SK 쉴더스

2023 클라우드 보안 가이드

- AWS

2023 클라우드 보안 가이드 발간사

안녕하십니까? SK쉴더스입니다.

지난 21년 SK쉴더스의 취약점진단팀은 "클라우드 보안 가이드 - AWS, Azure, GCP" 3종을 발간했습니다.

현재 On-Premise 환경에서 클라우드 환경으로 전환하거나, 하이브리드 형태로 전환하고 있는 기업들이 늘어나고 있으며, CSP(클라우드 서비스 제공업체) 별 네이티브 서비스와 관리 영역의 많은 변화로 인해 보안정책 설정 및 환경설정을 대응하고자 클라우드 운영자 및 관리자는 많은 어려움을 겪고 있습니다.

특히, 최근 AWS, Azure의 관리 영역 및 네이티브 서비스의 변화가 많았습니다.
이러한 트렌드를 분석하고 변화에 대응하고자 올해도 "2023 클라우드 보안 가이드 - AWS, Azure, GCP" 3종의 개정판을 발간하게 되었습니다.

이번 가이드는 ISMS 인증심사(기술영역)을 대응하고자 항목분류를 개편하였으며, 클라우드 운영자가 위협에 대응하고 변화된 관리 영역 및 컴플라이언스 기준을 충족할 수 있는 기준을 제시했습니다.

앞으로도 SK쉴더스는 클라우드 운영자와 더불어 관리자도 다양한 환경에 발빠르게 대응할 수 있도록 보안 가이드를 개선하여 발간할 계획입니다.

더불어, 1년 동안 클라우드 보안가이드 개선에 많은 시간과 노력을 투자해준 팀원들에게 감사의 인사를 드립니다.

감사합니다.

ICT사업그룹 취약점진단팀 팀장
김 상 춘

목 차

I. 전체목록

1. 체크리스트 항목

진단에 사용될 체크리스트는 국내/외 기술 자료를 바탕으로 작성 되었습니다. AWS 보안가이드에서의 영역은 계정 관리(10개 항목), 권한 관리(3개 항목), 가상 리소스 관리(8개 항목), 운영 관리(13개 항목)으로 총 4개 영역에서 34개 항목으로 구성 하였습니다.

[표] 1. AWS 보안진단 체크리스트

영역	항목코드	항목명	중요도
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
권한 관리	2.1	인스턴스 서비스 정책 관리	상
	2.2	네트워크 서비스 정책 관리	상
	2.3	기타 서비스 정책 관리	상
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	중
	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
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

2. AWS 보안가이드/ISMS 매칭 기준 항목

ISMS-P 영역의 "2. 보호대책 요구사항" 전체 64개 항목 중 31개 항목을 매핑(48%)하였습니다. 전체 항목 중 일부 영역 항목인 "정책 및 조직 관리", "보안 서약 및 교육 훈련", "물리 보안", "사고 예방 및 취약점 점검 조치" 등과 같은 클라우드 환경에서의 직접 확인 및 증적 마련이 불가능한 항목은 28개입니다. 이와 같은 항목은 회사 내규 및 자체적으로 관리되고 있는 문서로 증적을 대체하여야 합니다.

[표] 2. AWS 보안가이드와 ISMS 항목 매칭

영역	항목 코드	항목명	ISMS 기준항목
계정 관리	1.1	사용자 계정 관리	2.2.1 주요 직무자 지정 및 관리 2.2.5 퇴직 및 직무변경 관리 2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리
	1.2	IAM 사용자 계정 단일화 관리	2.5.1 사용자 계정 관리 2.5.2 사용자 식별
	1.3	IAM 사용자 계정 식별 관리	2.1.3 정보자산 관리 2.5.1 사용자 계정 관리 2.5.2 사용자 식별
	1.4	IAM 그룹 사용자 계정 관리	2.5.1 사용자 계정 관리
	1.5	Key Pair 접근 관리	2.6.2 정보시스템 접근 2.6.6 원격접근 통제
	1.6	Key Pair 보관 관리	2.7.1 암호정책 적용 2.7.2 암호키 관리
	1.7	Admin Console 관리자 정책 관리	2.5.5 특수 계정 및 권한 관리
	1.8	Admin Console 계정 Access Key 활성화 및 사용주기 관리	2.5.4 비밀번호 관리 2.5.5 특수 계정 및 권한 관리 2.7.2 암호키 관리
	1.9	MFA (Multi-Factor Authentication) 설정	2.5.3 사용자 인증 2.5.4 비밀번호 관리 2.6.2 정보시스템 접근 2.6.6 원격접근 통제
	1.10	AWS 계정 패스워드 정책 관리	2.5.4 비밀번호 관리
권한 관리	2.1	인스턴스 서비스 정책 관리	2.2.1 주요 직무자 지정 및 관리 2.2.2 직무 분리 2.2.5 퇴직 및 직무변경 관리 2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리 2.5.2 사용자 식별

			2.5.5 특수 계정 및 권한 관리 2.6.2 정보시스템 접근 2.10.2 클라우드 보안
	2.2	네트워크 서비스 정책 관리	2.2.1 주요 직무자 지정 및 관리 2.2.2 직무 분리 2.2.5 퇴직 및 직무변경 관리 2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리 2.5.2 사용자 식별 2.5.5 특수 계정 및 권한 관리 2.6.2 정보시스템 접근 2.10.2 클라우드 보안
	2.3	기타 서비스 정책 관리	2.2.1 주요 직무자 지정 및 관리 2.2.2 직무 분리 2.2.5 퇴직 및 직무변경 관리 2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리 2.5.2 사용자 식별 2.5.5 특수 계정 및 권한 관리 2.6.2 정보시스템 접근 2.6.3 응용프로그램 접근 2.8.5 소스 프로그램 관리 2.10.2 클라우드 보안
가상 리소스 관리	3.1	보안 그룹 인/아웃바운드 ANY 설정 관리	2.6.1 네트워크 접근 2.6.6 원격접근 통제
	3.2	보안 그룹 인/아웃바운드 불필요 정책 관리	2.6.1 네트워크 접근
	3.3	네트워크 ACL 인/아웃바운드 트래픽 정책 관리	2.6.1 네트워크 접근 2.8.3 시험과 운영 환경 분리
	3.4	라우팅 테이블 정책 관리	2.6.1 네트워크 접근
	3.5	인터넷 게이트웨이 연결 관리	2.6.1 네트워크 접근 2.6.6 원격접근 통제 2.6.7 인터넷 접속 통제
	3.6	NAT 게이트웨이 연결 관리	2.6.1 네트워크 접근
	3.7	S3 버킷/객체 접근 관리	2.6.1 네트워크 접근 2.6.2 정보시스템 접근 2.6.6 원격접근 통제 2.6.7 인터넷 접속 통제 2.10.3 공개서버 보안
	3.8	RDS 서브넷 가용 영역 관리	2.6.4 데이터베이스 접근

			2.6.6 원격접근 통제 2.8.4 시험 데이터 보안
운영 관리	4.1	EBS 및 볼륨 암호화 설정	2.7.1 암호정책 적용
	4.2	RDS 암호화 설정	2.7.1 암호정책 적용
	4.3	S3 암호화 설정	2.7.1 암호정책 적용
	4.4	통신구간 암호화 설정	2.7.1 암호정책 적용 2.10.5 정보전송 보안
	4.5	CloudTrail 암호화 설정	2.7.1 암호정책 적용 2.7.2 암호키 관리
	4.6	CloudWatch 암호화 설정	2.7.1 암호정책 적용 2.7.2 암호키 관리
	4.7	AWS 사용자 계정 로깅 설정	2.5.6 접근권한 검토 2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검 2.11.3 이상행위 분석 및 모니터링
	4.8	인스턴스 로깅 설정	2.9.1 변경관리 2.9.2 성능 및 장애관리 2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검 2.11.3 이상행위 분석 및 모니터링
	4.9	RDS 로깅 설정	2.9.1 변경관리 2.9.2 성능 및 장애관리 2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검 2.11.3 이상행위 분석 및 모니터링
	4.10	S3 버킷 로깅 설정	2.9.1 변경관리 2.9.2 성능 및 장애관리 2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검 2.11.3 이상행위 분석 및 모니터링
	4.11	VPC 플로우 로깅 설정	2.9.1 변경관리 2.9.2 성능 및 장애관리 2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검 2.11.3 이상행위 분석 및 모니터링

	4.12	로그 보관 기간 설정	2.9.4 로그 및 접속기록 관리
	4.13	백업 사용 여부	2.9.2 성능 및 장애관리 2.9.3 백업 및 복구 관리 2.11.5 사고 대응 및 복구 2.12.2 재해 복구 시험 및 개선

3. 위험도 구분

각 취약점으로 인해 발생 가능한 피해에 대하여 위험도 산정을 통해 상, 중, 하 3단계로 분류함.

[표] 3. 위험도 구분

위험도	내 용	조치기간	비고
상	관리자 계정 및 주요정보 유출로 인한 치명적인 피해 발생	단기	
중	노출된 정보를 통해 서비스/시스템 관련 추가 정보 유출 발생 우려	중기	
하	타 취약점과 연계 가능한 잠재적인 위협 내재	장기	

II. 전체목록

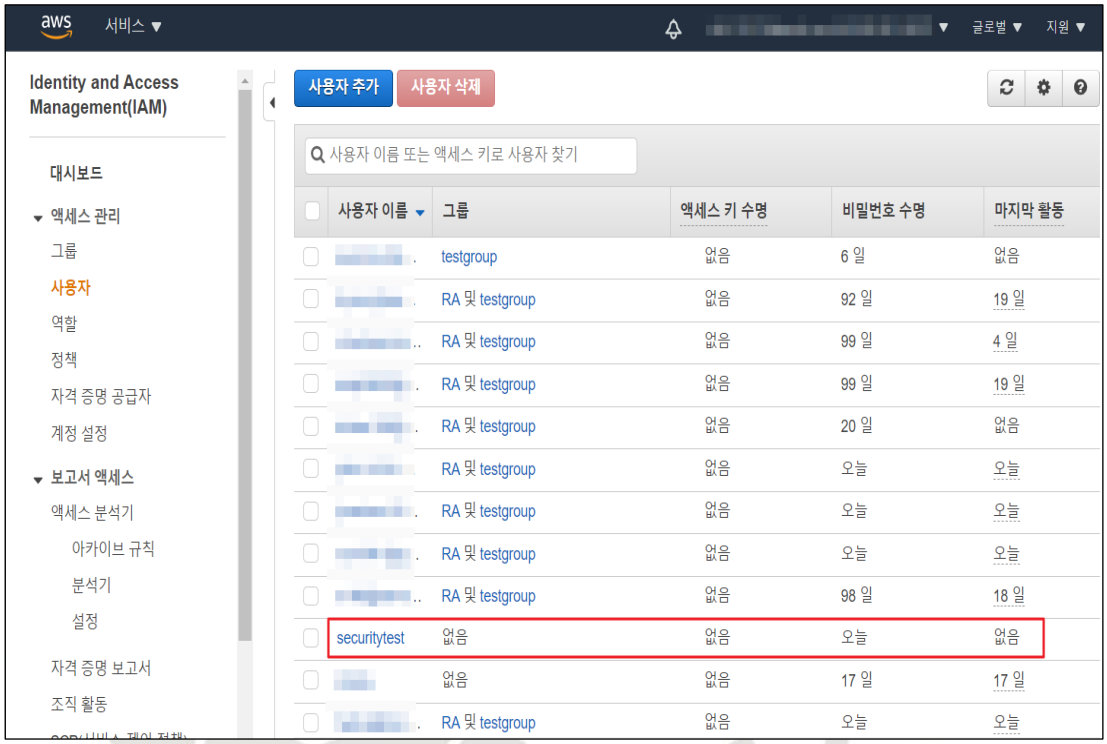
1. 계정 관리

1.1 사용자 계정 관리

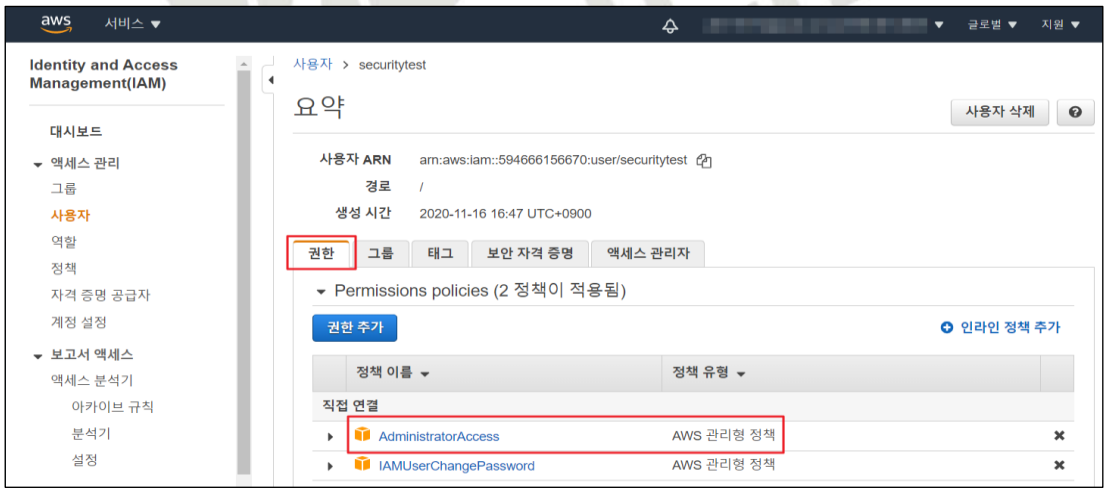
<table>
<tr><td>분류</td><td>계정 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">사용자 계정 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">모든 AWS 리소스는 AWS 계정의 소유이고, 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(즉, 사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다.

(*) AWS 관리형 정책
서비스 내 FULL ACCESS 등과 같이 중요도가 높은 AWS 관리형 정책은 EC2 서비스 관리/운영자 및 관련 담당자 외에 다른 IAM 계정에 아래와 같은 권한 할당이 되지 않도록 해야합니다. 그중에서도 AWS Admin Console 관리자(AdministratorAccess) 권한은 다수의 IAM 계정에 설정되지 않도록 관리 조치가 필요합니다.

(*) 계정 종류
<table>
<tr><th>계정 구분</th><th>Description</th><th>확인 필요 사항</th></tr>
<tr><td>Console Admin</td><td>최고 권한을 가지고 있는 단일 계정</td><td>가급적 사용을 지양해야 함</td></tr>
<tr><td>IAM</td><td>AWS IAM 서비스를 통해 생성된 별도 계정</td><td>IAM 역할 및 권한에 대한 현황을 확인해야 함</td></tr>
<tr><td>AD(Active Directory) 연동</td><td>기존 내부에서 사용중인 AD 를 AWS Organizations 서비스에 연동한 계정</td><td>기존 AD 서비스에서 사용중인 각 계정 중 IAM 역할 및 권한이 설정된 현황을 확인해야 함</td></tr>
<tr><td>Access Key</td><td>CLI 환경으로의 접속을 위한 단일 계정 (사용 기간에 대한 기준 명시가 필요함)</td><td>발급일 기준 6 개월을 초과한 Access Key 존재 유무</td></tr>
</table>
(*) 불필요한 계정 예시
1. 비 임직원 계정 (협력사 공통 계정)
2. 테스트 계정 (testuser, test01, test02....)
3. 미사용 계정 (퇴직 및 휴직자)</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. IAM 그룹에 포함되지 않은 단일 사용자 권한 확인
1) IAM 그룹에 포함되지 않은 단일 사용자 계정 전체 권한 확인</td></tr>
</table>

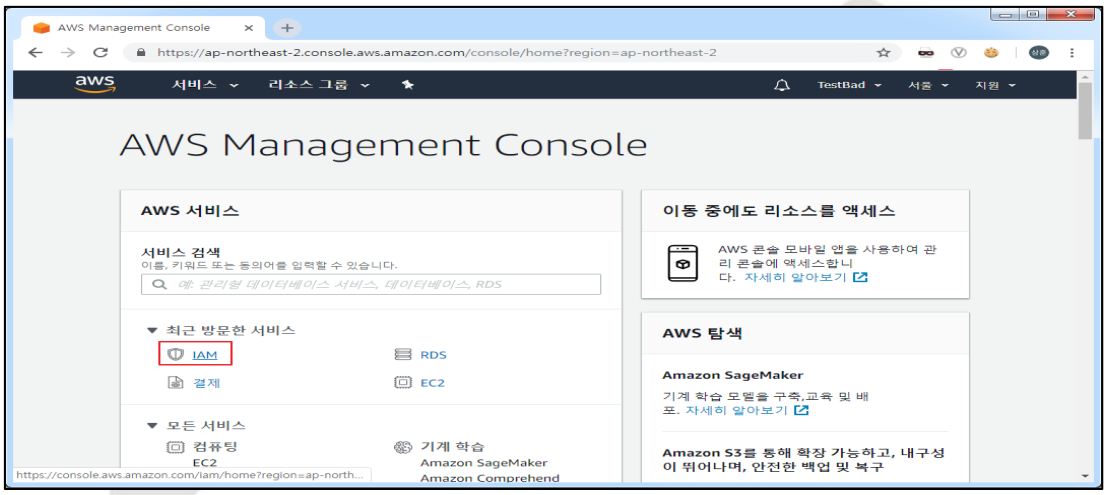
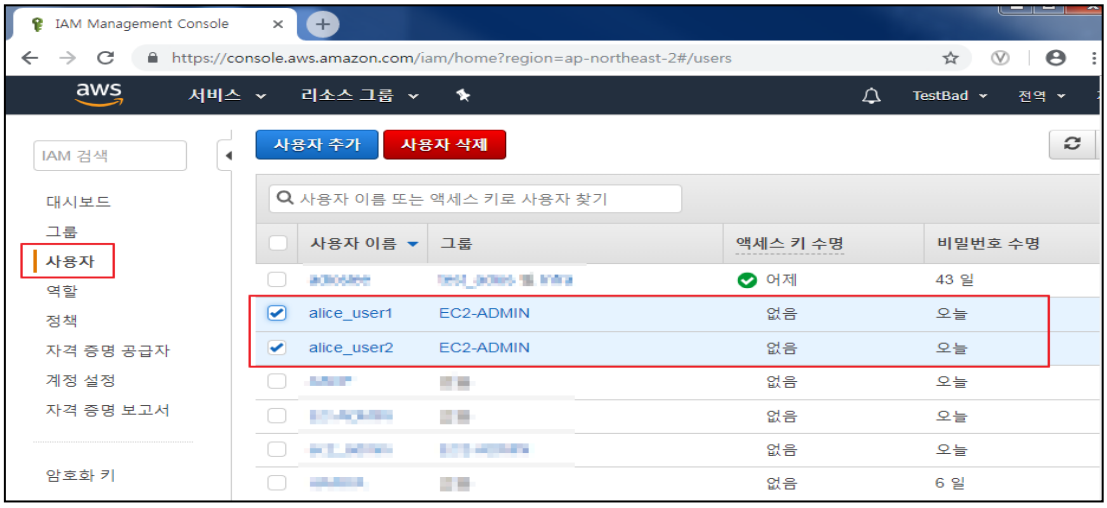


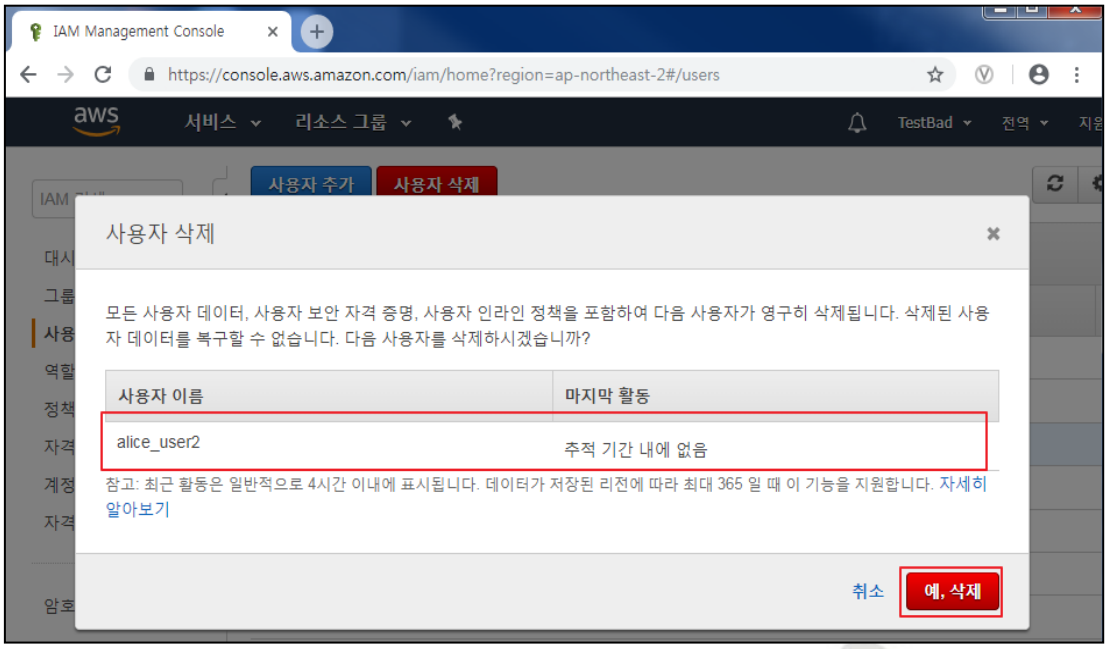
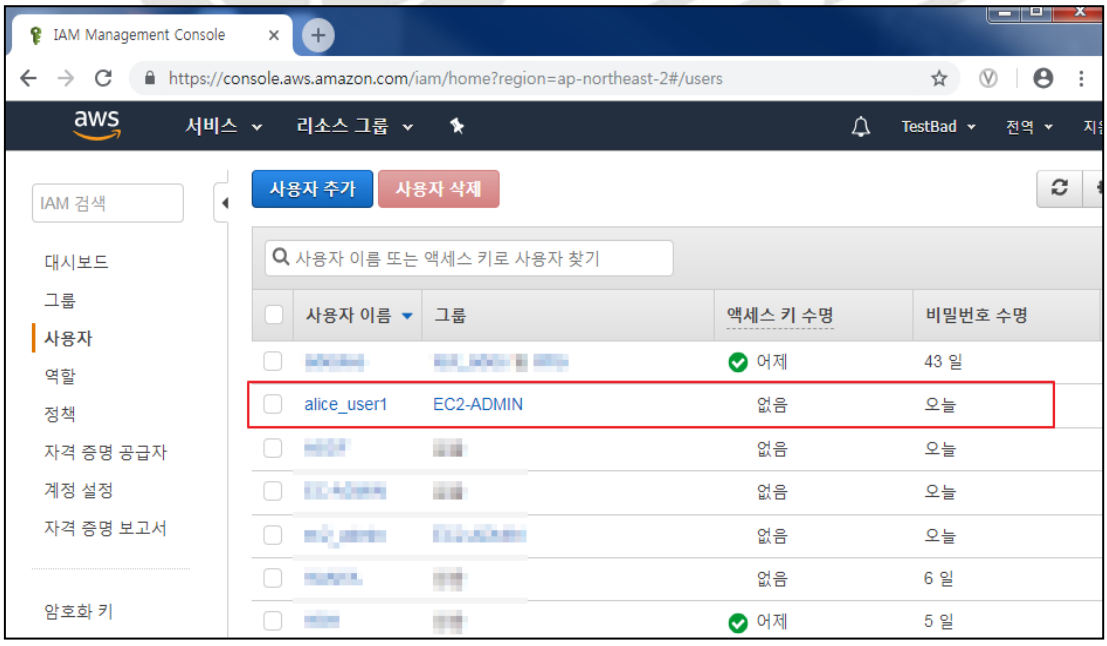
2) 전체 권한 여부 확인



진단 기준	**양호기준** : 관리자 권한을 보유한 다수 계정이 존재하지 않고 불필요한 계정이 존재하지 않을 경우 **취약기준** : 관리자 권한을 보유한 다수 계정이 존재하거나 불필요한 계정이 존재할 경우
비고	

1.2 IAM 사용자 계정 단일화 관리

분류	계정 관리	중요도	상
항목명	IAM 사용자 계정 단일화 관리		
항목 설명	모든 AWS 리소스는 AWS 계정의 소유이고, 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(즉, 사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다. **1) 적절한 IAM 계정 사용** - AWS IAM 계정 생성 시 1인 1계정 발급을 원칙으로 하며, 1명의 담당자가 다수의 IAM 계정을 보유하는 것을 지양해야 합니다. Cloud 서비스 리소스 사용이 필요할 경우 내부 정책을 기준으로 목적에 맞게 권한이 부여되어야 합니다. **※ Cloud 서비스 별 IAM 계정 생성 및 관리 금지**		
설정 방법	**가. 적절한 IAM 계정 사용** 1) AWS 주요 서비스 중 "IAM" 클릭  2) IAM "사용자" 클릭 및 계정 목록 확인  		

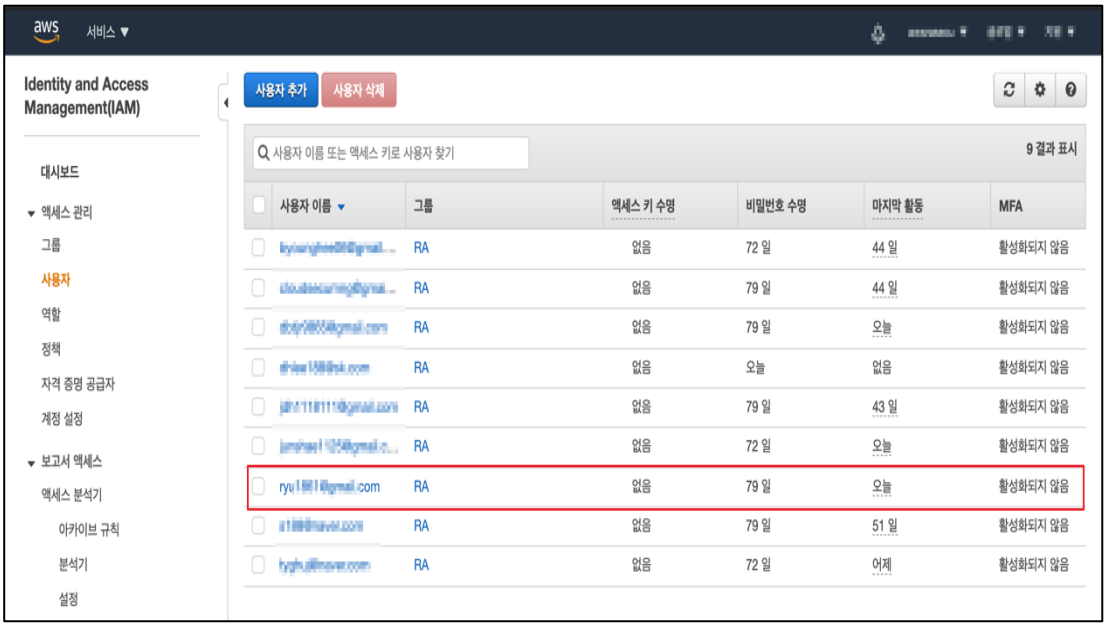
	3) 불필요한 사용자 삭제 버튼 클릭  4) 사용자 삭제 확인 
진단 기준	**양호기준** : IAM 사용자 계정을 1인 1계정으로 사용하고 있는 경우 **취약기준** : IAM 사용자 계정을 1인 1계정으로 사용하고 있지 않은 경우
비고	

1.3 IAM 사용자 계정 식별 관리

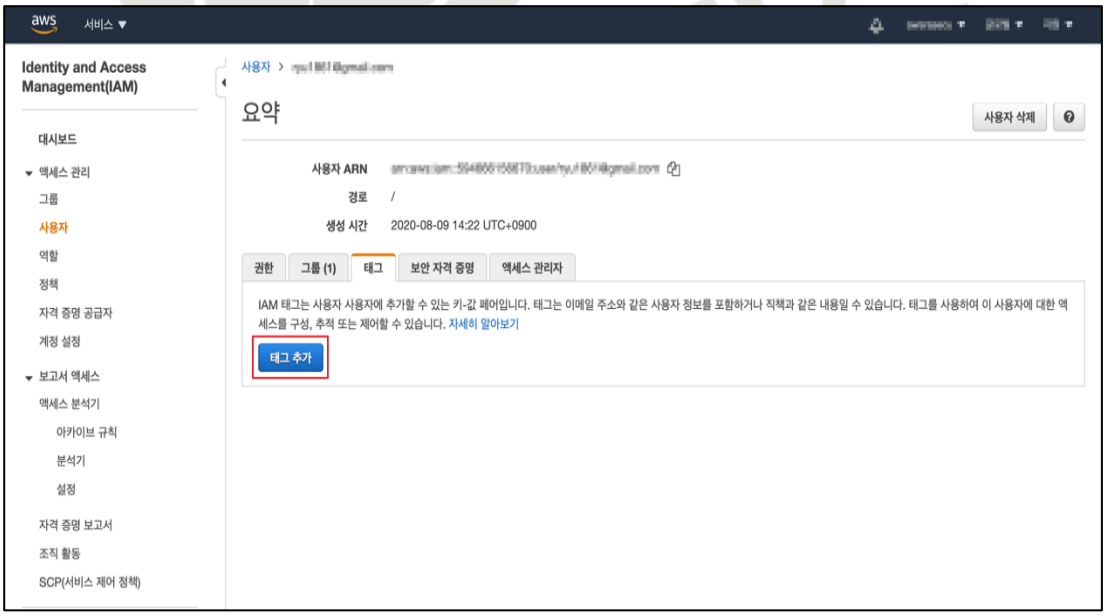
<table>
<tr><td>분류</td><td>계정 관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">사용자 계정 식별 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">IAM 사용자 계정에는 태그를 추가할 수 있으며, 해당 태그 설정은 사용자를 표현하는 정보 및 직책의 내용을 포함할 수 있습니다. 이러한 태그 사용은 IAM 사용자에 대한 액세스 구성, 추정 또는 제어가 가능합니다.

(*) 계정 종류
<table>
<tr><th>계정 구분</th><th>Description</th><th>확인 필요 사항</th></tr>
<tr><td>Console Admin</td><td>최고 권한을 가지고 있는 단일 계정</td><td>가급적 사용을 지양해야 함</td></tr>
<tr><td>IAM</td><td>AWS IAM 서비스를 통해 생성된 별도 계정</td><td>IAM 역할 및 권한에 대한 현황을 확인해야 함</td></tr>
<tr><td>AD(Active Directory) 연동</td><td>기존 내부에서 사용중인 AD 를 AWS Organizations 서비스에 연동한 계정</td><td>기존 AD 서비스에서 사용중인 각 계정 중 IAM 역할 및 권한이 설정된 현황을 확인해야 함</td></tr>
<tr><td>Access Key</td><td>CLI 환경으로의 접속을 위한 단일 계정 (사용기간에 대한 기준 명시가 필요함)</td><td>발급일 기준 6 개월을 초과한 Access Key 존재 유무</td></tr>
</table>
</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. IAM 사용자 정보 태그 설정 방법
1) AWS 주요 서비스 중 "IAM" 클릭
 
</td></tr>
</table>

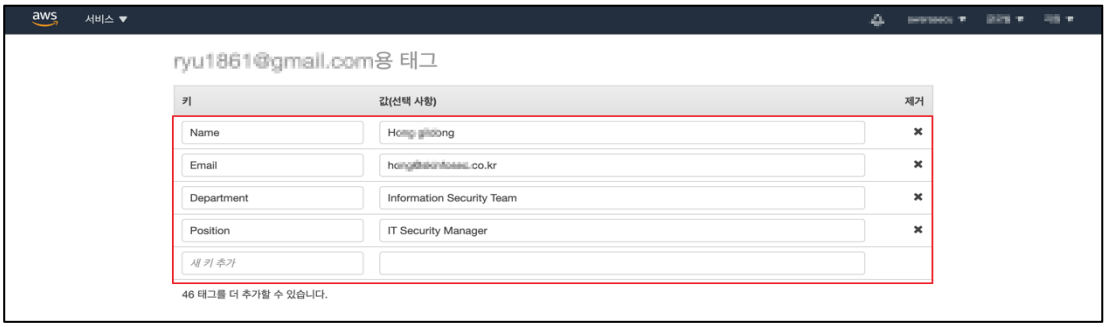
2) IAM "사용자" 클릭 및 계정 목록 확인

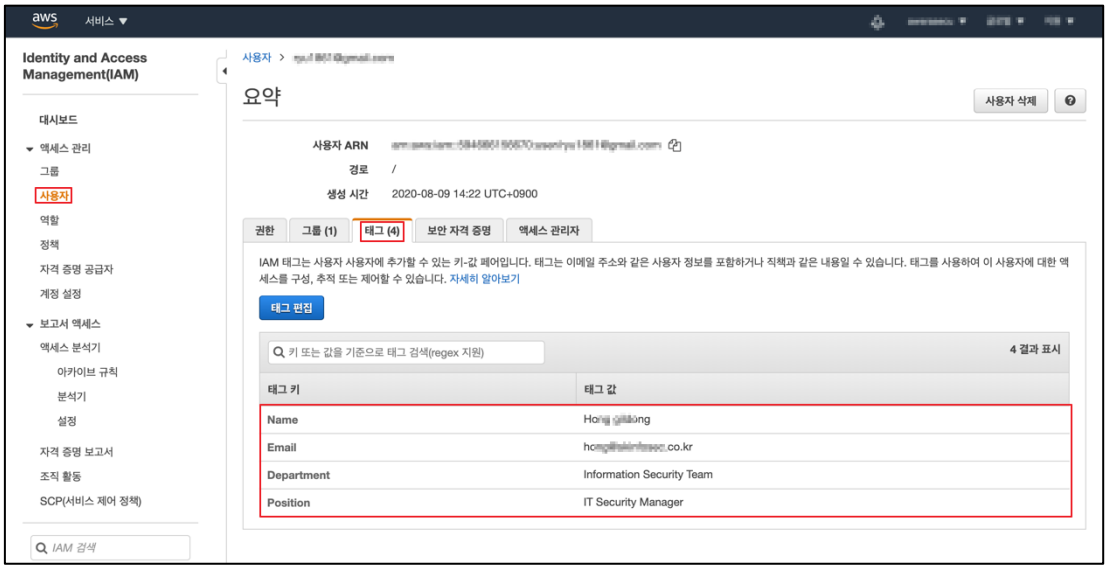


3) IAM 사용자 태그 확인 및 태그 추가 버튼 클릭

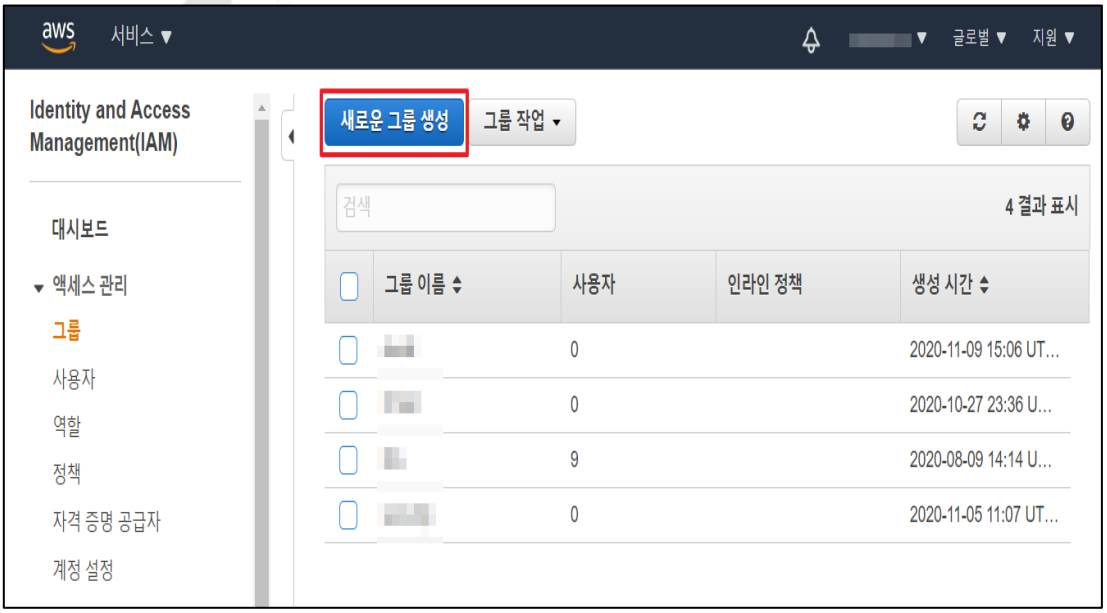


4) IAM 사용자 태그 입력 칸 내 계정 정보 입력 후 저장



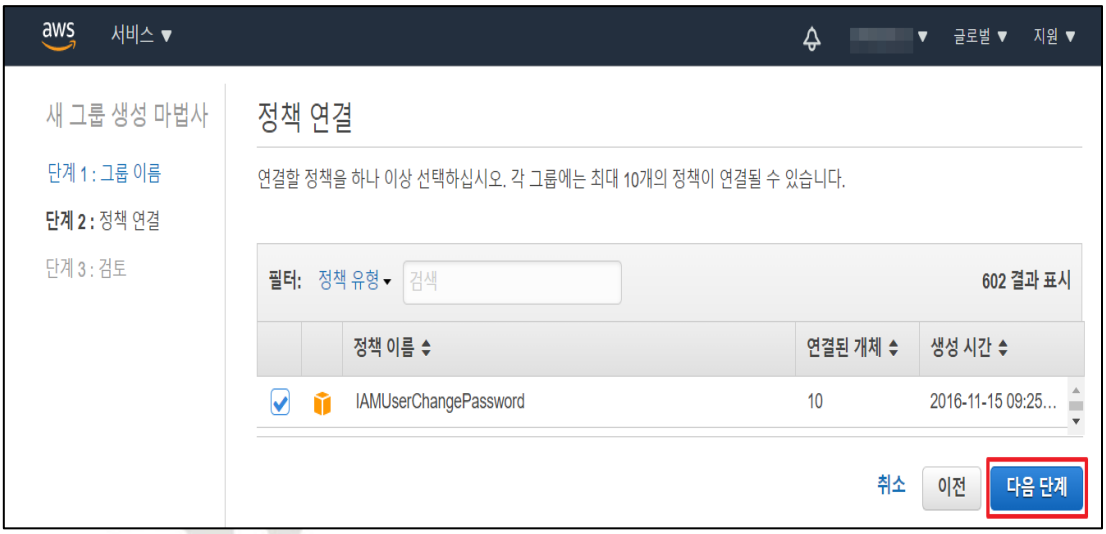
	5) IAM 사용자 태그 계정정보 확인 
진단 기준	**양호기준** : 사용자 정보(이름, 이메일, 부서 등)가 IAM 사용자 태그에 설정되어 있을 경우 **취약기준** : 사용자 정보(이름, 이메일, 부서 등)가 IAM 사용자 태그에 설정되어 있지 않을 경우
비고	Organizations 서비스 사용을 통해 계정을 관리하는 경우 AD 계정을 연동하여 사용하기 때문에 계정 정보를 태그 하지 않아도 양호로 처리될 수 있음

