



**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** | **준수기준** |
| --- | --- | --- | --- |
| 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 | 상 |

취약점진단 결과요약

3. 1. 총평
   2. 대상 별 취약점 요약

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

취약점진단 상세결과

* 1. EC2 공통영역 - 계정 보안
     1. 키 페어
        1. **문제점**

키 페어가 아예 인스턴스에 할당되지 않은 상황이고

AMI에서 제공하는 기본 사용자 이름과 암호가 기본값으로 설정됨

EC2 리눅스 AMI 생성 시 기본으로 적용되는 홈 디렉토리에 키 페어가 있음

텍스트이(가) 표시된 사진

자동 생성된 설명

[그림] 테스트 파일 확인

텍스트이(가) 표시된 사진

자동 생성된 설명

[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. **해결방안**

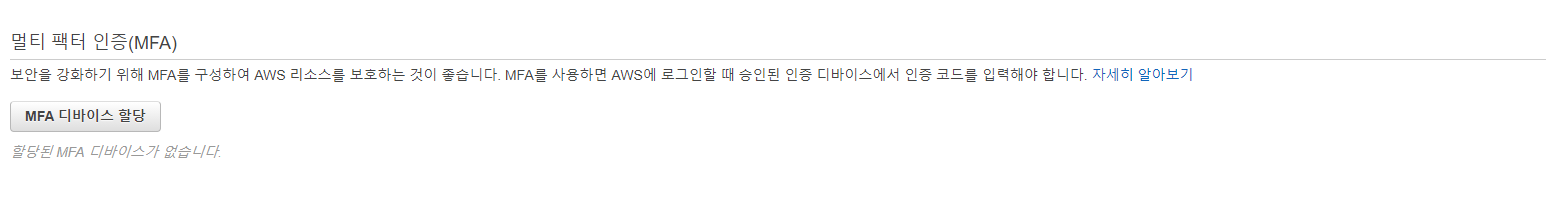
인스턴스를 다시 생성해서 인스턴스 생성 과정에서 기본으로 제공되는 키 페어를 발급받아 인스턴스 생성을 마무리한다

