



**클라우드 서비스**

**취약점진단 결과보고서**

2021. 5. 24.



**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 정보보호 서약에 대한 사항을 준수 합니다.

목 차

[1. 개요 8](#_Toc35530805)

[1.1. 진단 목적 8](#_Toc35530806)

[1.2. 진단 대상 8](#_Toc35530807)

[1.3. 진단 일정 8](#_Toc35530808)

[1.4. 진단 인력 8](#_Toc35530809)

[2. 진단 항목 및 참조 문서 9](#_Toc35530810)

[3. 취약점진단 결과요약 11](#_Toc35530813)

[3.1. 총평 11](#_Toc35530817)

[3.2. 대상 별 취약점 요약 12](#_Toc35530818)

[4. 취약점진단 상세결과 13](#_Toc35530819)

[4.1. EC2 공통영역 - 계정 보안 13](#_Toc35530820)

[(1) 키 페어 13](#_Toc35530821)

[(2) AWS 접근 패스워드 설정 14](#_Toc35530822)

[(3) Multi Factor 인증 15](#_Toc35530823)

[(4) 액세스 키 16](#_Toc35530824)

[(5) IAM(자격 증명 기반 정책) 계정 보안 17](#_Toc35530825)

[(6) IAM(자격 증명 기반 정책) 보안 정책 설정 (EC2/ECS/ECR) 18](#_Toc35530826)

. **4.2 EC2 공통영역 – 네트워크 보안**

[(1) Security Group 19](#_Toc35530827)

[(2) NACL 20](#_Toc35530828)

[(3) NAT Gateway 21](#_Toc35530829)

[(4) Internet Gateway 22](#_Toc35530830)

[(5) Routing Tables 23](#_Toc35530831)

[(6) Elastic IP 24](#_Toc35530832)

**4.3 RDS 공통영역**

[(1) RDS 리소스 액세스 권한 관리 25](#_Toc35530833)

[(2) RDS API 작업 권한 부여 26](#_Toc35530834)

[(3) 서브넷 가용 영역 27](#_Toc35530835)

[(4) IAM(자격 증명 기반 정책) 보안 정책 설정 (RDS) 28](#_Toc35530836)

[4.4 RDS 옵션정책 39](#_Toc35530847)

[(1) RDS 파라미터 관리 영역 설정 39](#_Toc35530848)

[(2) MariaDB/MySQL 감사 플러그인 설정 40](#_Toc35530849)

**4.5 RDS 로깅**

[(1) MariaDB/MySQL 보안 로그 설정 41](#_Toc35530850)

**4.6 데이터 보안**

[(1) 버킷 접근 보안 42](#_Toc35530851)

[(2) 기본 암호화 설정 43](#_Toc35530852)

[(3) 로그 파일의 수집 및 권한 설정 44](#_Toc35530853)

[(4) IAM(자격 증명 기반 정책) 보안 정책 설정(S3) 45](#_Toc35530854)

개요

* 1. 진단 목적

본 취약점 진단은 **쇼핑몰**에서 운영중인 애플리케이션 서비스를 AWS 클라우드로 구축한 서비스에 클라우드 취약점 진단 체크리스트를 기반으로 주요정보의 전자적 침해 행위에 대한 취약점을 분석ᆞ평가하고, 존재하는 위협 요소에 대해 정확한 분석을 통해 보안대책을 수립 및 취약점을 제거하여 보안 위협을 최소화함으로써 사고 예방 및 안전한 운영에 기여하고자 합니다.

* 1. 진단 대상

|  |  |
| --- | --- |
| AWS 서비스 | 항목명 |
| EC2 | 인스턴스 |
| 키 페어 |
| IAM | 계정 설정 |
| 보안 자격 증명  멀티 팩터 인증 |
| 보안 자격 증명  액세스 키 |
| 사용자 |
| 그룹 |
| 정책 |
| VPC | 보안 그룹 |
| 네트워크 ACL |
| NAT |
| 인터넷 게이트웨이 |
| 라우트 테이블 |
| 탄력적 IP |
| RDS | 파라미터 그룹 |
| 서브넷 그룹 |
| 옵션 그룹 |

* 1. 진단 일정

|  |  |
| --- | --- |
| 업무 수행 내역 | 일정 |
| 사전준비 및 대상 관련 자료 수령 | 2021.05.11이전 |
| 클라우드 구축 | 2021.05.13~2021.05.20 |
| 취약점 진단 및 결과 보고서 작성 | 2021.05.21~05.28 |
| 2차 취약점 진단 및 이행 점검 보고서 작성 | 2021.05.31~2021.06.04 |
| 보고서 최종 수정 및 완료 | 2021.06.07~2021.06.11 |

* 1. 진단 인력

|  |  |  |  |
| --- | --- | --- | --- |
| 이름 | 수행업무 | 연락처 | E-Mail |
| 길효민 | 취약점진단 | 010-4794-0055 | bigjoy22@naver.com |
| 이지선 | 취약점진단 | 010-9555-2873 | wia\_hawm@naver.com |
| 박진환 | 취약점진단 | 010-6676-8229 | [zkzlaptb@naver.com](mailto:zkzlaptb@naver.com) |
| 이지호 | 취약점진단 | 010-7979-3287 | leejeeho6661@naver.com |
| 김경한 | 취약점진단 | 010-0000-0000 | Jobapplication010@gmail.com |

진단 항목 및 참조 문서

참조 문서 - SK 인포섹에서 2019년에 제공한 AWS 취약점 진단 가이드라인 공식 기준을

및 SK 인포섹의 본 문서에서 참조한 <https://docs.aws.amazon.com/index.html#lang/ko_kr> 해당 문서 바탕으로 취약점 진단 시행했습니다

※ 취약점 심각도

상 : 관리자 계정 및 주요 정보 유출로 인한 치명적인 피해 발생

중 : 노출된 정보를 통해 서비스/시스템 관련 추가 정보 유출 발생

하 : 타 취약점과 연계 가능한 잠재적인 위협 내재

진단에 사용될 항목은 OWASP[[1]](#endnote-1), NIST[[2]](#endnote-2), 행정안전부 등에서 권고하는 내용을 기반으로 본 프로젝트와 연관성이 있는 보안상의 문제점을 주축으로 총 8개 분류 27개 항목의 체크리스트로 수립한 항목입니다.