1.4 IAM 그룹 사용자 계정 관리

분류	계정 관리	중요도	중
항목명	IAM 그룹 사용자 계정 관리		
항목 설명	IAM 그룹은 IAM 사용자들의 집합으로 AWS 사용자들에 대한 권한을 쉽게 관리할 수 있습니다. 그룹에 대한 IAM 권한 적용 시 그룹 내 사용자들에게 일괄 적용이 되기 때문에 그룹 별 적절한 권한을 할당하여 사용해야 합니다.		
설정 방법	**가. IAM 그룹 사용자 계정 관리 확인 방법** 1) IAM 대시보드 내 그룹 클릭  2) 새로운 그룹 생성 클릭 		

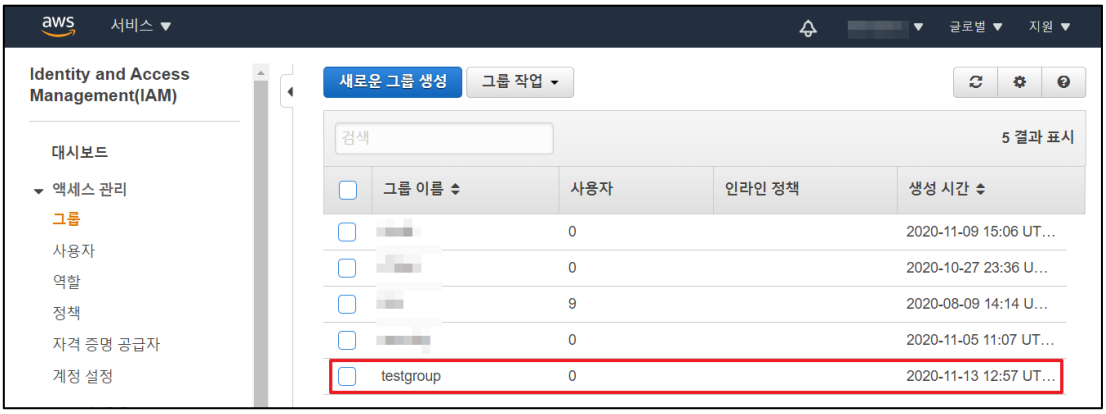
3) 그룹 이름 설정

4) 그룹 내 정책 연결

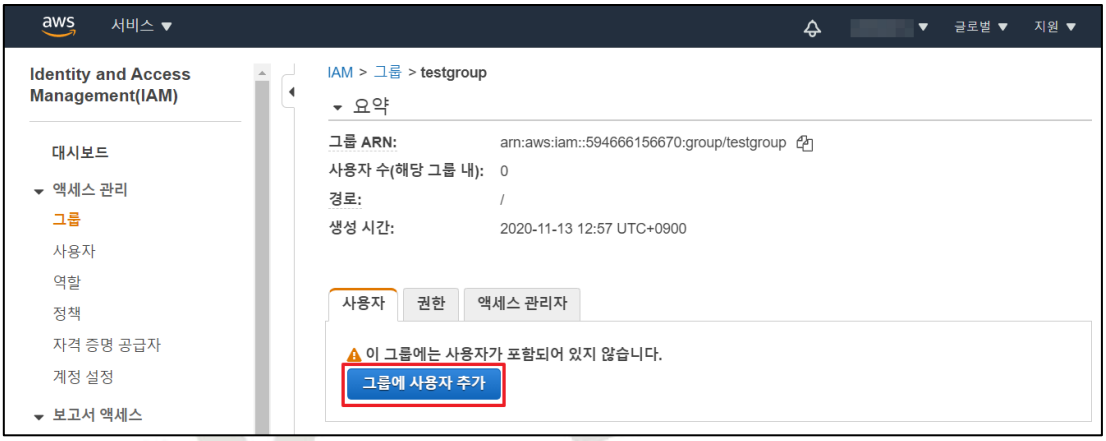


5) 그룹 생성 클릭

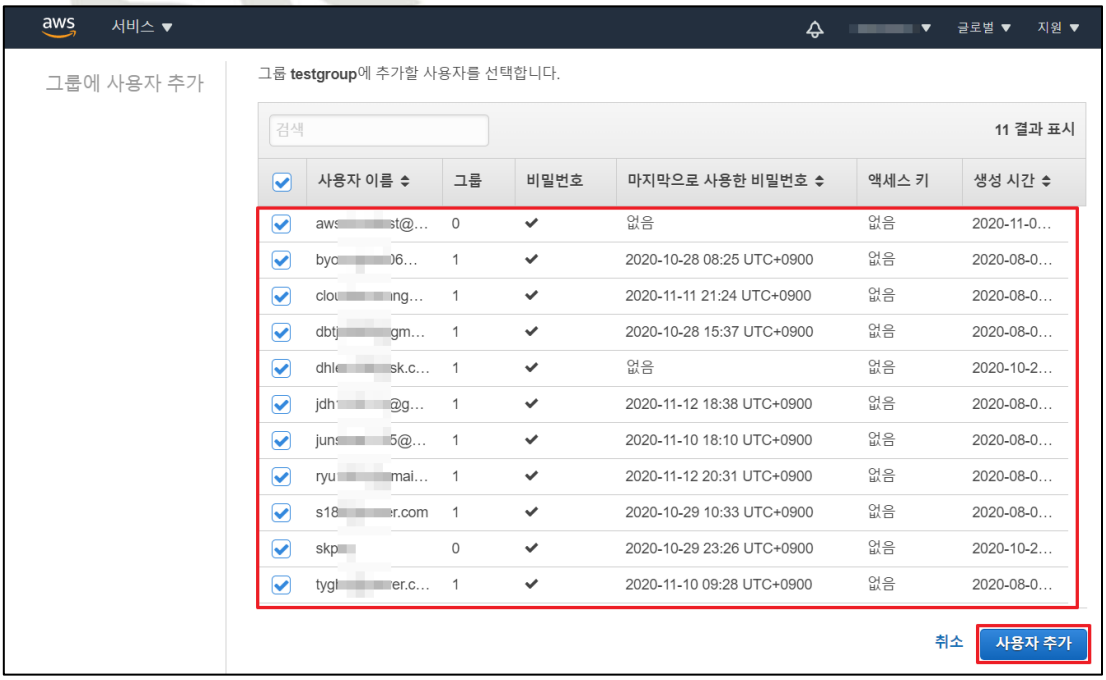
6) 그룹 생성 확인



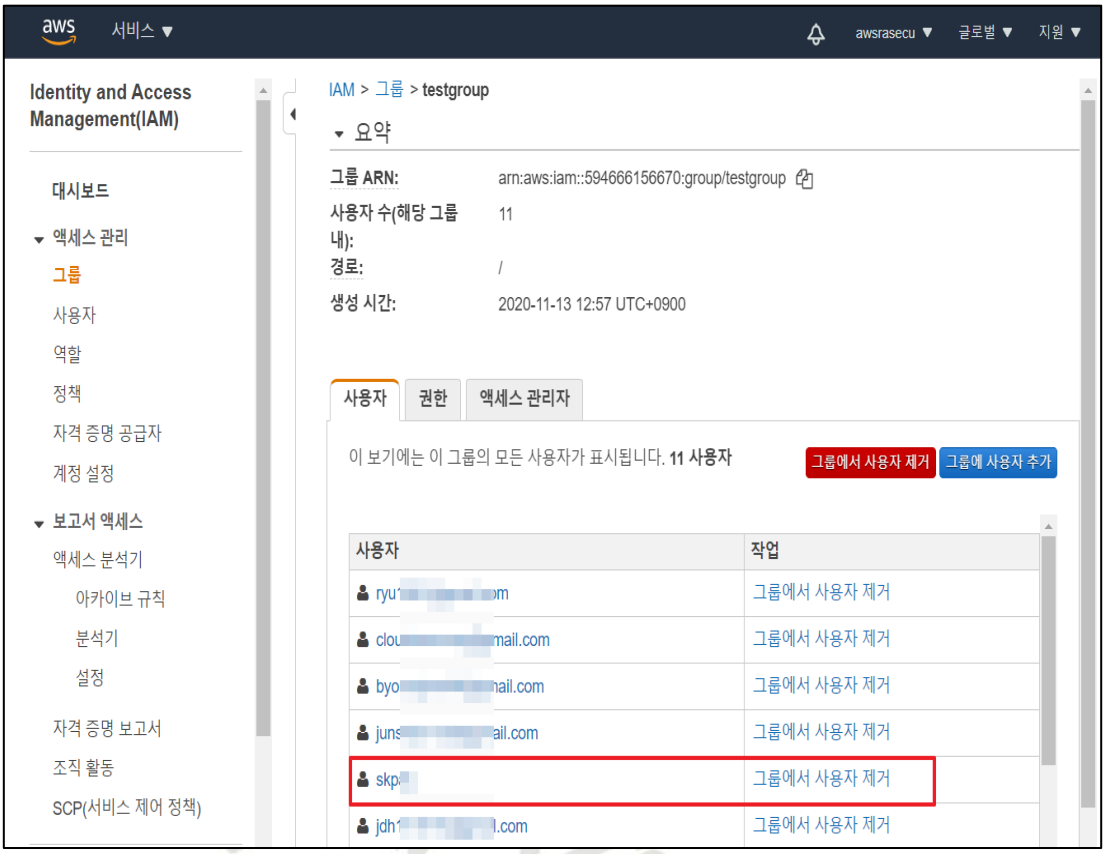
7) 그룹 내 사용자 추가 버튼 클릭



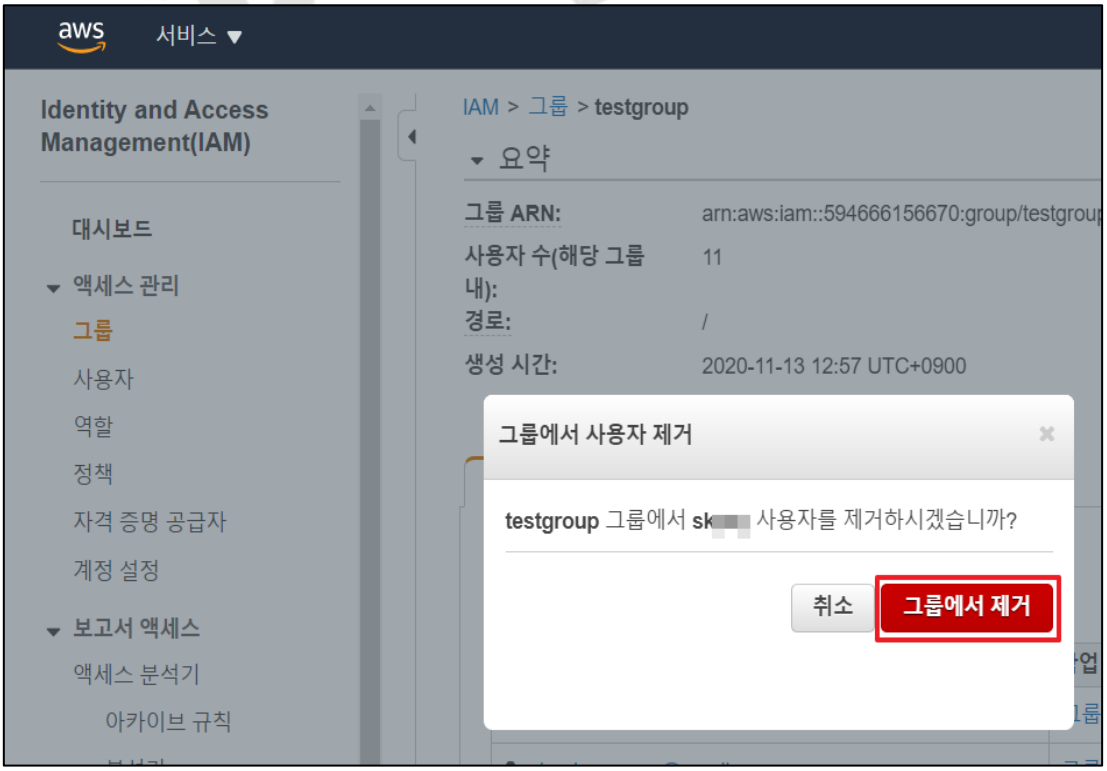
8) 그룹 내 사용자 추가

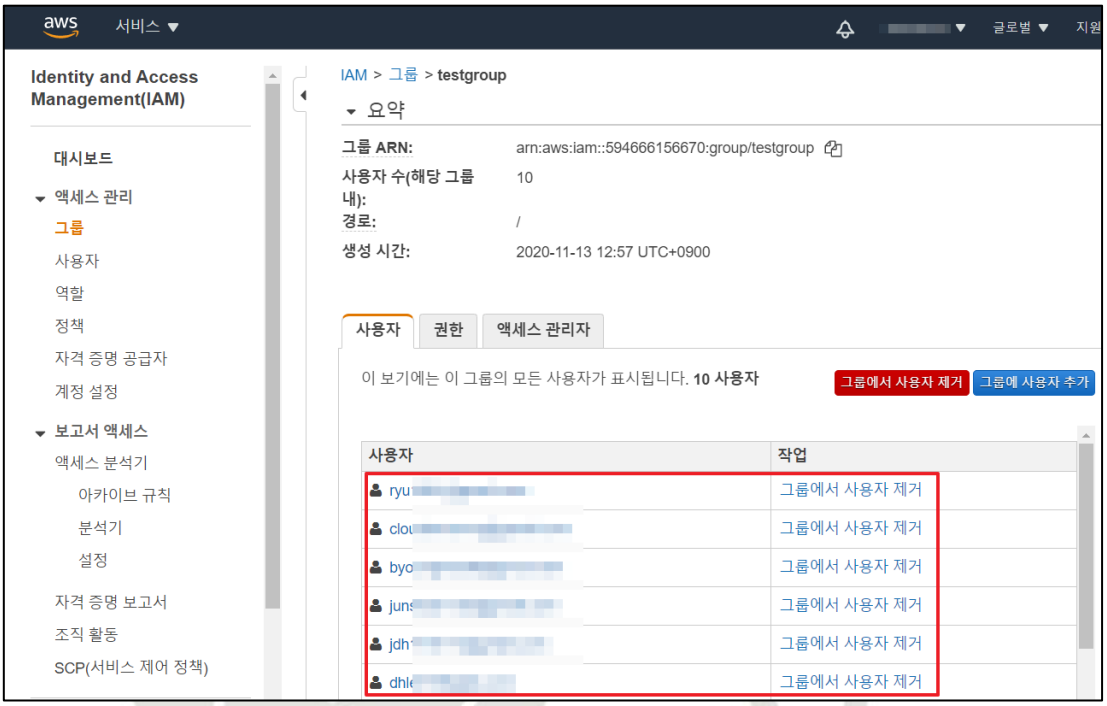


9) 그룹 내 불필요한 사용자 확인 및 그룹에서 사용자 제거 클릭

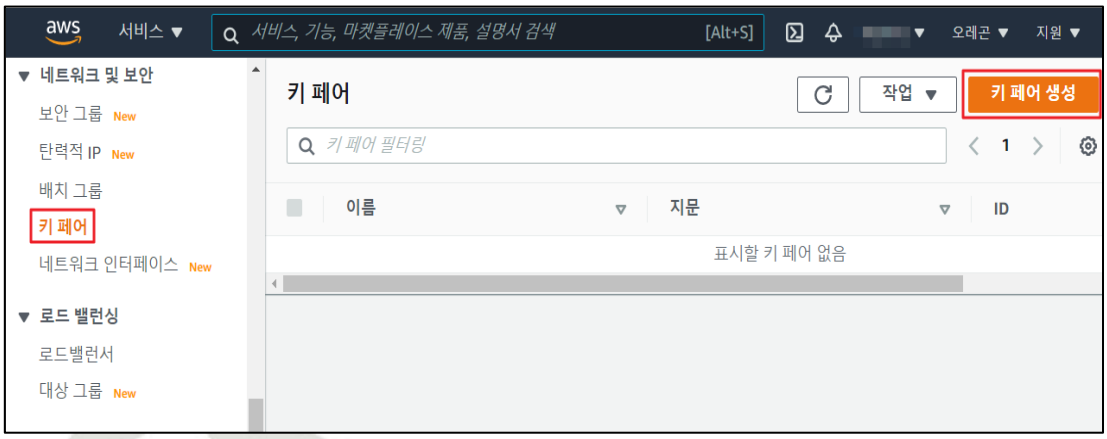
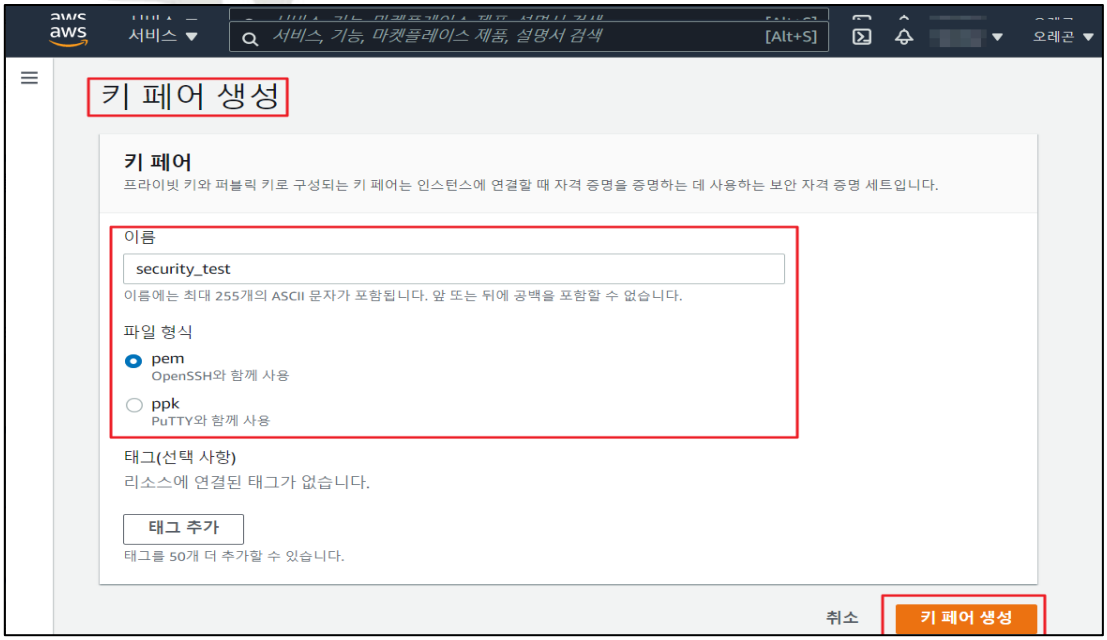


10) 그룹에서 제거 클릭

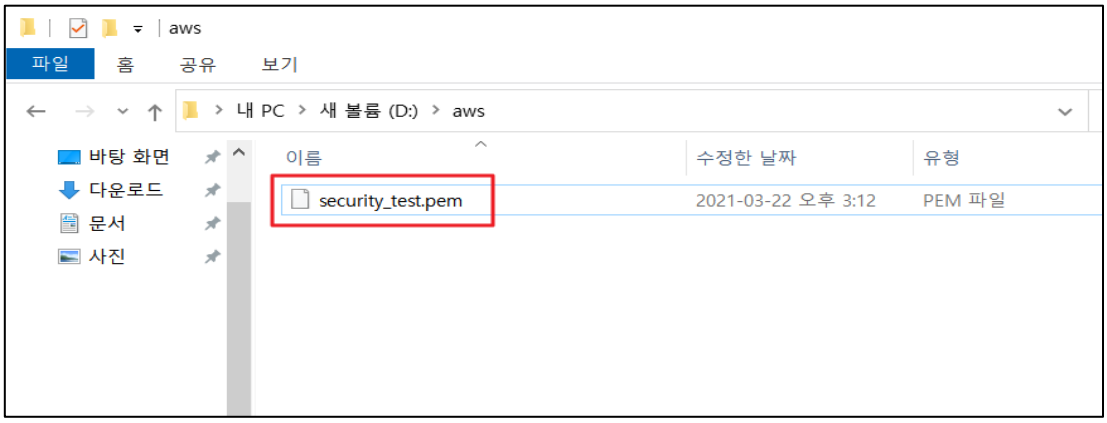


	11) 그룹 내 불필요한 사용자 제거 확인 
진단 기준	**양호기준** : IAM 그룹에 포함된 사용자 계정 중 불필요한 계정이 존재하지 않을 경우 **취약기준** : IAM 그룹에 포함된 사용자 계정 중 불필요한 계정이 존재할 경우
비고	

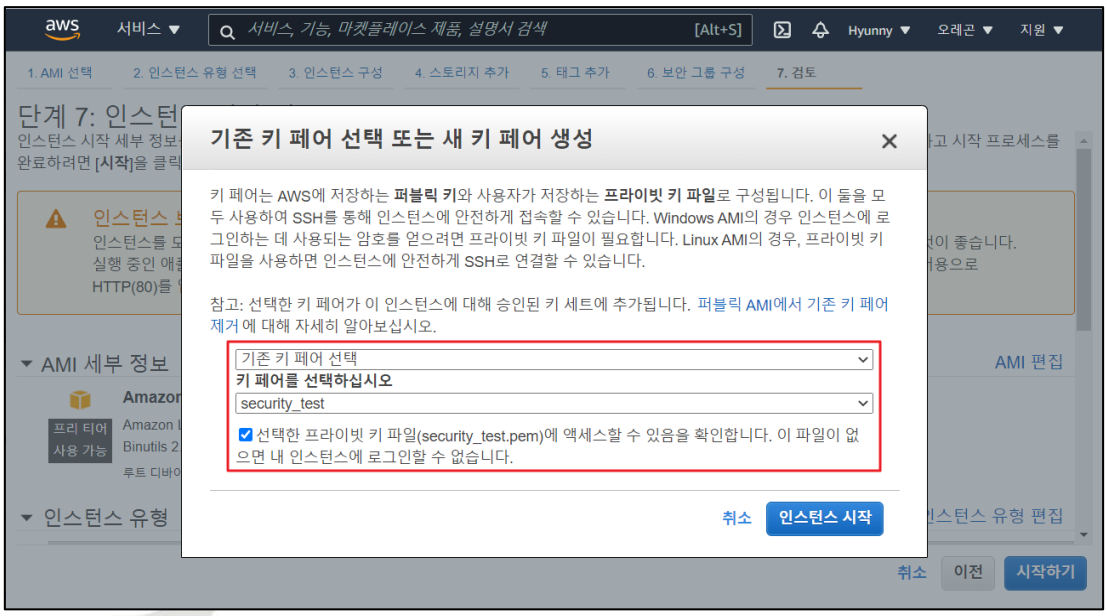
1.5 Key Pair 접근 관리

분류	계정 관리	중요도	상
항목명	Key Pair 접근 관리		
항목 설명	EC2는 키(Key)를 이용한 암호화 기법을 제공합니다. 해당 기법은 퍼블릭/프라이빗 키를 통해 각각 데이터의 암호화 및 해독을 하는 방식으로 여기에 사용되는 키를 'Key Pair' 라고 하며, 해당 암호화 기법을 사용할 시 EC2의 보안성을 향상시킬 수 있으므로 EC2 인스턴스 생성 시 Key Pair 등록을 권장합니다. 또한, Amazon EC2에 사용되는 키는 '2048비트 SSH-2 RSA 키'이며, Key Pair는 리전당 최대 5천 개까지 보유할 수 있습니다.		
설정 방법	**가. 키 생성 및 등록 방법** 1) 콘솔을 통한 키 생성: 네트워크 및 보안 → Key Pair → Key Pair 생성  2) Key Pair 생성 		

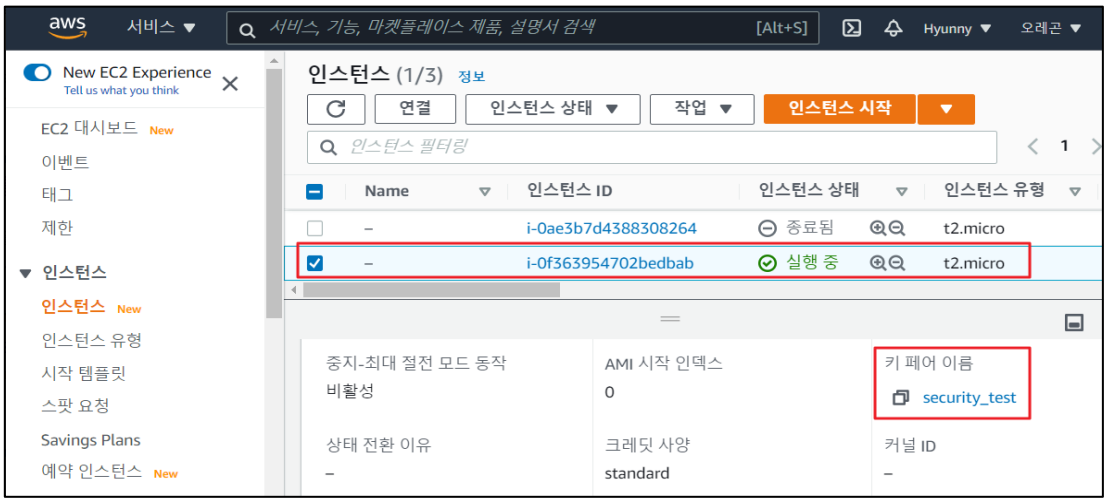
3) 생성된 Key Pair 파일을 쉽게 유추 및 접근할 수 없는 공간에 보관



4) 인스턴스 생성 시 생성된 Key Pair 등록

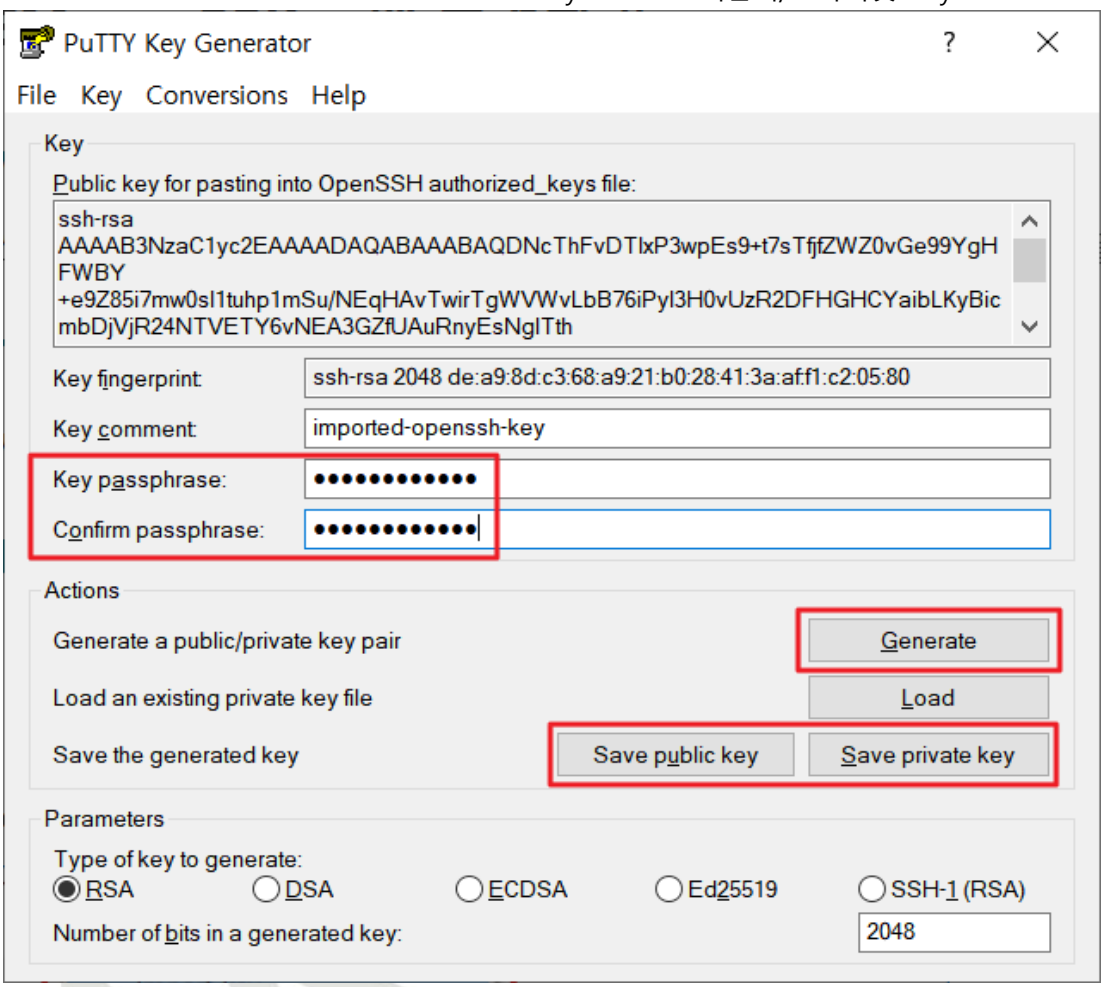


5) 인스턴트 생성 완료 시 Key Pair 정상 등록여부 확인

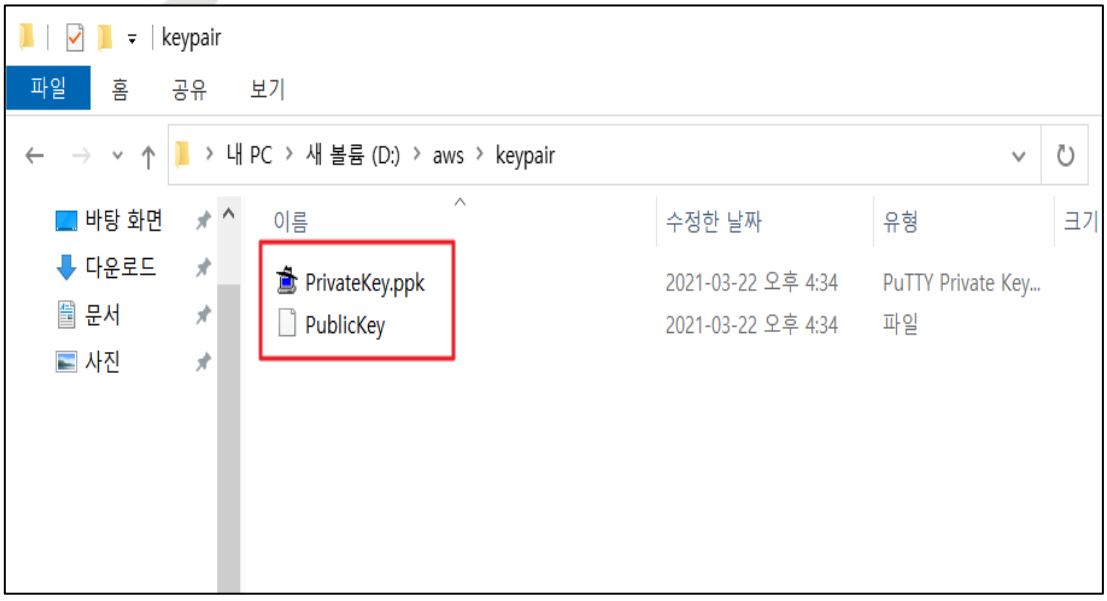


6) PuTTY-Gen을 통한 키 생성

: PuTTYGen.exe → Conversions → Im포트 Key → Save 퍼블릭/프라이빗 Key



7) 생성된 Key Pair 파일을 쉽게 유추 및 접근할 수 없는 공간에 보관



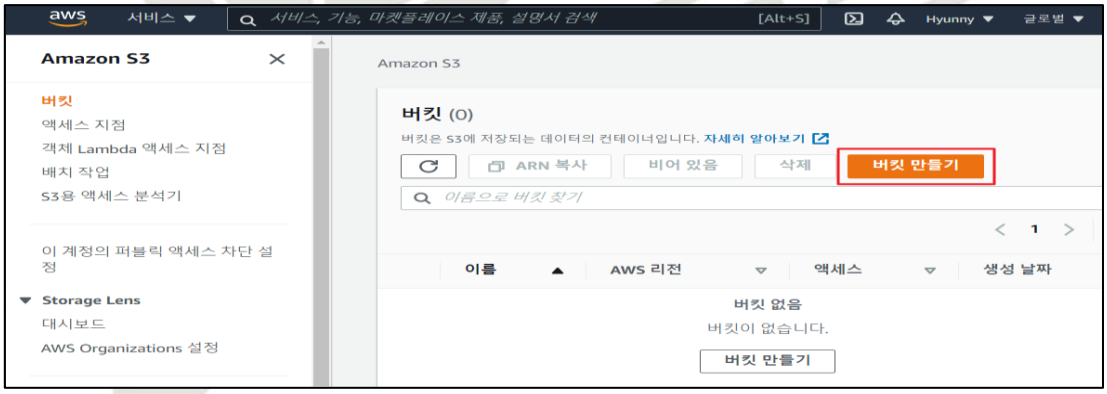
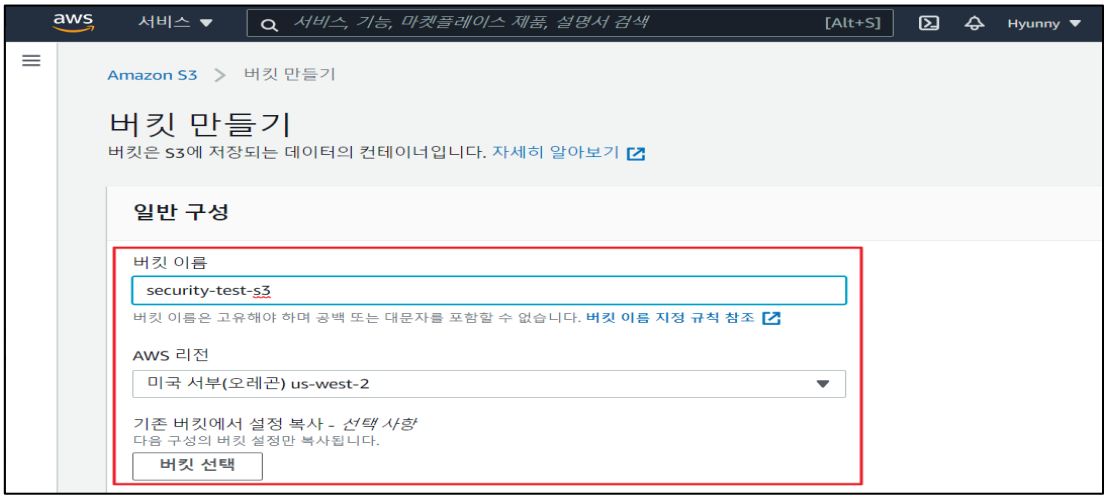
8) 생성된 키 콘솔로 가져오기: 네트워크 및 보안 → Key Pair → Key Pair 가져오기