모두에게 노출되지 않는 디렉토리 생성하고 인가자만 접근하도록 함

* + 1. Multi Factor 인증 -
       1. **문제점**

**멀티 팩터 인증이 되어있지 않고 멀티 팩트 디바이스가 적용되어있지않은 상태**

**1차 비밀번호로만 로그인 할 수 있게 되어있는 취약점이 발견됨**



[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. **해결방안**

**멀티 팩터 인증에서 필요한 OTP 앱 설치와 QR 코드 인증 후 디바이스를 등록해야함**

**디바이스 등록 후에는 인가된 접근 사용자만이 OTP 코드 넘버를 통해서만 로그인을 할 수 있음**

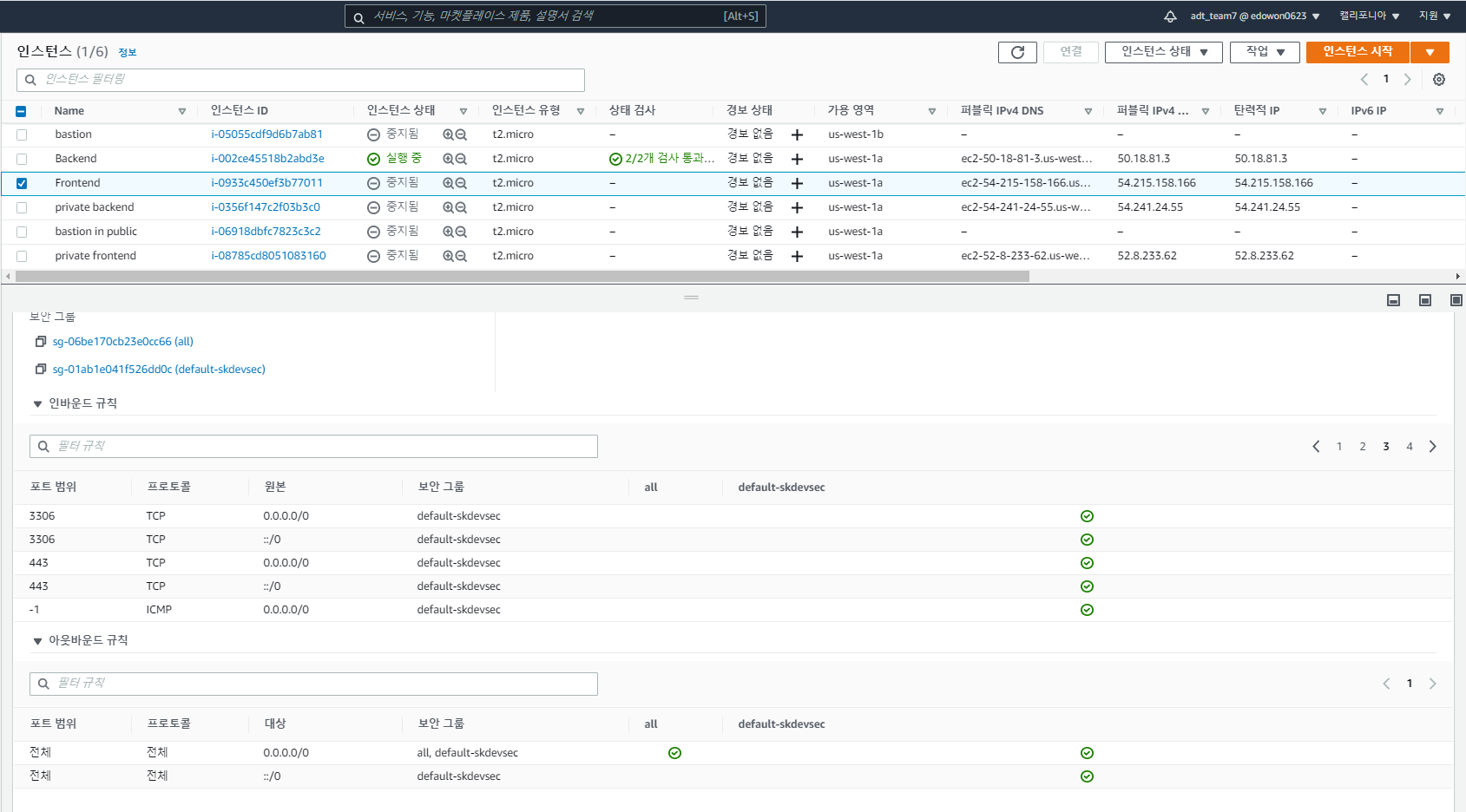
* 1. EC2 공통영역 - 네트워크 보안
     1. Security Group
        1. **문제점**