| **분류** | **취약점 번호** | **세부 진단 항목** | **심각도** |
| --- | --- | --- | --- |
| EC2 공통영역- 계정보안 | **1-1** | 키 페어 | 상 |
| **1-2** | AWS 접근 패스워드 설정 | 상 |
| **1-3** | Multi Factor 인증 | 중 |
| 1-4 | 액세스 키 | 상 |
| 1-5 | IAM(자격 증명 기반 정책) 계정 보안 | 하 |
| **1-6** | IAM(자격 증명 기반 정책) 보안 정책 설정 (EC2/ECS/ECR) | 상 |
| **EC2 공통영역 – 네트워크 보안** | 2-1 | Security Group | 중 |
| 2-2 | NACL | 중 |
| 2-3 | NAT Gateway | 하 |
| 2-4 | Internet Gateway | 하 |
| 2-5 | Routing Tables | 중 |
| 2-6 | Elastic IP | 하 |
| **RDS 공통영역** | 3-1 | RDS 리소스 액세스 권한 관리 | 중 |
| 3-2 | RDS API 작업 권한 부여 | 중 |
| 3-3 | 서브넷 가용 영역 | 하 |
| 3-4 | IAM(자격 증명 기반 정책) 보안 정책 설정 (RDS) | 상 |
| **RDS 옵션정책** | 4-1 | RDS 파라미터 관리 영역 설정 | 하 |
| **4-2** | MariaDB/MySQL 감사 플러그인 설정 | 하 |
| **RDS 로깅** | 5-1 | MariaDB/MySQL 보안 로그 설정 | 하 |
| **데이터 보안** | 6-1 | 버킷 접근 보안 | 중 |
| 6-2 | 기본 암호화 설정 | 상 |
| 6-3 | 로그 파일의 수집 및 권한 설정 | 중 |
| 6-4 | IAM(자격 증명 기반 정책) 보안 정책 설정(S3) | 상 |

취약점진단 결과요약

3. 1. 총평

본 취약점은 AWS에서 구축하고 진행하였으며

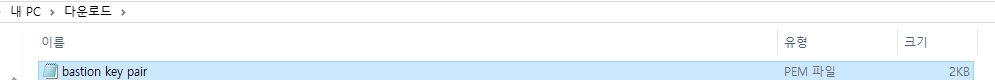
**1개의 IAM 계정만 제공되어 루트 계정을 요하는 권한 상승 등의 일부 항목은 진단에서 제외하였습니다.**

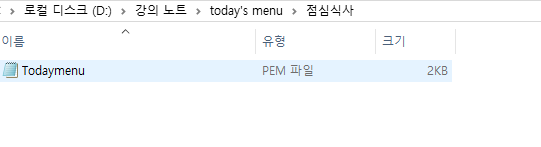
* 1. 대상 별 취약점 요약

| 대상 구역 | 취약점  심각도 | 취약점 명칭 | 개수 | 조치 이후 취약점 개수 |
| --- | --- | --- | --- | --- |
| IAM/EC2 | 상 | 키 페어 | **2** | **0** |
| 중 | Multi Factor 인증 | **1** | **0** |
| VPC | 중 | Security Group | 2 | 0 |
| 중 | NACL | 1 | 0 |
| 하 | Elastic IP | 1 | 0 |
| RDS | 하 | 서브넷 가용 영역 | 1 | 0 |
| 하 | RDS 파라미터 관리 영역 설정 | 2 | 0 |
| 하 | MariaDB/MySQL 감사 플러그인 설정 | 1 | 0 |
| S3/IAM | 중 | 버킷 접근 보안 | N/A | 사용하지 않은 상품 |
| 상 | 기본 암호화 설정 | N/A | 사용하지 않은 상품 |
| 중 | 로그 파일의 수집 및 권한 설정 | N/A | 사용하지 않은 상품 |

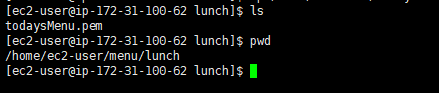
취약점진단 상세결과

* 1. EC2 공통영역 - 계정 보안
     1. 키 페어
        1. **조치 내용 (조치 완료)**

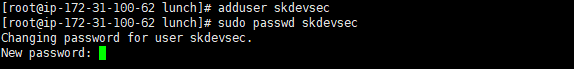




[그림] 테스트 파일 확인



[그림] 테스트 파일 확인



* + - 1. **관련 URL**

| **경로** | **URL** |
| --- | --- |
| EC2 – Instance – 상세 정보 | https://us-west-1.console.aws.amazon.com/ec2/v2/home?region=us-west-1#Instances: |

* + - 1. **조치 결과**

# \*.PEM 키 페어를 최대한 식별할 수 없게, 쉽게 유추할 수 없는 통로로 이동

실제 ec2 리눅스에서는 windows와 마찬가지로 유추할 수 없는 통로와 파일 이름으로 수정했습니다

기본 사용자 외에 다른 사용자를 추가하고 비밀번호를 특수문자 영문 숫자 조합으로 다시 만들었습니다

* + 1. Multi Factor 인증 (조치 완료)
       1. **조치 내용**



[그림] 테스트 파일 확인



[그림] 테스트 파일 확인

* + - 1. **관련 URL**

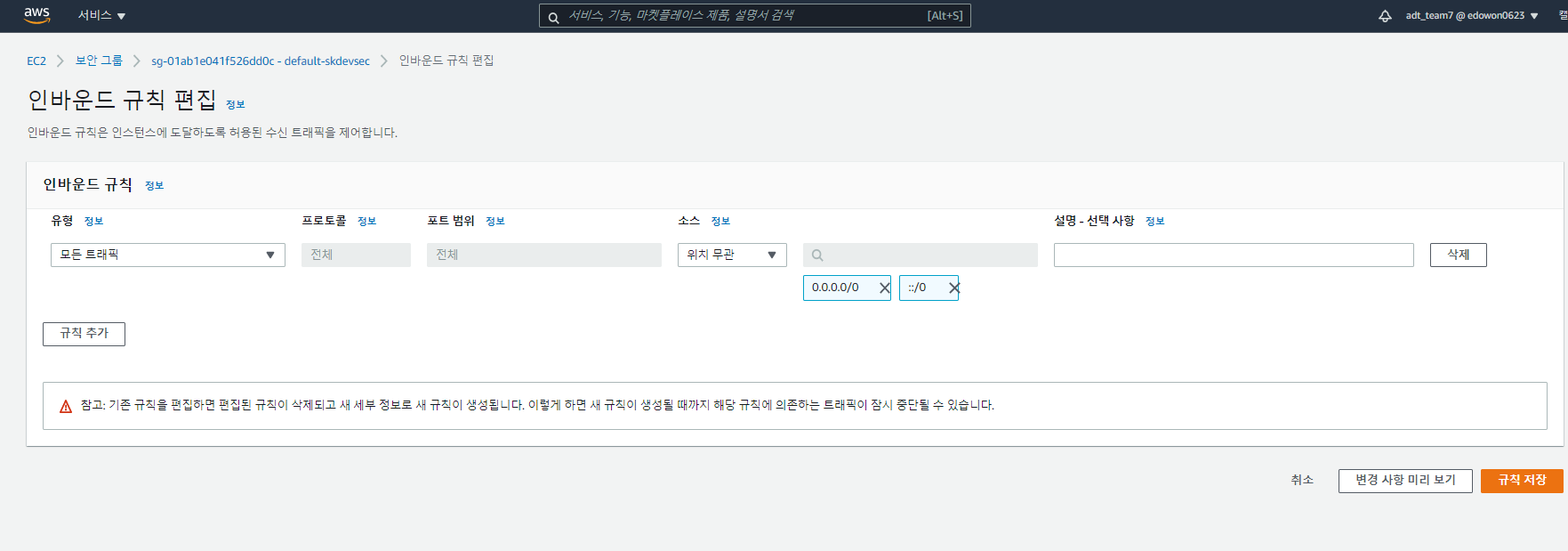
| **경로** | **URL** |
| --- | --- |
| 우측 상단 내 정보 – 내 보안 자격 증명 | https://console.aws.amazon.com/iam/home?region=us-west-1#/security\_credentials |