9) 가져오기 설정

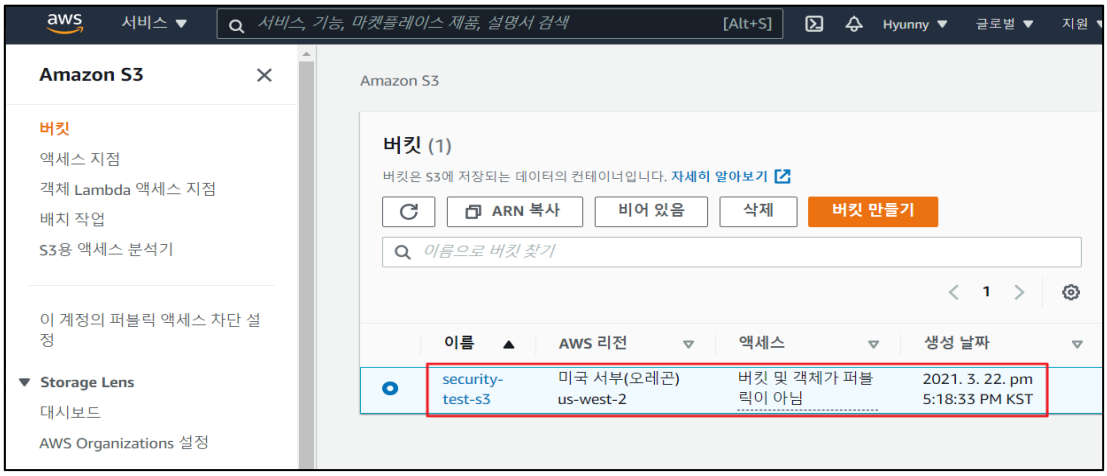
10) 생성된 키가 콘솔에 정상적으로 등록되었는지 확인

진단 기준	**양호기준** : Key Pair(PEM)를 통해 EC2 인스턴스에 접근할 경우 **취약기준** : Key Pair(PEM)가 아닌 일반 패스워드로 EC2 인스턴스에 접근할 경우
비고	

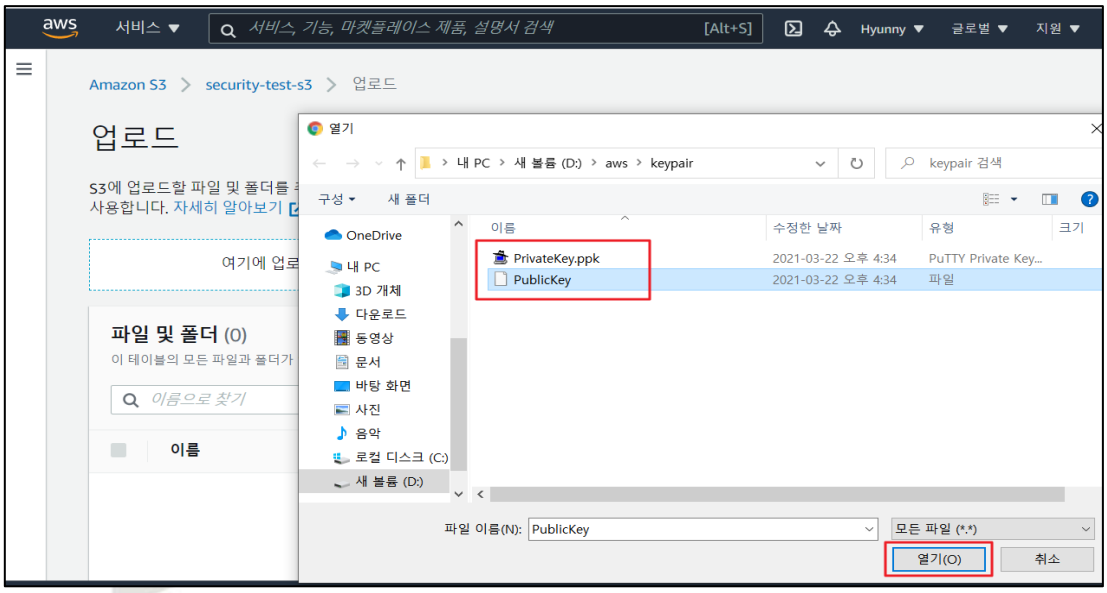
1.6 Key Pair 보관 관리

분류	계정 관리	중요도	상
항목명	Key Pair 보관 관리		
항목 설명	EC2는 키(Key)를 이용한 암호화 기법을 제공합니다. 해당 기법은 퍼블릭/프라이빗 키를 통해 각각 데이터의 암호화 및 해독을 하는 방식으로 여기에 사용되는 키를 'Key Pair' 라고 하며, 해당 암호화 기법을 사용할 시 EC2의 보안성을 향상시킬 수 있으므로 EC2 인스턴스 생성 시 Key Pair 등록을 권장합니다. 또한, Amazon EC2에 사용되는 키는 '2048비트 SSH-2 RSA 키'이며, Key Pair는 리전당 최대 5천 개까지 보유할 수 있습니다. **※ Key Pair는 타 사용자가 확인이 가능한 공개된 위치에 보관하게 될 경우 EC2 Instance에 무단으로 접근이 가능해지므로 비인가자가 쉽게 유추 및 접근이 불가능한 장소에 보관해야 합니다.**		
설정 방법	**가. S3 버킷 내 Key Pair 관리하기** 1) 버킷 접근  2) 버킷 생성하기 		

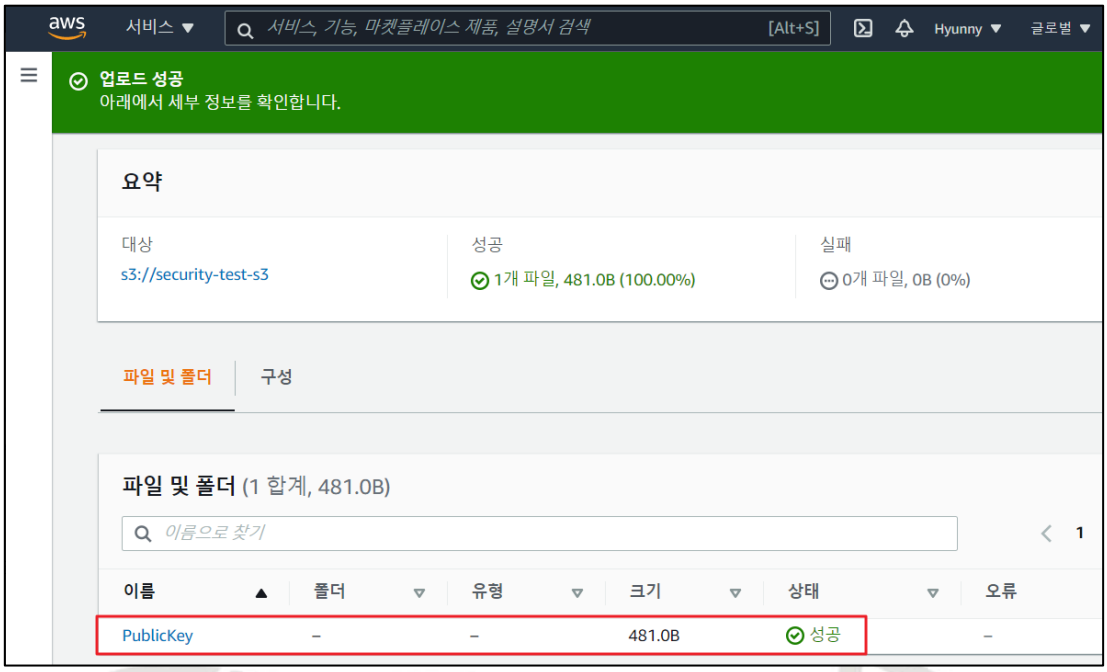
3) 생성된 버킷 확인



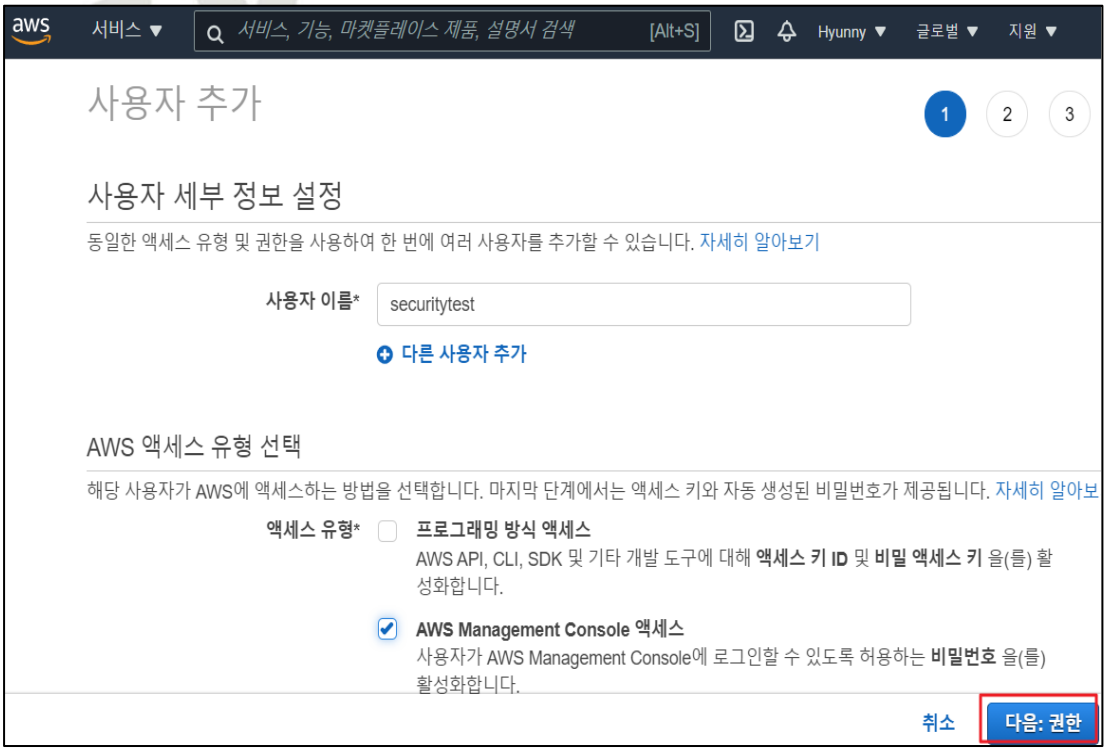
4) S3 버킷 내 KeyPair 업로드



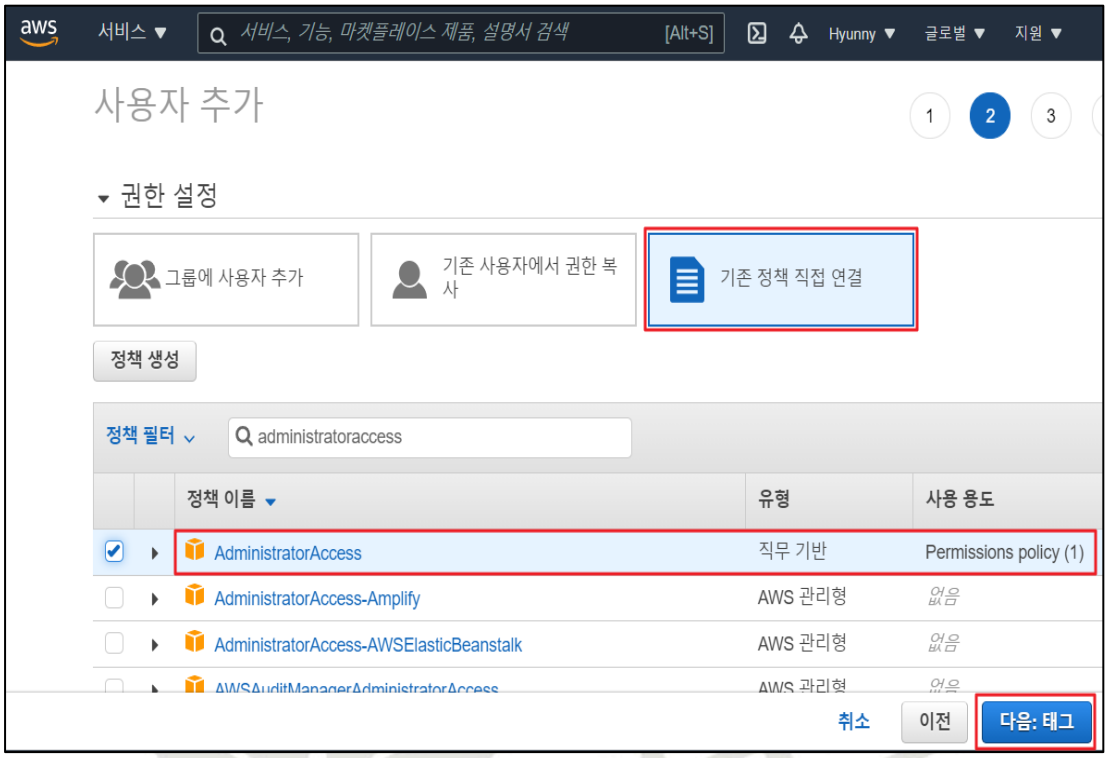
5) 업로드 된 KeyPair 확인

	6) Key Pair 보관 확인(프라이빗 S3 버킷) 
진단 기준	**양호기준** : Key Pair(PEM) File의 보관 위치가 쉽게 유추할 수 없는 공간에 보관되어 있을 경우 **취약기준** : Key Pair(PEM) File의 보관 위치가 다수 접근이 가능한 공용 공간(퍼블릭 S3, EC2 "Admin Console(/)" 디렉터리 등)에 보관되어 있을 경우
비고	

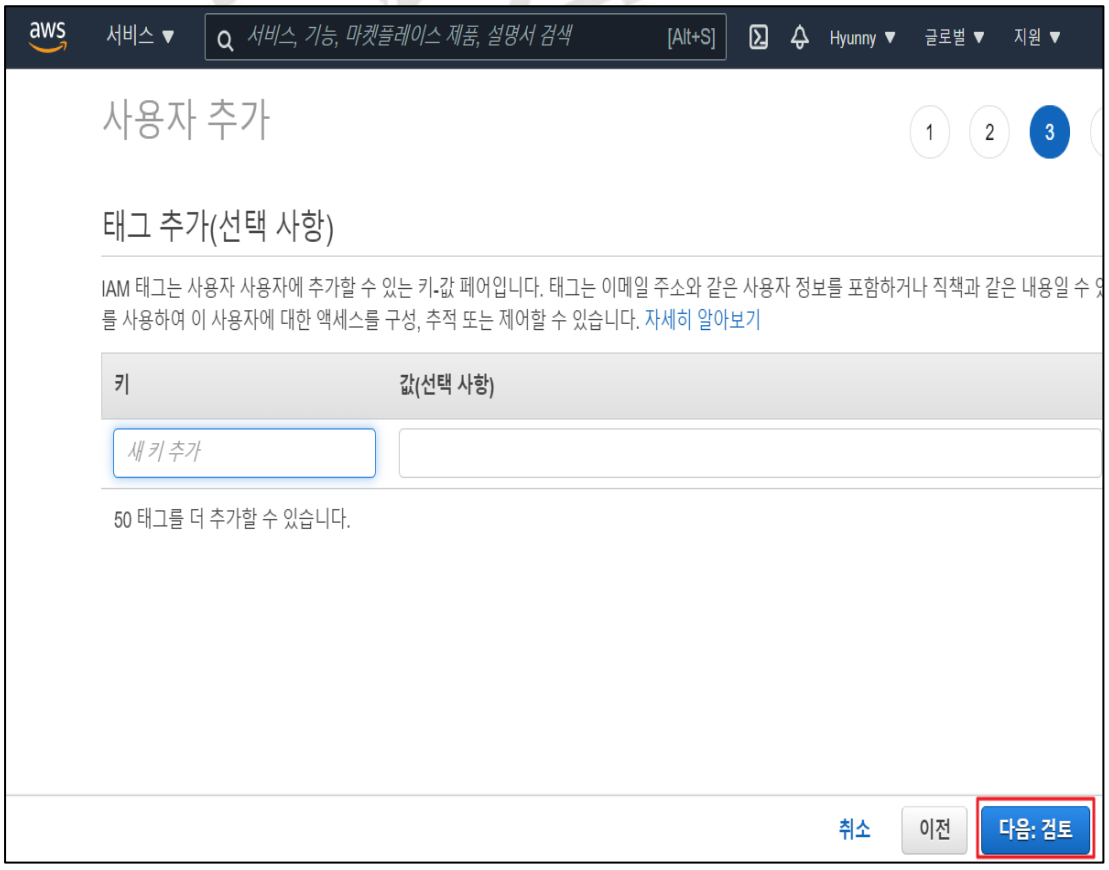
1.7 Admin Console 관리자 정책 관리

분류	권한 관리	중요도	중
항목명	Admin Console 관리자 정책 관리		
항목 설명	AWS Cloud 사용을 위해 처음 발급한 계정은 IAM 사용자 계정과 달리 모든 서비스에 접근할 수 있는 최고 관리자 계정입니다. Cloud 서비스 특성 상 인터넷 연결이 가능한 망에서 계정정보를 입력하여 WEB Console에 접근하게 됩니다. 이는 최고 권한을 보유하고 있는 관리자 계정이 아닌 권한이 조정된 IAM 사용자 계정을 기본으로 사용해야 보다 안전한 접근이 이뤄질 수 있습니다.		
설정 방법	**가. IAM 사용자 계정 생성** 1) 사용자 추가 버튼 클릭  2) 사용자 추가 (기본설정 - 이름, 액세스 유형 선택) 		

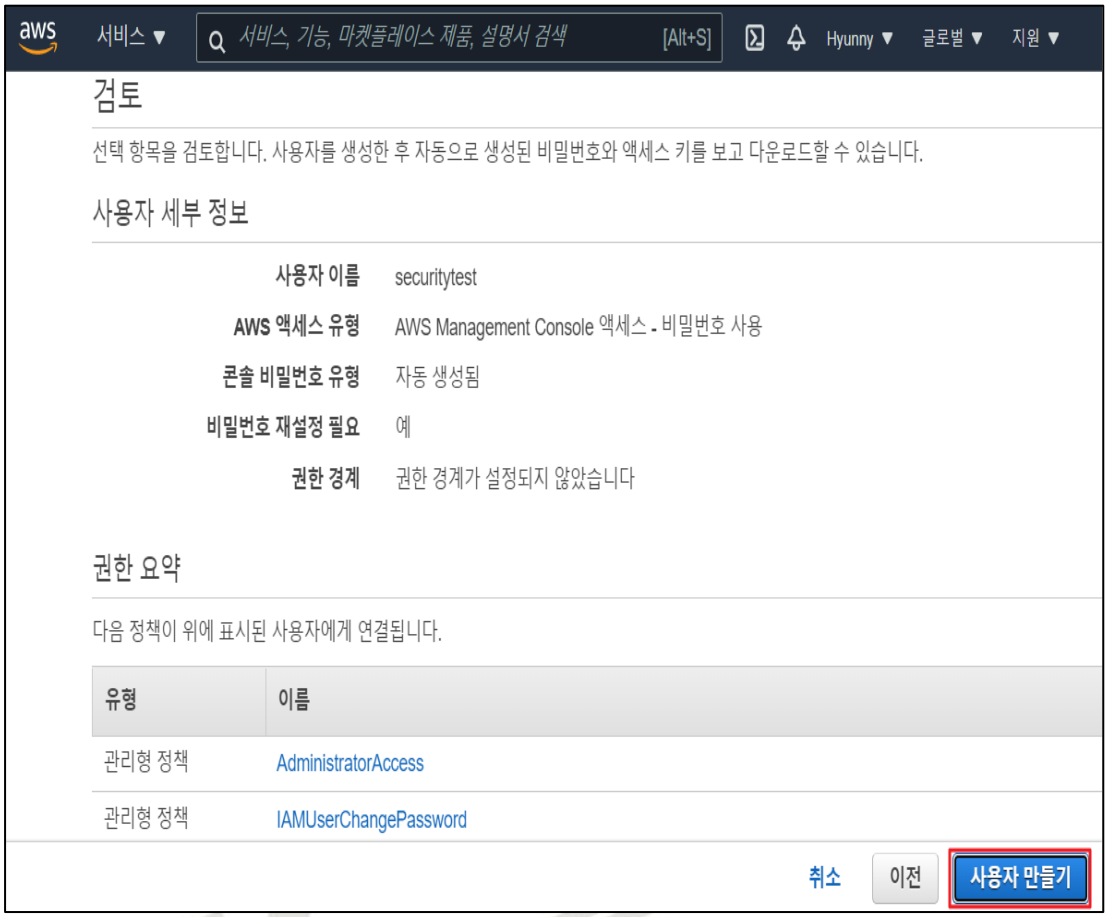
3) 사용자 추가 (기존 정책 직접 연결하기)



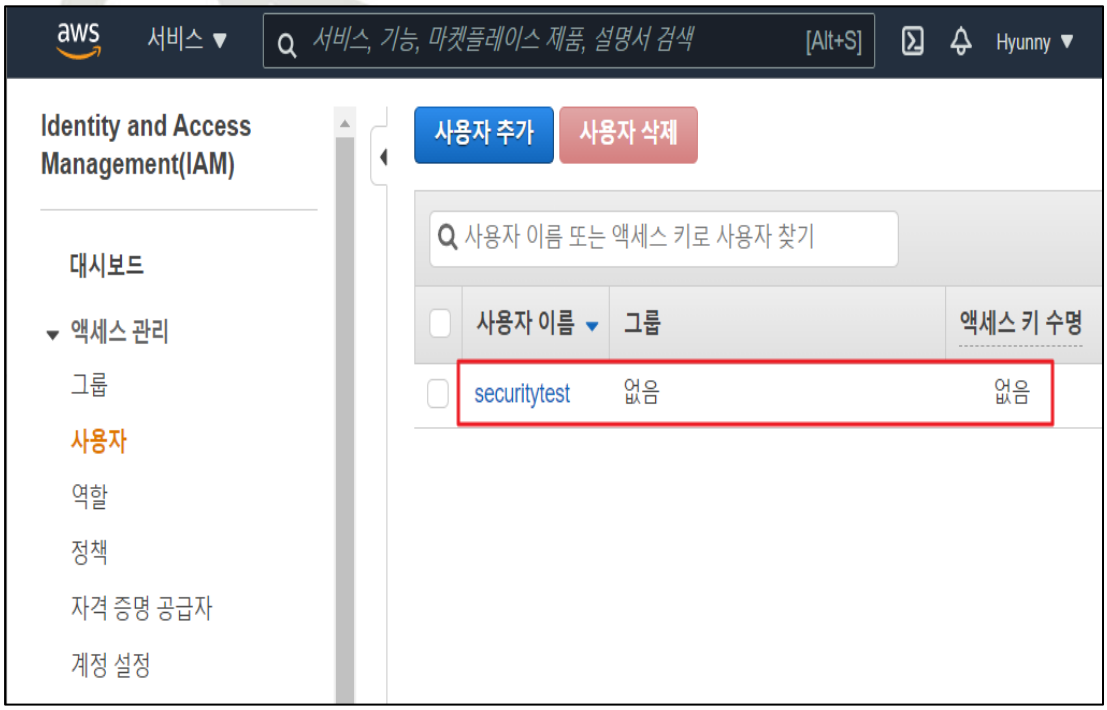
4) 사용자 추가 (태그 계정 정보 입력)

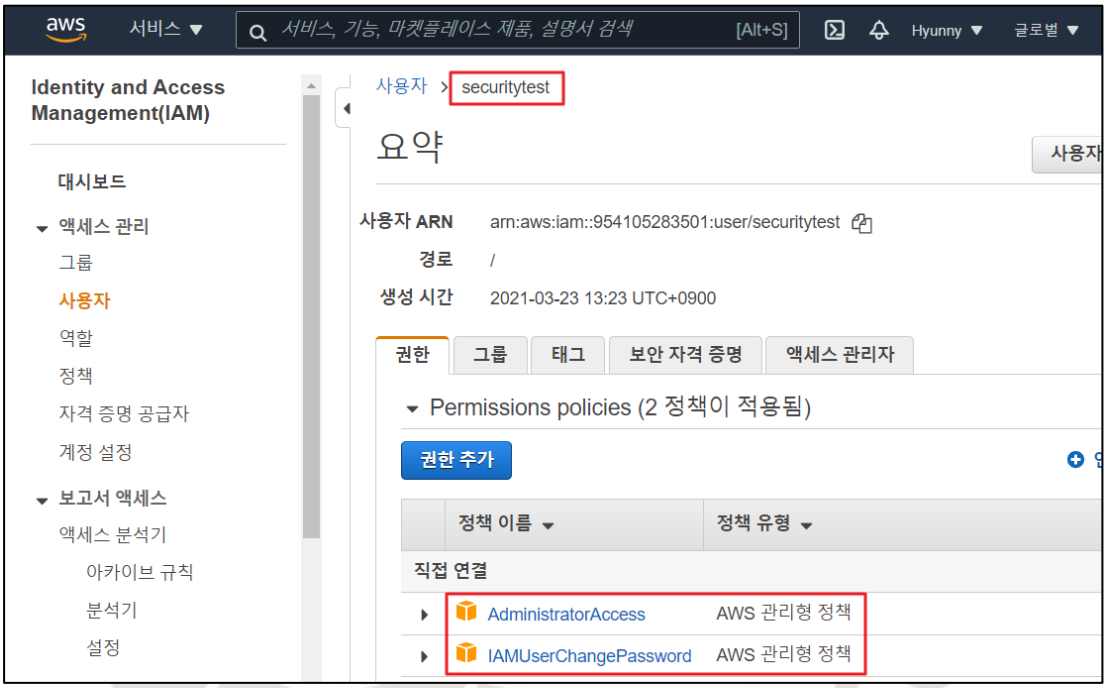


5) 사용자 추가 (검토하기)

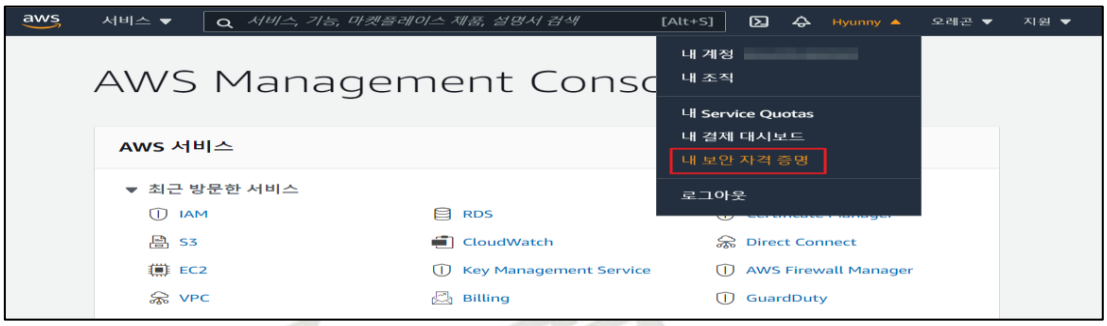
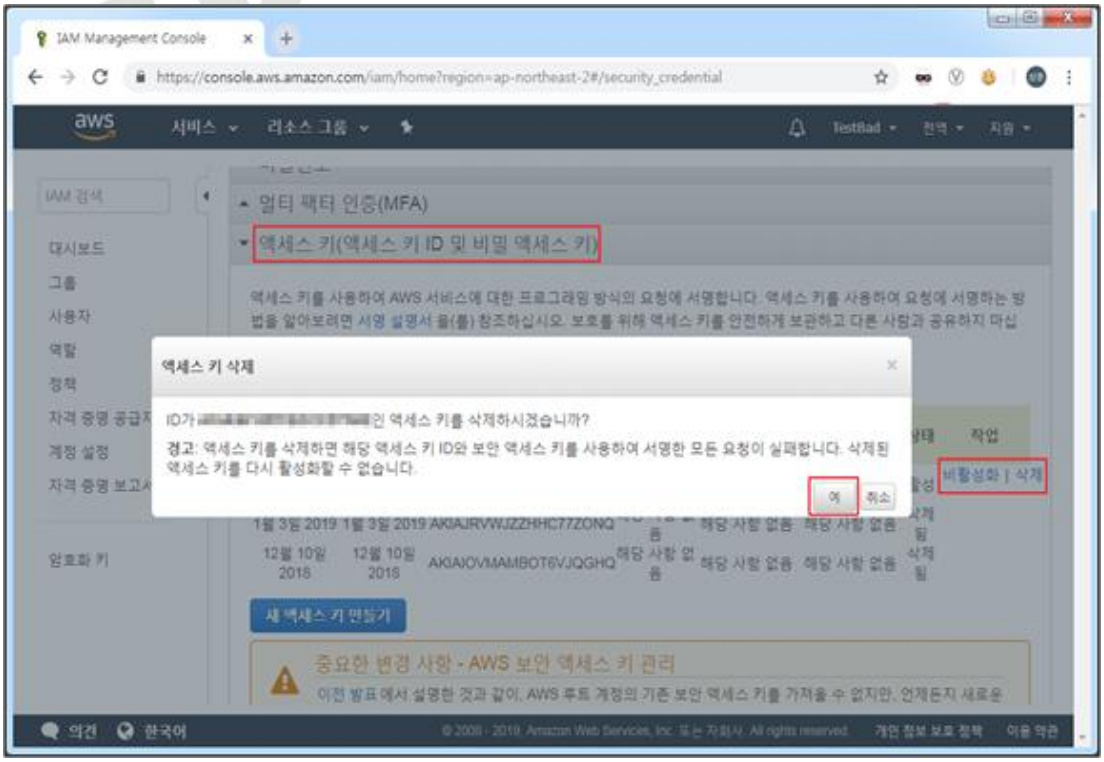


6) IAM 사용자에 추가된 신규 사용자 확인



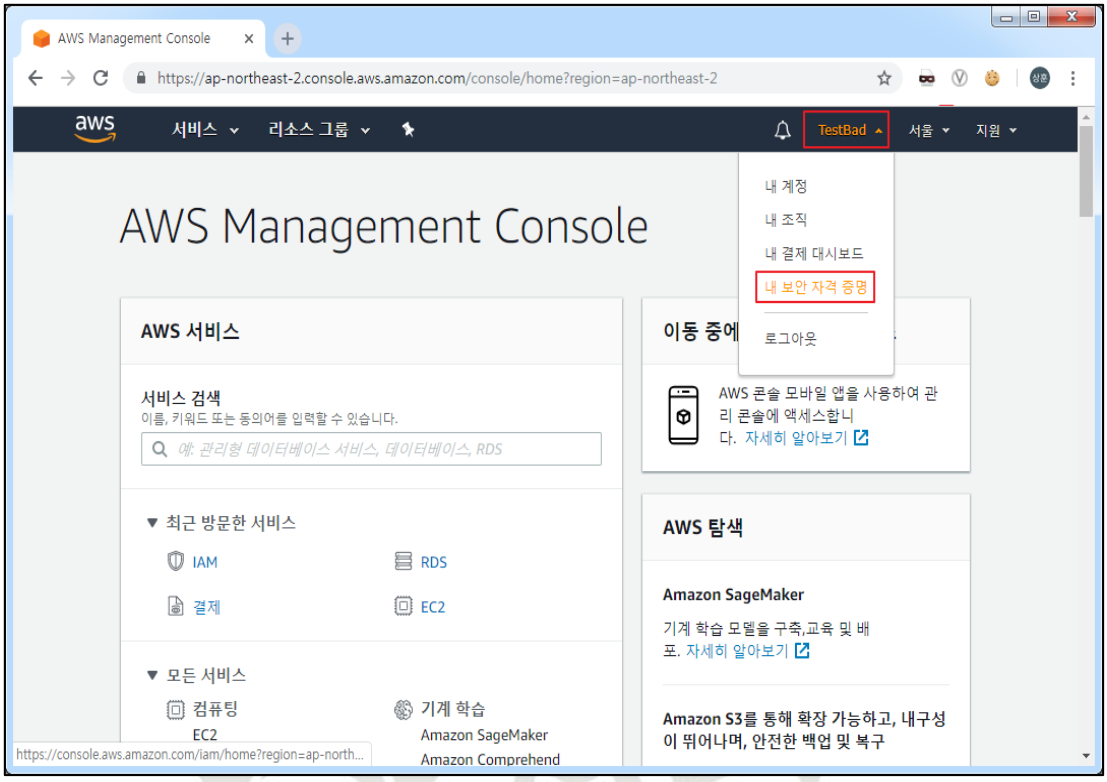
	7) 사용자 권한 확인 
진단 기준	**양호기준** : Admin Console 계정을 서비스 용도로 사용하지 않는 경우 **취약기준** : Admin Console 계정을 서비스 용도로 사용하는 경우
비고	