**개발 편의상 포트와 ip 대역대를 모두 허용 해놨음**

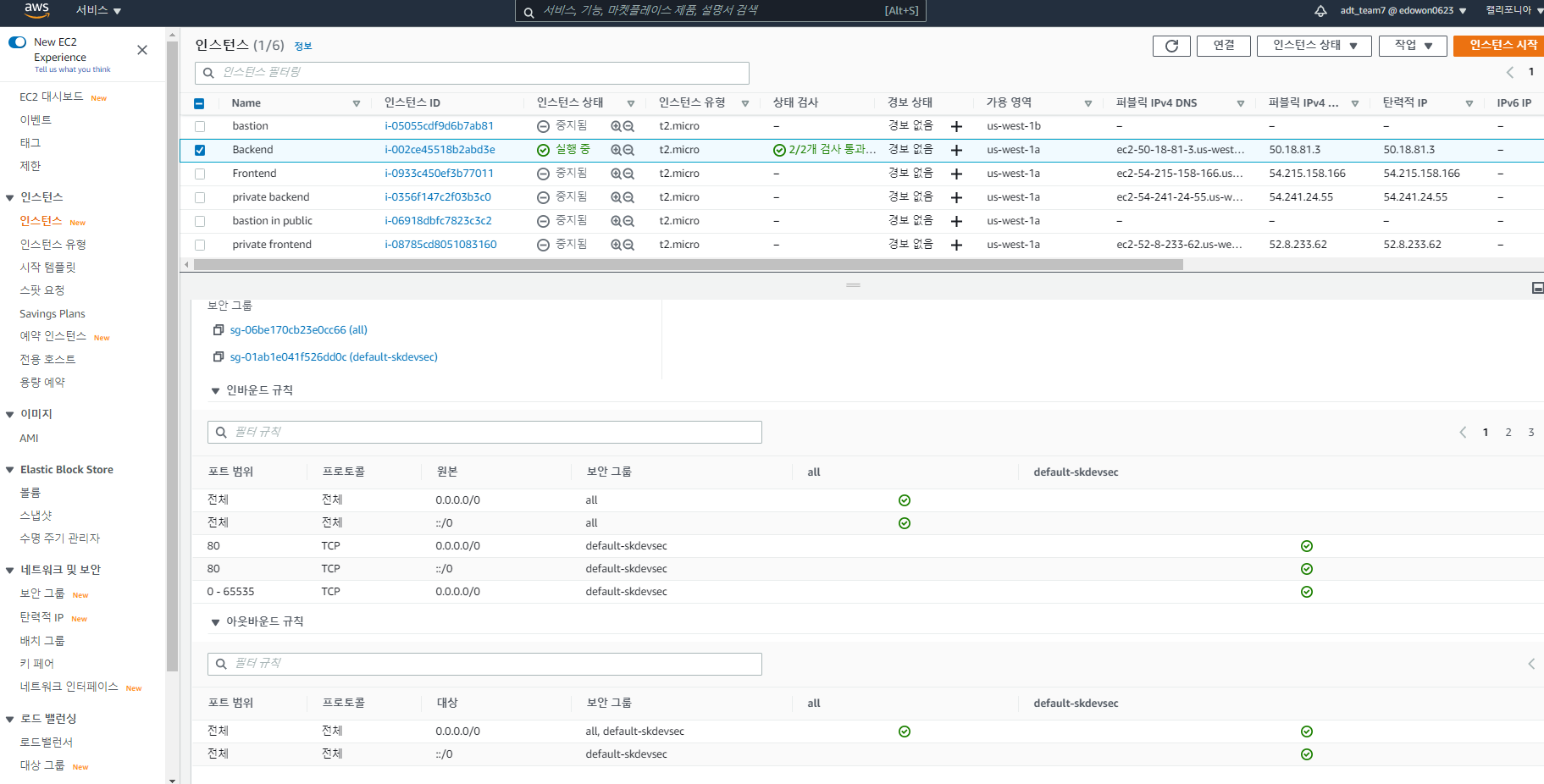
**모든 ip 대역대와 포트를 허용해놨기때문에 공격에 취약해짐**

**허용된 포트와 IP로 통신 자체가 가능해져서 네트워크 취약점에서 발견된 다방면의 공격 기법들로 공격이 가능해짐**

테스트



[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. **해결방안**

포트와 ip를 전면적으로 보안적으로 재구성해야함

모든 포트를 1~65535까지 허용해둔 이 포트들은 사용 협의된 포트들만 사용하고 나머진 차단시켜야함

* + 1. 네트워크 ACL
       1. **문제점**

기본값으로 인/아웃이 설정되어있고

모든 트래픽들이 들어오고 나가도록 다 허용 되어있음



[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#EditOutboundRules:networkAclId=acl-dcb414b9 |
| VPC – 네트워크 ACL | https://us-west-1.console.aws.amazon.com/vpc/home?region=us-west-1#EditInboundRules:networkAclId=acl-dcb414b9 |