* + - 1. **조치 결과**

상단 우측 메뉴 클릭 후 내 보안 자격 증명으로 들어가서 MFA를 활성화 시키고

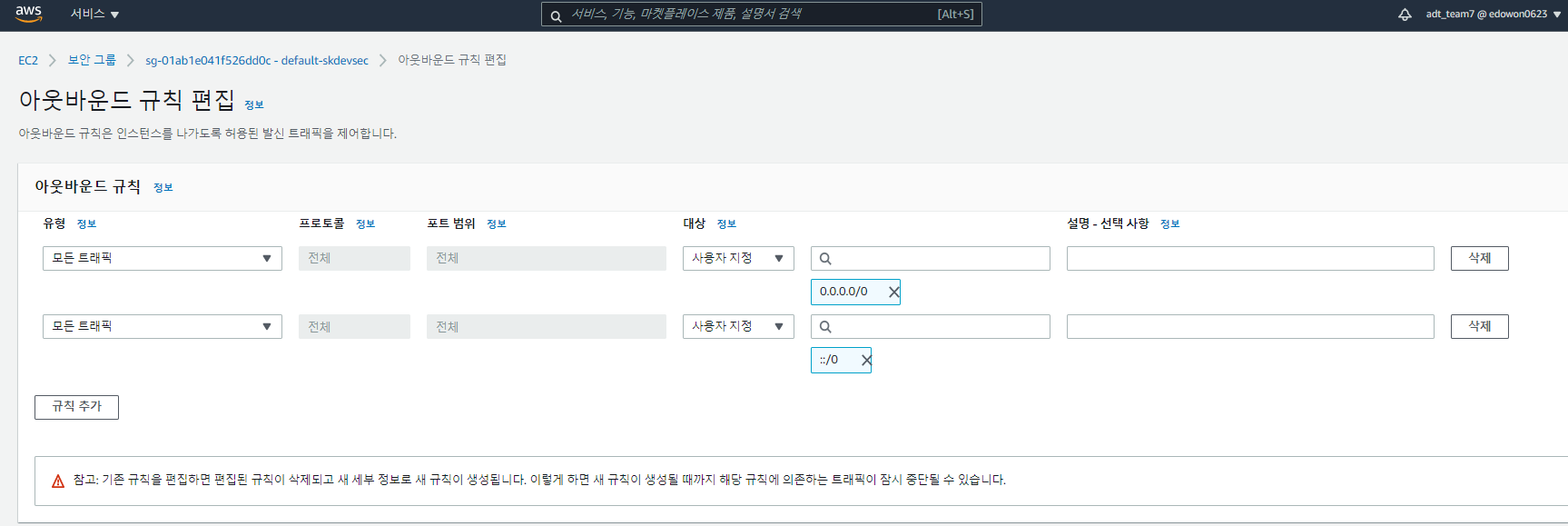
관련 설정대로 글 OTP 어플을 설치한 다음 디바이스를 등록해주면 조치가 완성됩니다

* 1. EC2 공통영역 - 네트워크 보안
     1. Security Group (조치 완료)
        1. **조치 내용**



[그림] 테스트 파일 확인

[그림] 테스트 파일 확인



[그림] 테스트 파일 확인

[그림] 테스트 파일 확인

* + - 1. **관련 URL**

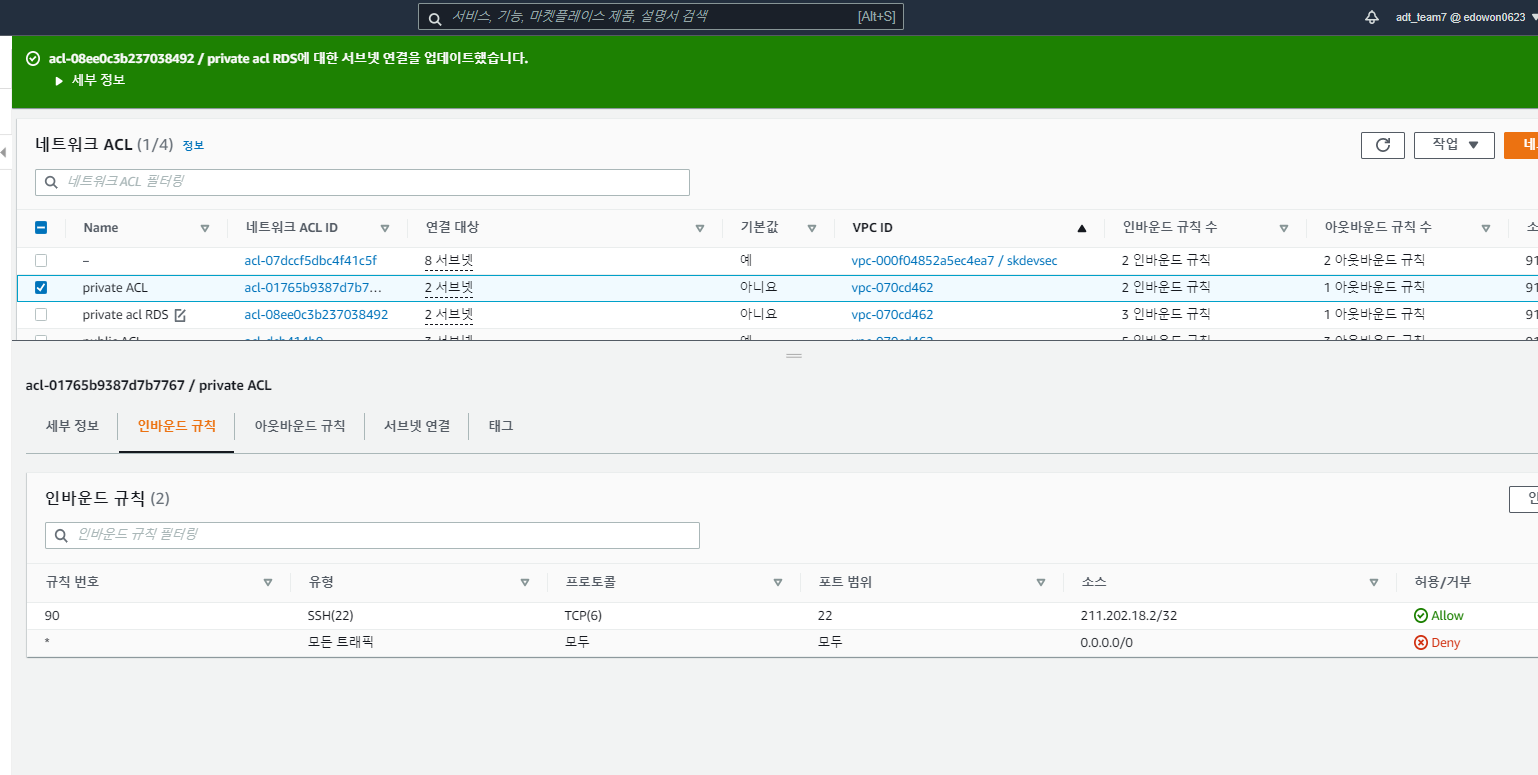
| **경로** | **URL** |
| --- | --- |
| EC2 – 인스턴스 – 인스턴스 세부 정보 | https://us-west-1.console.aws.amazon.com/ec2/v2/home?region=us-west-1#Instances: |
| EC2 – 보안 그룹 – 보안 그룹 세부 정보 | https://us-west-1.console.aws.amazon.com/ec2/v2/home?region=us-west-1#SecurityGroups: |

