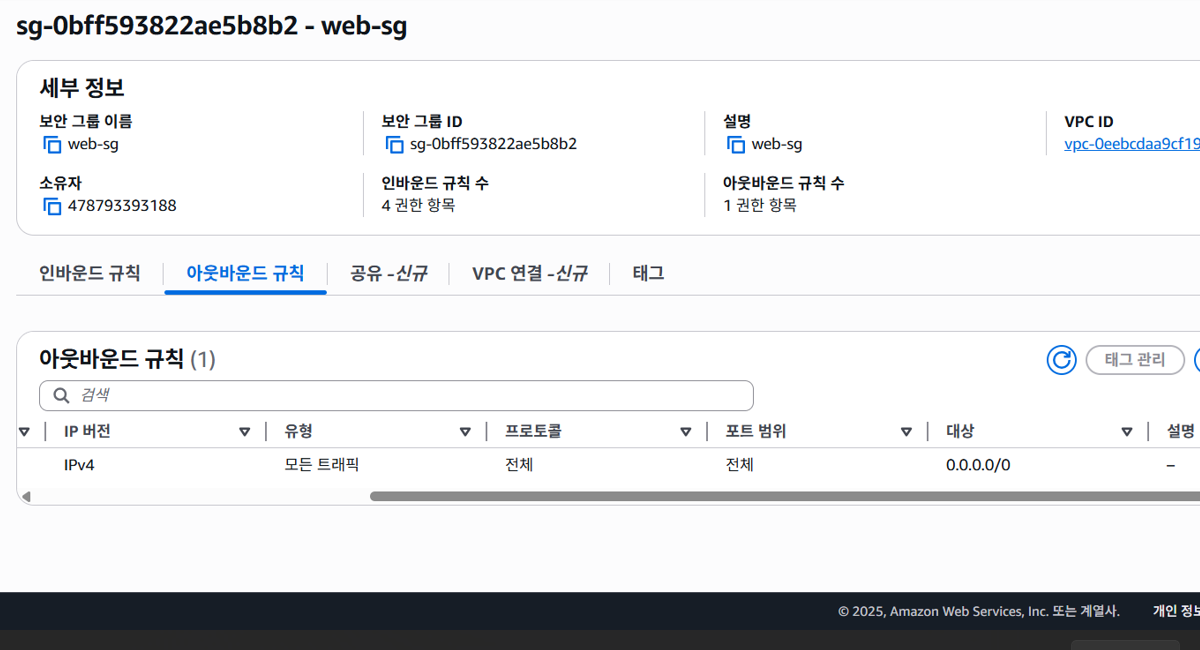
VPC에서의 보안 그룹은 EC2 인스턴스에 대한 인/아웃바운드 트래픽을 제어하는 가상 방화벽 역할을 합니다. 보안 그룹은 인/아웃바운드의 규칙 편집을 통해 특정 소스(출발지)에서의 통신이 가능하도록 유형(네트워크 프로토콜) 및 단일/범위 정책을 설정할 수 있습니다.