* + - 1. **해결방안**

필요한 트래픽들만 허용할 수 있도록 규칙을 다시 알맞게 편집

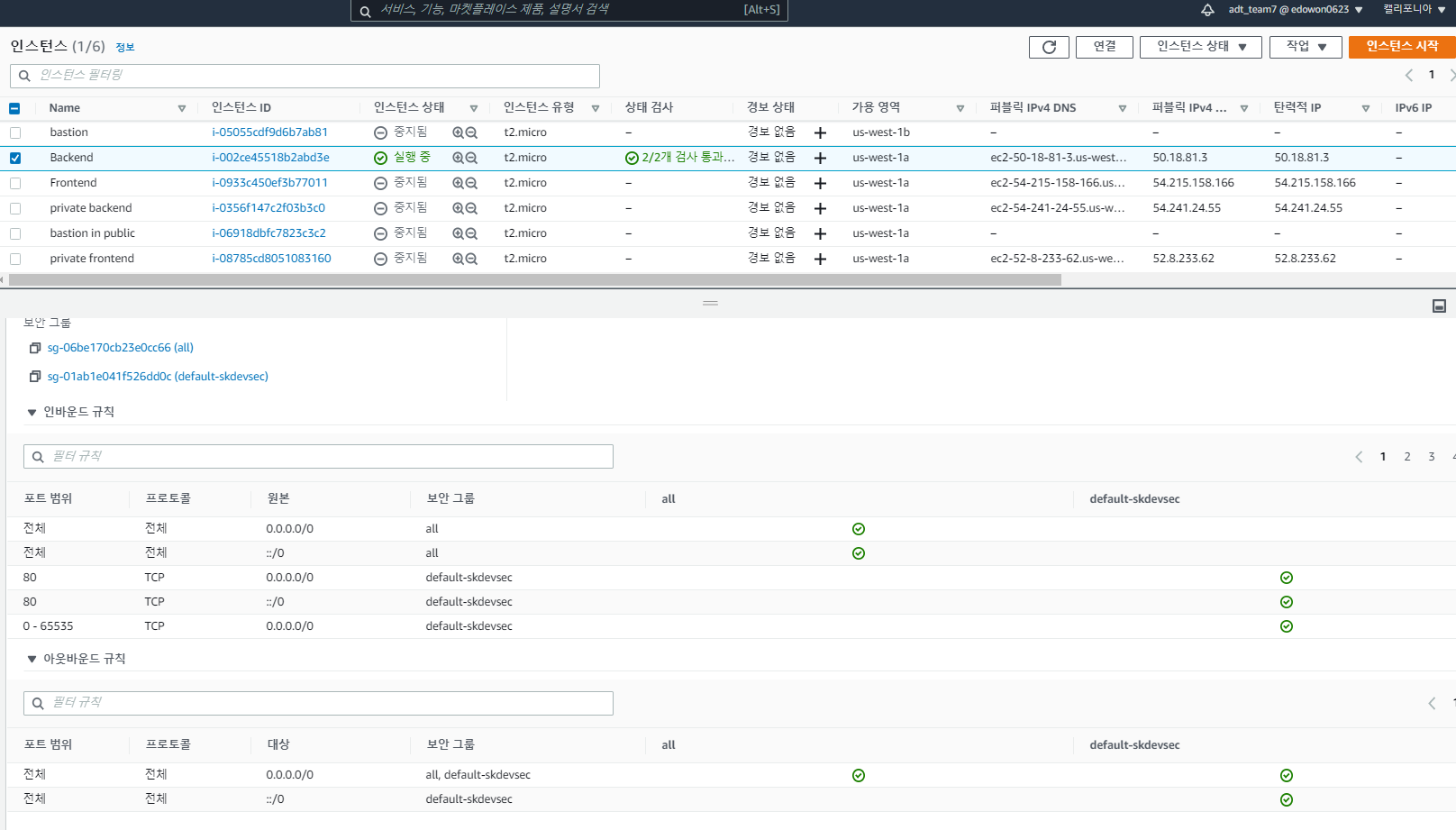
네트워크 ACL 트래픽상에서 적용될 거기 때문에 서브넷별로 퍼블릭과 프라이빗의 특징상 필요한 트래픽 이동경로와 도착지와 출발지의 속성,