* + - 1. **조치 결과**

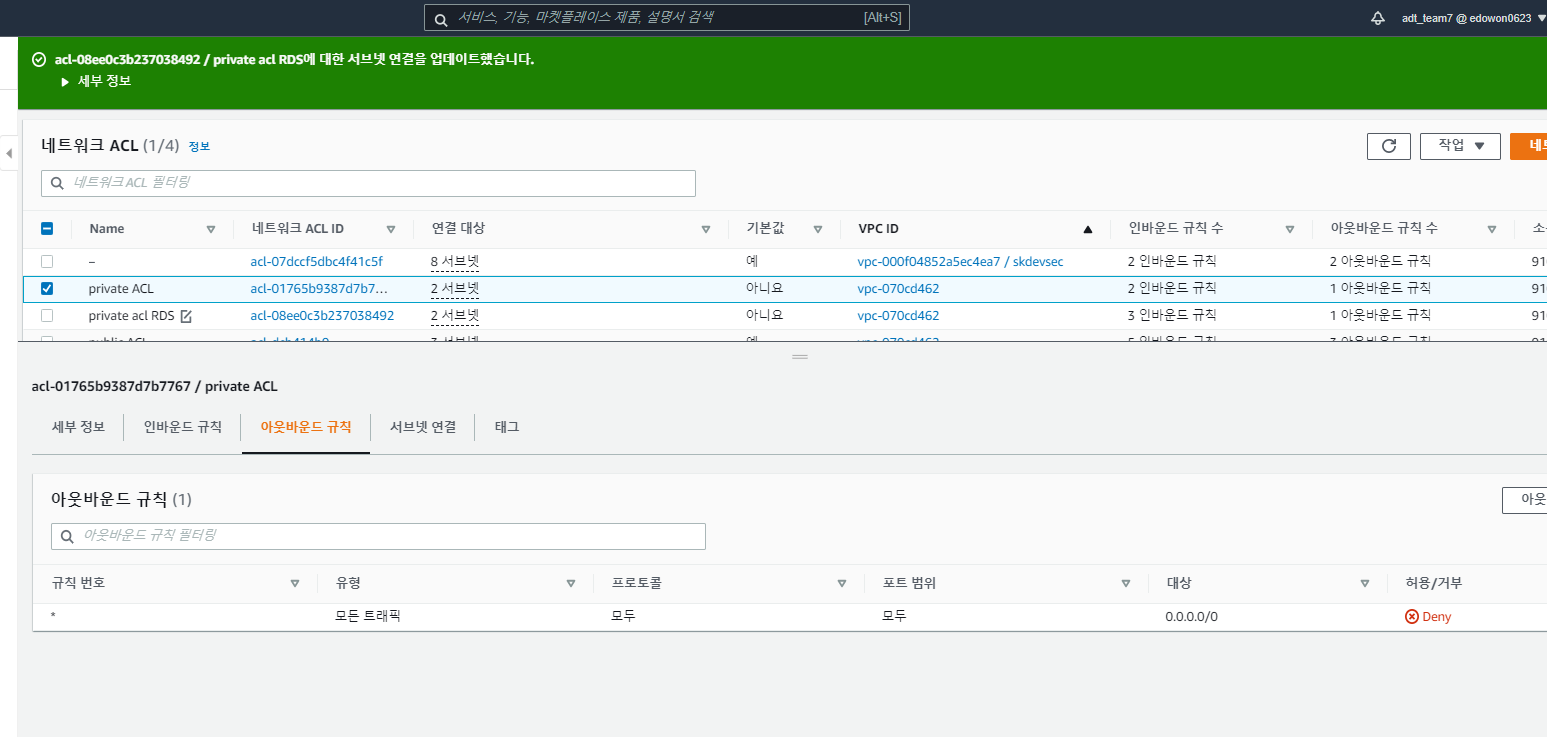
**내부에서 사용할 자원이 포함된 ec2 인스턴스 단위들은 해당 포트와 ip들로만 설정했고**

**나머지 웹 서비스의 가동을 위해서 http 80포트와 https 443포트만 인스턴스 단에서 허용했음**

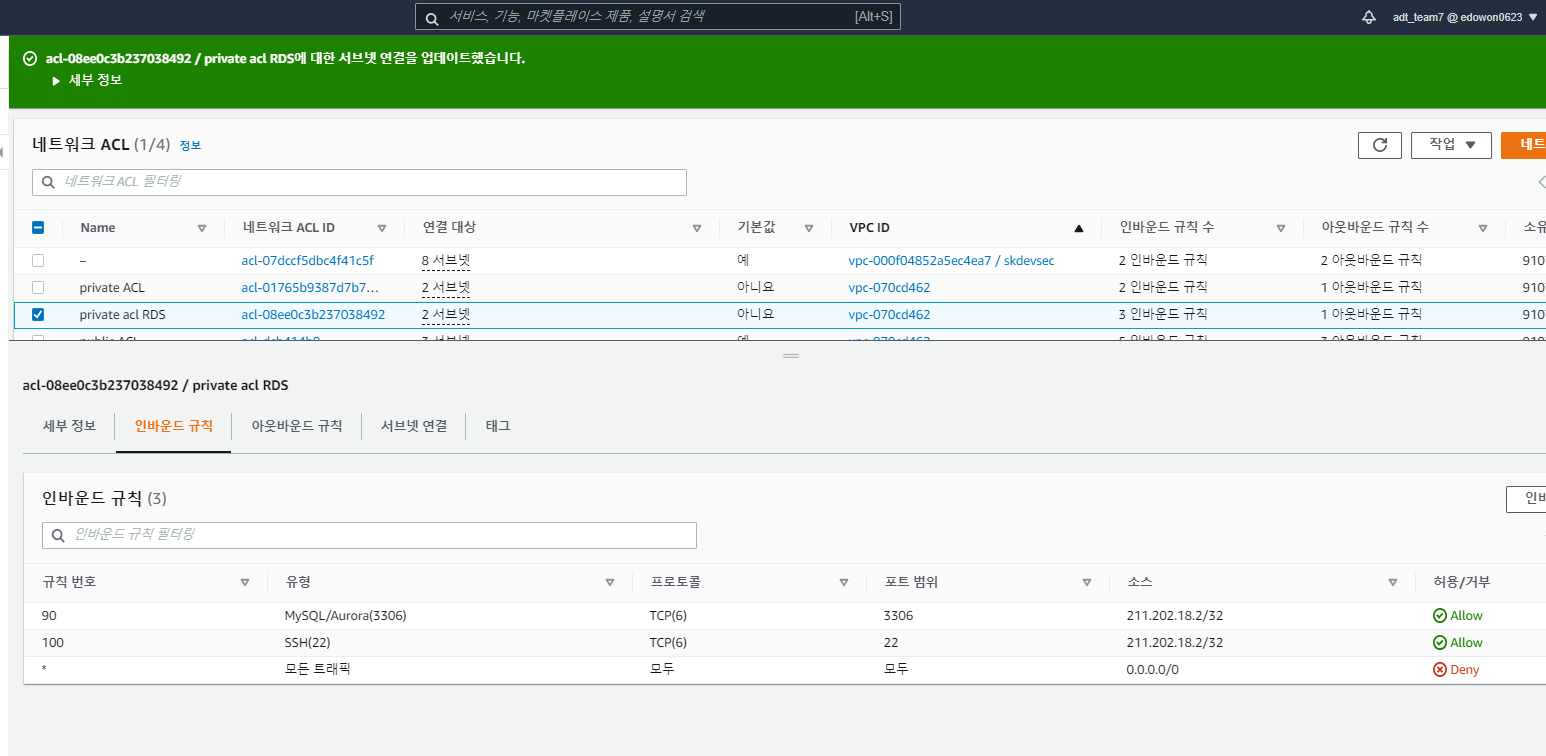
* + 1. 네트워크 ACL
       1. **조치 내용 (조치 완료)**