1.8 Admin Console 계정 Access Key 활성화 및 사용주기 관리

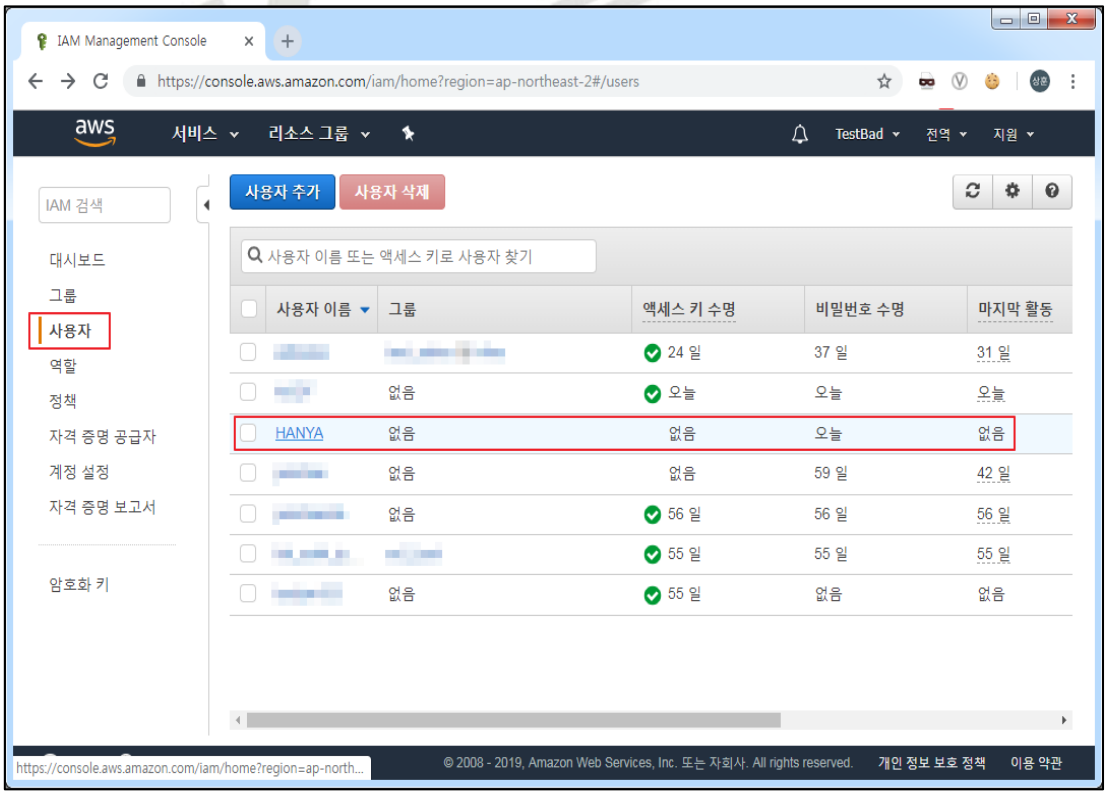
분류	계정 관리	중요도	상
항목명	Admin Console 계정 Access Key 활성화 및 사용주기 관리		
항목 설명	Access Key는 AWS의 CLI 도구나 API를 사용할 때 필요한 인증수단으로 생성 사용자에 대한 결제정보를 포함한 모든 AWS 서비스의 전체 리소스에 대한 권한을 갖고있으므로 유출 시 심각한 피해가 발생할 가능성이 높기에 AWS Admin Console Account에 대한 Access Key 삭제를 권장합니다. **※ Access Key 관리 주기** Key 수명(60일 이내), 비밀번호 수명(60일 이내), 마지막 활동(30일 이내)		
설정 방법	**가. AWS Admin Console Account Access Key 삭제 방법** 1) 메인 우측 상단 계정 → 내 보안 자격 증명  2) Access Key(Access Key ID 및 비밀 Access Key) → 삭제 → 예  		

나. IAM User Account Access Key 삭제 방법

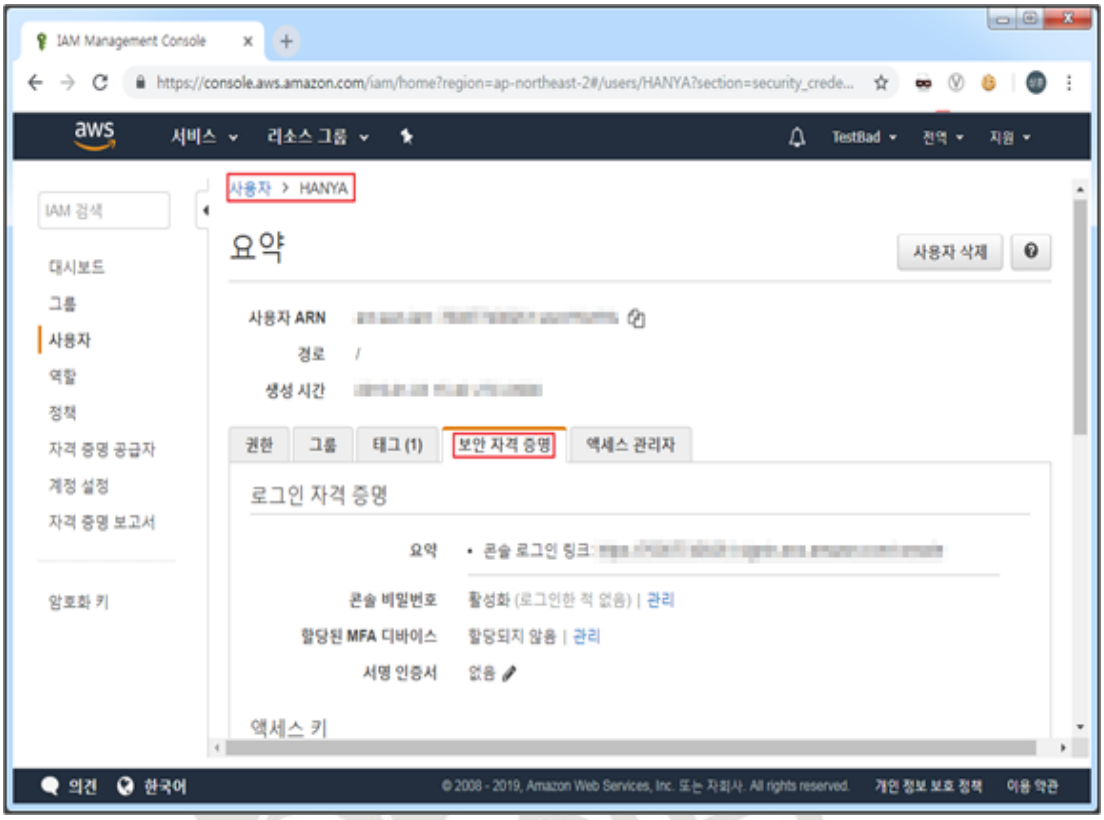
1) 메인 우측 상단 계정 → 내 보안 자격 증명



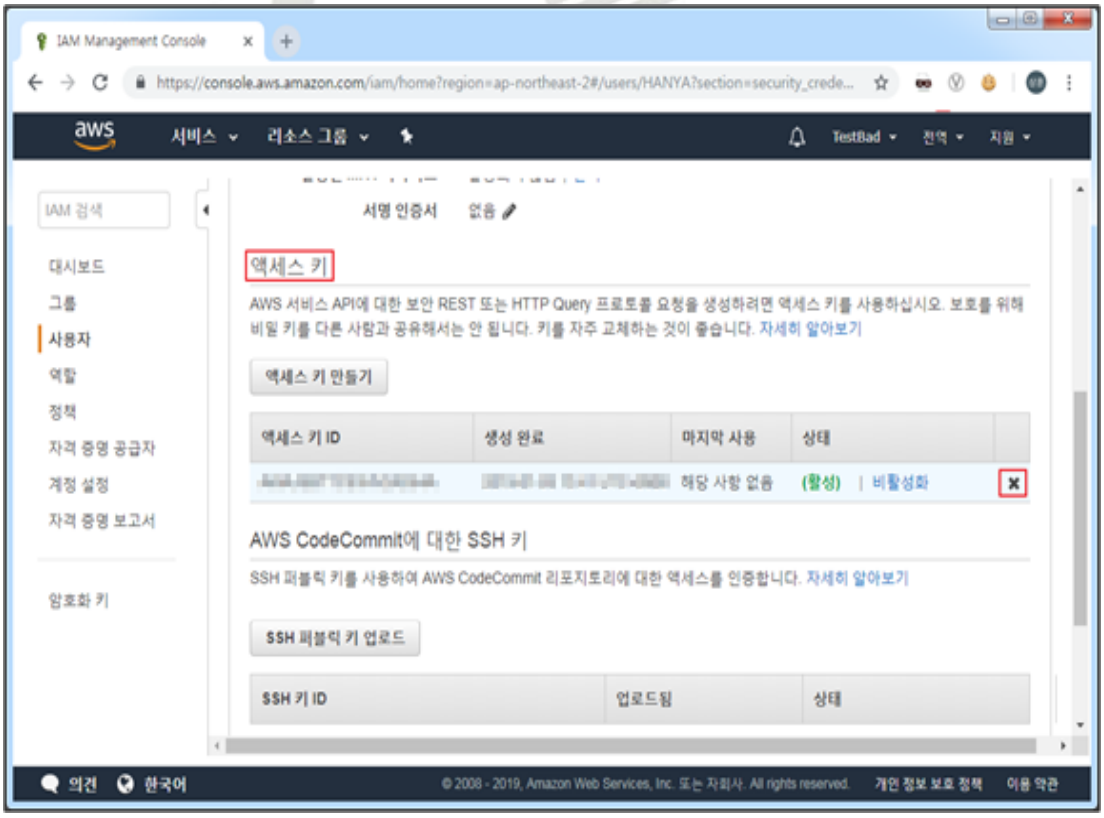
2) 사용자 → Access Key를 삭제할 계정 선택

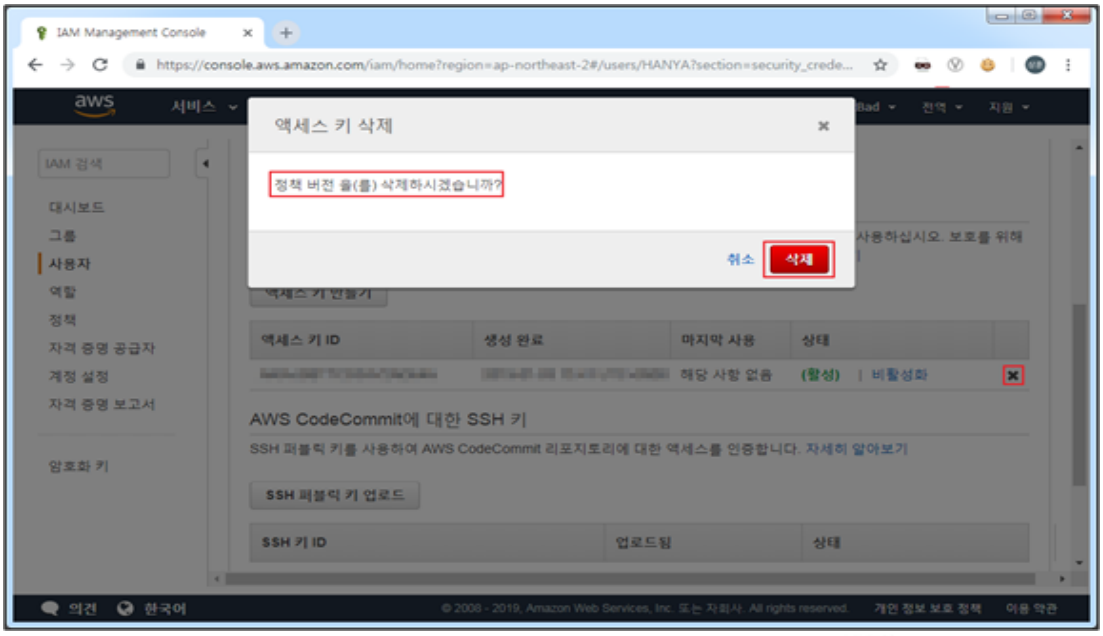


3) 요약 → 보안 자격 증명 탭



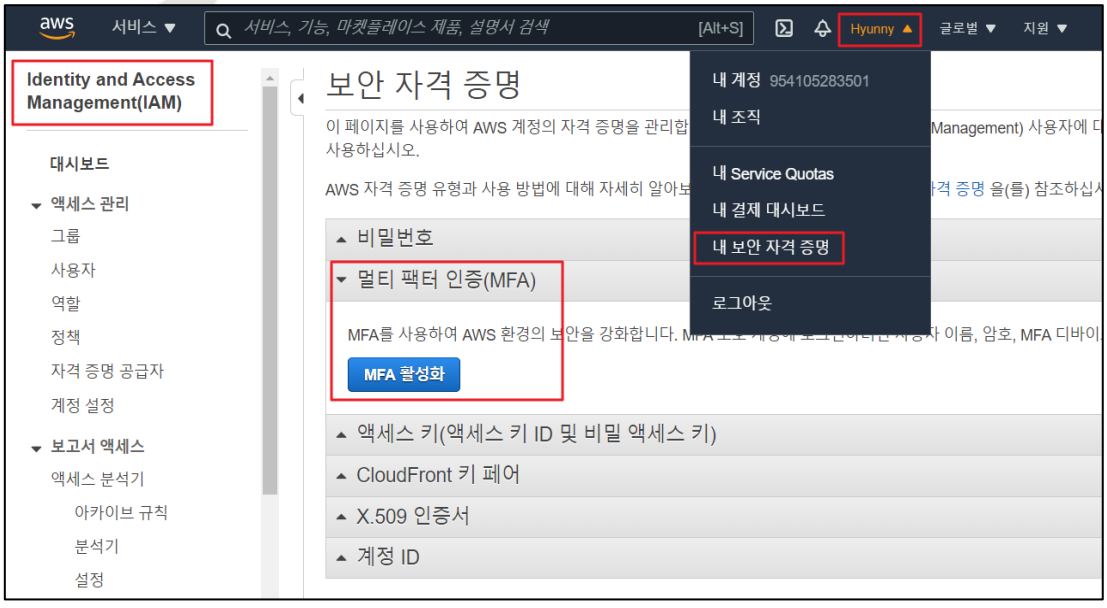
4) Access Key → Access Key ID → 'X'(삭제) 버튼



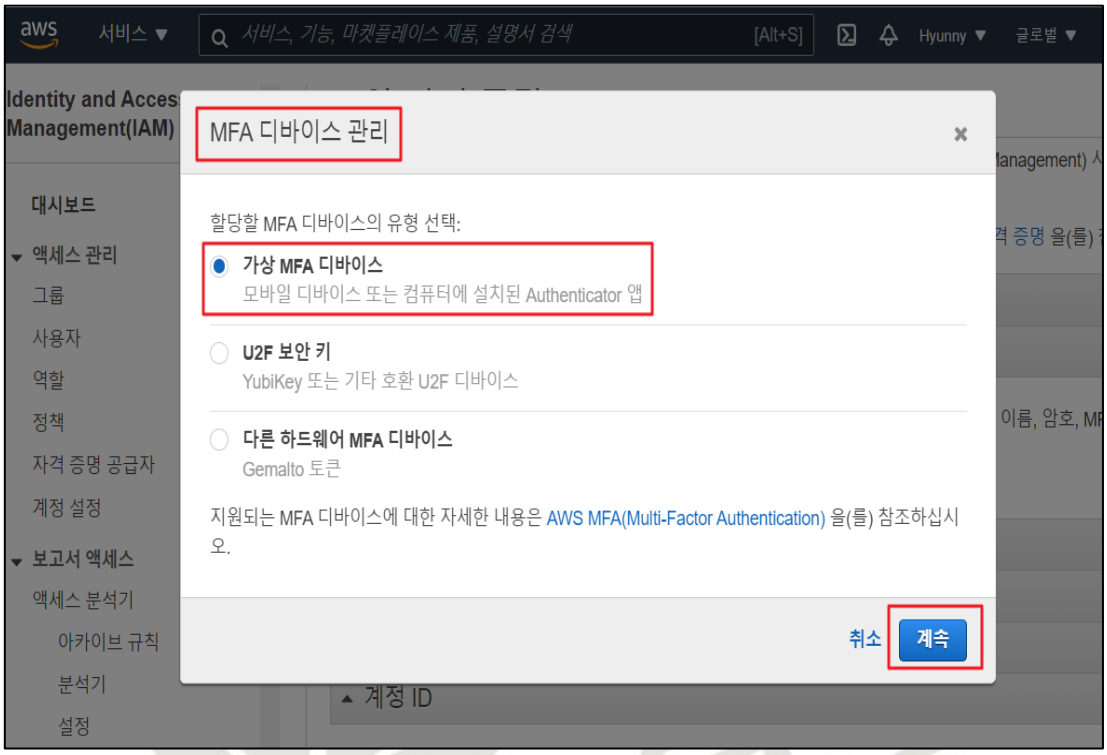
	5) Access Key 삭제 → 삭제 
진단 기준	**양호기준** : AWS Admin Console 계정에 Access Key가 존재하지 않고 IAM 사용자 계정에 대한 Access Key 사용 주기가 60일 이내일 경우 **취약기준** : AWS Admin Console 계정에 Access Key가 존재하거나 IAM 사용자 계정에 대한 Access Key 사용 주기가 60일 초과일 경우
비고	

1.9 MFA (Multi-Factor Authentication) 설정

<table>
<tr><td>분류</td><td>계정 관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">MFA (Multi-Factor Authentication) 설정</td></tr>
<tr><td>항목
설명</td><td colspan="3">AWS Multi-Factor Authentication(MFA)은 사용자 이름과 암호 외에 보안을 한층 더 강화할 수 있는 방법으로 MFA를 활성화하면 사용자가 AWS 웹 사이트에 로그인할 때 사용자 이름과 암호뿐만 아니라 AWS MFA 디바이스의 인증 응답을 입력하라는 메시지가 표시됩니다. 이러한 다중 요소를 통해 AWS 계정 설정 및 리소스에 대한 보안을 높일 수 있습니다.

(*) 계정 종류
<table>
<tr><th>계정 구분</th><th>Description</th><th>확인 필요 사항</th></tr>
<tr><td>Console Admin</td><td>최고 권한을 가지고 있는 단일 계정</td><td>가급적 사용을 지양해야 함</td></tr>
<tr><td>IAM</td><td>AWS IAM 서비스를 통해 생성된 별도 계정</td><td>IAM 역할 및 권한에 대한 현황을 확인해야 함</td></tr>
<tr><td>AD(Active Directory) 연동</td><td>기존 내부에서 사용중인 AD 를 AWS Organizations 서비스에 연동한 계정</td><td>기존 AD 서비스에서 사용중인 각 계정 중 IAM 역할 및 권한이 설정된 현황을 확인해야 함</td></tr>
<tr><td>Access Key</td><td>CLI 환경으로의 접속을 위한 단일 계정 (사용기간에 대한 기준 명시가 필요함)</td><td>발급일 기준 6 개월을 초과한 Access Key 존재 유무</td></tr>
</table>
※ 기존 내부 AD(Active Directory) 서버를 AWS Organizations 서비스와 연동해서 SSO(single Sign On)을 활성화하여 사용할 경우 양호로 처리될 수 있음</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. MFA 인증 설정 및 확인
1) IAM 메인 → 우측상단 계정 → 내 보안 자격 증명 → 멀티 팩터 인증 → MFA 활성화
 
</td></tr>
</table>

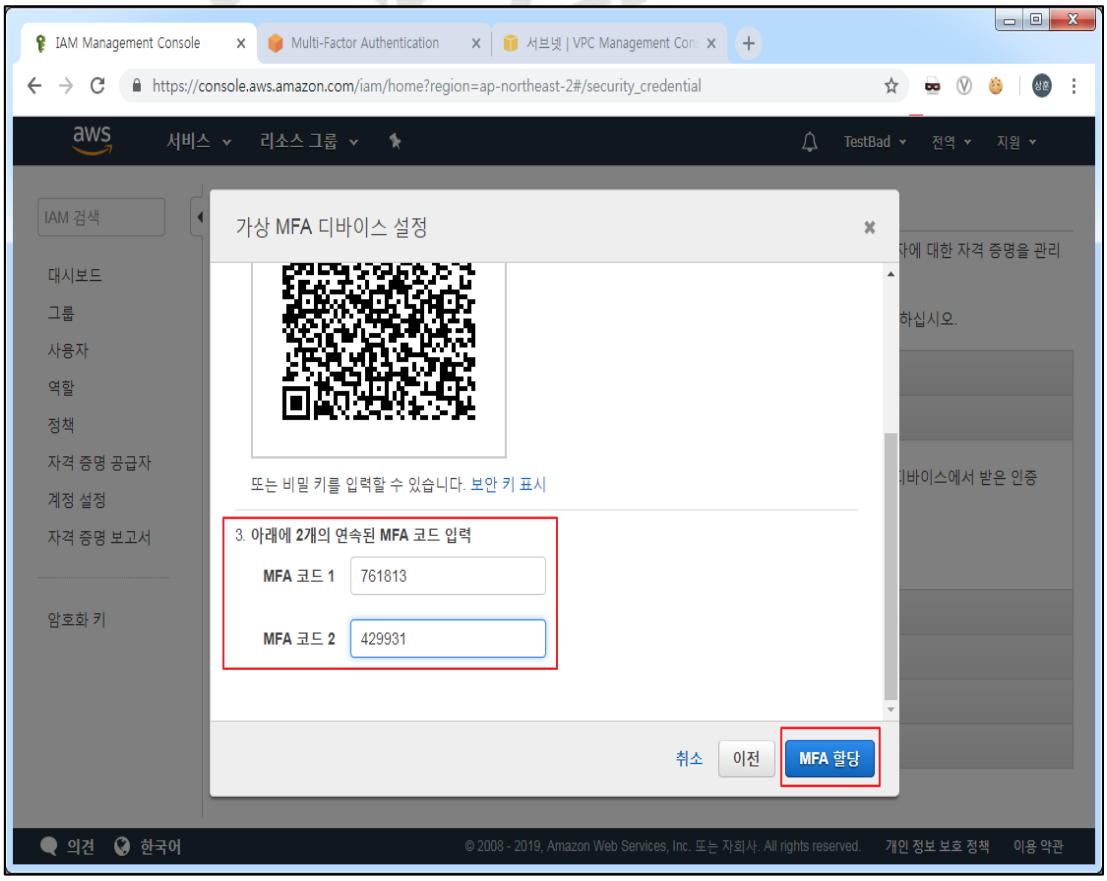
2) MFA 디바이스 관리 → 가상 MFA 디바이스 선택 → 계속



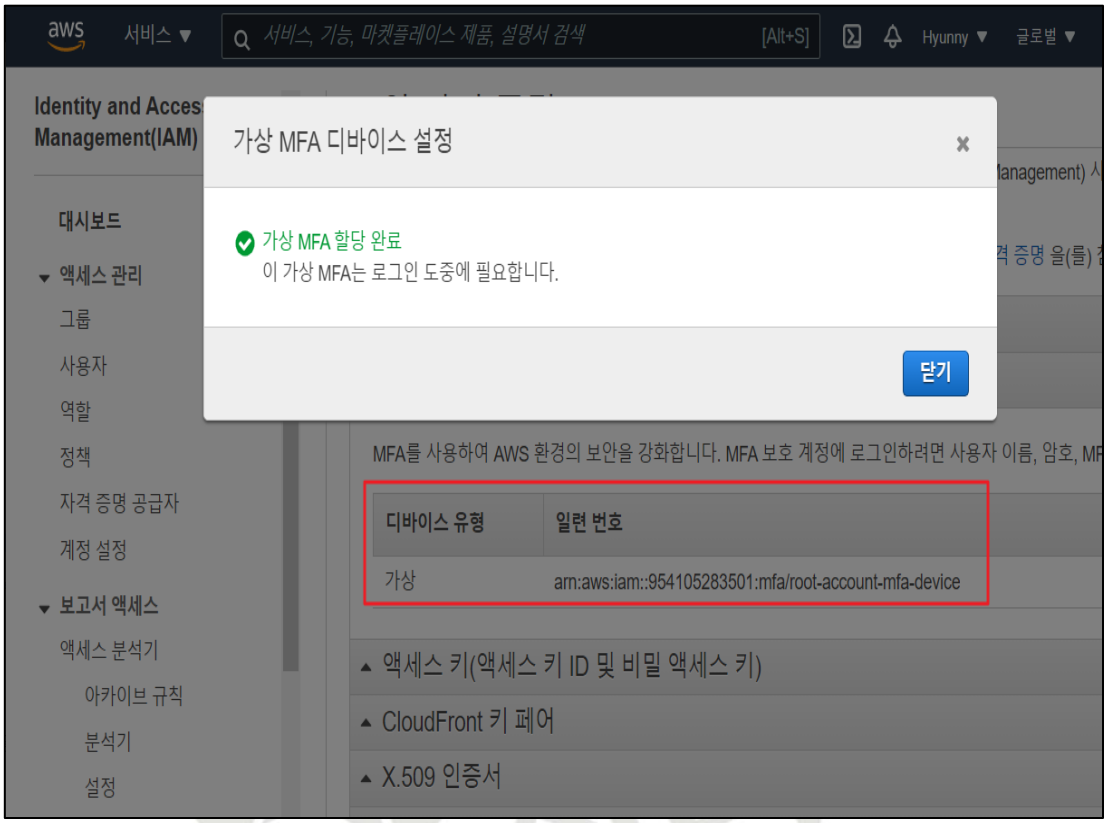
3) Google OTP 어플 설치 → '+' 버튼 → 바코드 스캔 → 나타난 QR코드를 어플에서 스캔

4) 스캔 후 나타난 숫자 MFA 코드 1 입력 → 재 생성된 숫자 MFA 코드 2 입력

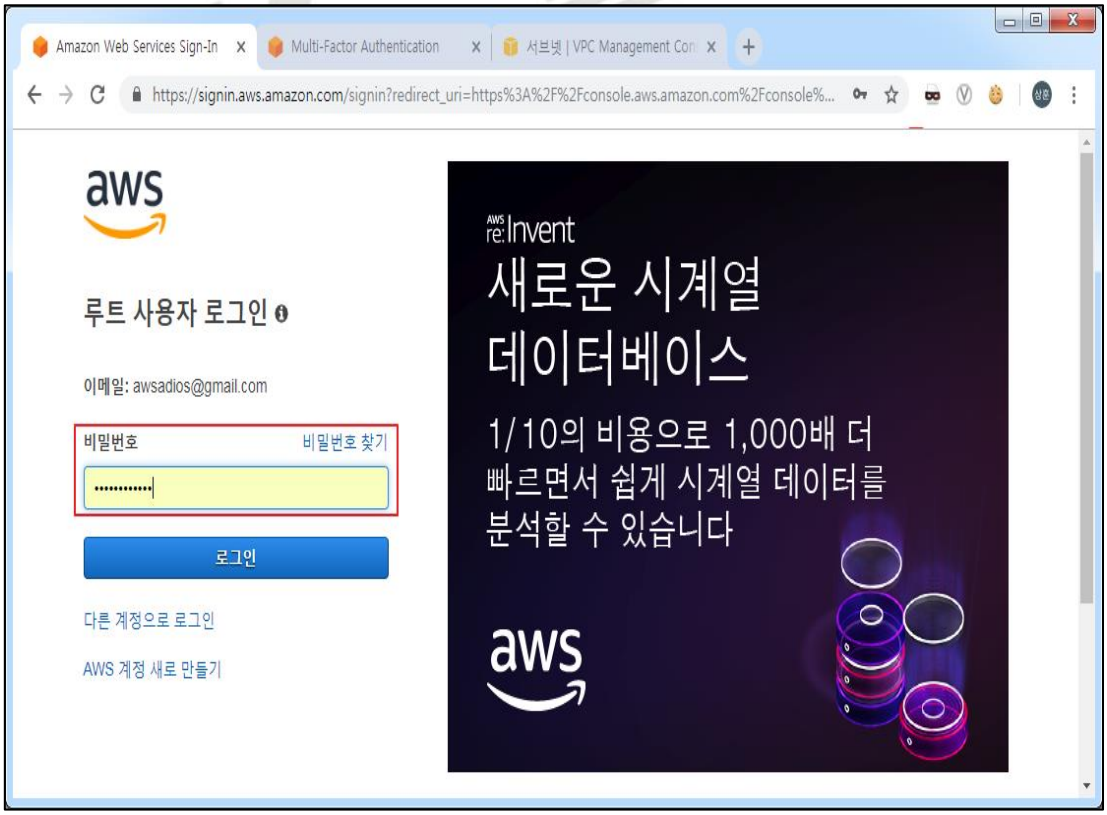
5) 2개의 연속된 MFA 코드 입력



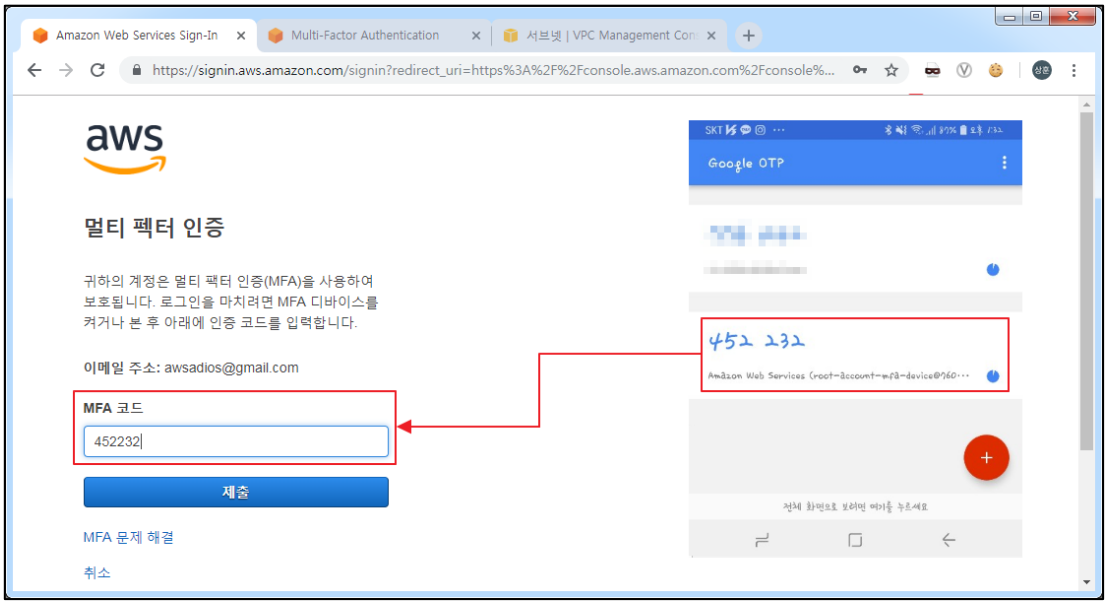
6) MFA 설정 완료



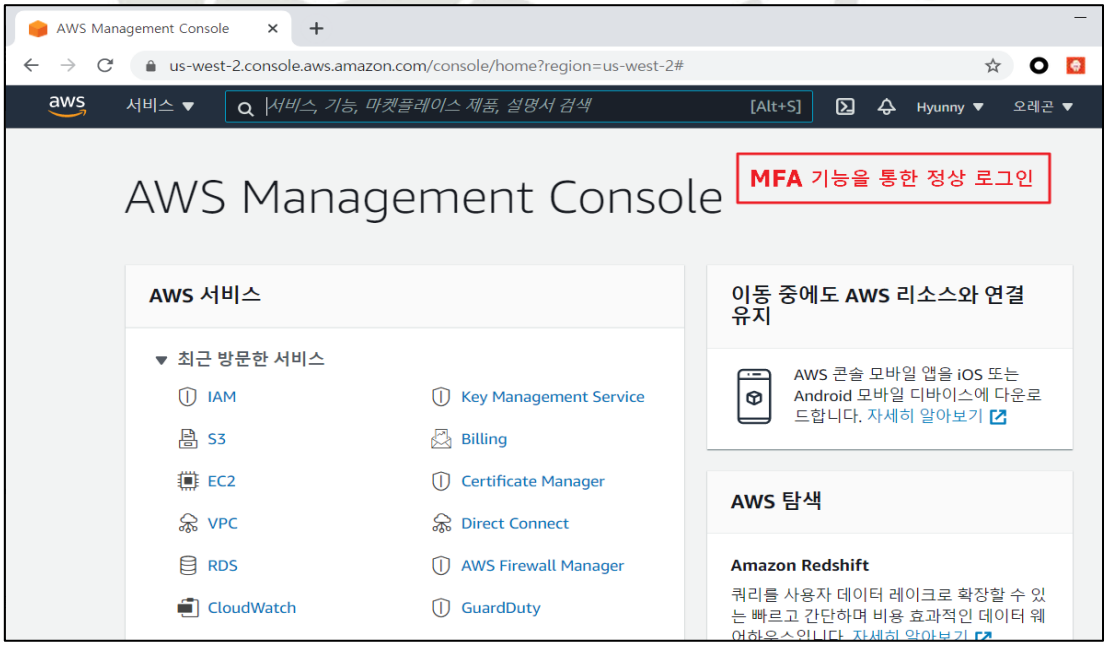
7) 로그인 시 비밀번호 입력



8) Google OTP 번호 입력 후 로그인 시도



9) 로그인 확인



진단 기준	**양호기준** : AWS 계정 및 IAM 사용자 계정 로그인 시 MFA가 활성화 되어 있을 경우 **취약기준** : AWS 계정 및 IAM 사용자 계정 로그인 시 MFA 가 비활성화 되어 있을 경우
비고	MFA 인증을 사용하지 않고 SSO 인증을 통해서 로그인할 경우 양호로 처리될 수 있음

1.10 AWS 계정 패스워드 정책 관리

분류	계정 관리	중요도	중
항목명	AWS 계정 패스워드 정책 관리		

항목 설명

AWS Admin Console Account 계정 및 IAM 사용자 계정의 암호 설정 시 일반적으로 유추하기 쉬운 암호를 설정하는 경우 비 인가된 사용자가 해당 계정을 획득하여 접근 가능성이 존재합니다.

<패스워드 설정 기준>

1) 패스워드는 아래의 4가지 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 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, 계정명, hostname과 같이 추측하기 쉬운 패스워드 사용 금지

1) 패스워드 최소길이
패스워드 추측공격을 피하기 위하여 패스워드 최소길이가 설정되어 있는지 점검함
패스워드 최소길이가 설정되어 있지 않거나 짧게 설정되어 있을 경우 취약한 패스워드를 사용함으로 인해 악의적인 사용자가 패스워드를 쉽게 유추 할 수 있음

2) 패스워드 최대 사용기간
패스워드가 임의의 경로를 통해 유출되었을 때, 임의로 접속한 사용자가 언제든 다시 접속할 수 있는 환경을 방지하기 위해 패스워드 날짜 제한을 점검함

3) 패스워드 최소 사용기간
패스워드가 임의의 경로를 통해 유출되었을 때, 임의로 접속한 사용자가 언제든 다시 접속할 수 있는 환경을 방지하기 위해 패스워드 날짜 제한을 점검함

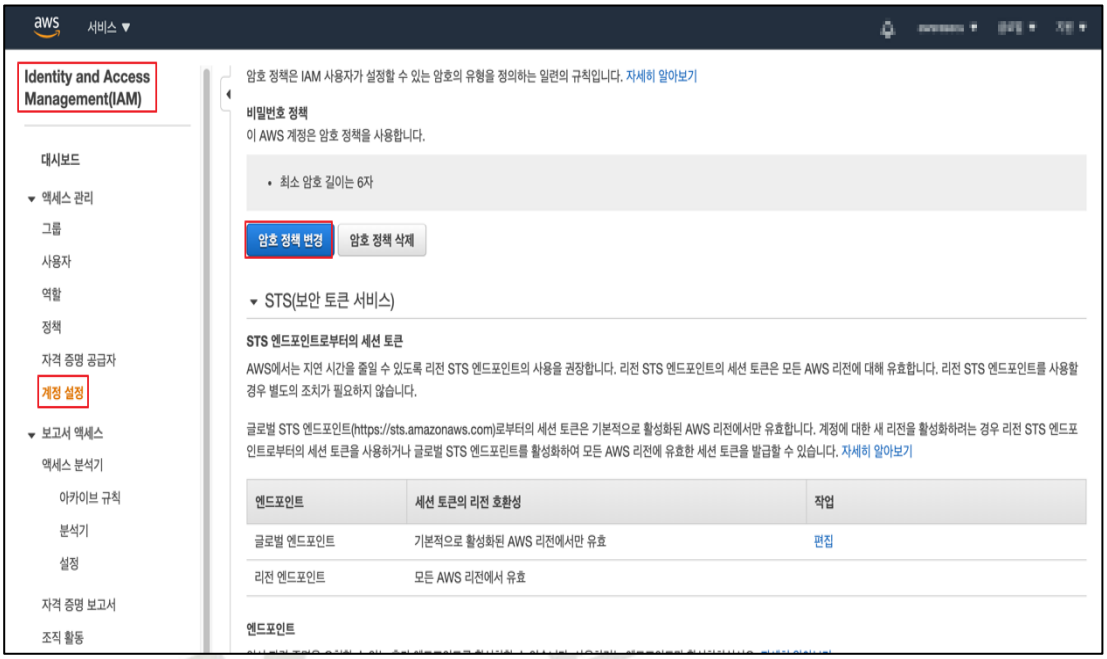
4) 이전 패스워드 기억
이전에 사용하였던 패스워드를 기억하여 패스워드 변경 시 기존에 사용하였던 패스워드 재사용 금지
- 패스워드 길이는 8자 이상 설정하는 것을 권고
- 패스워드 최대 사용 기간을 60일 이하로 설정할 것을 권고
- 패스워드 최소 사용 기간을 1일 이상으로 설정할 것을 권고

5) 암호 만료 활성화 및 재사용 제한
- 암호 만료 활성화, 암호 만료일은 90일 이하여야 함
- 암호 재사용 제한 최소 1개 이상이어야 함

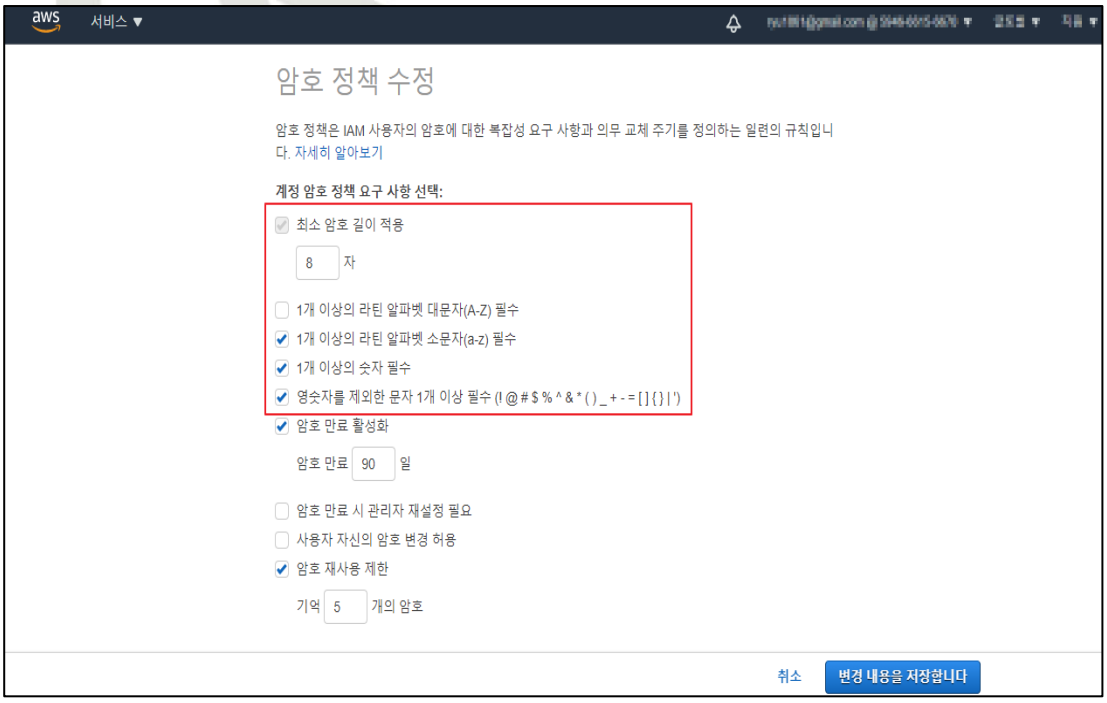
설정 방법

가. IAM 계정 비밀번호 정책 확인

1) 계정 설정 확인



2) 암호 정책 설정 확인



	3) IAM 사용자 계정 암호 만료 및 재사용 제한 설정 
진단 기준	**양호기준** : Admin Console 및 IAM 계정의 패스워드 복잡성 기준 준수 및 암호 만료/재사용 제한을 설정하고 있을 경우 **취약기준** : Admin Console 및 IAM 계정의 패스워드 복잡성 기준 준수 및 암호 만료/재사용 제한을 설정하고 있지 않을 경우
비고	

2. 권한 관리

2.1 인스턴스 서비스 정책 관리

<table>
<tr><td>분류</td><td>권한 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">인스턴스 서비스 정책 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">AWS 인스턴스 서비스(EC2, RDS, S3 등)의 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(즉, 사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다.