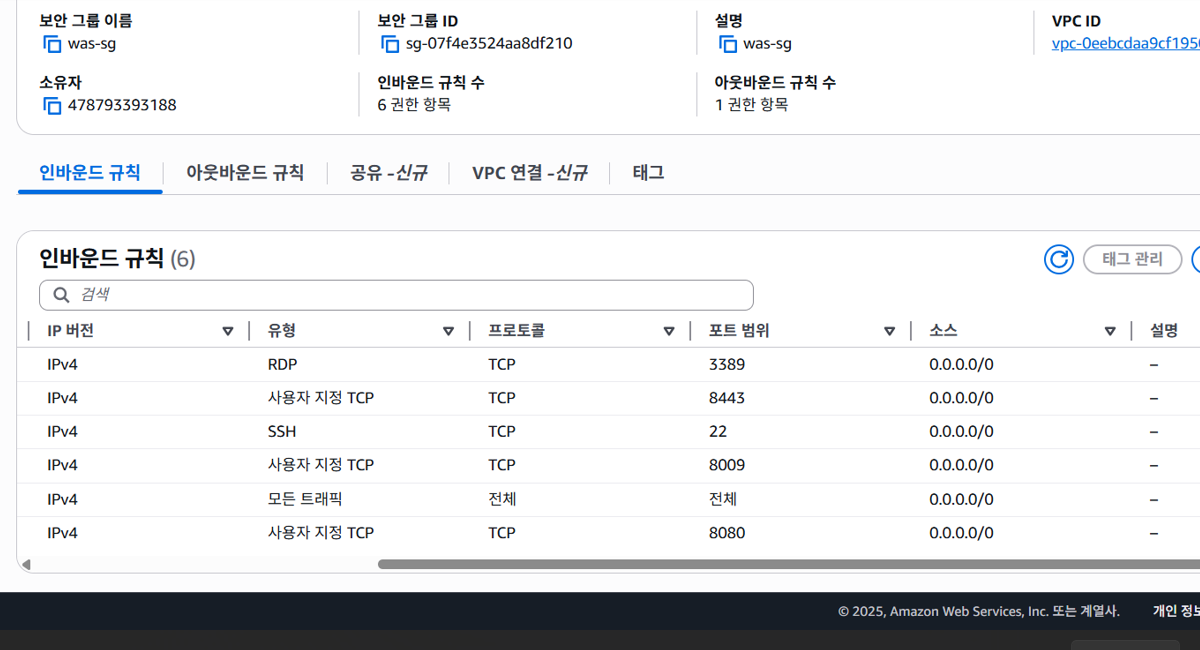
[그림] . EC2 보안그룹



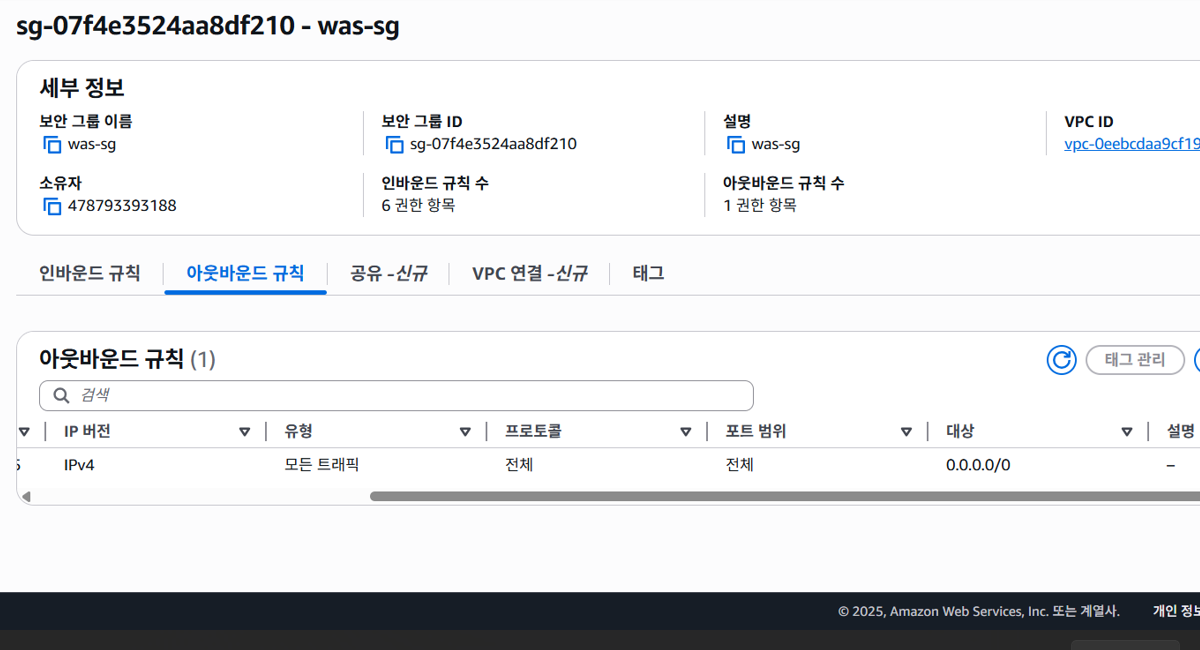
[그림] . WEB-EC2 보안그룹 인바운드



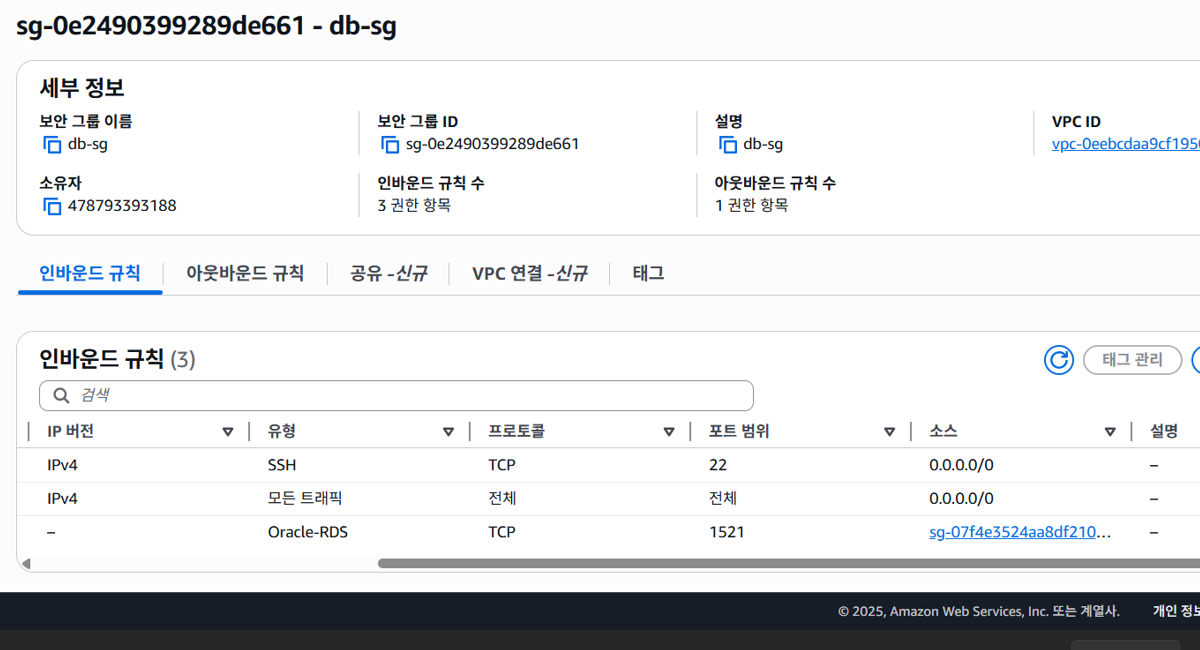
[그림] . WEB-EC2 보안그룹 아웃바운드



[그림] . WAS-EC2 보안그룹 인바운드



[그림] . WAS-EC2 보안그룹 아웃바운드



[그림] . DB-EC2 보안그룹 인바운드



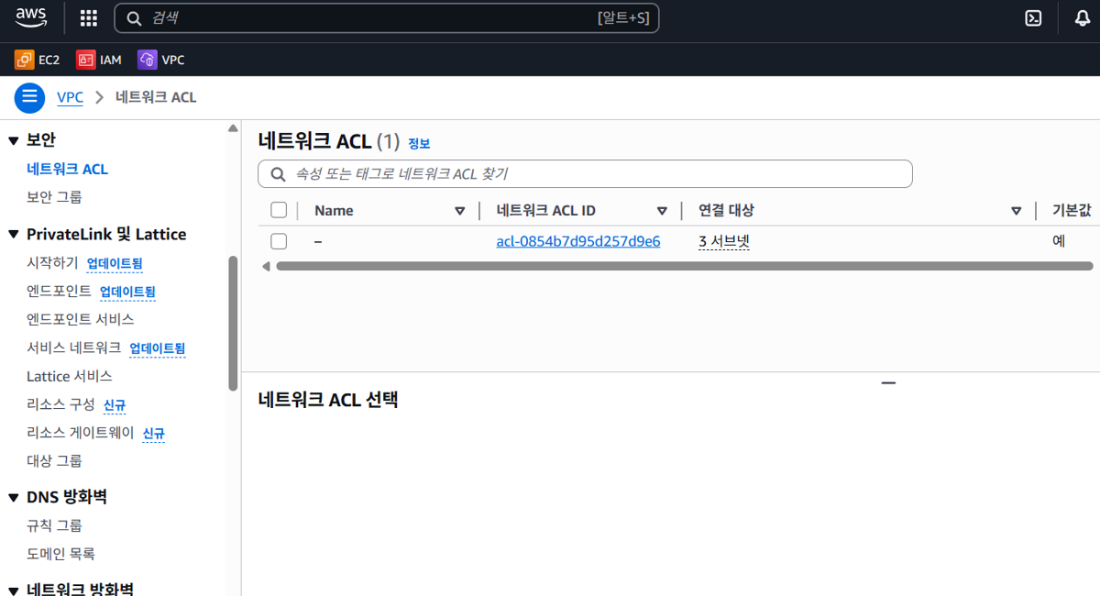
[그림] . DB-EC2 보안그룹 아웃바운드

* + - 1. **해결 방안**

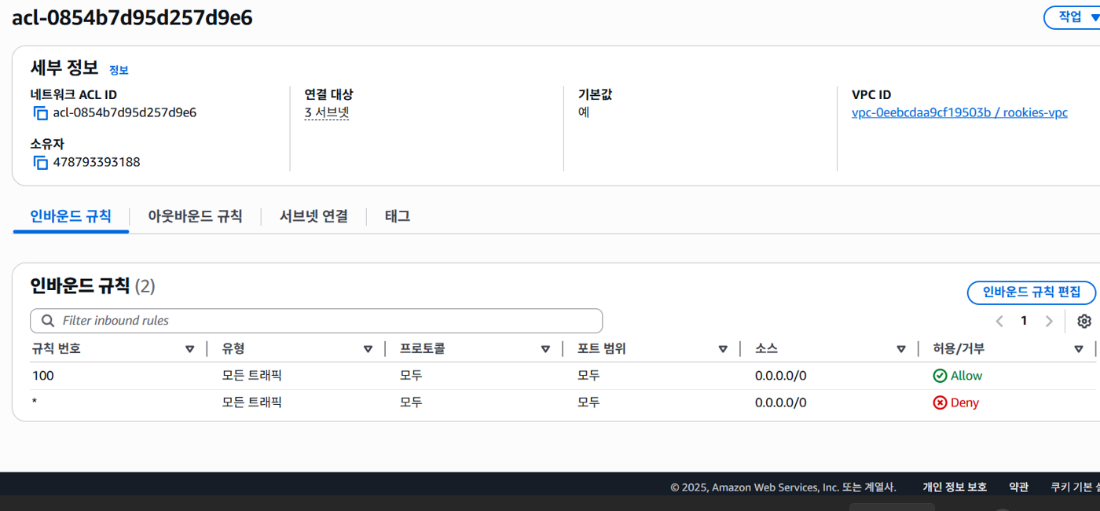
사용 중인 IP 주소들을 점검하여 해당 IP 주소들에 대해서만 인/아웃바운드를 적용시켜야 합니다. 서비스 운영 중 사용이 중단된 포트가 발생할 수 있으므로, 운영 담당자가 인지하지 못한 열린 포트가 없도록 주기적으로 사용 중인 포트를 점검해야 합니다.