필수적으로 사용해야하는 트래픽의 속성들을 종합적으로 착안해서 포트, IP 범위, 허용/차단 등을 작성한다

* + 1. Elastic IP
       1. **문제점**

고정 ip인 탄력적 ip 주소를 사용할 경우에는 열린 포트가 다수 허용 되고 있으면

그만큼 많은 위험에 노출될 가능성이 높아짐



[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. **해결방안**

0~65535까지 열려있는 포트들에 대해서 잘 알려진 포트가 아닌 사전에 사용할 포트들을 협의해 구성하고

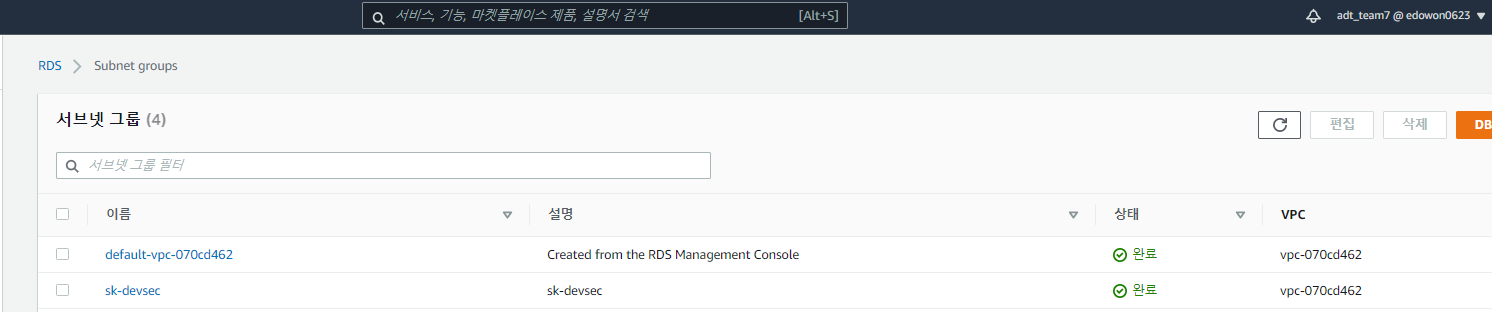
그 포트들만 열 수 있도록 포트를 수정해야한다

* + 1. 서브넷 가용 영역
       1. **문제점**

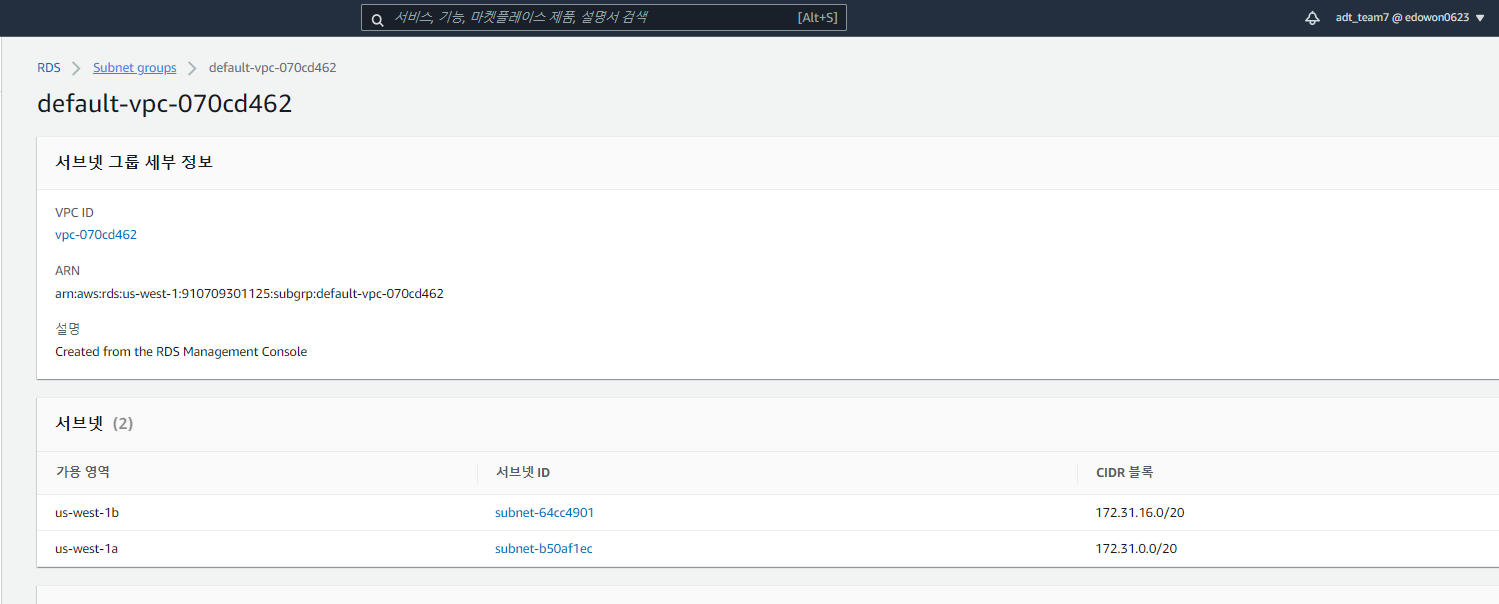
**Sk-devsec이라는 새로 생성했던 서브넷 그룹 발견**

**Default 서브넷 그룹과 비교헀을 때**

**서브넷 영역이 둘다 같고 다른 한 개의 서브넷은 생성 시 필수적으로 2개를 선택하게끔 되어있어서 생성했지만 불필요한 서브넷이 있을 시에 또 다른 공격 통로가 될 수 있음**



[그림] 테스트 파일 확인