1) 인스턴스 서비스 구분
<table><tr><th>서비스 구분</th><th>서비스 상세</th></tr><tr><td>EC2</td><td>가상 컴퓨팅 환경인 인스턴스를 제공하며 보안 및 네트워크 구성과 스토리지 관리가 가능함</td></tr><tr><td>ECS</td><td>클러스터에서 도커 컨테이너를 손쉽게 실행, 중지 및 관리 할 수 있게 해주는 컨테이너 관리가 가능함</td></tr><tr><td>ECR</td><td>컨테이너 이미지를 저장, 관리 및 배포 할 수 있게 지원하는 관리형 도커 레지스트리 서비스
레지스트리(이미지 레포지토리 생성 후 레포지토리에 이미지 저장),
사용자 권한 토큰(ECR 레지스트리 인증 시 Docker 클라이언트 활용)
레포지토리 정책(레포지토리 및 레포지토리 내 이미지에 대한 액세스 제어) 관리가 가능함</td></tr><tr><td>EKS</td><td>Kubernetes 제어 플레인을 설치하고 운영할 필요 없이 AWS에서 Kubernetes를 손쉽게 실행하도록 하는 관리형 서비스입니다.
Kubernetes는 컨테이너화된 애플리케이션의 배포, 조정 및 관리 자동화를 위한 오픈 소스 시스템임</td></tr><tr><td>EFS</td><td>AWS 클라우드 서비스와 온프레미스 리소스에서 사용할 수 있는 간단하고 확장 가능하며 탄력적인 완전 관리형 탄력적 NFS 파일 시스템</td></tr><tr><td>RDS</td><td>AWS 클라우드에서 관계형 데이터베이스를 더 쉽게 설치, 운영 및 확장할 수 있는 웹 서비스입니다. 이 서비스는 산업 표준 관계형 데이터베이스를 위한 경제적이고 크기 조절이 가능한 용량을 제공하고 공통 데이터베이스 관리 작업이 가능함</td></tr><tr><td>S3</td><td>Amazon Simple Storage Service(Amazon S3)는 인터넷용 스토리지입니다. Amazon S3을 사용하면 웹을 통해 언제 어디서든 원하는 양의 데이터를 저장하고 검색할 수 있습니다. 간편하고 직관적인 웹 인터페이스인 AWS Management 콘솔을 사용하여 이러한 작업을 수행할 수 있습니다.</td></tr></table>
2) 인스턴스 서비스 별 관리형 정책 (예시)</td></tr>
</table>

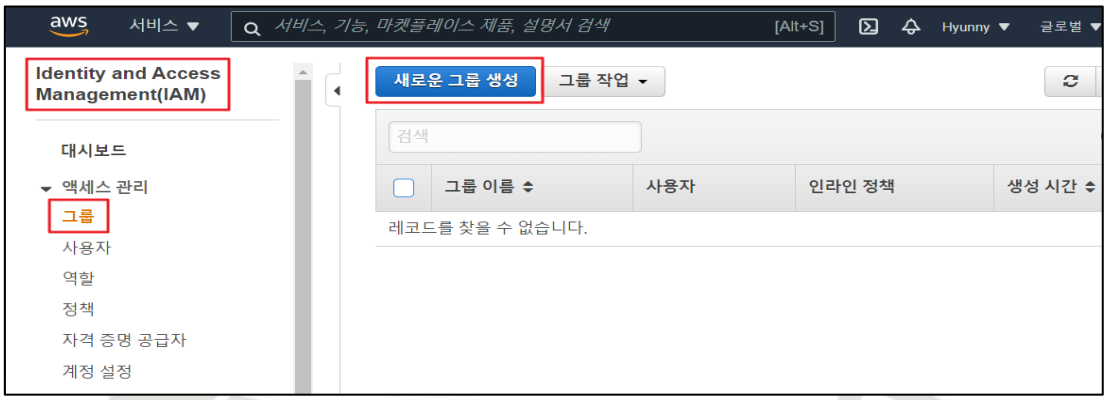
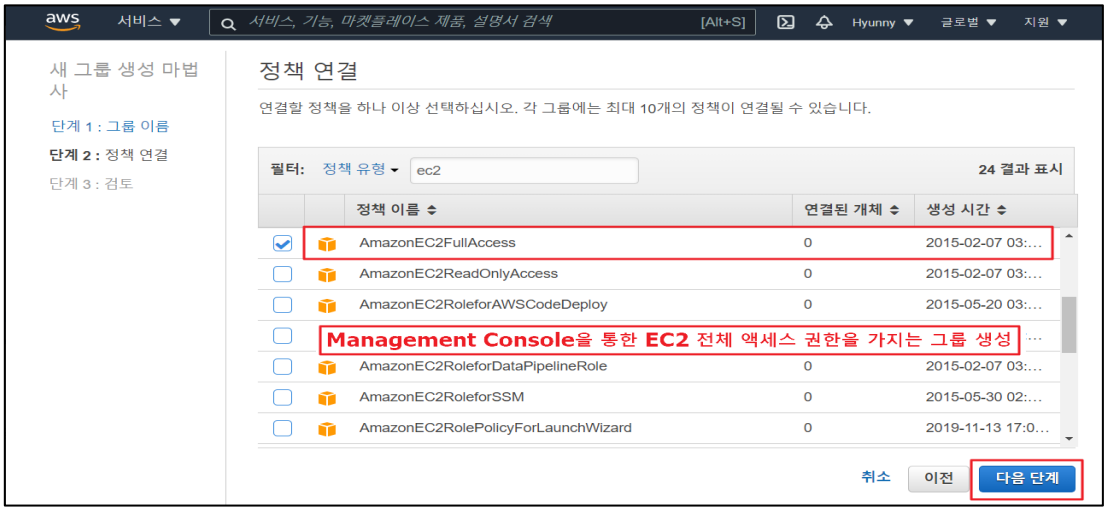
서비스 구분	정책명	정책설명
EC2	AmazonC2FullAccess	EC2 서비스 전체 권한
	AmazonC2ReadOnlyAccess	EC2 서비스 읽기 전용 액세스 권한
	AmazonSSMManaged EC2InstanceDefaultPolicy	EC2 인스턴스에서 AWS Systems Manager 기능 활성화 권한
	EC2InstanceConnect	EC2 Instance Connect를 호출하여 EC2 인스턴스에 임시 키를 게시하고 ssh 또는 EC2 Instance Connect CLI를 통해 연결할 수 있는 권한
ECS	AmazonCS_FullAccess	ECS 서비스 전체 권한
	AWSElasticBeanstalkRoleECS	다중 컨테이너 Docker 환경에서 Amazon ECS 클러스터를 생성/삭제 할 수 있는 권한
	AmazonCSTaskExecutionRolePolicy	Amazon ECS 작업을 실행하는 데 필요한 서비스 리소스에 대한 읽기 전용 액세스 권한
ECR	AmazonC2Container RegistryFullAccess	ECR 리소스에 대한 관리 전체 액세스 권한
	AmazonC2Container RegistryPowerUser	Container Registry 리포지토리에 대한 전체 권한이 부여되어 있지만 삭제 또는 정책 변경을 허용하지 않는 권한
	AmazonC2Container RegistryReadOnly	Container Registry 리포지토리에 대한 읽기 전용 액세스 권한
EKS	AmazonKSClusterPolicy	인스턴스, 보안 그룹 및 탄력적 네트워크 인터페이스를 포함하되 이에 국한되지 않는 EC2 리소스에 대한 식별 정보를 확인하는 권한
	AWSServiceRoleForAmazon EKSNodegroup	Amazon EKS 작업자 노드가 Amazon EKS 클러스터에 연결할 수 있도록 허용하는 권한
	AmazonKSServicePolicy	EKS 클러스터를 운영하는 데 필요한 리소스를 생성하고 관리할 수 있는 권한
EFS	AmazonlasticFileSystemFullAccess	Amazon EFS에 대한 전체 액세스 권한

	AmazonlasticFileSystemServiceRolePolicy	사용자를 대신하여 AWS 리소스를 관리하도록 허용하는 권한
	AmazonlasticFileSystemReadOnlyAccess	Amazon EFS에 대한 읽기 전용 액세스 권한
RDS	AmazonRDSFullAccess	Amazon RDS에 대한 전체 액세스 권한
	AmazonRDSDataFullAccess	RDS 데이터 API, RDS 데이터베이스 자격 증명을 위한 비밀 저장소 API 및 DB 콘솔 쿼리 관리 API를 사용하여 AWS 계정의 Aurora Serverless 클러스터에서 SQL 문을 실행할 수 있는 전체 액세스 권한
	AmazonRDSReadOnlyAccess	Amazon RDS에 대한 읽기 전용 액세스 권한
S3	AmazonS3FullAccess	든 버킷에 대한 전체 액세스 권한
	AmazonS3OutpostsFullAccess	Outposts의 Amazon S3에 대한 전체 액세스 권한
	AmazonS3ReadOnlyAccess	모든 버킷에 대한 읽기 전용 액세스 권한

(*) IAM 관리형 정책 권한 관리 List (예시)

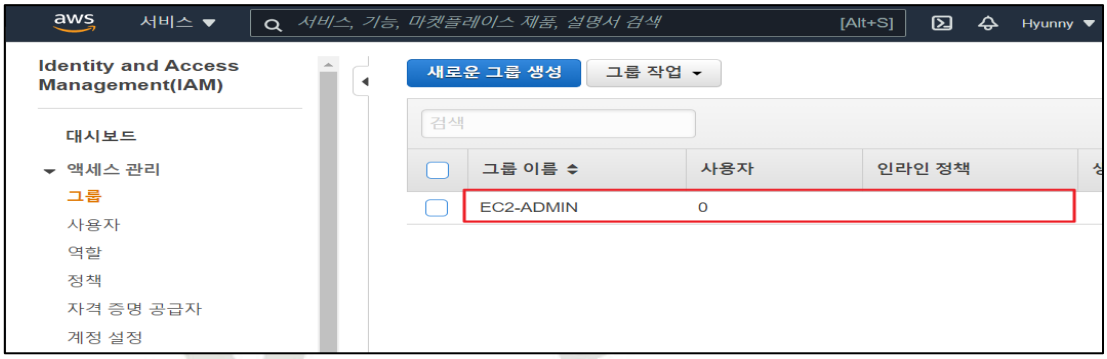
역할	계정 관리 (그룹 및 계정명)	AWS 관리형 정책	취약 유/무
AWS Admin Console 관리자	Ex)EC2_Admin (admin_accout)	Ex) EC2_Admin (AmazonC2FullAcces)	N/A
Infra 운영/관리자 및 담당자			N/A
Application 운영/관리자 및 담당자			N/A
개발 관리자 및 담당자			N/A
재무 / 비용 관리자 및 담당자			N/A

설정	**가. 인스턴스 IAM 관리자/운영자 권한 그룹 생성**

방법	- 인스턴스 서비스의 운영/관리를 위한 IAM 그룹 생성 **※ 인스턴스 서비스 운영/관리에 필요한 IAM FULL Access 등의 권한과 같이 중요도가 높은 권한은 Infra 운영/관리자 및 담당자에게만 정책이 되도록 해야하며 최소한의 계정 수가 유지되어야 함** 1) IAM 내 그룹 탭 접근 후 새로운 그룹 생성 클릭  2) 그룹 이름 설정  3) 정책 연결 (AmazonC2FullAccess 선택) 

4) 검토 및 그룹 생성 클릭

5) 그룹 생성 확인



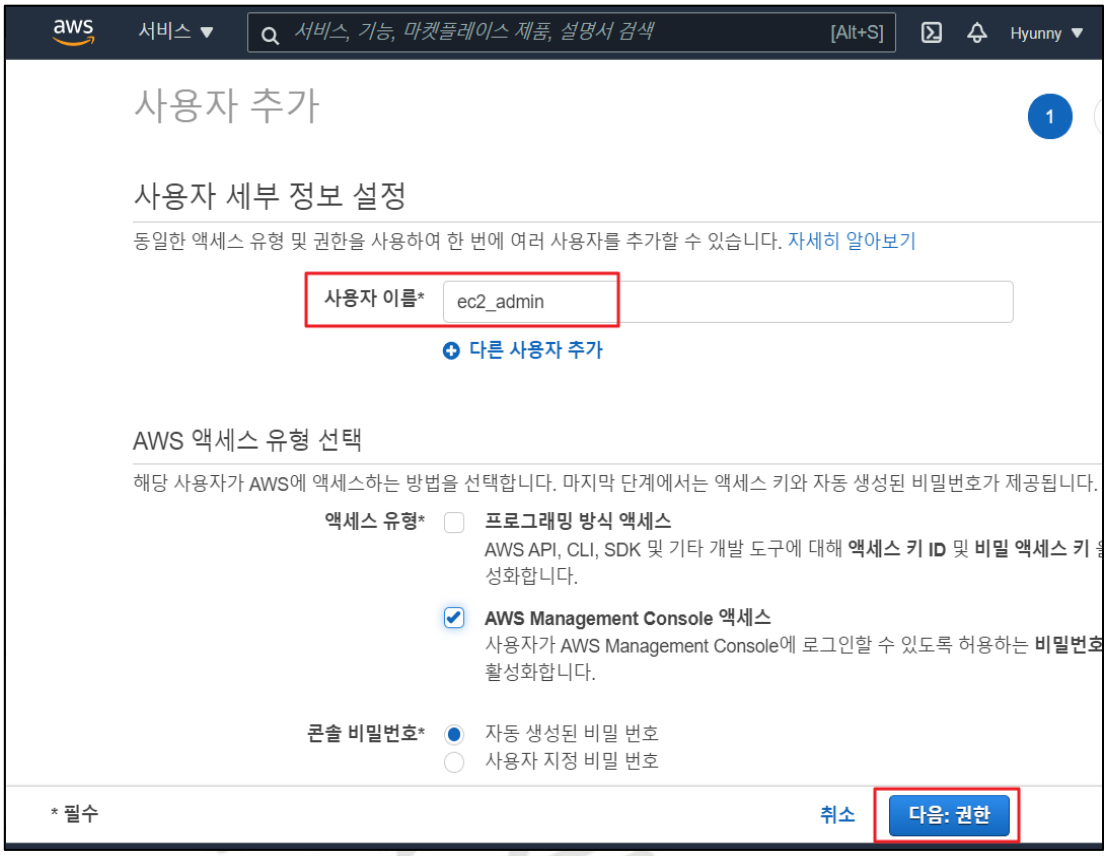
나. 인스턴스 IAM 관리자/운영자 권한 사용자 추가

- 인스턴스 서비스의 운영/관리를 위한 IAM 사용자 추가

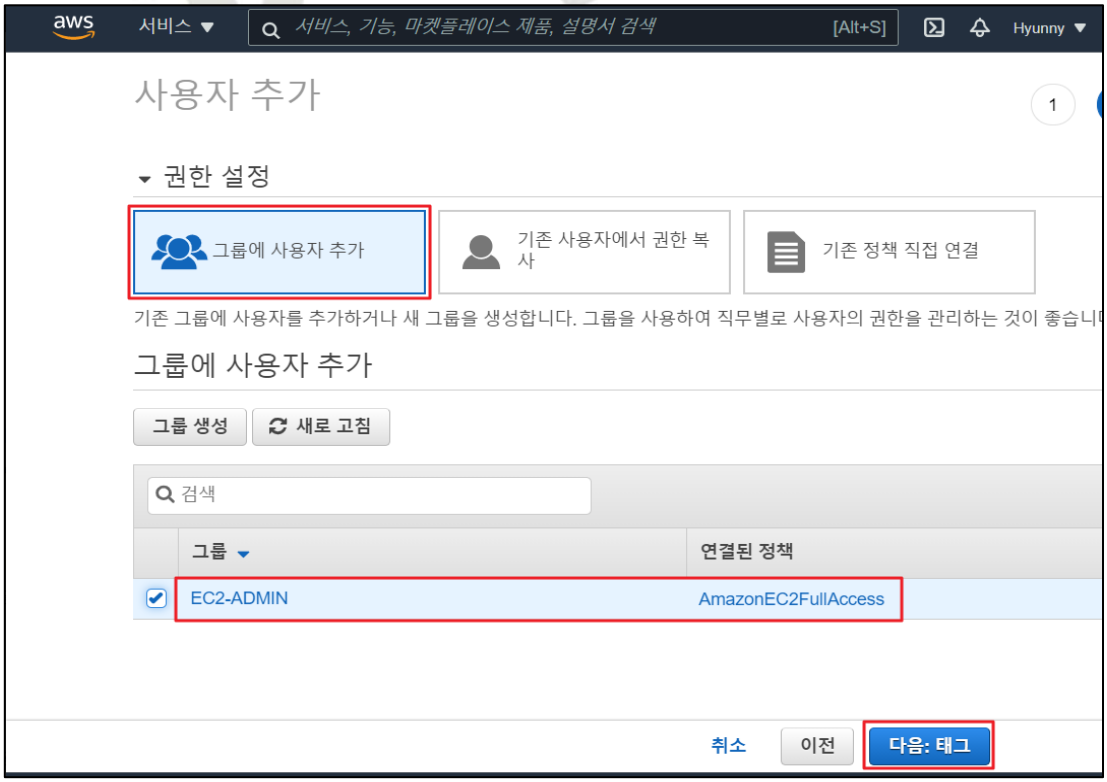
※ 인스턴스 서비스 운영/관리에 필요한 IAM FULL Access 등의 권한과 같이 중요도가 높은 권한은 Infra 운영/관리자 및 담당자에게만 정책이 되도록 해야하며 최소한의 계정 수가 유지되어야 함

1) IAM 내 사용자 탭 접근 후 사용자 추가 클릭

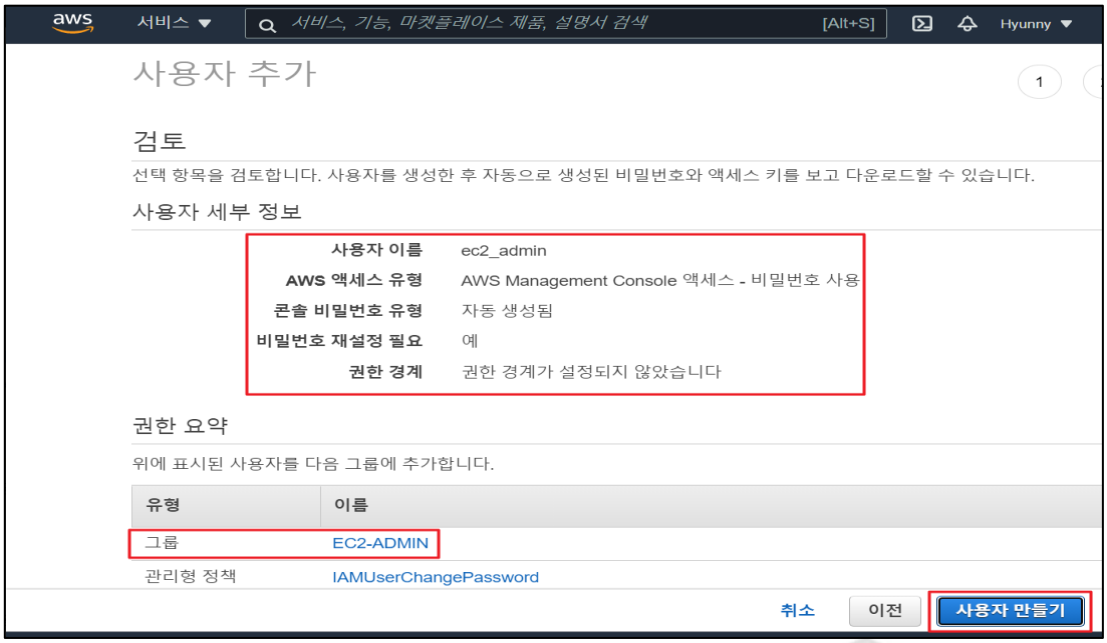
2) 사용자 이름 설정 및 다음 클릭



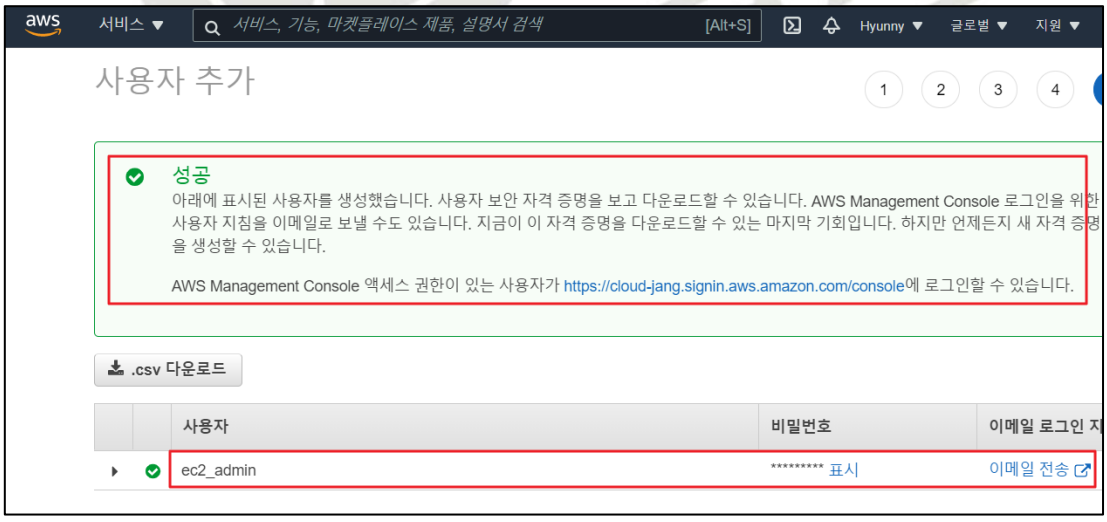
3) 그룹에 사용자 추가 설정



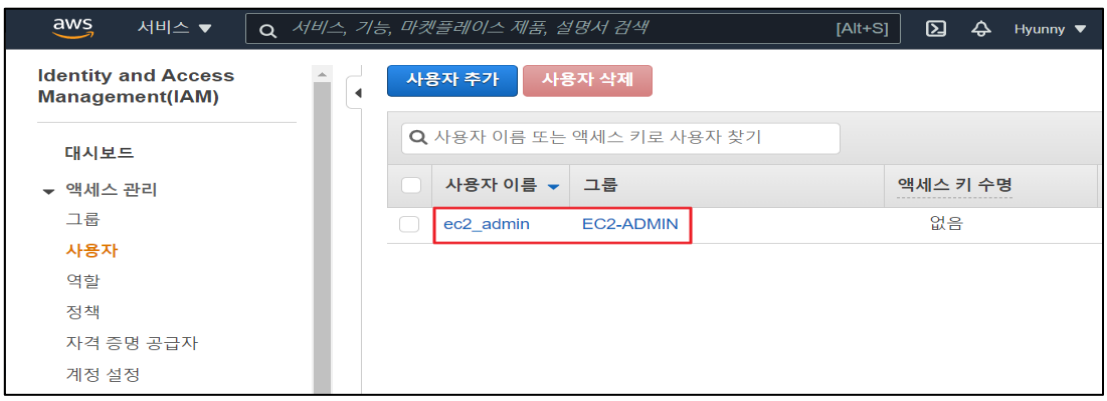
4) 검토 및 사용자 만들기 클릭

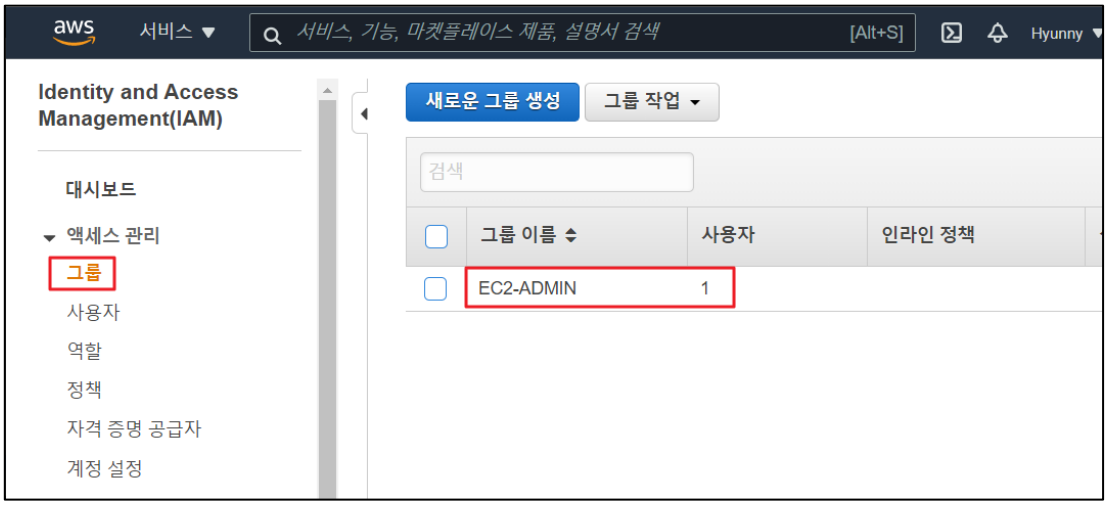


5) 사용자 추가 확인



6) IAM "사용자" 클릭 및 계정 목록 확인



	7) IAM "그룹" 클릭 및 그룹 목록 확인  8) 그룹 내 추가된 사용자 확인 
진단 기준	**양호기준** : 인스턴스 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있을 경우 **취약기준** : 인스턴스 서비스 IAM 사용 권한이 각각 서비스 역할에 맞지 않게 설정되어 있을 경우
비고	

2.2 네트워크 서비스 정책 관리

분류	권한 관리	중요도	상
항목명	네트워크 서비스 정책 관리		

항목 설명

AWS 네트워크 서비스(VPC, Route 53, Direct Connect 등)의 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(즉, 사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다.

1) 네트워크 서비스 구분

서비스 구분	서비스 상세
VPC	사용자가 정의한 가상 네트워크로 AWS 리소스를 시작할 수 있습니다. 이 가상 네트워크는 AWS의 확장 가능한 인프라를 사용한다는 이점과 함께 고객의 자체 데이터 센터에서 운영하는 기존 네트워크와 매우 유사합니다.
CloudFront	.html, .css, .js 및 이미지 파일과 같은 정적 및 동적 웹 콘텐츠를 사용자에게 더 빨리 배포하도록 지원하는 웹 서비스
Route 53	가용성과 확장성이 우수한 DNS(도메인 이름 시스템) 웹 서비스입니다. Route 53을 사용하여 세 가지 주요 기능, 즉 도메인 등록, DNS 라우팅, 상태 확인을 조합하여 실행할 수 있는 서비스
API Gateway	규모와 상관없이 REST 및 WebSocket API를 생성, 게시, 유지하고 모니터링 및 보안하기 위한 AWS 서비스
Direct Connect	표준 이더넷 광섬유 케이블을 통해 내부 네트워크를 AWS Direct Connect 위치에 연결할 수 있습니다. 케이블의 한쪽 끝을 사용자의 라우터에 연결하고 다른 쪽 끝을 AWS Direct Connect 라우터에 연결하는 서비스
AppMesh	애플리케이션의 모든 서비스에 대해 일관된 가시성과 네트워크 트래픽 제어를 제공하는 서비스
CloudMap	AWS Cloud Map를 사용하여 Amazon API Gateway에 배포된 API, Amazon EC2 인스턴스, Amazon DynamoDB 테이블, Amazon S3 버킷, Amazon Simple Queue Service(Amazon SQS) 대기열 등과 같은 모든 클라우드 리소스를 등록해 찾을 수 있는 서비스

2) 네트워크 서비스 별 관리형 정책 (예시)

서비스 구분	정책명	정책설명
VPC	AmazonVPCFullAccess	Amazon VPC에 대한 전체 액세스 권한
	AmazonVPCCrossAccount NetworkInterfaceOperations	네트워크 인터페이스를 생성하고 교차 계정 리소스에 연결할 수 있는 액세스 권한
	AmazonVPCReadOnlyAccess	Amazon VPC에 대한 읽기 전용

		액세스 권한
CloudFront	CloudFrontFullAccess	전체 액세스 권한과 AWS Management 콘솔을 통해 Amazon S3 버킷을 나열하는 권한
	AWSCloudFrontLogger	CloudFront Logger에 CloudWatch Logs에 대한 쓰기 권한
	CloudFrontReadOnlyAccess	CloudFront 배포 구성 정보 및 목록 배포에 대한 액세스 권한
Route 53	AmazonRoute 53FullAccess	Amazon Route 53에 대한 전체 액세스 권한
	AmazonRoute 53DomainsFullAccess	모든 Route 53 도메인 작업 및 호스팅 영역 생성에 대한 전체 액세스 권한
	AmazonRoute 53ReadOnlyAccess	Amazon Route 53에 대한 읽기 전용 액세스 권한
API Gateway	AmazonAPIGatewayAdministrator	Amazon API Gateway에서 API 생성/편집/삭제에 대한 전체 액세스 권한
	APIGatewayServiceRolePolicy	API Gateway가 고객을 대신하여 연결된 AWS 리소스를 관리하는 권한
	AmazonAPIGatewayInvokeFullAccess	Amazon API Gateway에서 API를 호출할 수 있는 전체 액세스 권한
Direct Connect	AWSDirectConnectFullAccess	AWS Direct Connect에 대한 전체 액세스 권한
	AWSDirectConnectServiceRolePolicy	리소스를 생성하고 관리할 수 있는 AWS Direct Connect 권한
	AWSDirectConnectReadOnlyAccess	AWS Direct Connect에 대한 읽기 전용 액세스 권한
AppMesh	AWSAppMeshFullAccess	AWS App Mesh API 및 관리 콘솔에 대한 전체 액세스 권한
	AWSAppMeshServiceRolePolicy	AWS AppMesh에서 사용하거나 관리하는 AWS 서비스 및 리소스에 대한 액세스 권한
	AWSAppMeshReadOnly	AWS App Mesh API 및 관리 콘솔에 대한 읽기 전용 액세스 권한
CloudMap	AWSCloudMapFullAccess	모든 AWS Cloud Map 작업에 대한 전체 액세스 권한
	AWSCloudMapRegisterInstanceAccess	AWS Cloud Map 작업에 대한

		등록자 수준 액세스 권한
	AWSCloudMapReadOnlyAccess	모든 AWS Cloud Map 작업에 대한 읽기 전용 액세스 권한

3) IAM 관리형 정책 권한 관리 List (예시)

역할	계정 관리 (그룹 및 계정명)	AWS 관리형 정책	취약 유/무
AWS Root 관리자	Ex)RDS_Admin (admin_accout)	Ex) RDS_Admin (AmazonRDSFullAccess)	
Infra 운영/관리자 및 담당자			
Application 운영/관리자 및 담당자			
개발 관리자 및 담당자			
재무 / 비용 관리자 및 담당자			

설정 방법

가. 네트워크 서비스 별 IAM 관리자/운영자 권한 그룹 생성

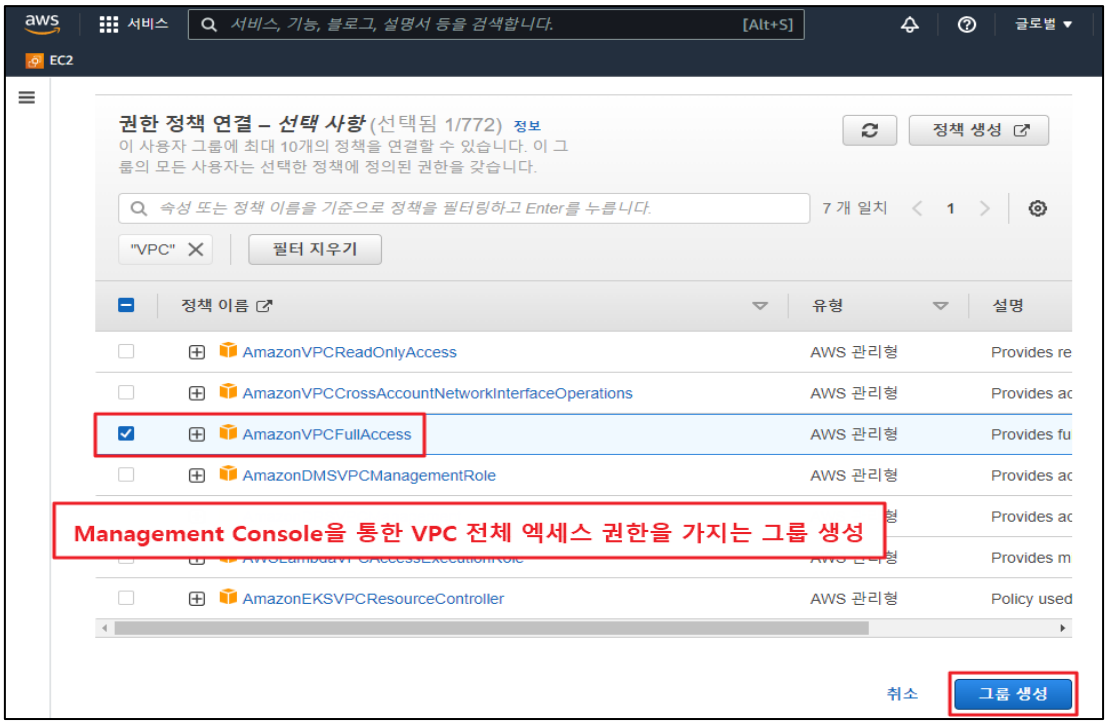
- 네트워크 서비스의 운영/관리를 위한 IAM 그룹 생성

※ 네트워크 서비스 운영/관리에 필요한 IAM FULL Access 등의 권한과 같이 중요도가 높은 권한은 Infra 운영/관리자 및 담당자에게만 정책이 되도록 해야하며 최소한의 계정 수가 유지되어야 함