* + 1. 네트워크 ACL 인/아웃바운드 트래픽 정책 관리
       1. **문제점**

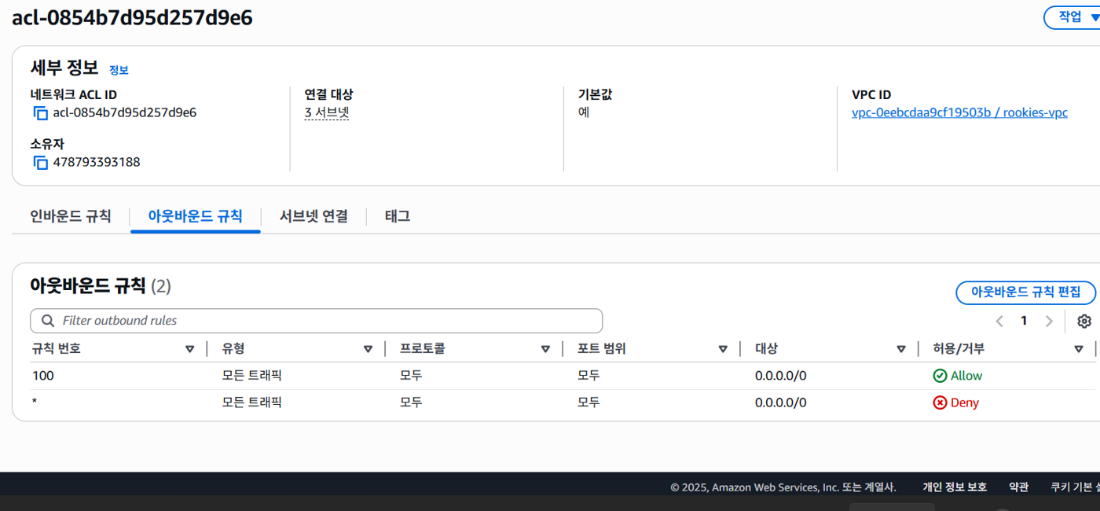
네트워크 ACL(Access Control List)은 1개 이상의 서브넷 내부와 외부의 트래픽을 제어하기 위한 방화벽 역할을 하는 VPC의 선택적 보안 계층입니다. 보안 그룹과 비슷한 규칙으로 네트워크 ACL을 설정하여 VPC에 보안 계층을 더 추가할 수 있습니다. 정책의 방식은 허용(Allow) 및 거부(Deny) 정책(WhiteList 또는 BlackList) 기능으로 Stateless 방식으로 사용됩니다. 보안 그룹의 포트 및 소스의 정책이 ANY로 허용되어 있어, 중요도가 상으로 변경되었습니다.