[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: |

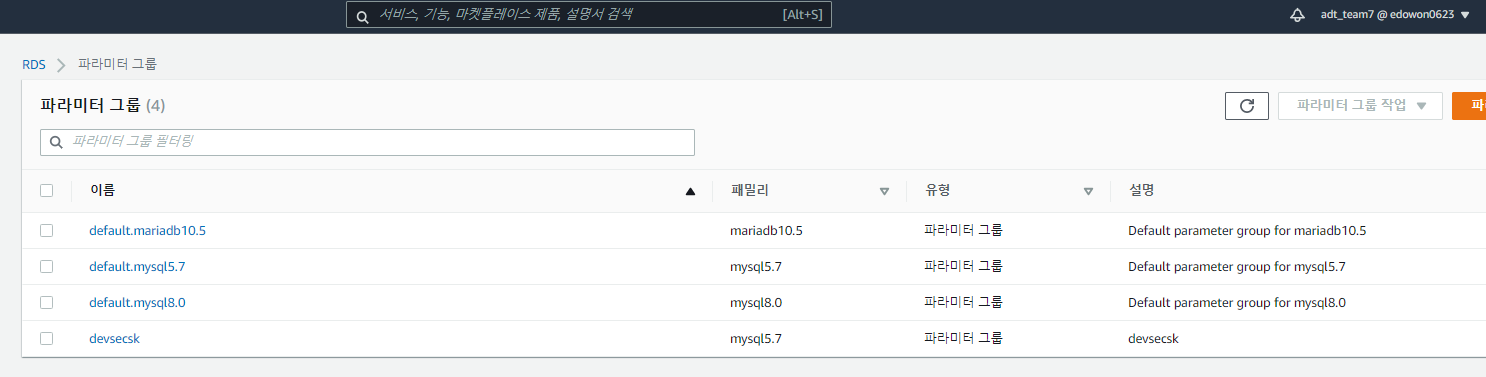
* + - 1. **해결방안**

# 다른 한 개의 서브넷을 삭제해서 공격 통로를 최소화 해야함

* 1. RDS 옵션 정책
     1. RDS 파라미터 관리 영역 설정
        1. **문제점**

**기본값 그룹이 아닌 Devsecsk 라는 그룹이 새로 생성되어있음**

**기본값 그룹 외에 다른 사용자가 만든 devsecsk 라는 그룹을 생성할 시에 보안상 내의 권한 문제가 발생할 수도 있고 default 값이 아닌 새로 생성된 값에는 보안에 취약할 수도 있는 설정이 수정되어있을 수도 있기 때문에 담당자의 확인이 필요함**



[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. **해결방안**