1) IAM 내 사용자 그룹 탭 접근 후 그룹 생성 클릭

2) 그룹 이름 설정

3) 정책 연결 (AmazonVPCFullAccess 선택) 및 그룹 생성



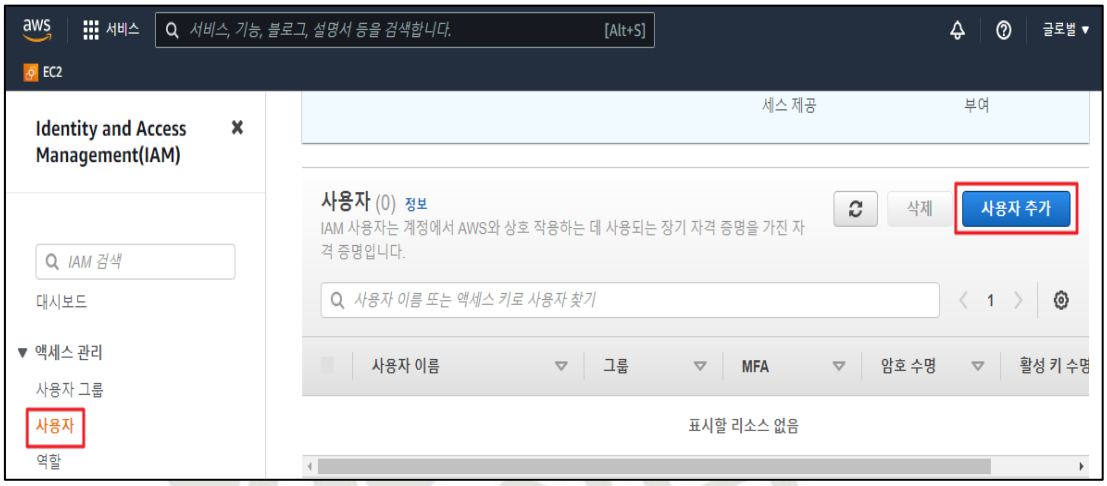
4) 그룹 생성 확인

나. 네트워크 서비스 별 IAM 관리자/운영자 권한 사용자 추가

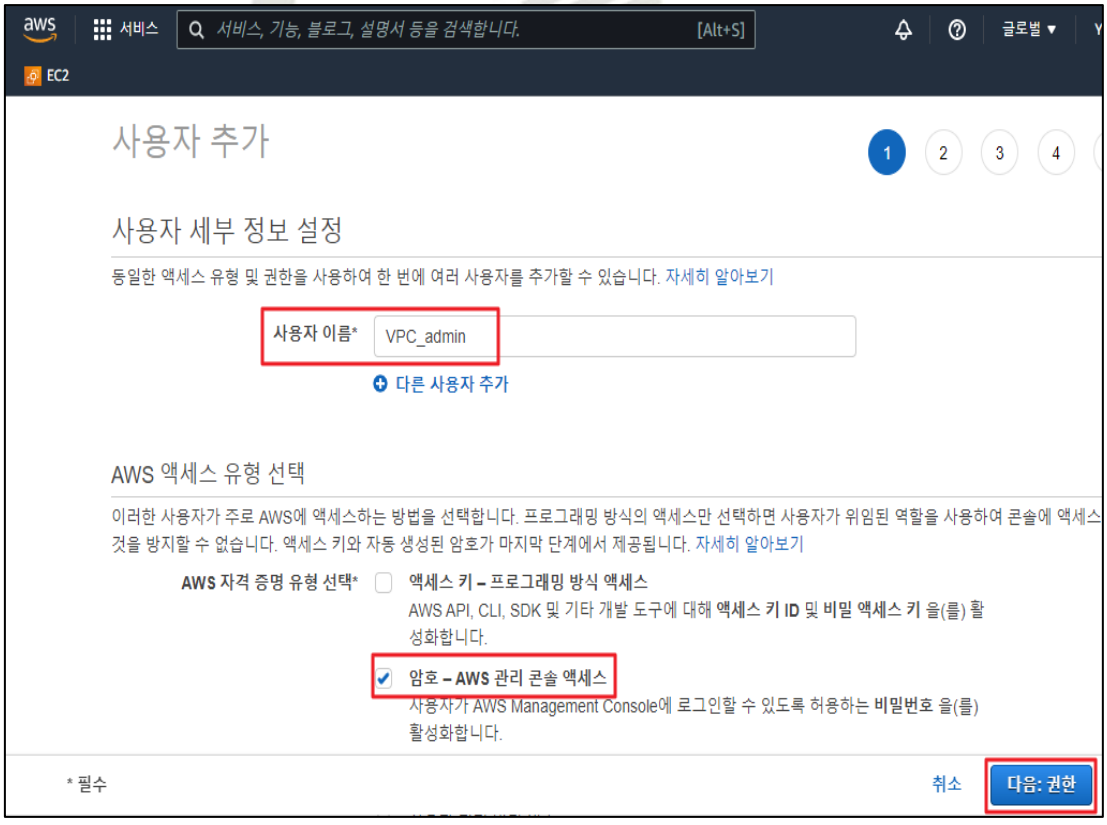
- 네트워크 서비스의 운영/관리를 위한 IAM 사용자 추가

※ 네트워크 서비스 운영/관리에 필요한 IAM FULL Access 등의 권한과 같이 중요도가 높은 권한은 Infra 운영/관리자 및 담당자에게만 정책이 되도록 해야하며 최소한의 계정 수가 유지되야함

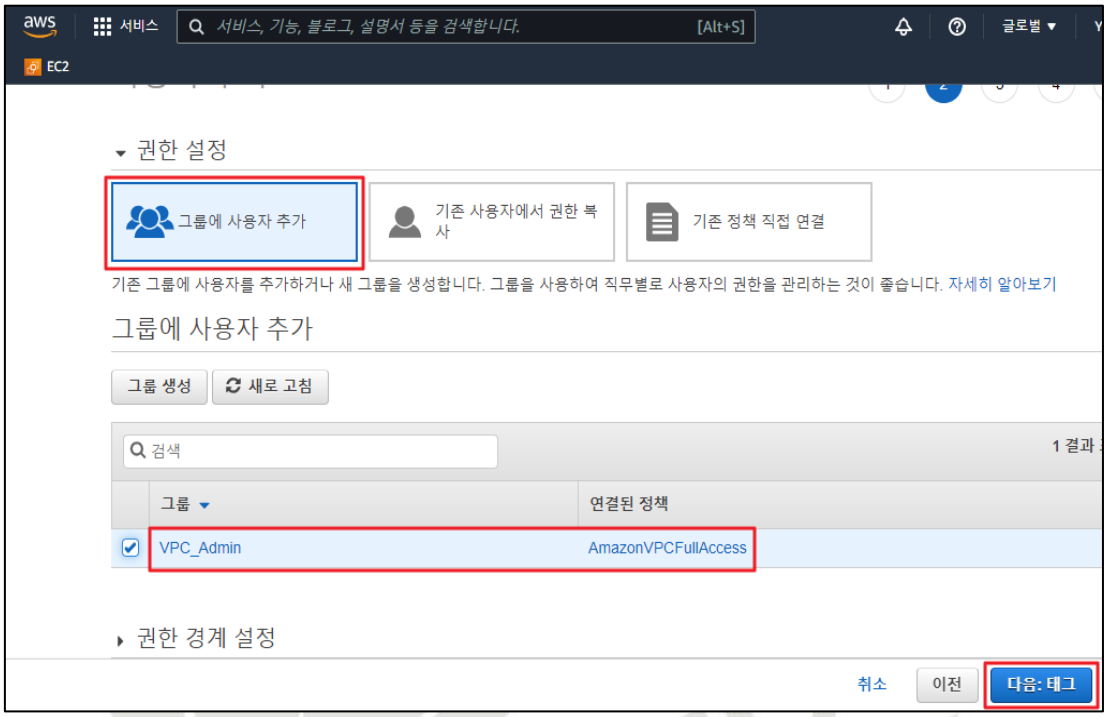
1) IAM 내 사용자 탭 접근 후 사용자 추가 클릭



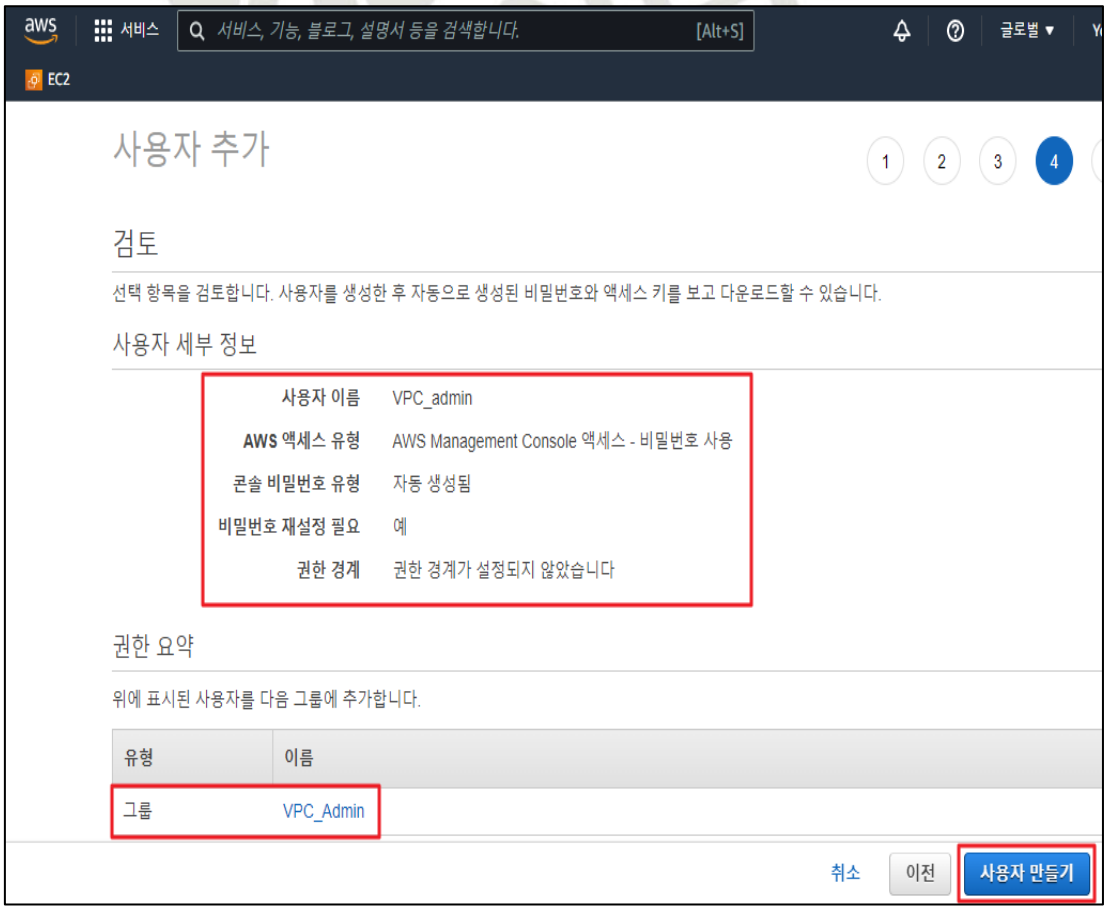
2) 사용자 이름 설정 및 다음 클릭



3) 그룹에 사용자 추가 설정

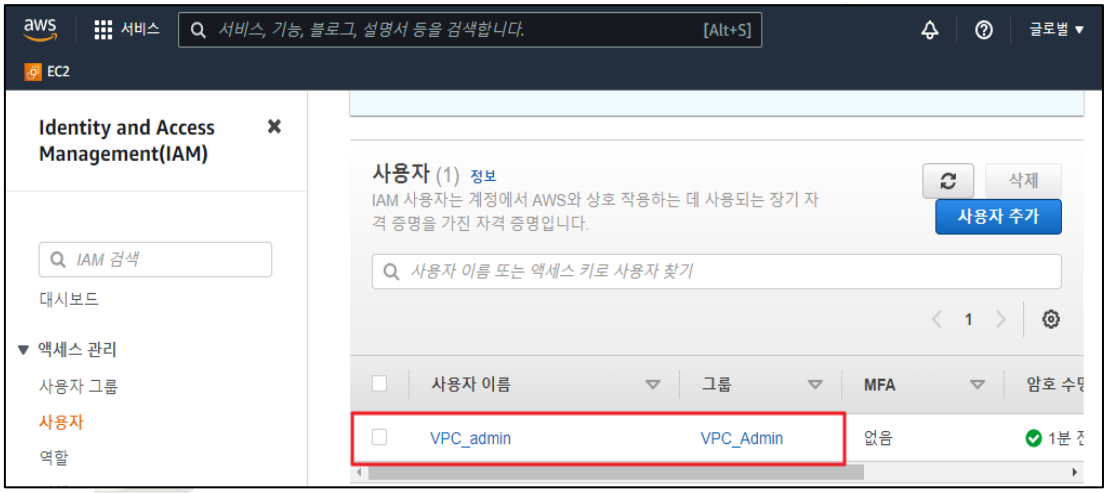


4) 검토 및 사용자 만들기 클릭

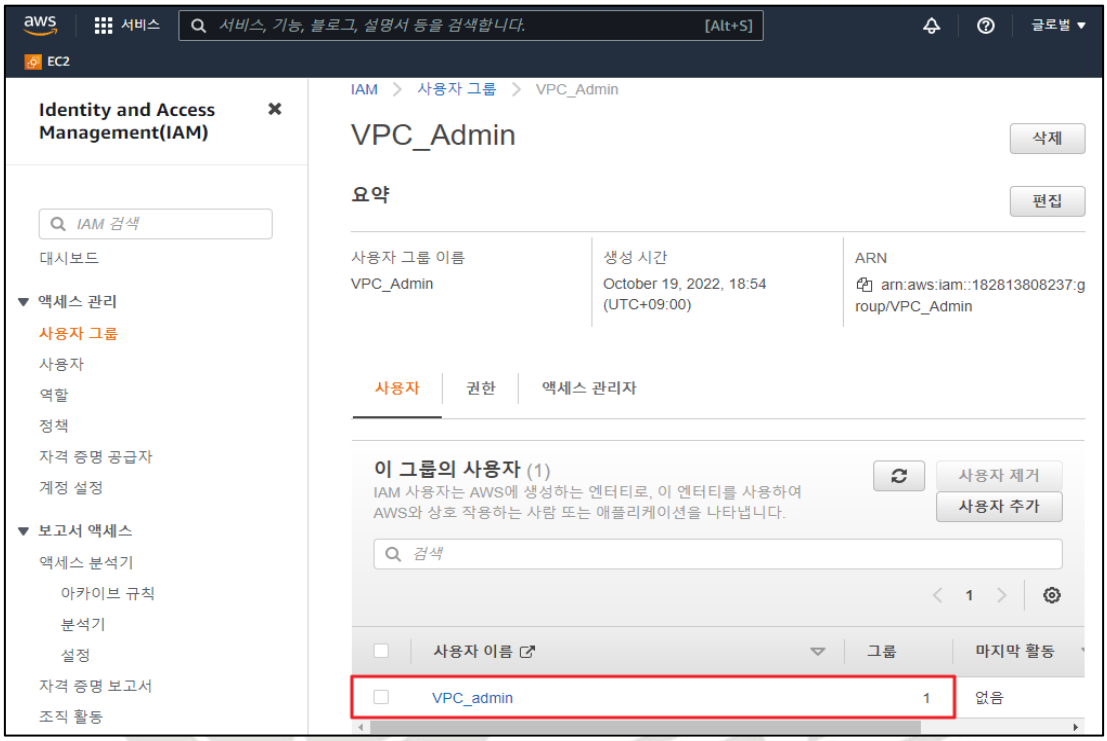


5) 사용자 추가 확인

6) IAM "사용자" 클릭 및 계정 목록 확인



7) IAM "그룹" 클릭 및 그룹 목록 확인

	8) 그룹 내 추가된 사용자 확인 
진단 기준	**양호기준** : 네트워크 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있을 경우 **취약기준** : 네트워크 서비스 IAM 사용 권한이 각각 서비스 역할에 맞지 않게 설정되어 있을 경우
비고	

2.3 기타 서비스 정책 관리

분류	권한 관리	중요도	상
항목명	기타 서비스 정책 관리		

항목 설명

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

1) 기타 서비스 구분

서비스 구분	서비스 상세
Organizations	AWS Organizations는 사용자가 생성해 중앙에서 관리하는 조직으로 여러 AWS 계정을 통합할 수 있는 계정 관리 서비스
CloudWatch	Amazon Web Services(AWS) 리소스와 AWS에서 실시간으로 실행 중인 애플리케이션을 모니터링하는 서비스
Auto Scaling	AWS Auto Scaling 콘솔은 단일 사용자 인터페이스가 여러 AWS 서비스의 자동 조정 기능 사용하는 서비스
CloudFormation	Amazon Web Services 리소스를 모델링하고 설정하여 리소스 관리 시간을 줄이고 AWS에서 실행되는 애플리케이션에 더 많은 시간을 사용하도록 해 주는 서비스
CloudTrail	계정의 거버넌스, 규정 준수, 운영 및 위험 감사를 활성화하도록 도와주는 서비스
Config	AWS 계정에 있는 AWS 리소스의 구성을 자세히 보여 줍니다. 이러한 보기에는 리소스 간에 어떤 관계가 있는지와 리소스가 과거에 어떻게 구성되었는지도 포함되므로, 시간이 지나면서 구성과 관계가 어떻게 변하는지 확인할 수 있는 서비스
Systems Manager	Systems Manager 콘솔을 사용하여, 여러 AWS 서비스의 운영 데이터를 볼 수 있고 AWS 리소스 전체에 걸쳐 운영 작업을 자동화할 수 있는 서비스
GuardDuty	VPC 흐름 로그, AWS CloudTrail 이벤트 로그, DNS 로그 같은 데이터 원본을 분석하고 처리하는 지속적 보안 모니터링 서비스
Inspector	Amazon EC2 instances의 네트워크 액세스 가능성 및 해당 인스턴스에서 실행되는 애플리케이션의 보안 상태를 확인할 수 있는 서비스
Single Sign-On	모든 AWS 계정 및 클라우드 애플리케이션에 대한 SSO 액세스를 중앙에서 쉽게 관리 할 수있는 클라우드 기반 싱글 사인온 (SSO) 서비스
Certificate Manager	AWS 기반 웹 사이트 및 애플리케이션에 대한 공인 SSL/TLS 인증서를 생성 및 관리하는 서비스
KMS	데이터 암호화에 사용하는 암호화 키를 쉽게 생성하고 제어할 수 있게 해주는 관리형 서비스

WAF	Amazon CloudFront 배포, Amazon API Gateway API 또는 Application Load Balancer에 전달되는 HTTP(S) 요청을 모니터링할 수 있게 해주는 웹 애플리케이션 방화벽 서비스
Shield	Amazon Elastic Compute Cloud 인스턴스, Elastic Load Balancing 로드 밸런서, Amazon CloudFront 배포 및 Amazon Route 53 호스팅 영역 및 AWS Global Accelerator에 확장 DDoS 공격 보호를 제공하는 서비스
Security Hub	AWS 계정, 서비스 및 지원되는 타사 파트너 제품 전반에 걸쳐 보안 데이터를 수집하고, 보안 동향을 분석하고 우선 순위가 가장 높은 보안 문제를 식별할 수 있는 서비스
Data Pipeline	데이터의 이동과 변환을 자동화하는 데 사용할 수 있는 웹 서비스
Glue	완전 관리형 ETL(추출, 변환, 로드) 서비스로, 효율적인 비용으로 간단하게 여러 데이터 스토어 간에 원하는 데이터를 분류, 정리, 보강, 이동할 수 있는 서비스
MSK	Amazon Managed Streaming for Apache Kafka(Amazon MSK)는 Apache Kafka를 사용해 스트리밍 데이터를 처리하는 애플리케이션을 빌드하고 실행할 수 있는 완전관리형 서비스
Backup	클라우드 및 온프레미스에서 AWS 서비스 전반에 걸쳐 데이터 백업을 중앙 집중화하고 자동화할 수 있는 완전 관리형 백업 서비스

2) 기타 서비스 별 관리형 정책 (예시)

서비스 구분	정책명	정책설명
Organizations	AWSOrganizationsFullAccess	AWS Organizations에 대한 전체 액세스 권한
	AWSOrganizationsServiceTrustPolicy	객 구성을 단순화하기 위해 AWS Organizations가 다른 승인된 AWS 서비스와 신뢰를 공유하도록 허용하는 권한
	AWSOrganizationsReadOnlyAccess	AWS Organizations에 대한 읽기 전용 액세스 권한
CloudWatch	CloudWatchFullAccess	CloudWatch에 대한 전체 액세스 권한
	CloudWatchLogsFullAccess	CloudWatch Logs에 대한 전체 액세스 권한
	CloudWatchReadOnlyAccess	CloudWatch에 대한 읽기 전용 액세스 권한
Auto Scaling	AutoScalingFullAccess	Auto Scaling에 대한 전체 액세스 권한
	AutoScalingConsoleFullAccess	AWS Management 콘솔을 통해

		Auto Scaling에 대한 전체 액세스 권한
	AutoScalingReadOnlyAccess	Auto Scaling에 대한 읽기 전용 액세스 권한
CloudFormation	AWSCloudFormationFullAccess	AWS CloudFormation에 대한 전체 액세스 권한
	CloudFormationStackSetsOrgAdminServiceRolePolicy	CloudFormation StackSets에 대한 서비스 역할(조직 마스터 계정) 권한
	AWSCloudFormationReadOnlyAccess	AWS Management 콘솔을 통해 AWS CloudFormation에 대한 액세스 권한
CloudTrail	AWSCloudTrail_FullAccess	AWS CloudTrail에 대한 전체 액세스 권한
	CloudTrailServiceRolePolicy	CloudTrail ServiceLinkedRole에 대한 권한
	AWSCloudTrail_ReadOnlyAccess	AWS CloudTrail에 대한 읽기 전용 액세스 권한
Config	AWSConfigMultiAccountSetupPolicy	Config가 AWS 서비스를 호출하고 조직 전체에 구성 리소스를 배포하도록 허용하는 권한
	AWSConfigServiceRolePolicy	Config가 AWS 서비스를 호출하고 사용자를 대신하여 리소스 구성을 수집하도록 허용하는 권한
	AWSConfigRoleForOrganizations	WS Config가 읽기 전용 AWS Organizations API를 호출하도록 허용하는 권한
Systems Manager	AWSSystemsManagerChangeManagementServicePolicy	AWS Systems Manager 변경 관리 프레임워크에서 관리하거나 사용하는 AWS 리소스에 대한 액세스 권한
	AWSSystemsManagerOpsDataSyncServiceRolePolicy	OpsData 관련 작업을 관리하기 위한 SSM Explorer의 IAM 역할 권한
	AWSSystemsManagerAccountDiscoveryServicePolicy	WS 계정 정보를 검색할 수 있는 AWS Systems Manager(SSM) 권한

GuardDuty	AmazonGuardDutyFullAccess	Amazon GuardDuty를 사용할 수 있는 전체 액세스 권한
	AmazonGuardDutyServiceRolePolicy	Amazon Guard Duty에서 사용하거나 관리하는 AWS 리소스에 대한 액세스 권한
	AmazonGuardDutyReadOnlyAccess	mazon GuardDuty 리소스에 대한 읽기 전용 액세스 권한
Inspector	AmazonInspectorFullAccess	Amazon Inspector에 대한 전체 액세스 및 조직과 같은 기타 관련 서비스에 대한 액세스 권한
	AmazonInspectorServiceRolePolicy	보안 평가를 수행하는 데 필요한 AWS 서비스에 대한 액세스 권한
	AmazonInspectorReadOnlyAccess	Amazon Inspector에 대한 읽기 전용 액세스 권한
Single Sign-On	AWSSSODirectoryAdministrator	SSO 디렉터리에 대한 관리자 액세스 권한
	AWSSSOServiceRolePolicy	IAM 역할, 정책 및 SAML IdP를 비롯한 AWS 리소스를 관리할 수 있는 AWS SSO 권한
	AWSSSOReadOnly	AWS SSO 구성에 대한 읽기 전용 액세스 권한
Certificate Manager	AWSCertificateManagerFullAccess	AWS Certificate Manager(ACM)에 대한 전체 액세스 권한
	CertificateManagerServiceRolePolicy	Amazon Certificate Manager 서비스 역할 권한
	AWSCertificateManagerReadOnly	AWS Certificate Manager(ACM)에 대한 읽기 전용 액세스 권한
KMS	AWSKeyManagementServicePowerUser	AWS Key Management Service(KMS)에 대한 액세스 권한
	AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy	AWS KMS가 다중 리전 키의 공유 속성을 동기화할 수 있는 권한
WAF	AWSWAFFullAccess	AWS WAF 작업에 대한 전체 액세스 권한
	AWSWAFConsoleFullAccess	AWS Management 콘솔을 통해 AWS WAF에 대한 전체 액세스 권한
	AWSWAFReadOnlyAccess	AWS WAF 작업에 대한 읽기

		전용 액세스 권한
Shield	AWSShieldDRTAccessPolicy	AWS DDoS 대응 팀에 AWS 계정에 대한 제한된 액세스 권한을 제공하여 심각도가 높은 이벤트 동안 DDoS 공격 완화를 지원하는 권한
	AWSShieldServiceRolePolicy	AWS Shield가 DDoS 보호를 제공하기 위해 사용자를 대신하여 AWS 리소스에 액세스하는 권한
Security Hub	AWSSecurityHubFullAccess	AWS Security Hub를 사용할 수 있는 전체 액세스 권한
	AWSSecurityHubServiceRolePolicy	AWS Security Hub가 리소스에 액세스하는 데 필요한 서비스 연결 역할 권한
	AWSSecurityHubReadOnlyAccess	AWS Security Hub 리소스에 대한 읽기 전용 액세스 권한
Data Pipeline	AWSDataPipeline_FullAccess	Data Pipeline에 대한 전체 액세스 권한, S3, DynamoDB, Redshift, RDS, SNS 및 IAM 역할에 대한 목록 액세스 권한
	AWSDataPipeline_PowerUser	Data Pipeline에 대한 전체 액세스 권한, S3, DynamoDB, Redshift, RDS, SNS 및 IAM 역할에 대한 목록 액세스 권한, 기본 역할에 대한 passRole 액세스 권한
	AmazonC2RoleforDataPipelineRole	Data Pipeline 서비스 역할에 대한 Amazon EC2 역할에 대한 기본 정책 권한
Glue	AWSGlueConsoleFullAccess	AWS Management 콘솔을 통해 AWS Glue에 대한 전체 액세스 권한
	AWSGlueServiceRole	EC2, S3 및 Cloudwatch Logs를 포함한 관련 서비스에 대한 액세스 권한
	AWSGlueSchemaRegistryReadonlyAccess	AWS Glue Schema Registry Service에 대한 읽기 전용 액세스 권한

MSK	AmazonMSKFullAccess	Amazon MSK에 대한 전체 액세스 및 종속성에 대한 기타 필수 권한
	AmazonMSKConnect ReadOnlyAccess	Amazon MSK Connect에 대한 읽기 전용 액세스 권한
	AmazonMSKReadOnlyAccess	Amazon MSK에 대한 읽기 전용 액세스 권한
Backup	AWSBackupFullAccess	AWS 백업 작업에 대한 전체 액세스 권한
	AWSBackupOperatorAccess	AWS 리소스를 백업 계획에 할당하고 주문형 백업을 생성하고 백업을 복원할 수 있는 권한
	AWSBackupAuditAccess	AWS 백업 리소스 및 작업을 감사할 수 있는 권한

3) IAM 관리형 정책 권한 관리 List (예시)

역할	계정 관리 (그룹 및 계정명)	AWS 고객관리형 정책	취약 유/무
AWS Root 관리자	Ex)S3_Admin (admin_accout)	Ex) S3_Admin (CustomS3FullAccess)	
Infra 운영/관리자 및 담당자			
Application 운영/관리자 및 담당자			
개발 관리자 및 담당자			
재무 / 비용 관리자 및 담당자			

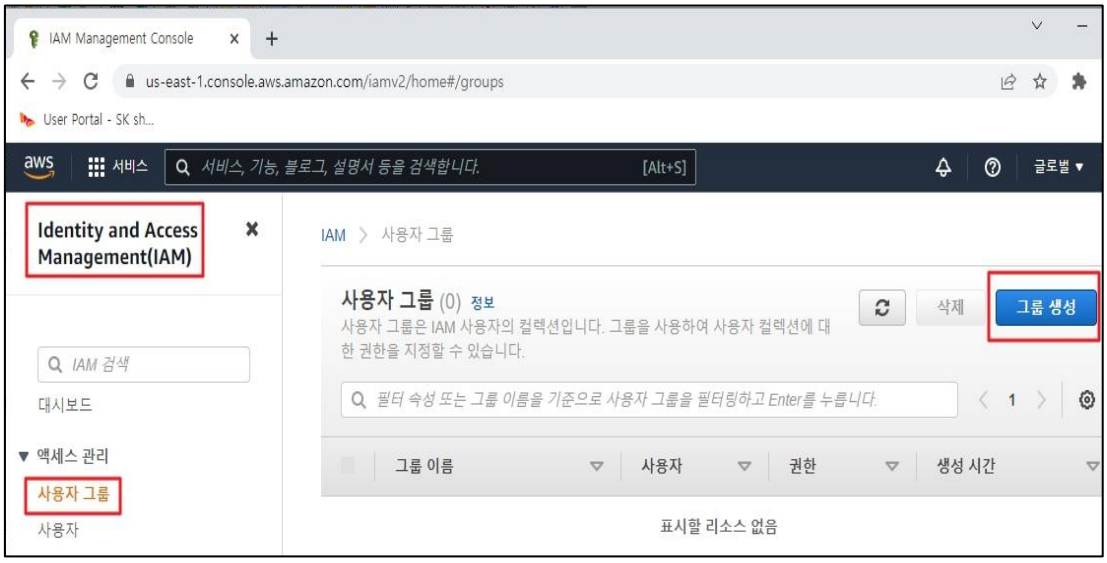
설정 방법

가. 기타 서비스 IAM 관리자/운영자 권한 그룹 생성 및 사용자 추가

- S3 서비스의 운영/관리를 위한 IAM 그룹 생성 및 사용자 추가

※ 기타 서비스 운영/관리에 필요한 IAM FULL Access 등의 권한과 같이 중요도가 높은 권한은 Infra 운영/관리자 및 담당자에게만 정책이 되도록 해야하며 최소한의 계정 수가 유지되어야 함

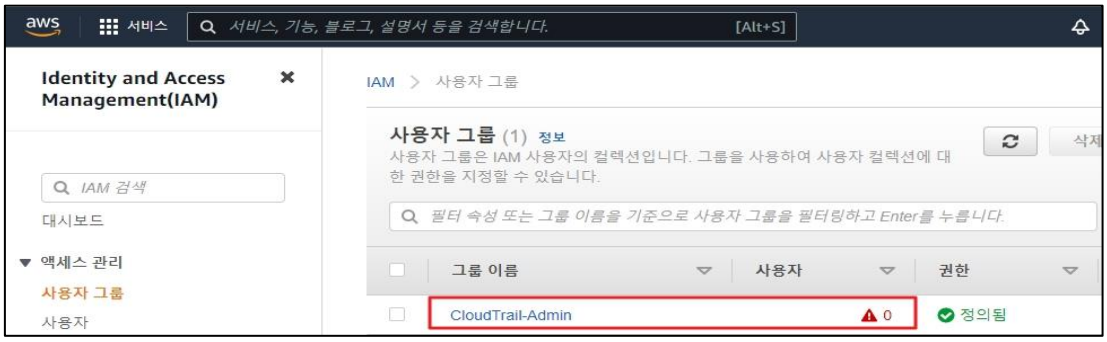
1) IAM 내 사용자 그룹 탭 접근 후 그룹 생성 클릭



2) 그룹 이름 설정

3) 정책 연결 (AWSCloudTrail_FullAccess 선택) 및 그룹 생성

4) 그룹 생성 확인



나. 기타 서비스 IAM 관리자/운영자 권한 그룹 생성 및 사용자 추가

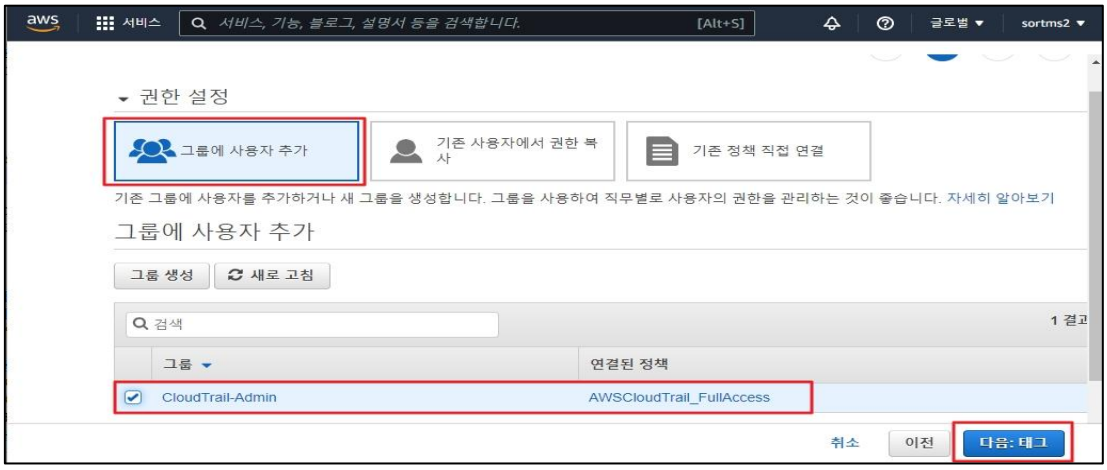
- S3 서비스의 운영/관리를 위한 IAM 그룹 생성 및 사용자 추가

※ 기타 서비스 운영/관리에 필요한 IAM FULL Access 등의 권한과 같이 중요도가 높은 권한은 Infra 운영/관리자 및 담당자에게만 정책이 되도록 해야하며 최소한의 계정 수가 유지되어야 함