[그림] 테스트 파일 확인



[그림] 테스트 파일 확인



[그림] 테스트 파일 확인

* + - 1. **관련 URL**

| **경로** | **URL** |
| --- | --- |
| VPC – 네트워크 ACL | https://us-west-1.console.aws.amazon.com/vpc/home?region=us-west-1#NetworkAclDetails:networkAclId=acl-dcb414b9 |

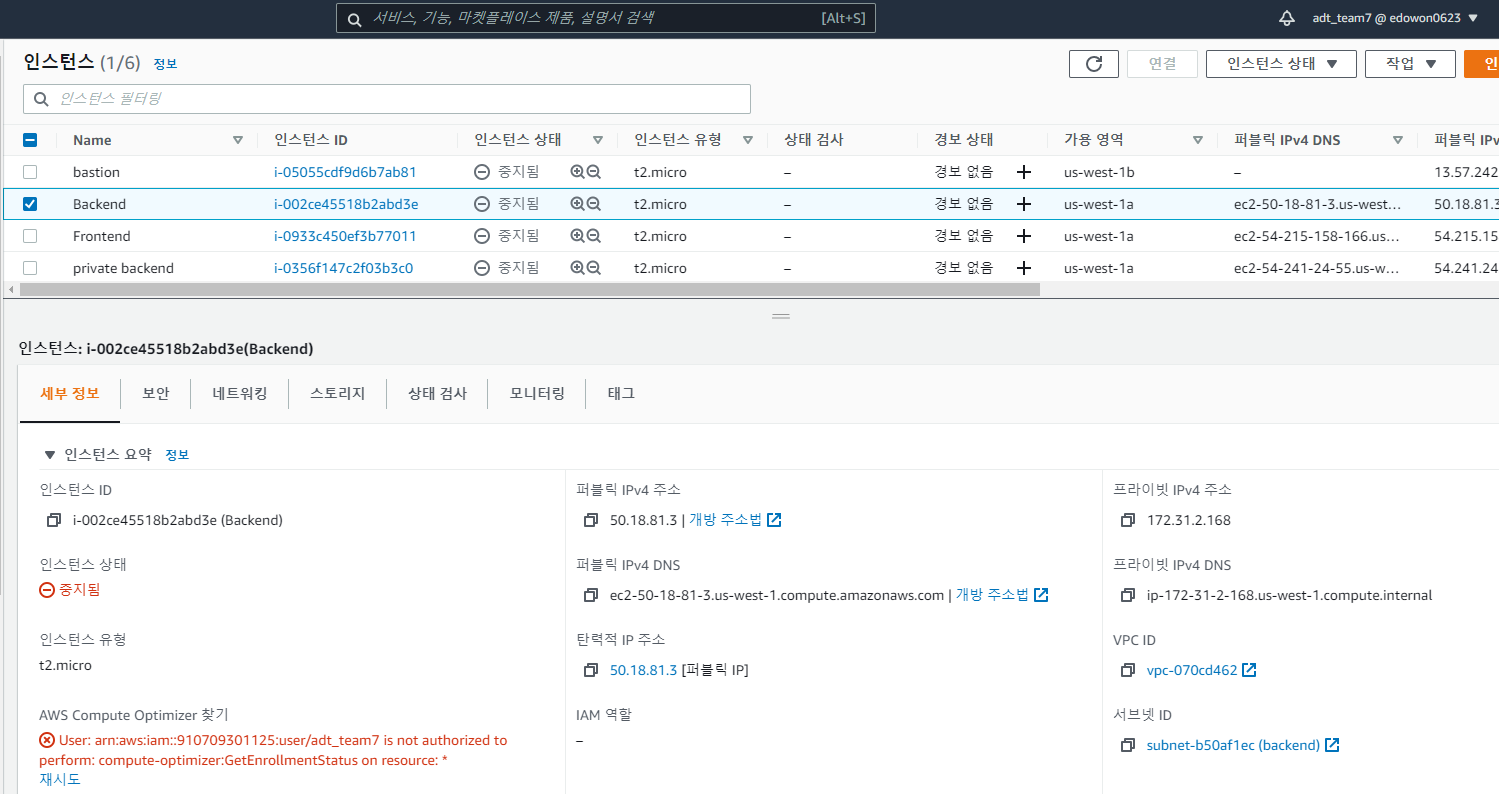
* + - 1. **조치 결과**

**서브넷 단위로 적용되는 ACL에 대해서**

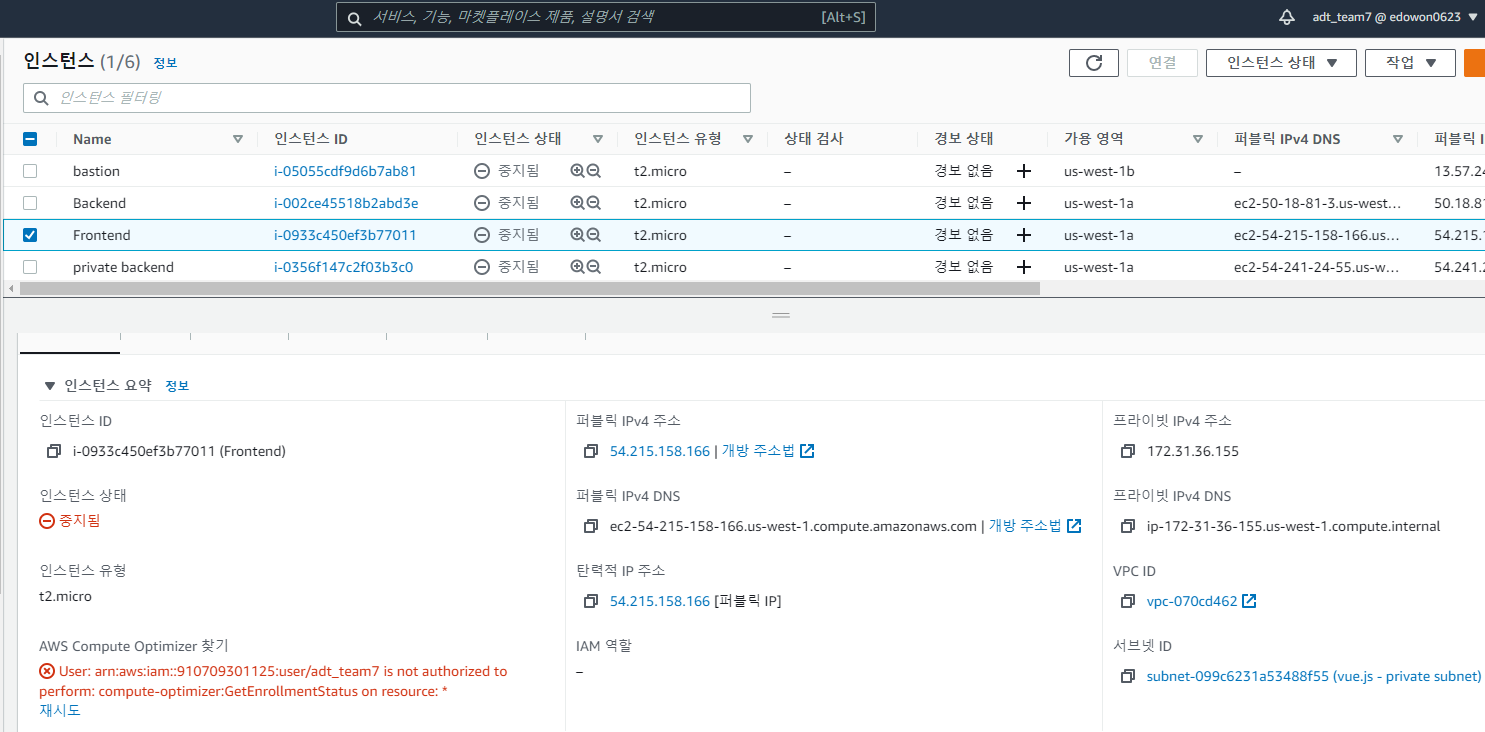
**http, https 라는 고객이 이 웹서비스에 접속할 수 있는 해당 80, 443과 any ip로 허용해줘야 서비스 트래픽들이 원활히 전달될 수 있기 때문에 해당 허용 규칙을 정했고**

**SSH로 개발자들이 접근할 수 있도록 또한 응답 