[그림] . VPC 네트워크 ACL



[그림] . NACL 인바운드 규칙



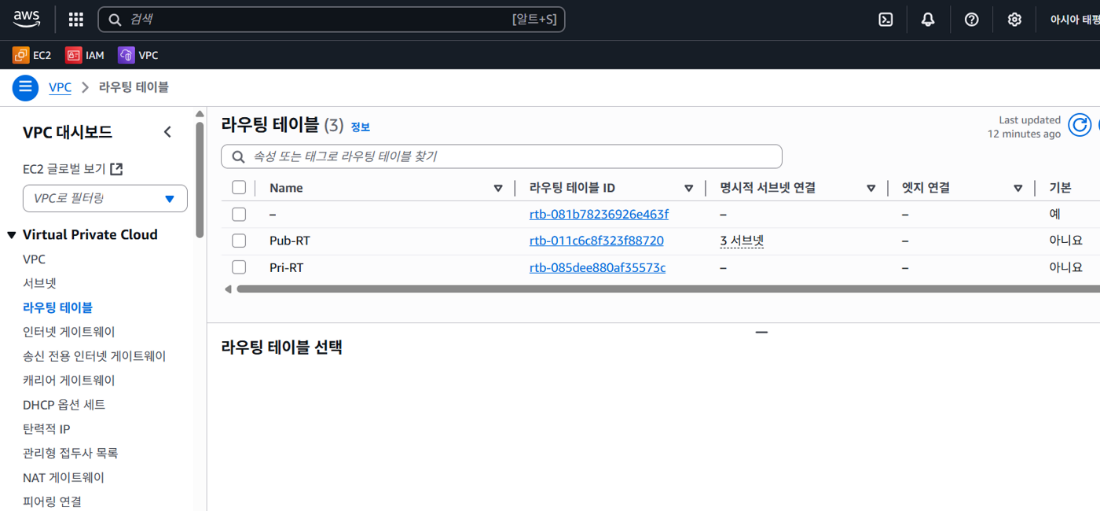
[그림] . NACL 아웃바운드 규칙

* + - 1. **해결 방안**

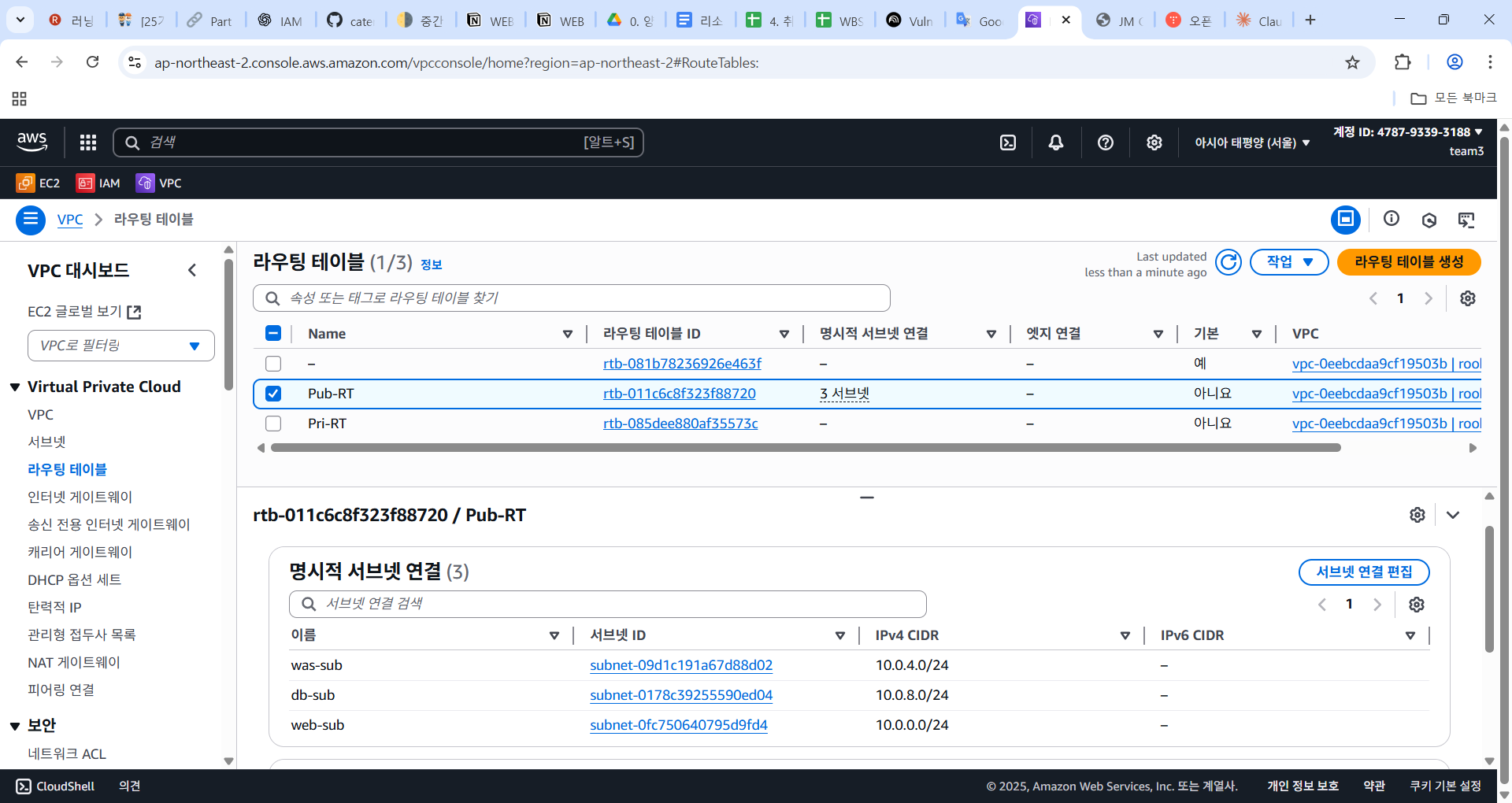
현재 NACL의 인/아웃바운드에 기본 NACL 규칙만 존재하기 때문에 사용 중인 포트와 IP 주소를 확인하여 새로운 NACL의 인/아웃바운드 규칙을 생성해야 합니다. 또한 NACL의 인/아웃바운드 규칙을 생성할 때 보안 그룹의 규칙과 상충하거나, 중복되는 불필요한 규칙이 없는지 확인해야 합니다.

* + 1. 라우팅 테이블 정책 관리
       1. **문제점**

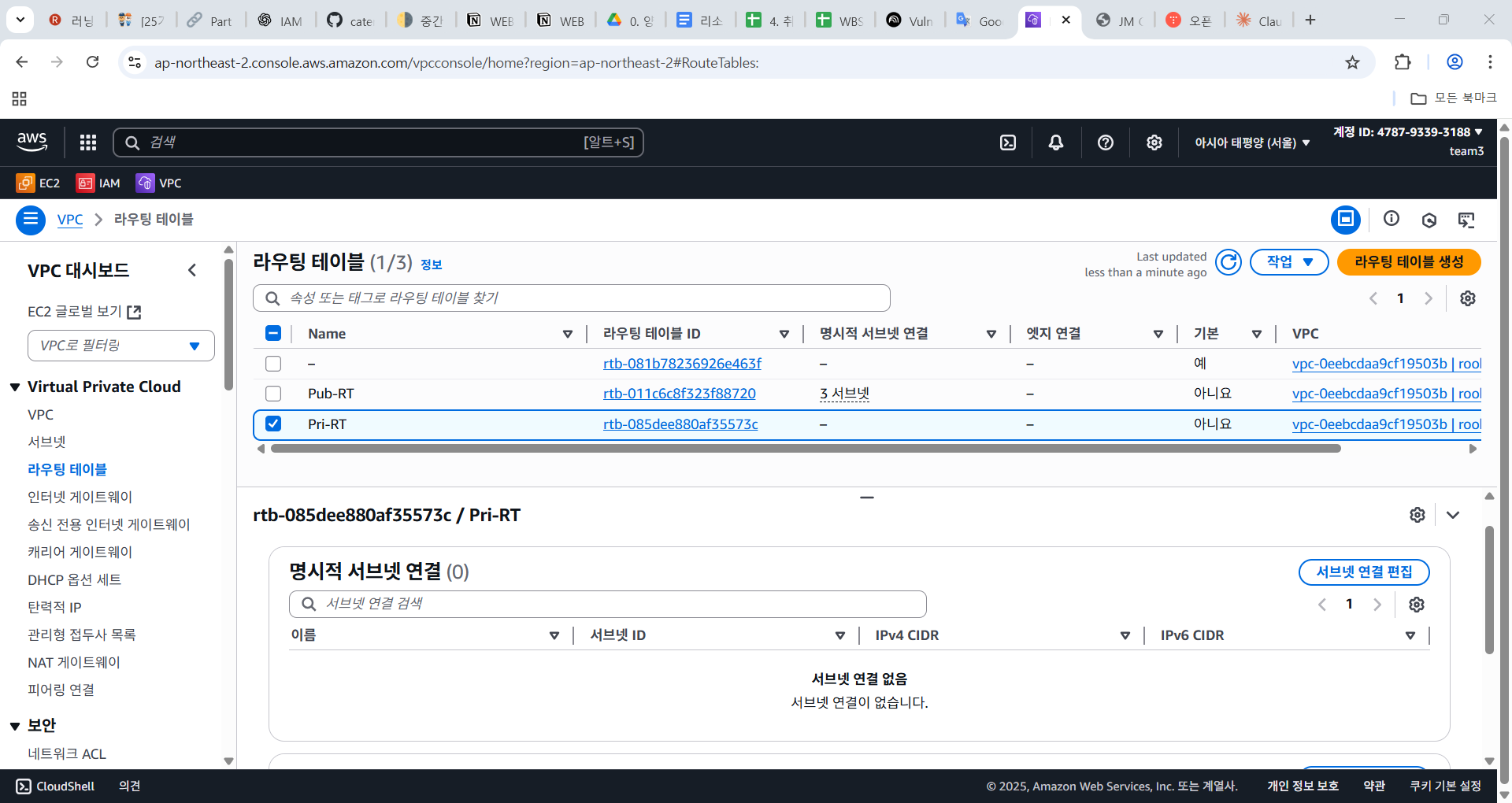
라우팅 테이블은 네트워크 트래픽을 전달할 위치 결정 시 사용되는 규칙입니다. VPC의 각 서브넷을 라우팅 테이블에 연결해야 하며, 라우팅 테이블에서는 서브넷에 대한 라우팅을 제어하게 됩니다. 라우팅 테이블 내 ANY 정책이 설정되어 있지 않고 서비스 타깃 별로 설정해야 보안에 취약하지 않습니다.