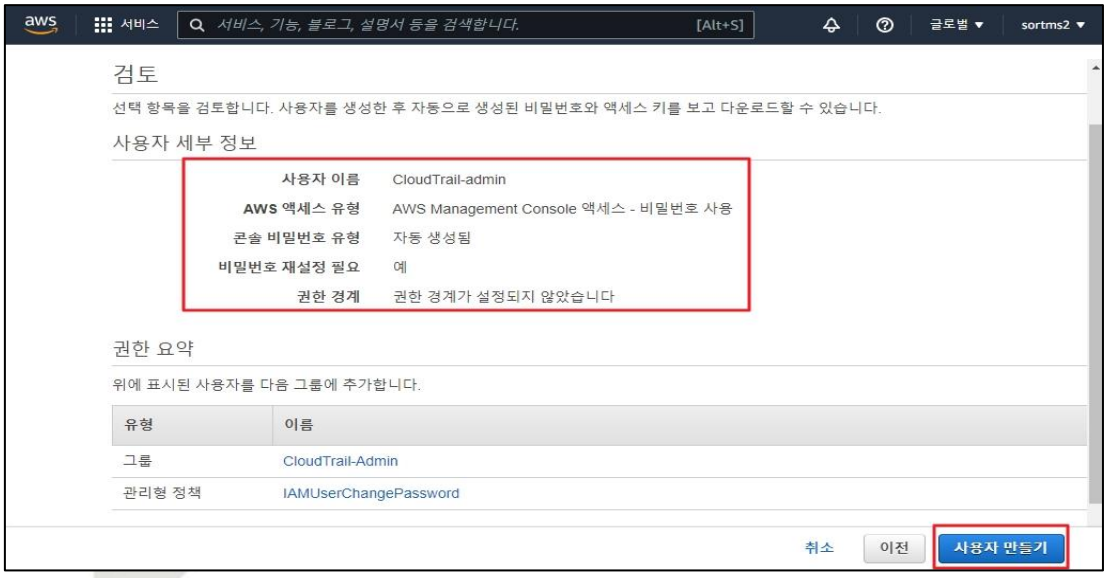
1) IAM 내 사용자 탭 접근 후 사용자 추가 클릭

2) 사용자 이름 설정 및 다음 클릭

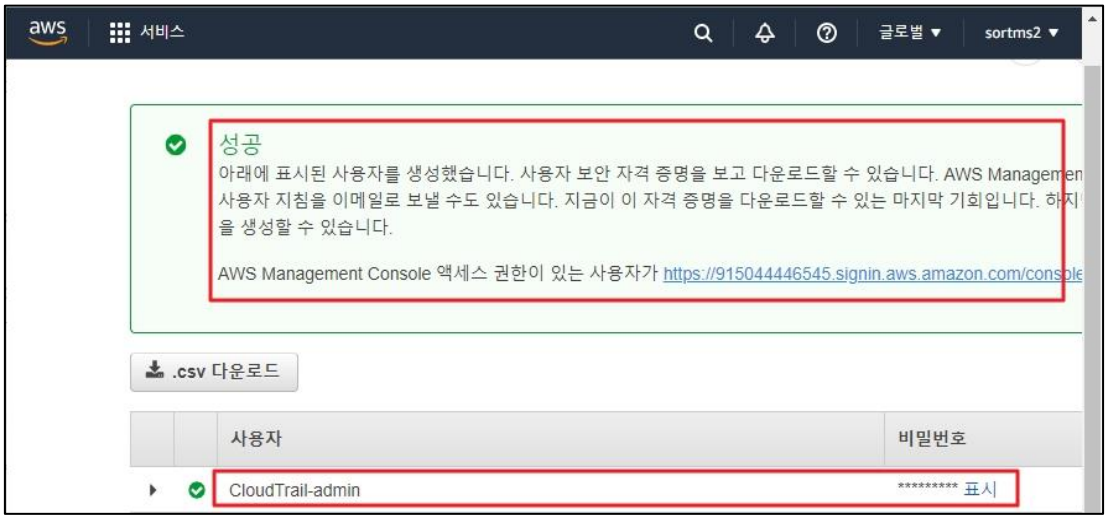
3) 그룹에 사용자 추가 설정



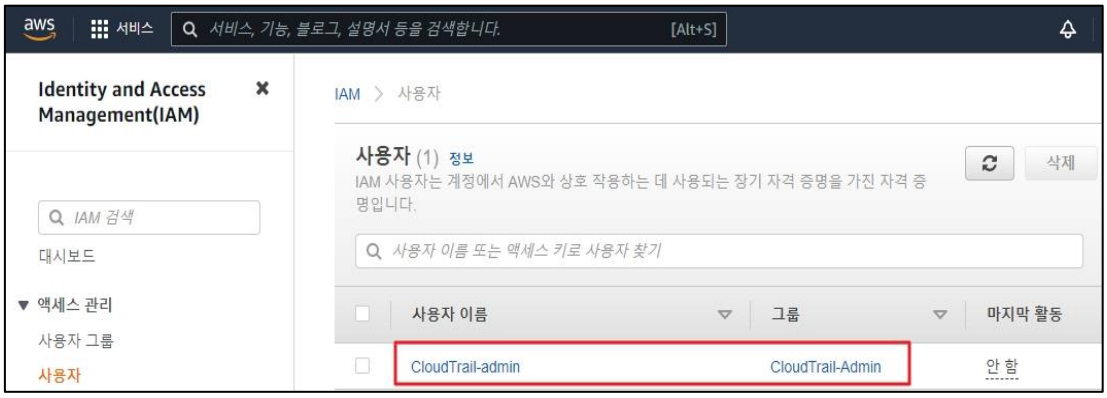
4) 검토 및 사용자 만들기 클릭



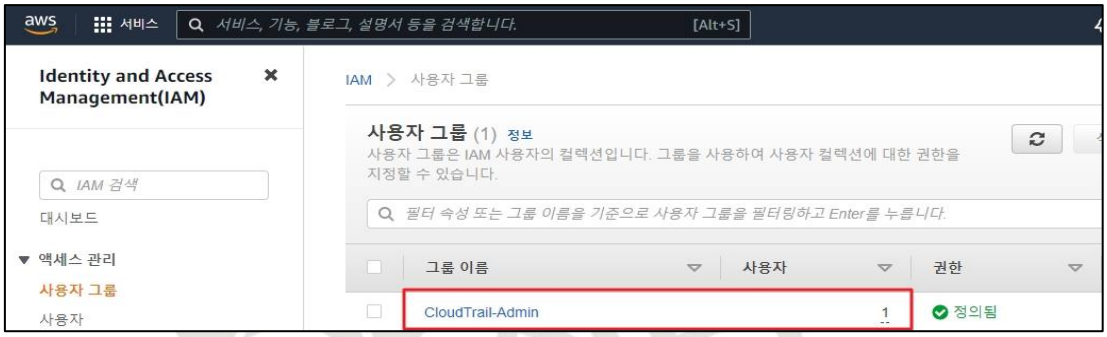
5) 사용자 추가 확인



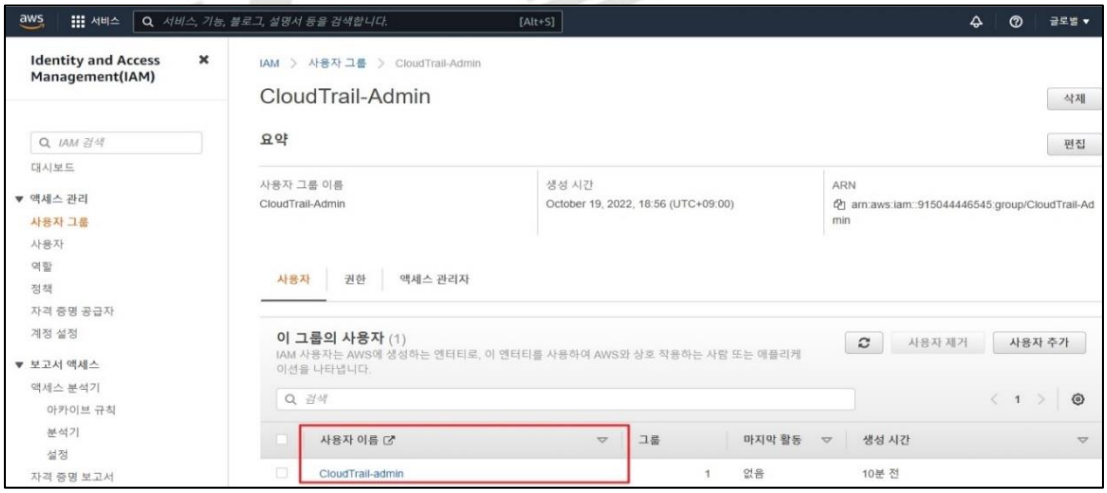
6) IAM "사용자" 클릭 및 계정 목록 확인



7) IAM "그룹" 클릭 및 그룹 목록 확인



8) 그룹 내 추가된 사용자 확인



진단 기준

양호기준

: 기타 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있을 경우

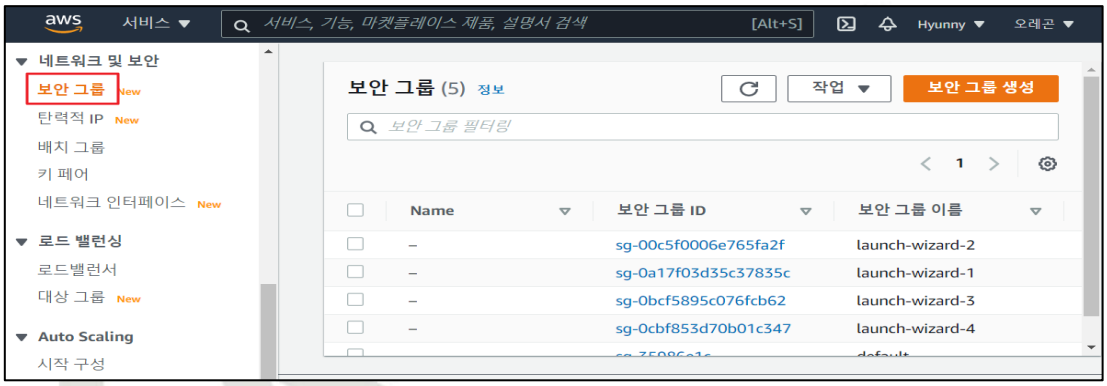
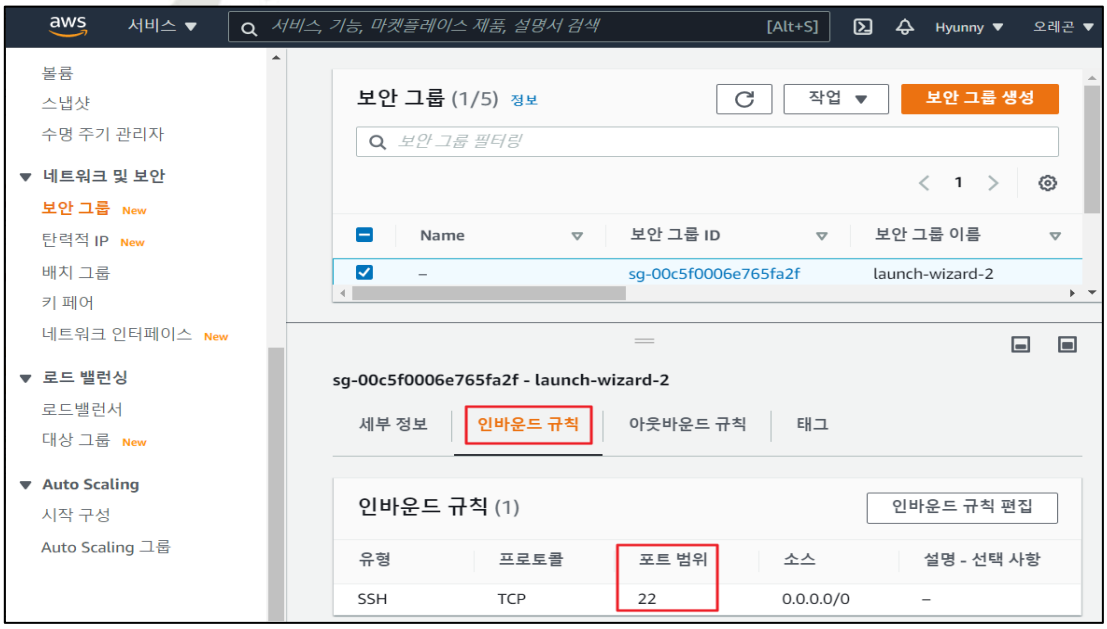
취약기준

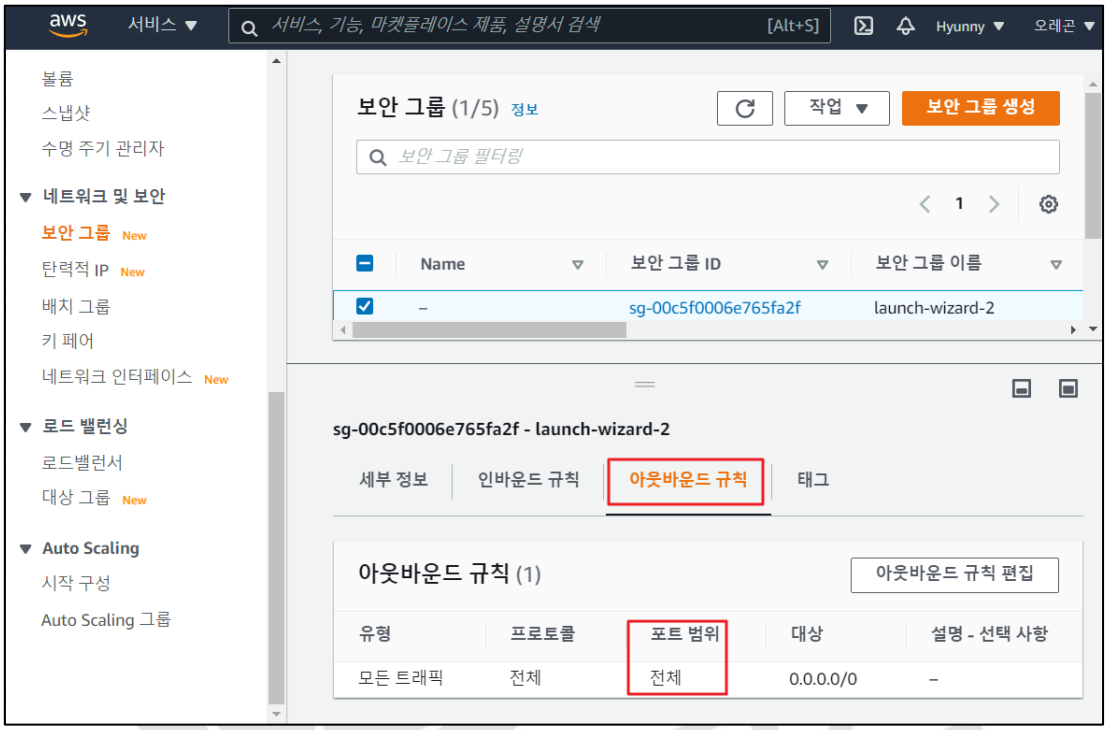
: 기타 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있지 않을 경우

비고

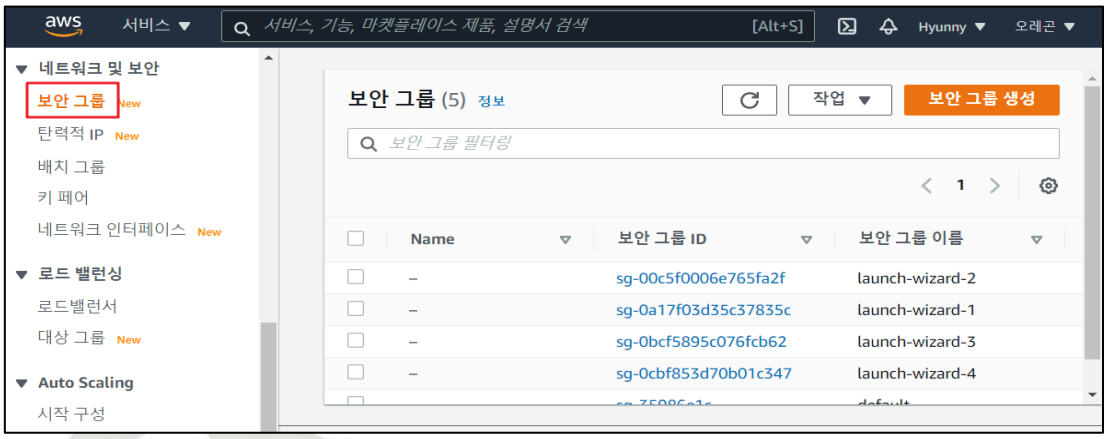
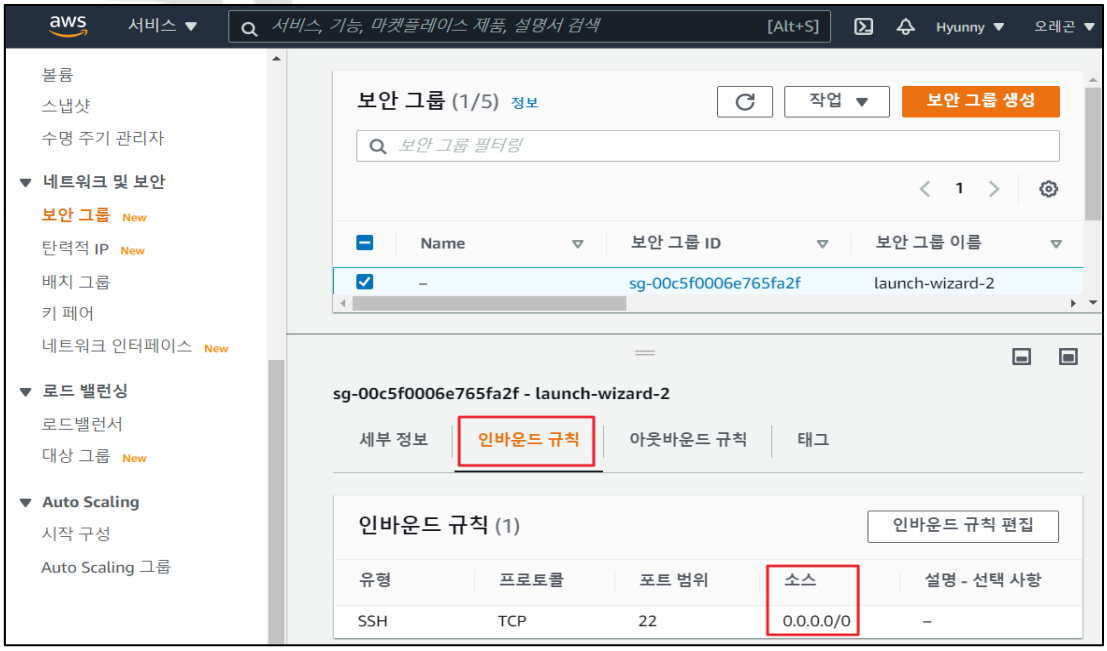
3. 가상 리소스 관리

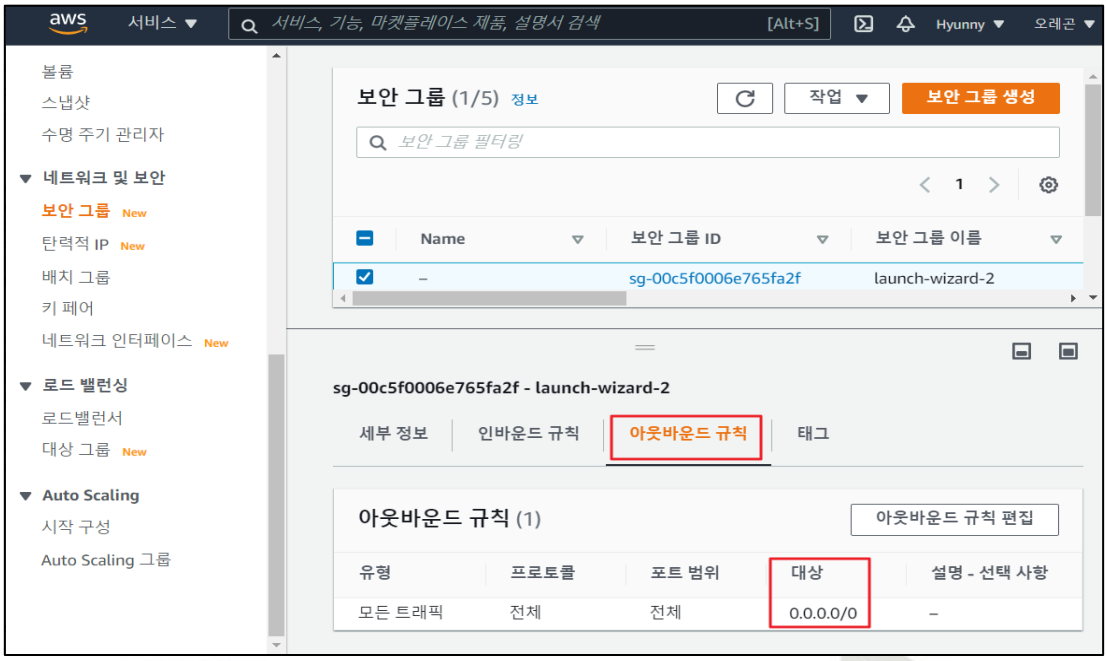
3.1 보안 그룹 인/아웃바운드 ANY 설정 관리

분류	가상 리소스 관리	중요도	상
항목명	보안 그룹 인/아웃바운드 ANY 설정 관리		
항목 설명	VPC에서의 보안 그룹은 EC2 인스턴스에 대한 인/아웃바운드 트래픽을 제어하는 가상 방화벽 역할을 합니다. VPC에서 EC2 인스턴스를 시작할 때 최대 5개의 보안 그룹에 인스턴스를 할당할 수 있습니다. 보안 그룹은 서브넷 수준이 아니라 인스턴스 수준에서 작동하므로 VPC에 있는 서브넷의 각 인스턴스를 서로 다른 보안 그룹 세트에 할당할 수 있습니다. 보안 그룹은 인/아웃바운드의 규칙 편집을 통해 특정 소스(출발지)에서의 통신이 가능하도록 유형(네트워크 프로토콜) 및 단일/범위 포트를 설정할 수 있습니다.		
설정 방법	**가. 보안 그룹 인/아웃바운드 포트 정책 확인** 1) EC2 내 보안 그룹 탭 접근 -> 보안 그룹 ID 선택  2) 선택된 보안 그룹 인바운드 규칙 내 포트 확인  		

	3) 선택된 보안 그룹 아웃바운드 규칙 내 포트 확인 
진단 기준	**양호기준** : 보안 그룹 내 인/아웃바운드의 포트가 Any로 허용되어 있지 않을 경우 **취약기준** : 보안 그룹 내 인/아웃바운드의 포트가 Any로 허용되어 있을 경우
비고	

3.2 보안 그룹 인/아웃바운드 불필요 정책 관리

분류	가상 리소스 관리	중요도	상
항목명	보안 그룹 인/아웃바운드 불필요 정책 관리		
항목 설명	VPC에서의 보안 그룹은 EC2 인스턴스에 대한 인/아웃바운드 트래픽을 제어하는 가상 방화벽 역할을 합니다. VPC에서 EC2 인스턴스를 시작할 때 최대 5개의 보안 그룹에 인스턴스를 할당할 수 있습니다. 보안 그룹은 서브넷 수준이 아니라 인스턴스 수준에서 작동하므로 VPC에 있는 서브넷의 각 인스턴스를 서로 다른 보안 그룹 세트에 할당할 수 있습니다. 보안 그룹은 인/아웃바운드의 규칙 편집을 통해 특정 소스(출발지)에서의 통신이 가능하도록 유형(네트워크 프로토콜) 및 단일/범위 정책을 설정할 수 있습니다.		
설정 방법	**가. 보안 그룹 인/아웃바운드 소스 정책 확인** 1) EC2 내 보안 그룹 탭 접근 -> 보안 그룹 ID 선택  2) 선택된 보안 그룹 인바운드 규칙 내 소스 확인 		

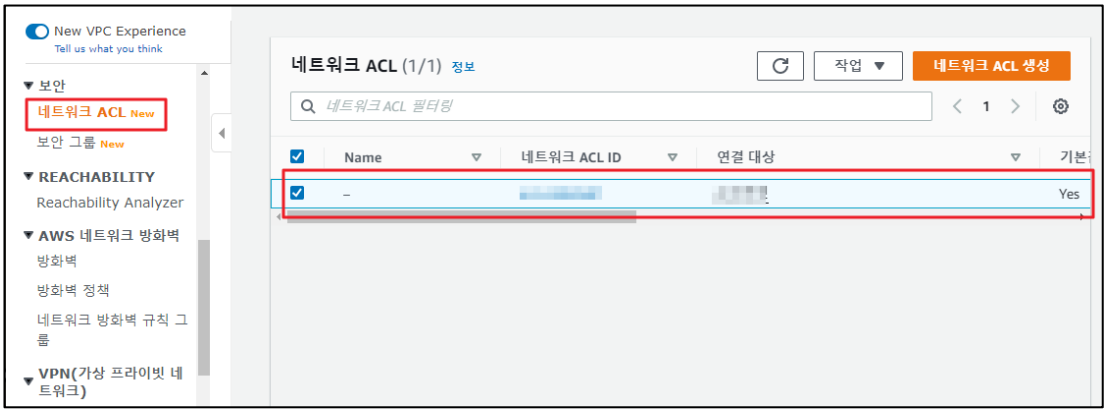
	3) 선택된 보안 그룹 아웃바운드 규칙 내 소스 확인 
진단 기준	**양호기준** : 보안 그룹 인/아웃바운드 규칙 내 불필요한 정책(Source, Destination)이 존재하지 않는 경우 **취약기준** : 보안 그룹 인/아웃바운드 규칙 내 불필요한 정책(Source, Destination)이 존재하는 경우
비고	

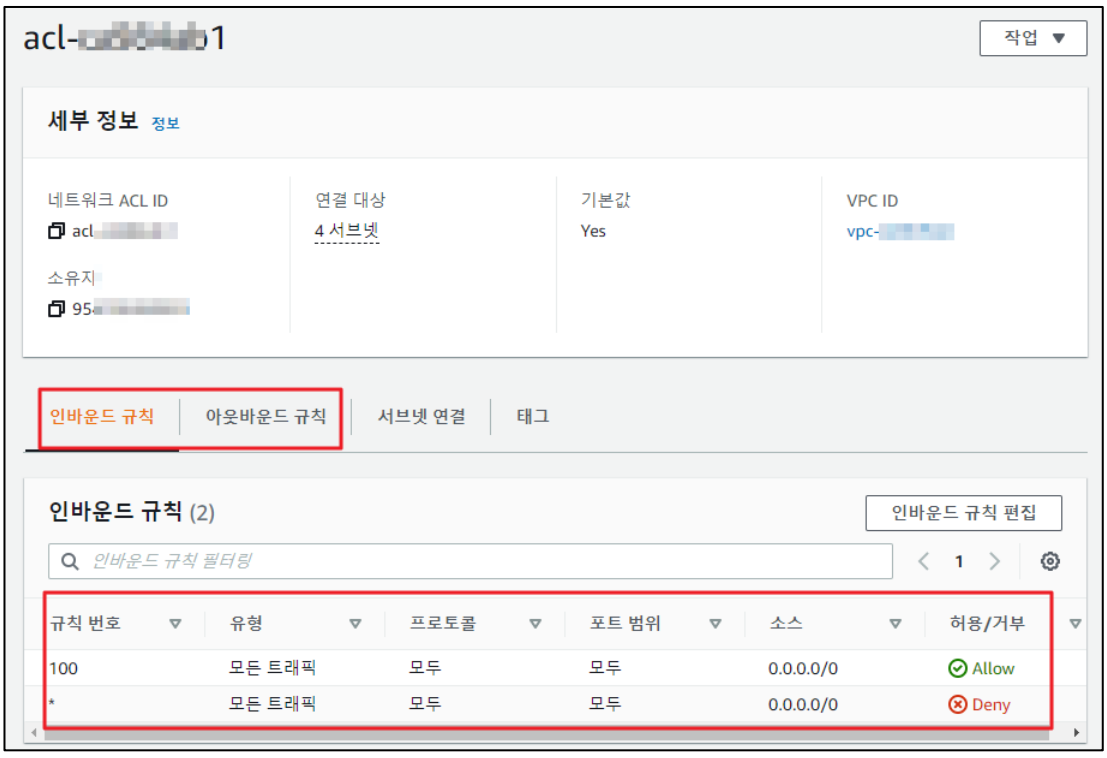
3.3 네트워크 ACL 인/아웃바운드 트래픽 정책 관리

<table>
<tr><td>분류</td><td>가상 리소스 관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">네트워크 ACL 인/아웃바운드 트래픽 정책 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">
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. ACL은 VPC 서브넷 계층에서 동작하며 VPC 서브넷과는 1:1로 대응합니다. 정책의 방식은 허용(Allow) 및 거부(deny) 정책(WhiteList or BlackList) 기능으로 Stateless 방식으로 사용이 됩니다.

VPC에 있는 각 서브넷을 네트워크 ACL과 연결하여 사용할 수 있으며, 서브넷을 네트워크 ACL에 명시적으로 연결하지 않을 경우, 서브넷은 기본 네트워크 ACL에 자동적으로 연결합니다.
(단, 하나의 네트워크 ACL은 다수의 서브넷과 연결할 수 있지만 하나의 서브넷은 하나의 ACL에만 연결할 수 있음)

(*) 기본 네트워크 ACL 규칙
기본 네트워크 ACL은 연결된 서브넷 트래픽 흐름을 모두 허용하도록 구성되어 있습니다. 각 네트워크 ACL에는 규칙 번호가 별표로 되어 있는 규칙도 포함되어 있습니다. 이 규칙은 패킷이 번호가 매겨진 다른 어떤 규칙과도 일치하지 않을 경우에는 거부되도록 되어 있습니다. 이 규칙을 수정하거나 제거할 수 없습니다.
<table>
<tr><th colspan="6">인바운드 정책</th></tr>
<tr><th>규칙 #</th><th>유형</th><th>프로토콜</th><th>포트</th><th>소스</th><th>허용/거부</th></tr>
<tr><td>100</td><td>모든 IPv4 트래픽</td><td>모두</td><td>모두</td><td>0.0.0.0/0</td><td>ALLOW</td></tr>
<tr><td>*</td><td>모든 IPv4 트래픽</td><td>모두</td><td>모두</td><td>0.0.0.0/0</td><td>DENY</td></tr>
</table>
<table>
<tr><th colspan="6">아웃바운드 정책</th></tr>
<tr><th>규칙 #</th><th>유형</th><th>프로토콜</th><th>포트</th><th>소스</th><th>허용/거부</th></tr>
<tr><td>100</td><td>모든 IPv4 트래픽</td><td>모두</td><td>모두</td><td>0.0.0.0/0</td><td>ALLOW</td></tr>
<tr><td>*</td><td>모든 IPv4 트래픽</td><td>모두</td><td>모두</td><td>0.0.0.0/0</td><td>DENY</td></tr>
</table>
</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. 네트워크 ACL 정책 확인
1) 네트워크 ACL 확인</td></tr>
</table>

<table>
<tr>
<td></td>
<td>


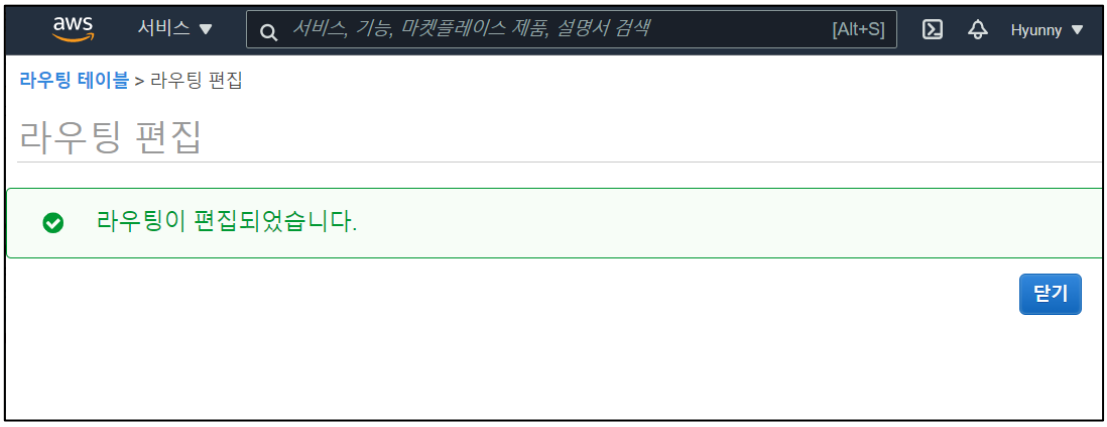
2) 인바운드/아웃바운드 규칙 확인


</td>
</tr>
<tr>
<td>진단 기준</td>
<td>
양호기준
: 네트워크 ACL 내 인/아웃바운드에 대한 모든 트래픽이 허용되어 있지 않을 경우

취약기준
: 네트워크 ACL 내 인/아웃바운드에 대한 모든 트래픽이 허용되어 있을 경우
</td>
</tr>
<tr>
<td>비고</td>
<td>보안 그룹의 포트 및 소스의 정책이 ANY로 허용되어 있을 경우 중요도가 상으로 변경될 수 있음</td>
</tr>
</table>

3.4 라우팅 테이블 정책 관리

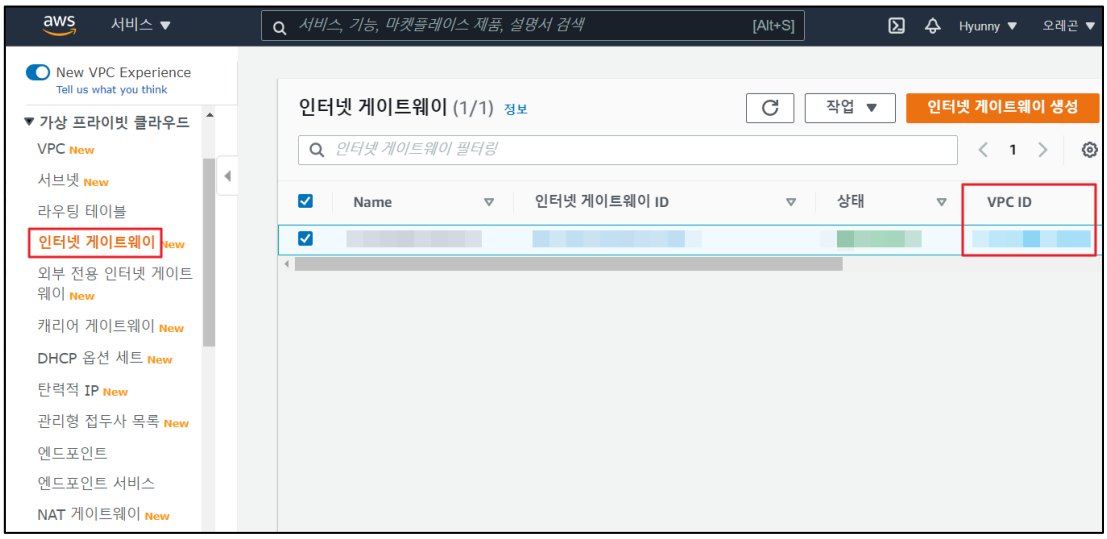
분류	가상 리소스 관리	중요도	중
항목명	라우팅 테이블 정책 관리		
항목 설명	라우팅 테이블에는 네트워크 트래픽을 전달할 위치 결정 시 사용되는 규칙입니다. VPC의 각 서브넷을 라우팅 테이블에 연결해야 하며, 테이블에서는 서브넷에 대한 라우팅을 제어하게 됩니다. 서브넷을 한 번에 하나의 라우팅 테이블에만 연결 할 수 있지만 여러 서브넷을 동일한 라우팅 테이블에 연결하는 것은 가능합니다. VPC를 신규 생성하게 될 경우 기본 라우팅 테이블이 자동으로 생성됩니다. Amazon VPC 콘솔의 [라우팅 테이블] 페이지의 [Main] 열에서 [Yes]를 찾아 VPC에 대한 기본 라우팅 테이블을 볼 수 있습니다. 기본 라우팅 테이블은 다른 라우팅 테이블과 명시적으로 연결되지 않은 모든 서브넷에 대한 라우팅을 제어합니다. 기본 라우팅 테이블에서 라우팅을 추가 및 제거하고 수정할 수 있습니다.		
설정 방법	**가. 라우팅 테이블 설정 방법** 1) VPC 내 라우팅 테이블 탭 접근 후 라우팅 편집 클릭  2) 라우팅 테이블 설정 및 저장 		

	3) 라우팅 테이블 설정 완료 
진단 기준	**양호기준** : 라우팅 테이블 내 ANY 정책이 설정되어 있지 않고 서비스 타깃 별로 설정되어 있을 경우 **취약기준** : 라우팅 테이블 내 ANY 정책이 설정되어 있거나 서비스 타깃 별로 설정되어 있지 않을 경우
비고	서비스 구성 시 게이트웨이 및 아웃바운드 통신이 필요한 경우 ANY 허용은 양호로 처리될 수 있음 (ex. 클라우드 프라이빗 Network를 IDC 네트워크 대역(On-Premise)으로 허용할 경우)

3.5 인터넷 게이트웨이 연결 관리

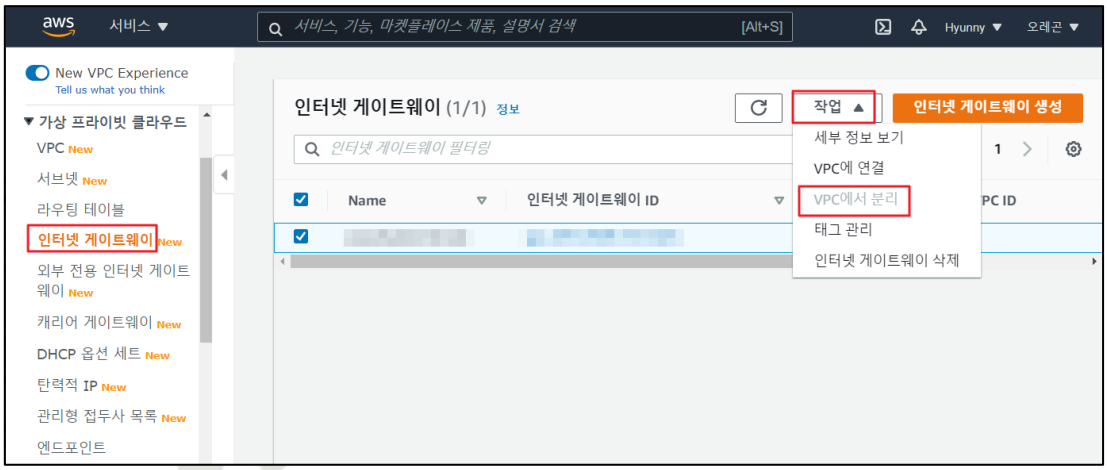
<table>
<tr><td>분류</td><td>가상 리소스 관리</td><td>중요도</td><td>하</td></tr>
<tr><td>항목명</td><td colspan="3">인터넷 게이트웨이 연결 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">인터넷 게이트웨이는 수평 확장되고 가용성이 높은 중복 VPC 구성요소로, VPC의 인스턴스와 인터넷 간에 통신이 가능할 수 있게 해주는 기능이며 네트워크 트래픽 가용성 위험이나 대역폭 제약조건이 별도로 발생하진 않습니다.
인터넷 게이트웨이에는 인터넷 Route 가능 트래픽에 대한 VPC 라우팅 테이블에 대상을 제공하고, 퍼블릭 IPv4 주소가 할당된 인스턴스에 대해 NAT(네트워크 주소 변환)를 수행하는 두 가지 목적이 있으며, IPv4, IPv6 트래픽을 모두 지원합니다.