담당자 확인 후 새로 생성된 그룹은 삭제되어야하며 보안 표준인 기본값 그룹으로 사용해야함

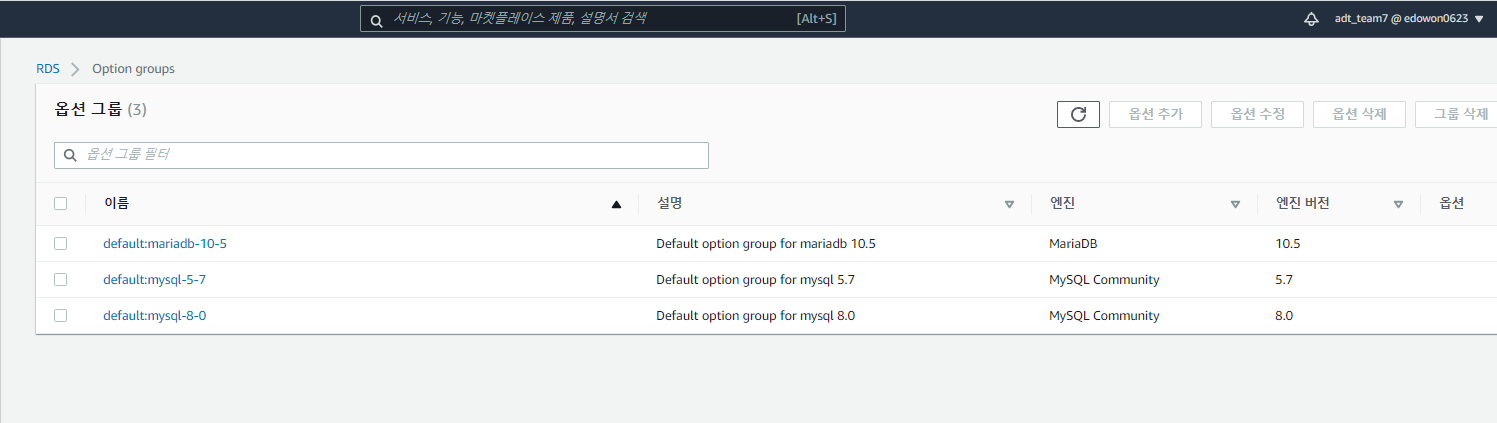
새로 생성된 그룹에 기본값이 아닌 보안에 취약할 수도 있는 값이 설정되었을 시에는 담당자에게 알리고

이를 확인 후 새로 생성된 그룹은 삭제해야함

* + 1. MariaDB/MySQL 감사 플러그인 설정
       1. **문제점**

**감사 플러그인이 설정되어있지않고 있음**

**공격이나 피해 발생 시 공격자를 추적하거나 내부 사용자들에 대한 관리가 허술해질 수 있는 문제점이 발생할 수 있음**



[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. **해결방안**

# 책임 추적성과 시스템 내부 데이터와 정보 자산에 대한 피해를 예방하기위해서

# 감사 플러그인을 설정해야함

감사 로그에 필요한 설정 사항들을 확인하고 감사 플러그인이 실행될 수 있도록 설정을 해야함

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