[그림] . VPC 라우팅 테이블



[그림] . 퍼블릭 라우팅 테이블의 서브넷 설정



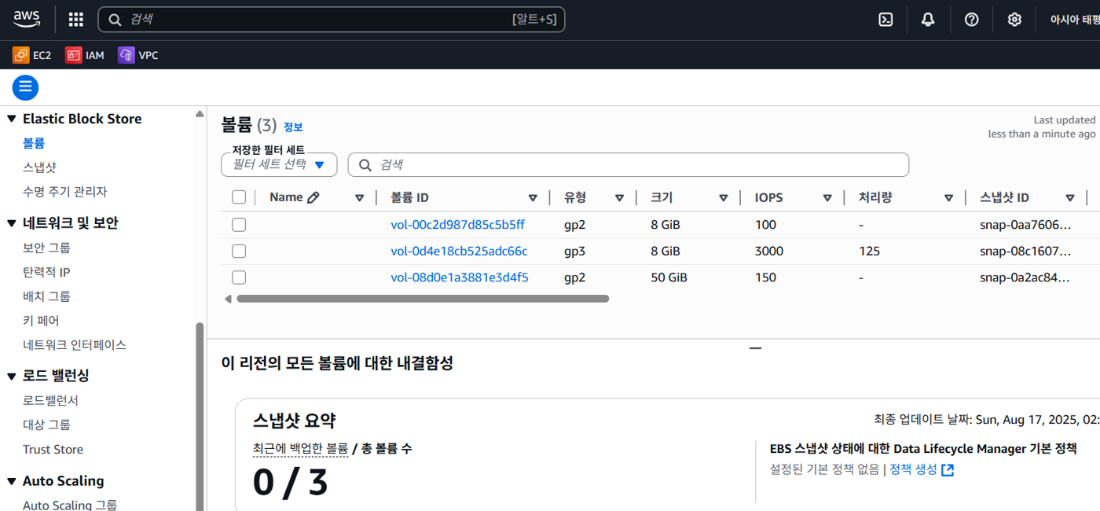
[그림] . 프라이빗 라우팅 테이블의 서브넷 설정

* + - 1. **해결 방안**

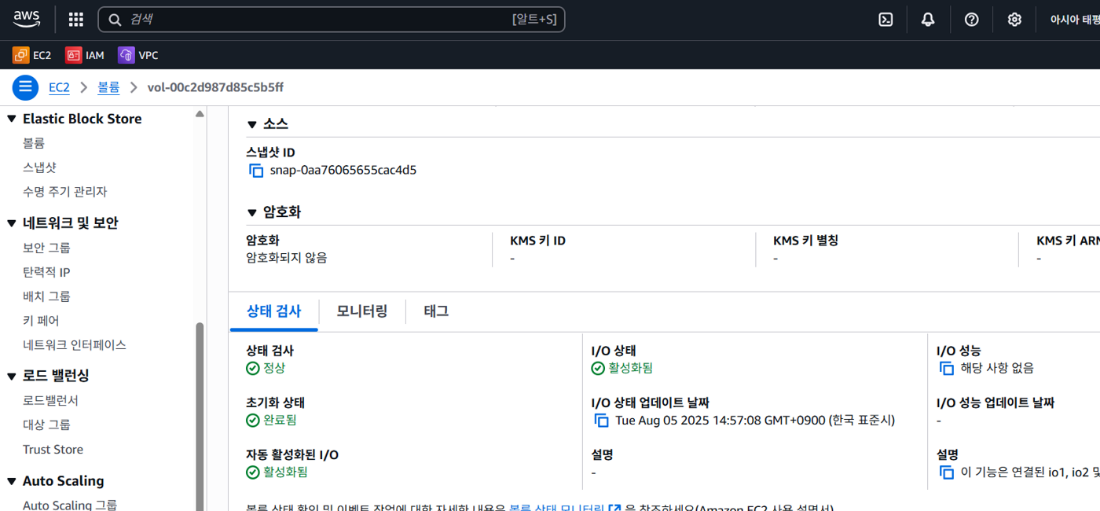
현재 서비스 중인 대상의 IP 주소를 점검하여 라우팅 테이블을 수정해야 합니다. 퍼블릭 라우팅 테이블에 프라이빗 서브넷이 전부 들어가 있기 때문에, 프라이빗 망에 있어야 하는 WAS 인스턴스가 연결된 서브넷이나 DB 인스턴스가 연결된 서브넷은 퍼블릭 라우팅 테이블에서 연결을 끊은 뒤 NAT Gateway를 라우팅한 프라이빗 라우팅 테이블에 연결해야 합니다.

* 1. 운영 관리
     1. EBS 및 볼륨 암호화 설정
        1. **문제점**

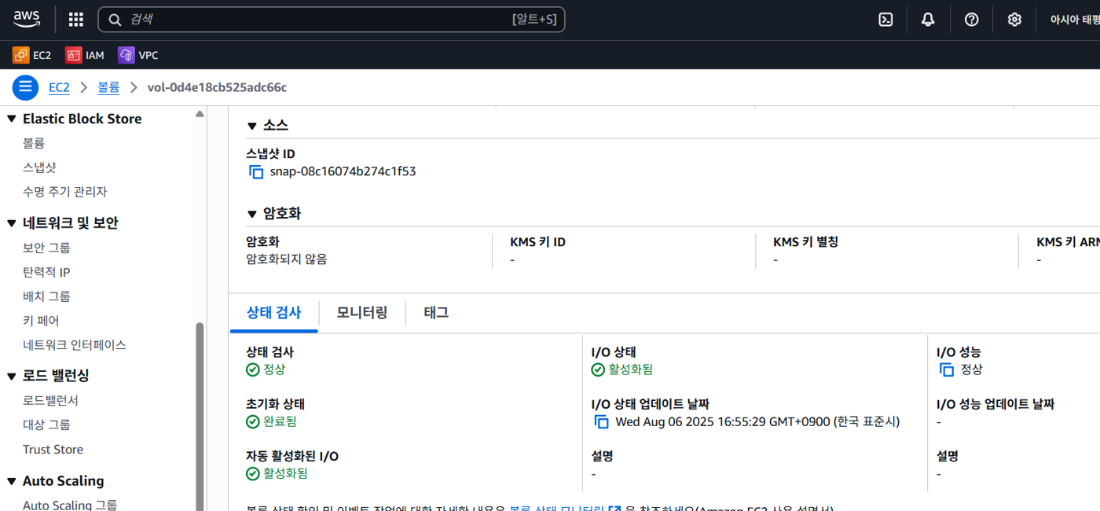
EBS는 EC2 인스턴스 생성 및 이용 시 사용되는 블록 형태의 스토리지 볼륨이며 파일시스템 생성 및 블록 디바이스 사용 등을 할 수 있습니다. EBS를 사용할 때에는 암호화를 사용하여야 보안에 취약하지 않습니다. 확인 결과 EBS를 암호화하지 않고 사용 중이므로 보안에 취약한 상태입니다.