값 오류 출력을 목적으로 ICMP 도 퍼블릭 서브넷 단에서 허용해주고 이를 제외한 나머지 모든 트래픽은 거부되도록 이전과 다르게 보안을 향상시켰다.**

* + 1. Elastic IP(조치 완료)
       1. **조치 내용**



[그림] 테스트 파일 확인



[그림] 테스트 파일 확인

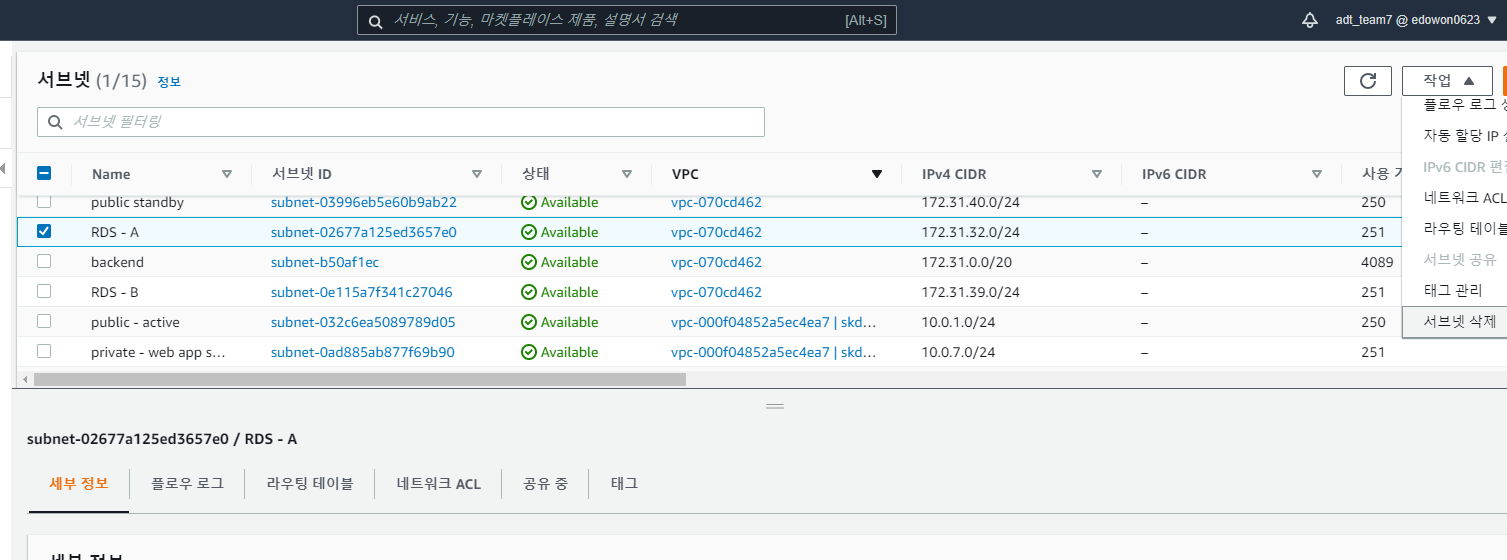
* + - 1. **관련 URL**

| **경로** | **URL** |
| --- | --- |
| EC2 – 인스턴스 – 인스턴스 세부 정보 | https://us-west-1.console.aws.amazon.com/ec2/v2/home?region=us-west-1#Instances: |

* + - 1. **조치 결과**

각 EIP가 적용된 인스턴스들의 보안 그룹을 전면 수정해서 기존 모든 포트와 모든 IP를 허용해놨던 보안 그룹을 필요한 포트와 인가자만 접근할 수 있도록 사용될 내부 IP만 쓰도록 보안 그룹 조치