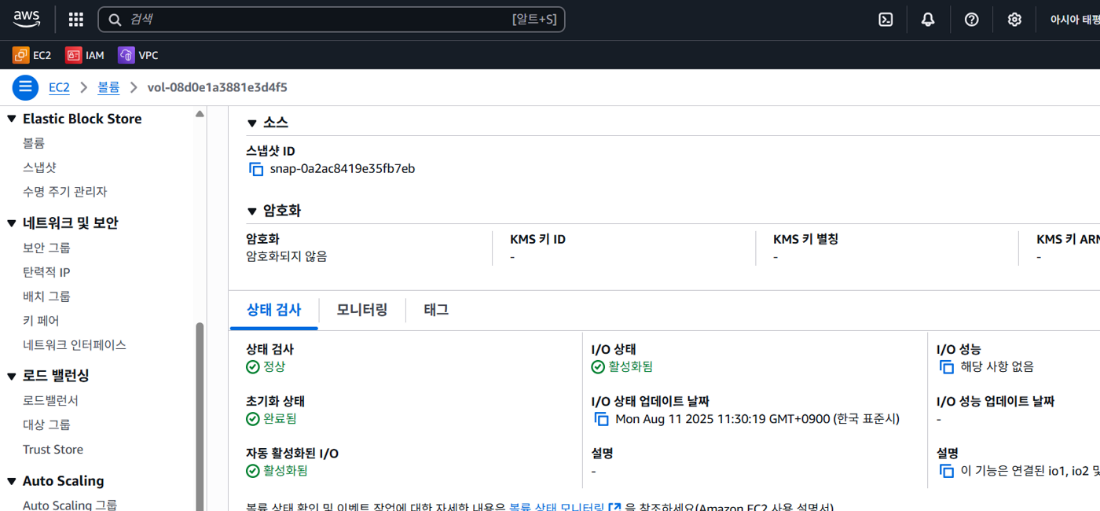
[그림] . EC2 볼륨 화면



[그림] . WEB-EC2 EBS 볼륨 화면



[그림] . WAS-EC2 EBS 볼륨 화면



[그림] . DB-EC2 EBS 볼륨 화면

* + - 1. **해결 방안**

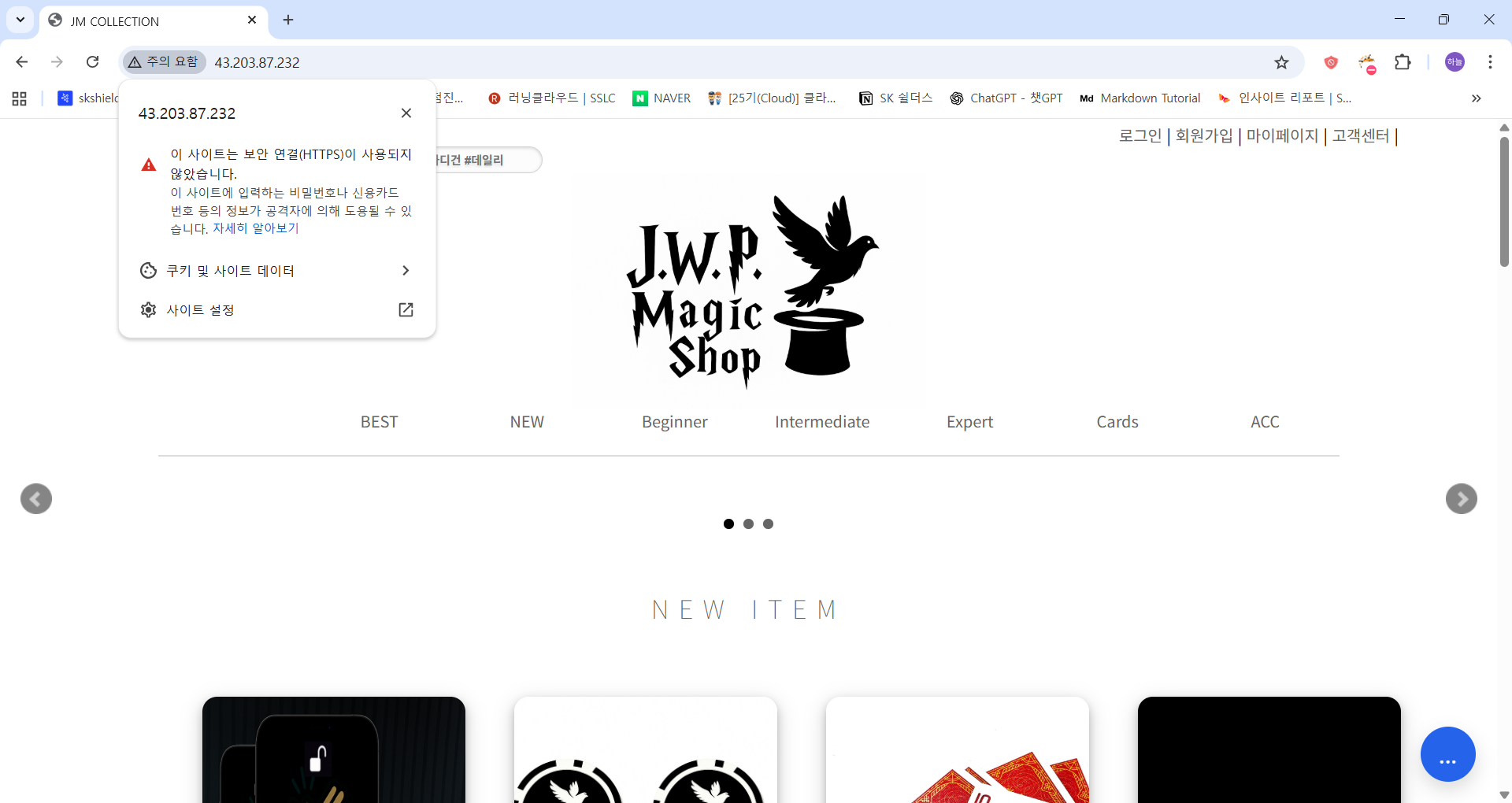
사용 중인 EBS 및 볼륨 리소스에 대해서 암호화를 활성화해야 합니다. 기존의 암호화되지 않은 볼륨은 스냅샷을 만들어 내용을 저장한 뒤, AWS KMS를 이용한 암호화 기능으로 암호화를 설정한 볼륨으로 새로 생성해 다시 연결해야 합니다.

AWS KMS에선 기본적으로 AWS가 자동으로 생성하고 관리하는 기본 키가 있으나, 키에 대한 액세스 제어나 로깅, 로테이션 주기를 관리해야 하며, 특정 유저나 서비스에게만 키 접근을 허용할 필요가 있다면 고객 관리형 KMS 키를 생성하여 설정하여야 합니다.

또한, 앞으로 EBS 및 볼륨 리소스를 생성할 때 기본적으로 암호화하도록 회사의 보안 정책을 수정해야합니다.

* + 1. 통신구간 암호화 설정
       1. **문제점**

클라우드 리소스를 통해 대/내외 서비스에서 정보를 송/수신하는 경우 중간에서 공격자가 패킷을 가로채 공격에 활용하지 못하도록 통신구간을 암호화하여 설정해야 합니다.



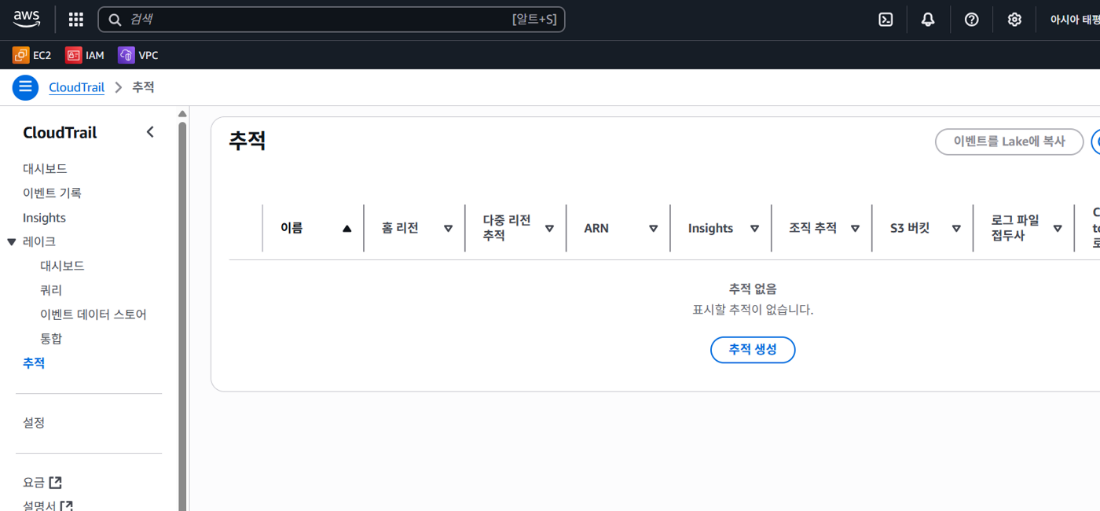
[그림] . 사용되지 않는 HTTPS 인증서

* + - 1. **해결 방안**

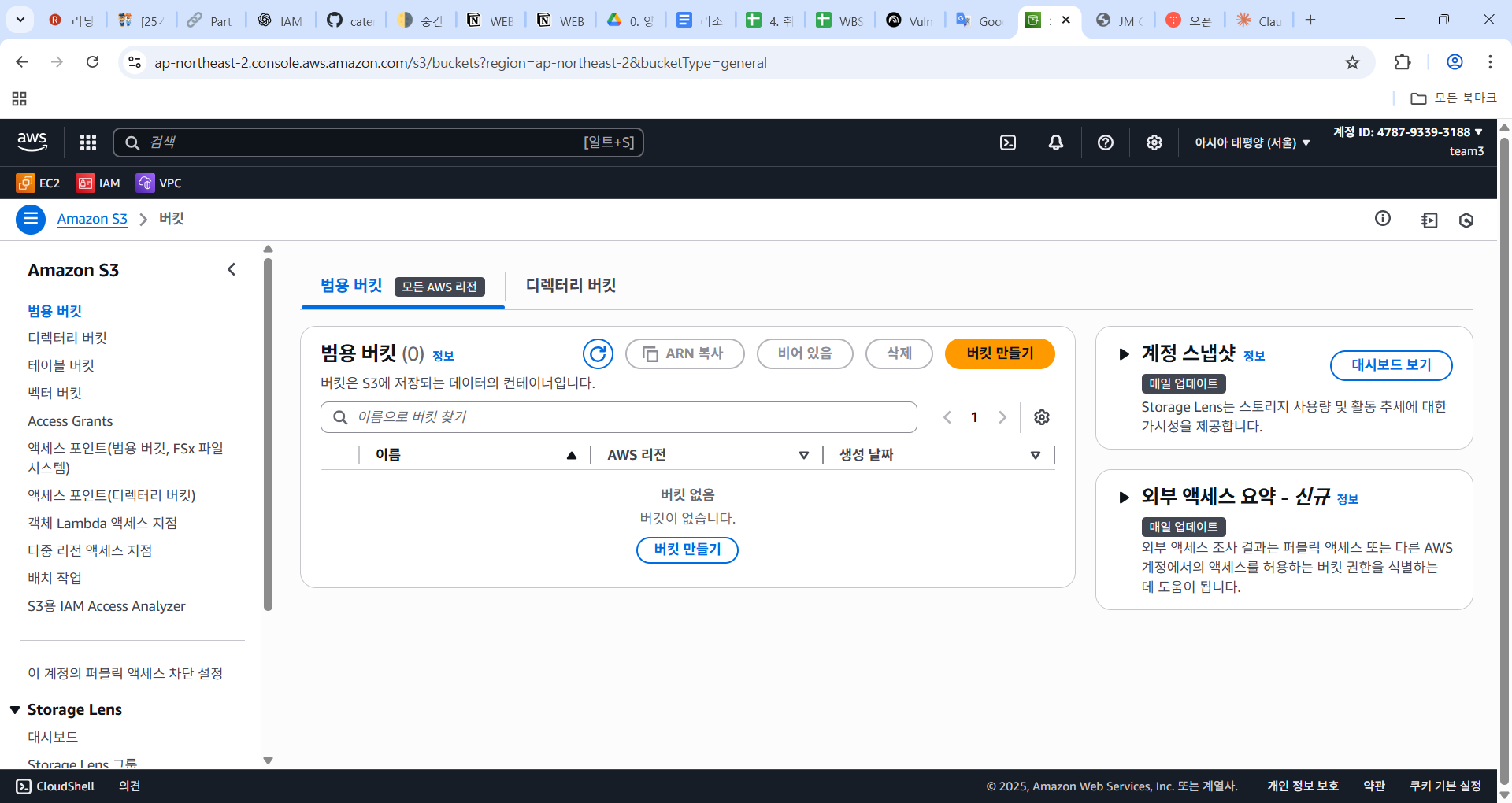
클라우드 리소스의 퍼블릭 통신 구간에는 SSL/TLS 암호화를 적용하여 HTTPS 기반으로 서비스를 제공해야 하며, 신뢰할 수 있는 인증서를 사용해야 합니다. 또한, TLS 1.2 이상 최신 보안 프로토콜을 적용하고, 취약한 암호화 알고리즘 및 구버전 프로토콜은 비활성화해야 합니다.

* + 1. AWS 사용자 계정 로깅 설정
       1. **문제점**

AWS CloudTrail은 계정의 거버넌스, 규정 준수, 운영 및 위험 감사를 활성화하도록 도와주는 서비스로서 사용자, 역할 또는 AWS 서비스가 수행하는 작업들의 이벤트가 기록됩니다. 하지만, 현재 클라우드 환경에서는 CloudTrail과 S3 버킷이 생성되어 있지 않습니다.



[그림] . CloudTrail 추적 화면



[그림] 44. S3 버킷 화면

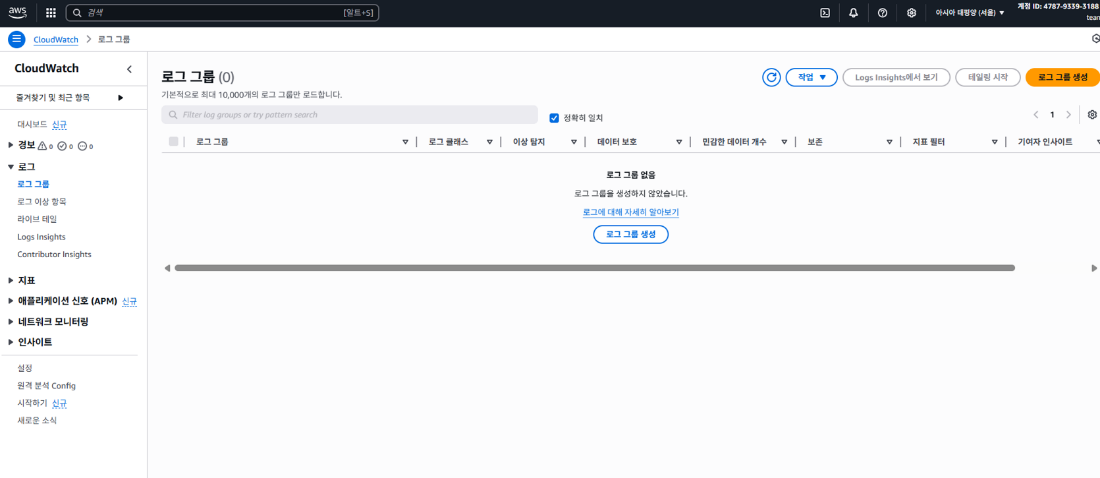
* + - 1. **해결 방안**

CloudTrail에서 추적을 생성하여 AWS 사용자 계정(Console, IAM)에 대한 로깅을 설정해야 합니다. CloudTrail 콘솔에서는 최근 90일간의 Management Event만 확인할 수 있으므로, 그 이상 기간의 로그를 보관하려면 S3 버킷을 생성하여 장기 저장하도록 구성해야 합니다.