* + 1. 서브넷 가용 영역(조치 완료)
       1. **조치 내용**



[그림] 테스트 파일 확인

* + - 1. **관련 URL**

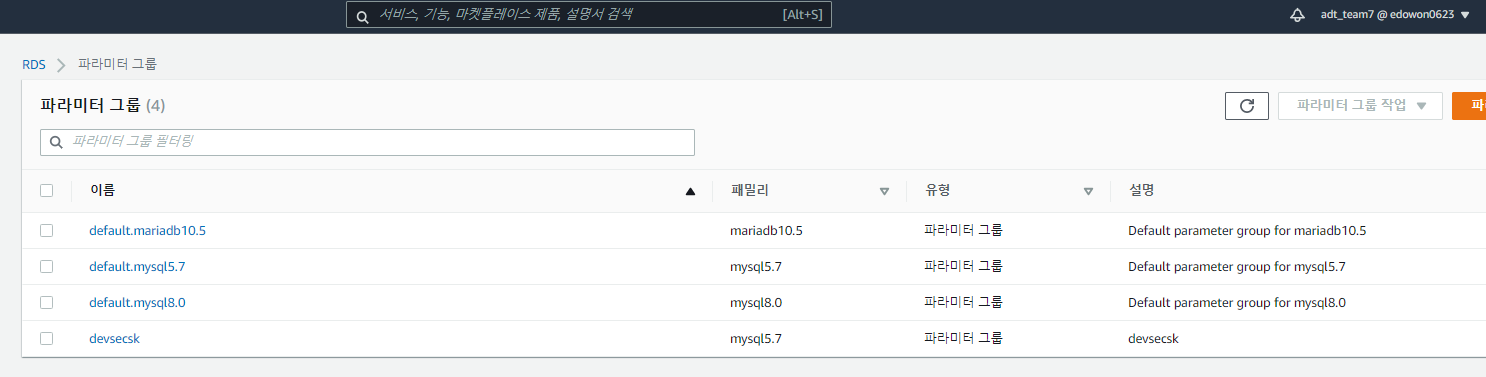
| **경로** | **URL** |
| --- | --- |
| RDS – 서브넷 그룹 – 서브넷 그룹 세부정보 | https://us-west-1.console.aws.amazon.com/rds/home?region=us-west-1#db-subnet-groups-list: |

* + - 1. **조치 결과**

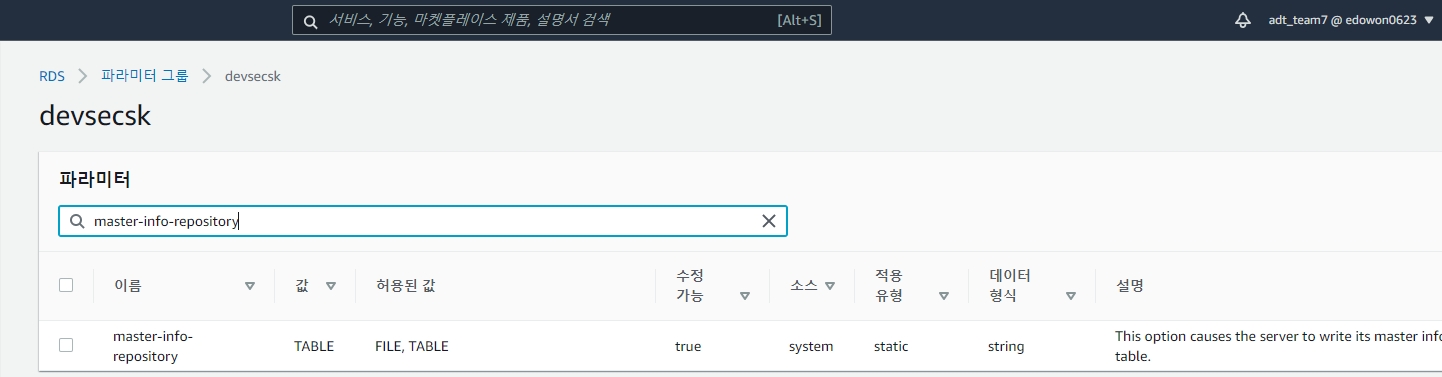
초기 DB 인스턴스 구성 시 필수적으로 가용 존을 2개 선택하게 되어있어서

사용하지 않는 서브넷을 확인 후 삭제 조치

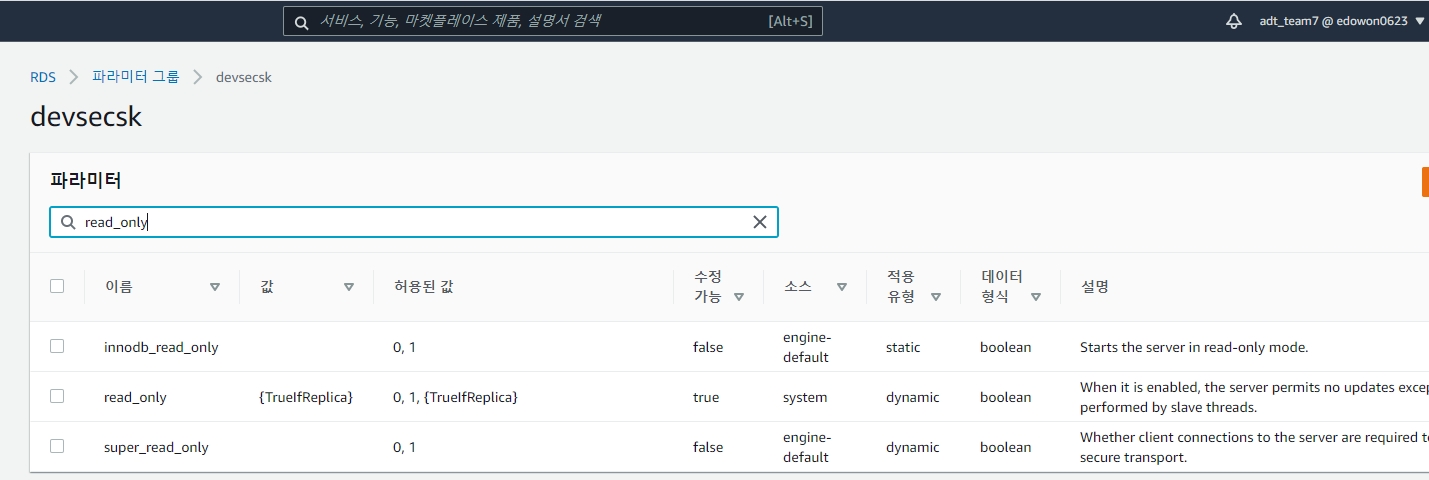
* 1. RDS 옵션 정책
     1. RDS 파라미터 관리 영역 설정(조치 완료)
        1. **조치 내용**