* + 1. 인스턴스 로깅 설정
       1. **문제점**

Amazon CloudWatch Logs는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스, AWS CloudTrail, Route 53 및 기타 소스에서 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다.

또한, 가상 인스턴스에 에이전트를 설치하여 로그 그룹에 등록된 로그 스트림을 통해 관련 로그를 확인할 수 있습니다. 하지만, CloudWatch의 로그 그룹이 생성되어 있지 않아 인스턴스 로깅 기능이 설정되지 않은 것으로 확인되었습니다.



[그림] . CloudWatch 화면

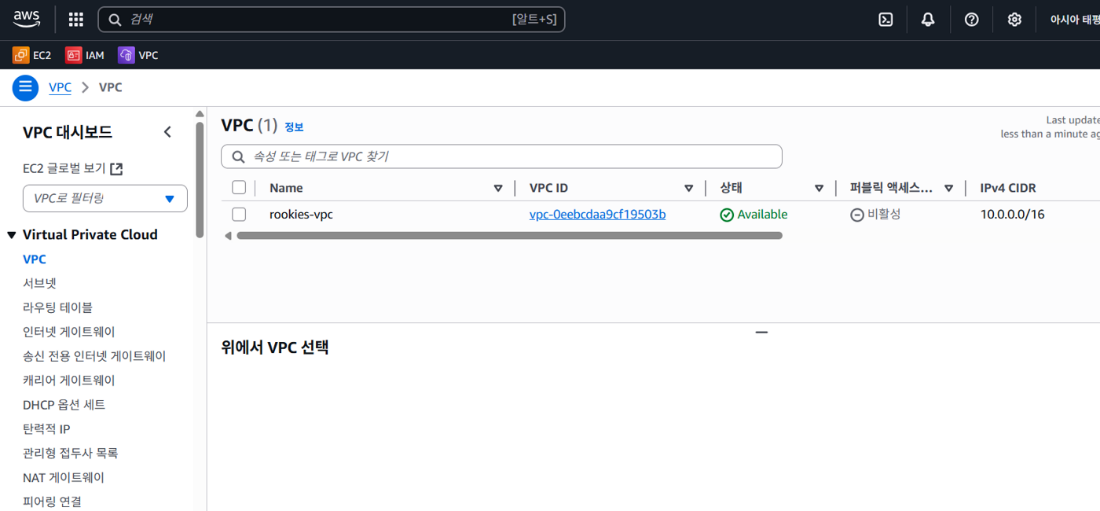
* + - 1. **해결 방안**

EC2 내에 CloudWatch 에이전트를 설치하고 CloudWatch에 로그 그룹을 생성하여 로그 스트림을 보관해야 합니다. 이를 통해 운영 중 발생하는 로그를 중앙에서 통합적으로 모니터링 할 수 있습니다.

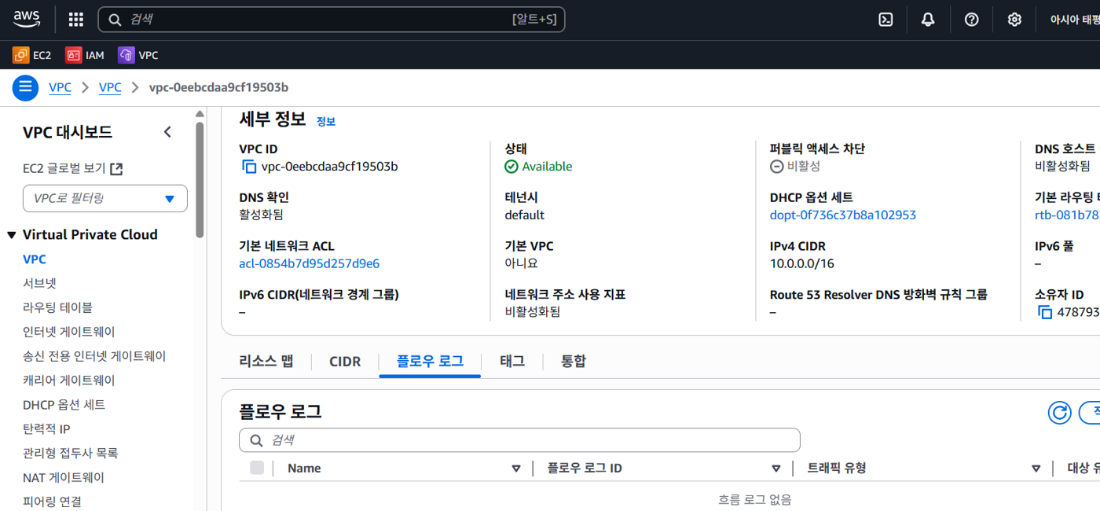
장기 보관과 외부 분석을 위해서 로그를 주기적으로 S3 버킷으로 내보내는 기능을 활성화하는 것이 좋습니다.

* + 1. VPC 플로우 로깅 설정
       1. **문제점**

VPC 플로우 로그는 VPC의 네트워크 인터페이스에서 송/수신되는 IP 트래픽에 대한 정보를 수집할 수 있는 기능으로 VPC, 서브넷 또는 네트워크 인터페이스에 생성할 수 있습니다. 현재 생성된 VPC는 플로우 로깅을 설정하지 않고 있습니다.



[그림] . VPC 화면



[그림] . VPC 플로우 로그 화면

* + - 1. **해결 방안**

VPC 플로우 로그를 생성하여 네트워크 인터페이스에서 송수신 되는 IP 트래픽에 대한 정보를 수집하고 CloudWatch Logs 혹은 S3 버킷에 저장해야 합니다. 보안 사고 발생 시, 플로우 로그를 통해 언제 어디서 어떤 IP가 통신했는지 추적할 수 있습니다.

* + 1. 백업 사용 여부
       1. **문제점**

운영 중인 클라우드 리소스에 대한 시스템 충돌, 장애 발생, 인적 재해 등 기업의 사업 연속성을 해치는 모든 상황에 대비하기 위해 백업 서비스를 구성해서 데이터를 안전하게 보관해야 합니다. 담당자 인터뷰 결과, 백업이 사용되지 않는 것을 확인했습니다.

* + - 1. **해결 방안**

회사에서 백업 및 복구 절차 정책을 수립하고 담당자를 지정해야 합니다. AWS에서는 AWS Backup 서비스를 지원하여, EC2, RDS, EBS, DynamoDB 등 주요 리소스에 대한 자동 백업 정책을 수립하고, 주기적 스케줄링 및 백업 상태를 모니터링할 수 있습니다.

|  |
| --- |
| <백업 및 복구 절차 수립> |
| - 백업 대상(서버 이미지, DB 데이터, 보안로그 등) 선정  - 백업대상별 백업 주기 및 보존기한 정의  - 백업 담당자 및 책임자 지정  - 백업방법 및 절차: 백업시스템 활용, 매뉴얼 방식 등(백업매체 관리 포함)  - 복구절차  - 백업이력관리 (백업 관리 대장)  - 백업 소산에 대한 물리적‧지역적 사항 고려  - 백업 사이트 구축 및 운영 |