[그림] 테스트 파일 확인



[그림] 테스트 파일 확인



[그림] 테스트 파일 확인

* + - 1. **관련 URL**

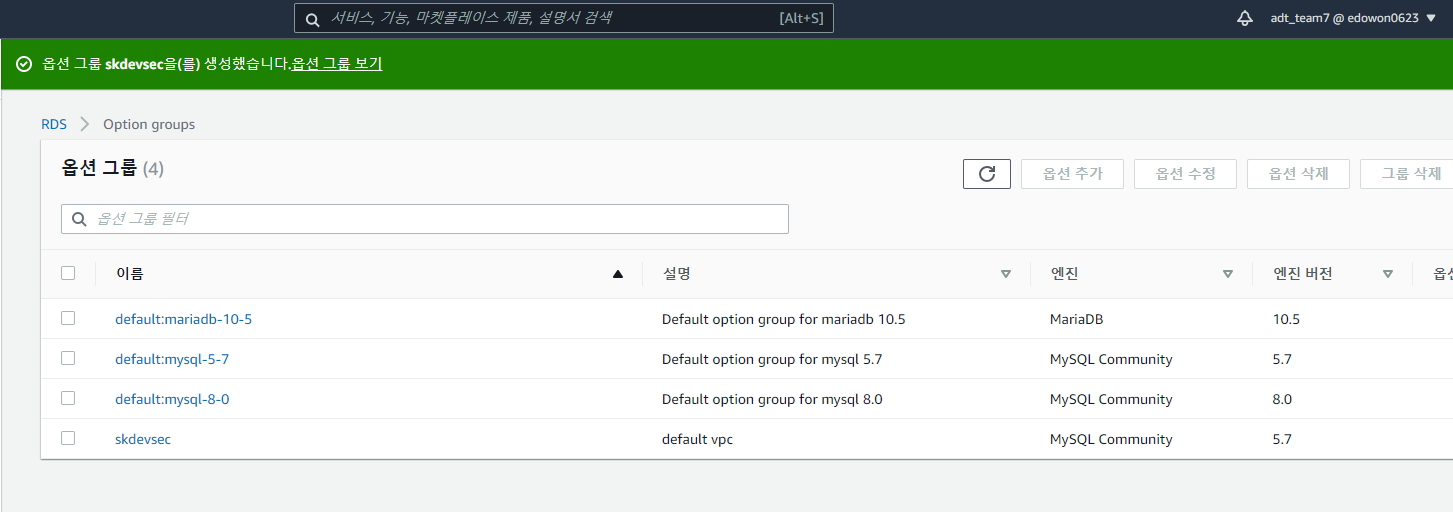
| **경로** | **URL** |
| --- | --- |
| RDS – 파라미터 그룹 | https://us-west-1.console.aws.amazon.com/rds/home?region=us-west-1#parameter-groups-detail:ids=default.mysql5.7;type=DbParameterGroup;editing=false |

* + - 1. **조치 결과**

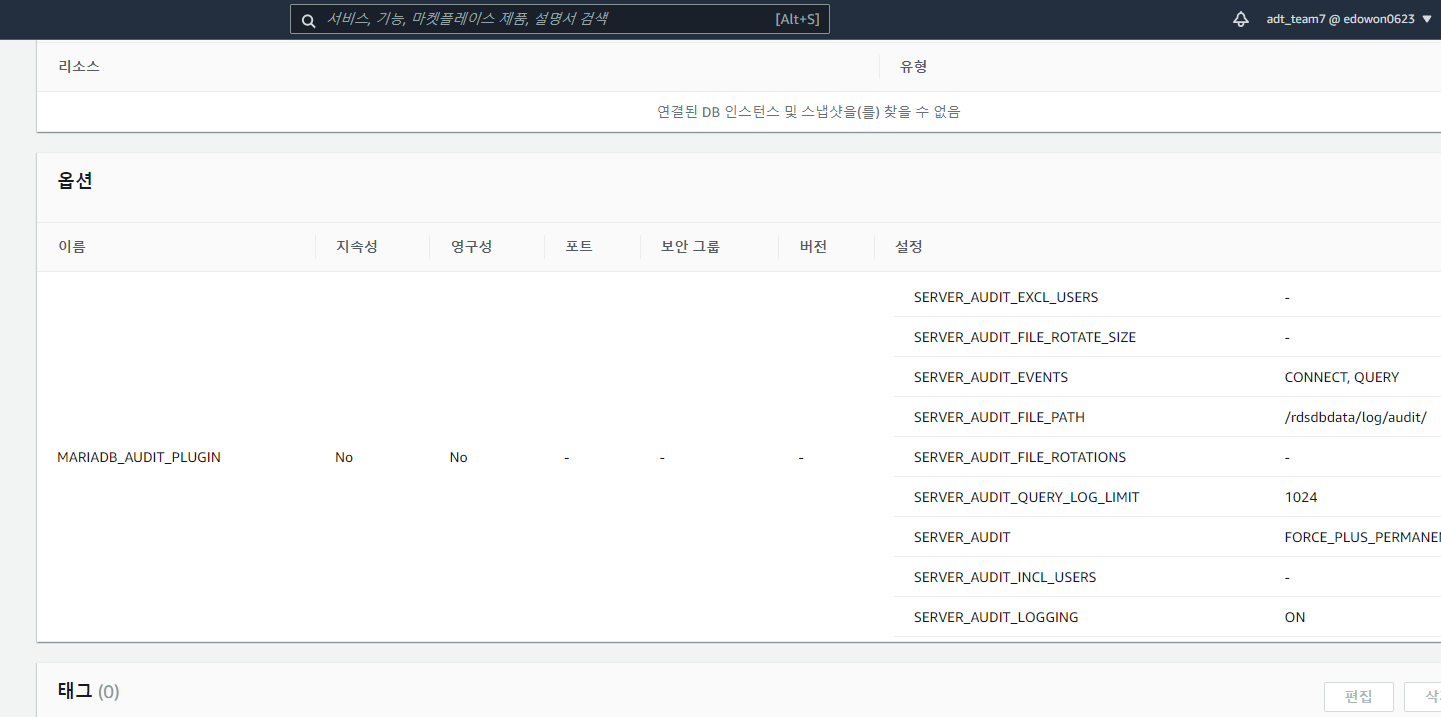
Default 그룹 외에 새로 생성된 그룹을 발견, 담당자 확인 후 상단 그림 내용들대로 DB 그룹들을 조치 및 default 상태로 수정 변경

확인 결과 새로 생성된 그룹에는 default 내용과 일치하지만 불필요하므로 삭제 조치

* + 1. MariaDB/MySQL 감사 플러그인 설정(조치 완료)
       1. **조치 내용**



[그림] 테스트 파일 확인



[그림] 테스트 파일 확인

* + - 1. **관련 URL**

| **경로** | **URL** |
| --- | --- |
| RDS – 옵션 그룹 | https://us-west-1.console.aws.amazon.com/rds/home?region=us-west-1#option-groups-list: |

* + - 1. **조치 결과**

Default 옵션 그룹은 옵션을 추가할 수 없게 지정되어있으므로

새로 옵션 그룹을 생성 후 감사 플러그인 설정을 적용

감사 플러그인을 적용 후 DB 인스턴스에 변경 사항 적용

1. [↑](#endnote-ref-1)
2. [↑](#endnote-ref-2)