(*) 기본 VPC와 기본이 아닌 VPC에 대한 인터넷 액세스
<table>
<tr><th>구분</th><th>기존 VPC</th><th>기본이 아닌 VPC</th></tr>
<tr><td>인터넷 게이트웨이</td><td>예</td><td>VPC 마법사의 첫 번째 또는 두 번째 옵션을 사용하여 VPC를 생성한 경우.
그렇지 않은 경우, 인터넷 게이트웨이를 수동으로 생성하여 연결해야 합니다.</td></tr>
<tr><td>IPv4 트래픽을 위한 인터넷 게이트웨이로 가는 경로가 있는 라우팅 테이블(0.0.0.0/0)</td><td>예</td><td>VPC 마법사의 첫 번째 또는 두 번째 옵션을 사용하여 VPC를 생성한 경우.
그렇지 않은 경우, 라우팅 테이블을 수동으로 생성하여 경로를 추가해야 합니다.</td></tr>
<tr><td>IPv6 트래픽을 위한 인터넷 게이트웨이로 가는 경로가 있는 라우팅 테이블(::/0)</td><td>아니요</td><td>VPC 마법사의 첫 번째 또는 두 번째 옵션을 사용하여 VPC를 생성한 경우, 그리고 IPv6 CIDR 블록을 VPC와 연결하기 위해 옵션을 지정한 경우.
그렇지 않은 경우, 라우팅 테이블을 수동으로 생성하여 경로를 추가해야 합니다.</td></tr>
<tr><td>서브넷에서 시작된 인스턴스에 자동 할당된 퍼블릭 IPv4 주소</td><td>예
(기본 서브넷)</td><td>아니요(기본이 아닌 서브넷)</td></tr>
<tr><td>서브넷에서 시작된 인스턴스에 자동 할당된 IPv6 주소</td><td>아니요
(기본 서브넷)</td><td>아니요(기본이 아닌 서브넷)</td></tr>
</table></td></tr>
<tr><td>설정
방법</td><td colspan="3">가. 인터넷 게이트웨이 설정 확인
1) 인터넷 게이트웨이 확인</td></tr>
</table>



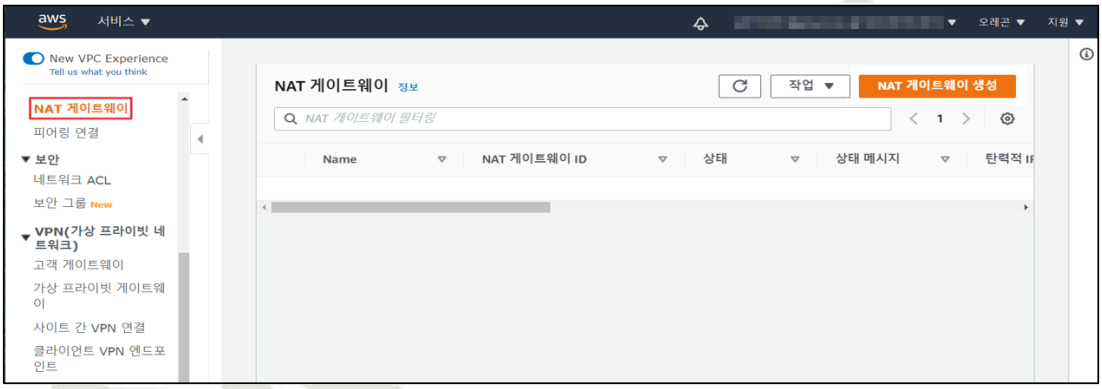
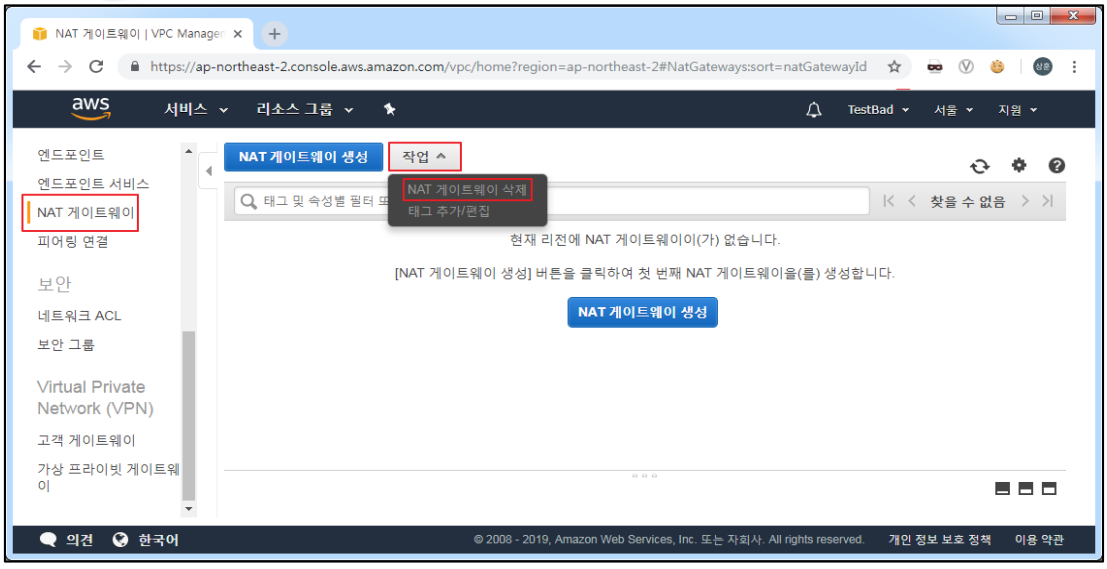
나. 인터넷 게이트웨이 삭제 방법

1) VPC → "인터넷 게이트웨이" → "인터넷 게이트웨이" 선택 → 작업 → VPC에서 분리



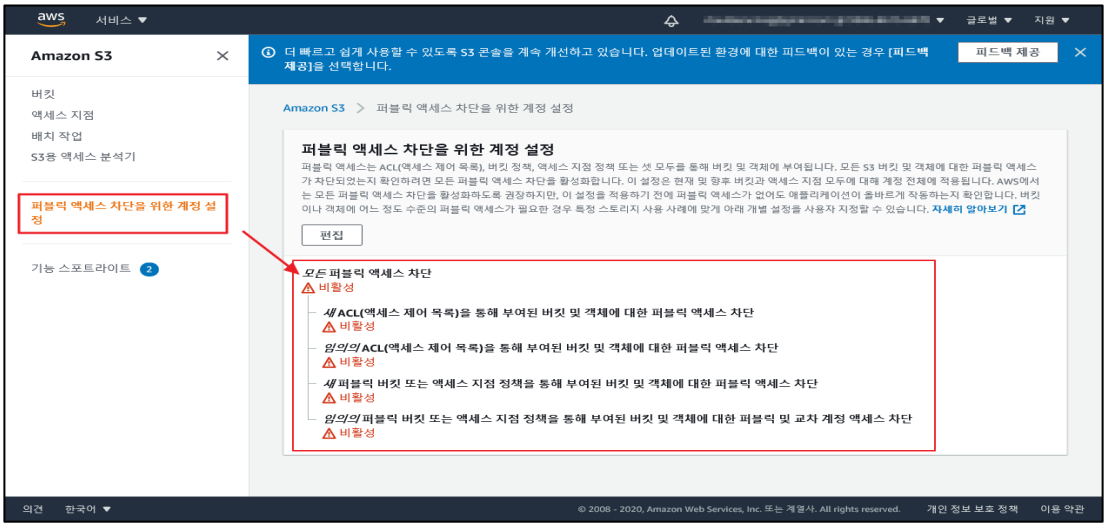
진단 기준	**양호기준** : 인터넷 게이트웨이에 불필요하게 연결된 NAT 게이트웨이가 존재하지 않을 경우 **취약기준** : 인터넷 게이트웨이에 불필요하게 연결된 NAT 게이트웨이가 존재하는 경우
비고	

3.6 NAT 게이트웨이 연결 관리

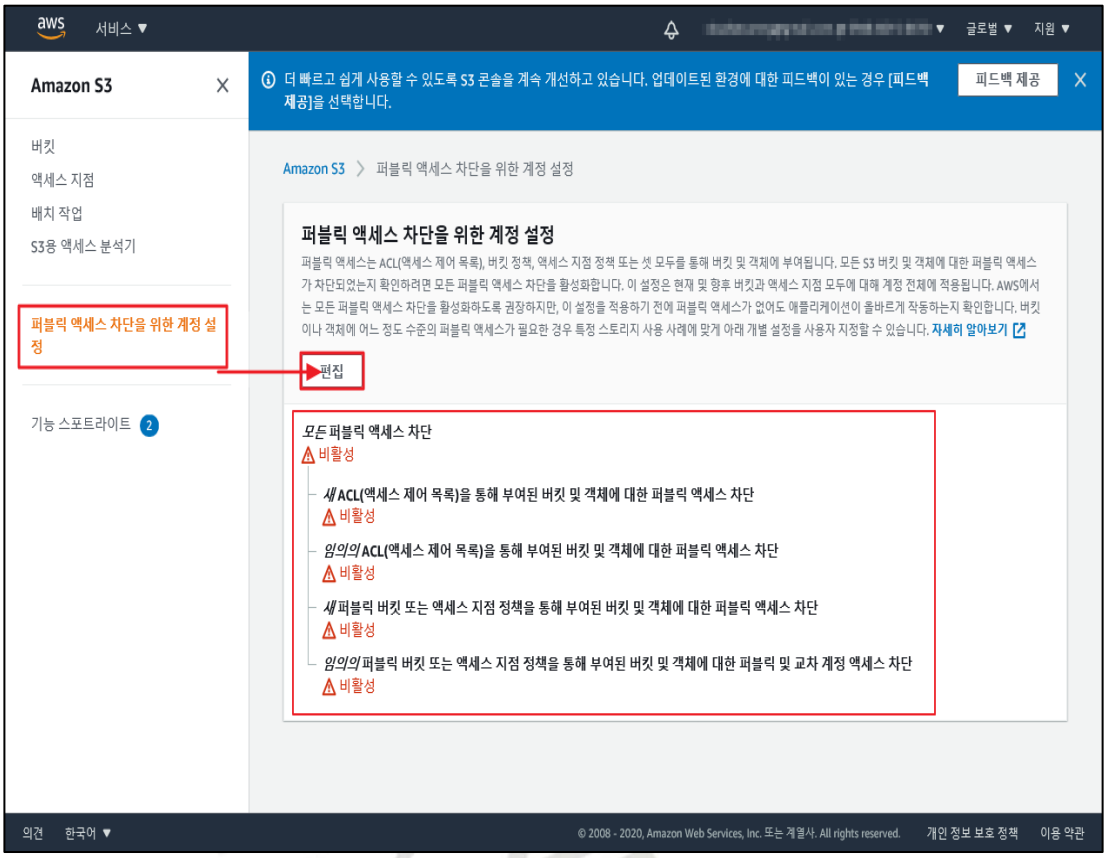
분류	가상 리소스 관리	중요도	중
항목명	NAT 게이트웨이 연결 관리		
항목 설명	NAT 게이트웨이는 NAT 디바이스를 사용하여 프라이빗 서브넷의 인스턴스를 인터넷(예: 소프트웨어 업데이트용) 또는 기타 AWS 서비스에 연결하는 한편, 인터넷에서 해당 인스턴스와의 연결을 시작하지 못하도록 할 수 있습니다. NAT 디바이스는 프라이빗 서브넷의 인스턴스에서 인터넷 또는 기타 AWS 서비스로 트래픽을 전달한 다음 인스턴스에 응답을 다시 보냅니다. 트래픽이 인터넷으로 이동하면 소스 IPv4 주소가 NAT 디바이스의 주소로 대체되고, 이와 마찬가지로 응답 트래픽이 해당 인스턴스로 이동하면 NAT 디바이스에서 주소를 해당 인스턴스의 프라이빗 IPv4 주소로 다시 변환합니다.		
설정 방법	**가. NAT 게이트웨이 생성 및 프라이빗 연결 확인** 1) NAT 게이트웨이 확인  **나. NAT 게이트웨이 삭제 방법** 1) VPC 내 NAT 게이트웨이 탭 접근 후 NAT 게이트웨이 삭제 클릭  		

진단 기준	**양호기준** : 외부 통신이 필요한 리소스가 NAT 게이트웨이가 연결되어 있을 경우 **취약기준** : 목적이 확인되지 않은 리소스가 NAT 게이트웨이에 연결되어 있을 경우
비고	외부에 오픈을 금지해야 하는 서비스(DBMS, 개인정보 보관 웹 서비스 등)

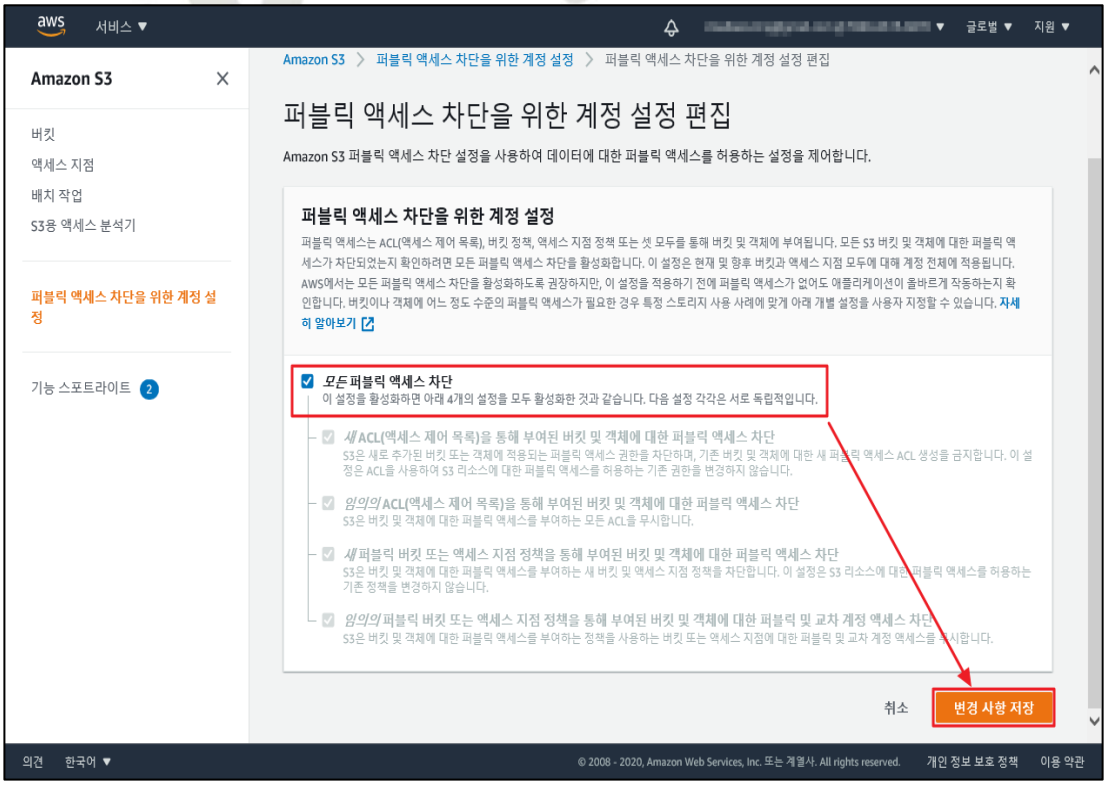
3.7 S3 버킷/객체 접근 관리

분류	가상 리소스 관리	중요도	중
항목명	S3 버킷/객체 접근 관리		
항목 설명	S3 버킷의 경우 리소스(버킷)를 생성한 소유자에 대해 리소스 액세스가 가능하며 액세스 정책을 별도(버킷, 객체) 설정하여 다른 사람에게 액세스 권한을 부여할 수 있습니다. 또한, 퍼블릭 액세스 차단 설정이 되지 않을 경우 외부로부터 버킷 및 객체가 노출되므로 안전한 버킷/객체 접근을 위해 목적에 맞는 접근 설정을 해야합니다. **1) 퍼블릭 액세스 차단 관리** - 퍼블릭 S3: 외부 사용의 관한 연결 통로를 제공하는 것이기 때문에 설정을 제한해야 합니다. - 프라이빗 S3: 접근 가능한 IAM 계정에 대한 권한이 설정되어 있어야 합니다. **※ AWS Admin Console Account로의 접근은 지양하며 가급적 IAM 계정을 통한 S3 접근을 권장함** **2) 버킷/객체 ACL 권한 관리** S3 버킷/객체 권한은 "ACL 권한(버킷소유자, 모든 사람, 외부계정)", "객체 권한(읽기, 쓰기)" 등으로 나뉘어 지며 버킷에 대한 접근 권한이 허용될 경우 객체에 설정된 정책이 적용되기 때문에 가급적 "ACL 권한(모든 사람, 외부계정)"에 대해 권한 허용을 지양해야 합니다. **3) 버킷 정책(JSON)** S3 버킷에 접근하고자 하는 계정에 대한 액세스 권한을 JSON 구문의 형태로 설정할 수 있는 기능입니다. "Sid(권한명)", "Effect(Allow, Deny)", "Principal(ARN 계정명)", "Action(액세스 권한명)		
설정 방법	**가. 퍼블릭 액세스 차단을 위한 계정 설정 확인** 1) 서비스 > S3 > 퍼블릭 액세스 차단을 위한 계정 설정 내 상태 확인 		

2) 서비스 > S3 > 퍼블릭 액세스 차단을 위한 계정 설정 > 편집 (비활성화 시)

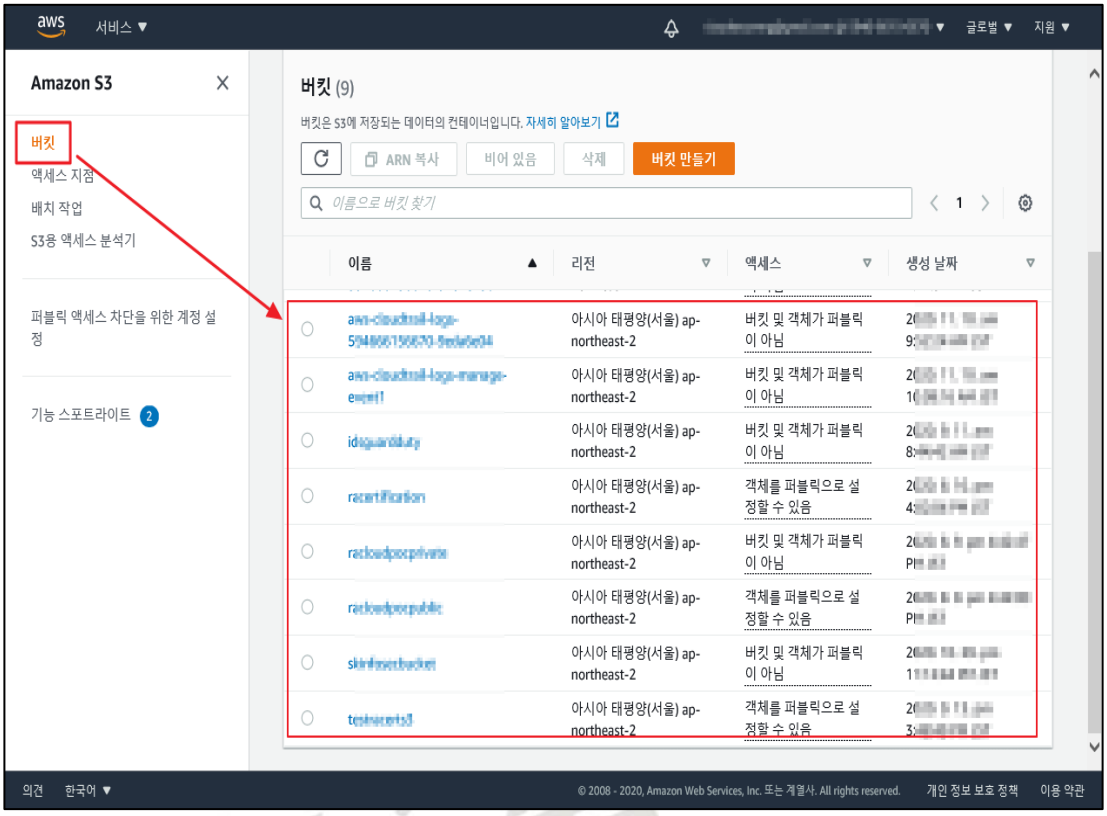


3) 모든 퍼블릭 액세스 차단 활성화

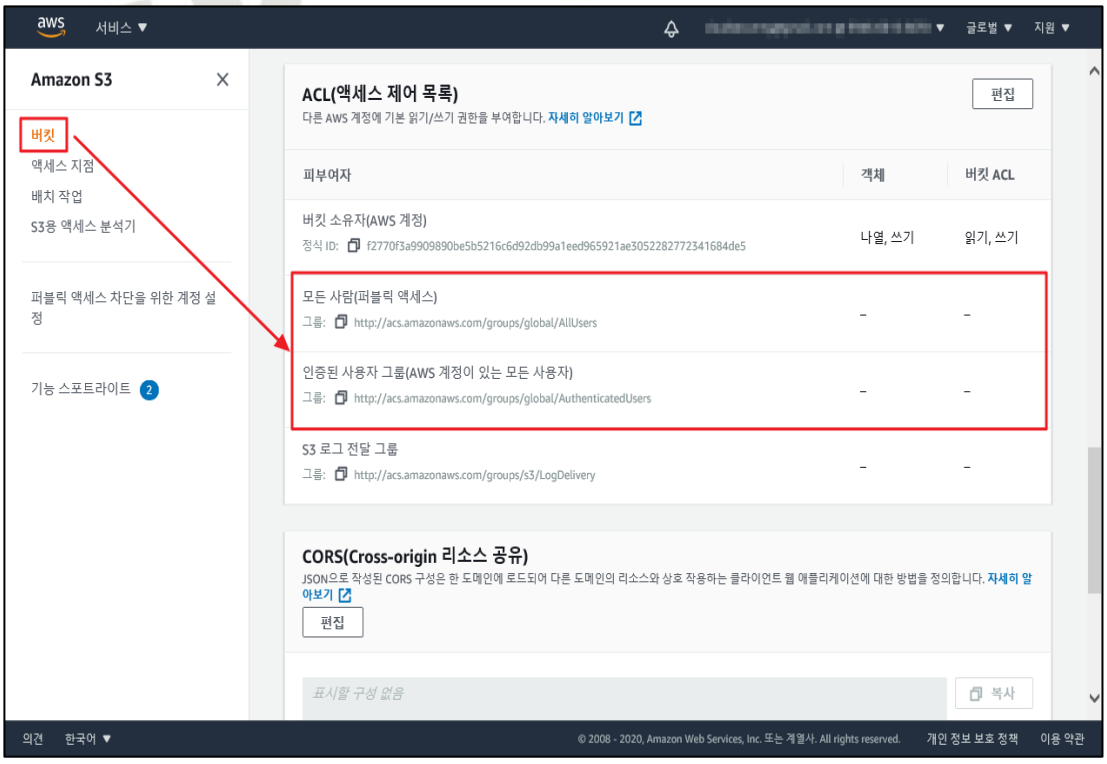


나. 버킷 ACL(액세스 제어 목록) 확인

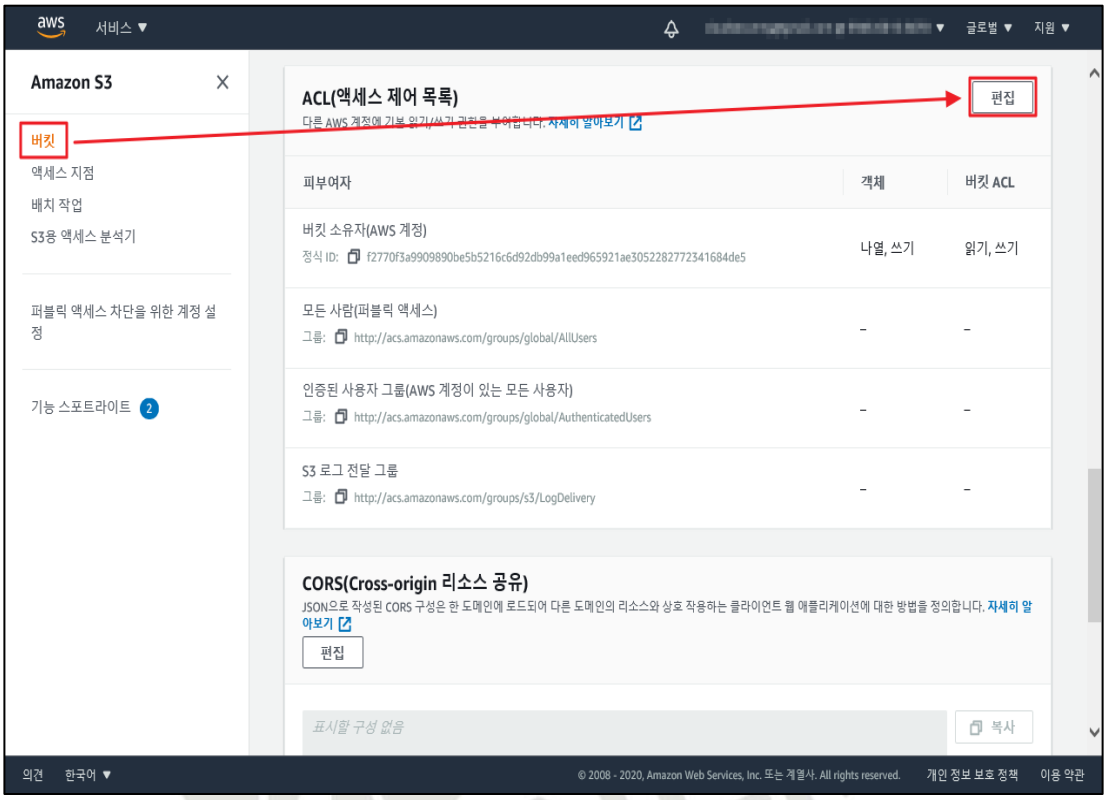
1) 서비스 > S3 > 버킷 > 설정 된 버킷 선택



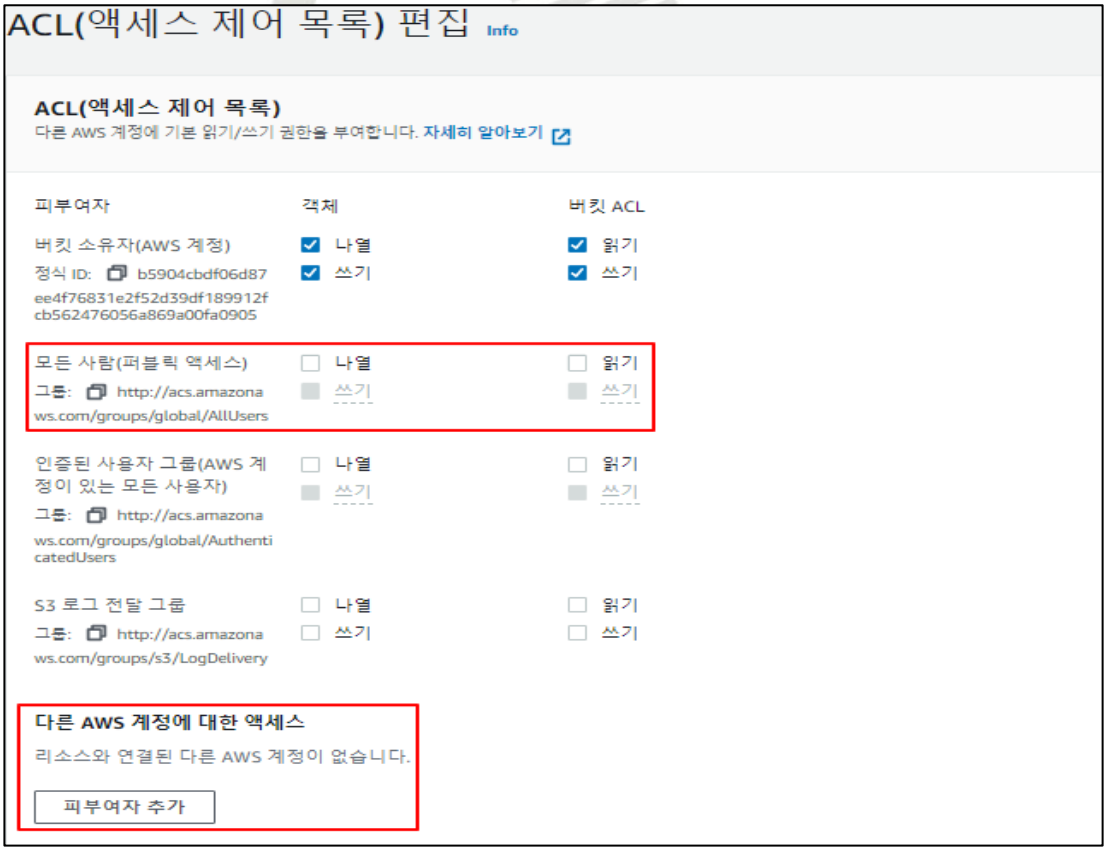
2) 권한 > ACL(액세스 제어 목록) 확인



3) 권한 > ACL(액세스 제어 목록) > 편집 (기타 권한 존재 시)

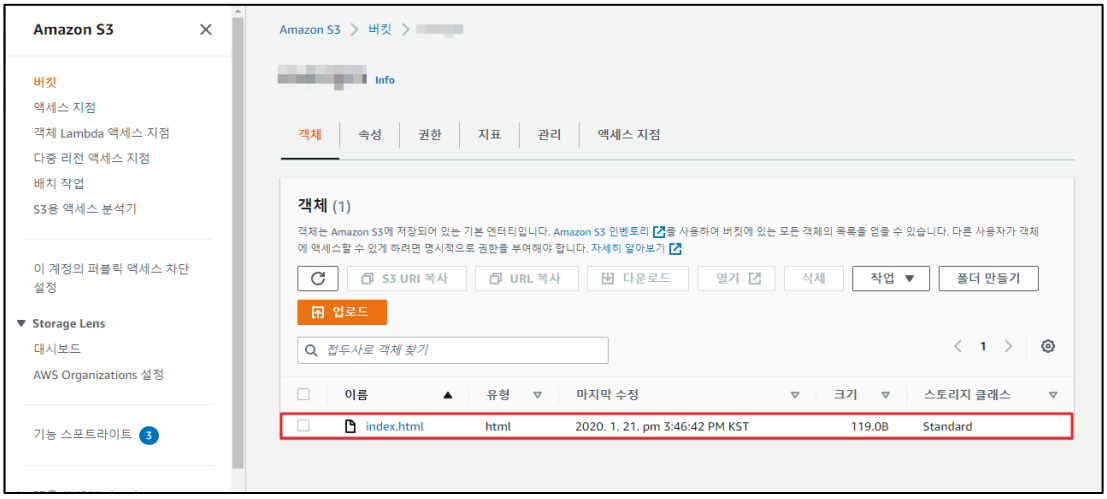


4) 불필요 권한 비활성화



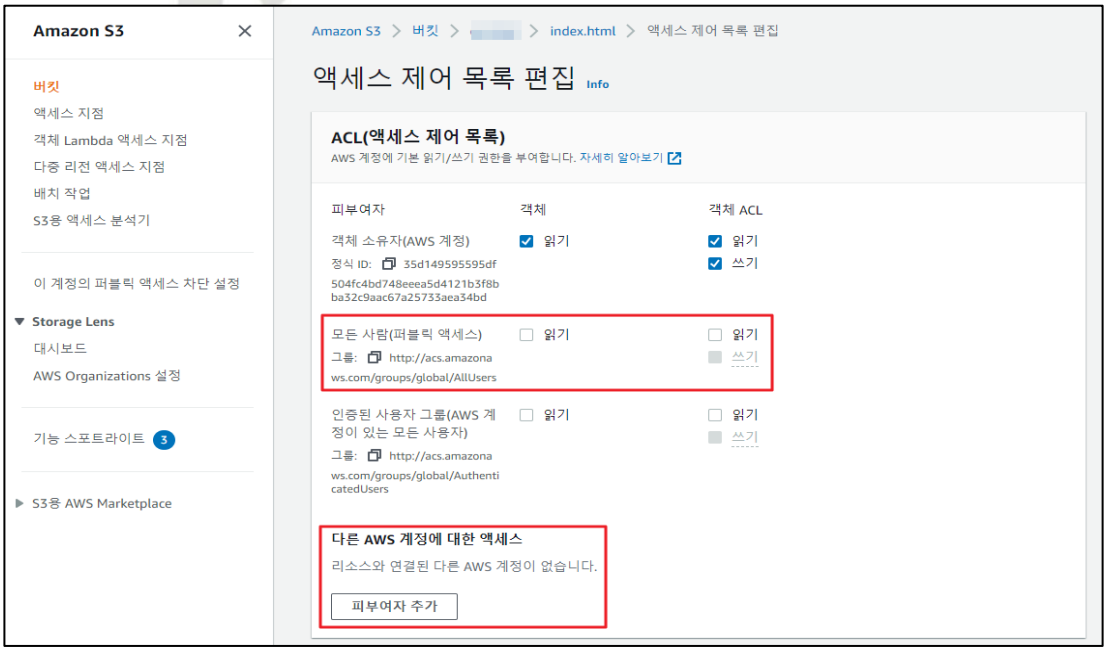
다. 객체 ACL(액세스 제어 목록) 확인

1) 서비스 > S3 > 버킷 > 버킷 내 객체 선택



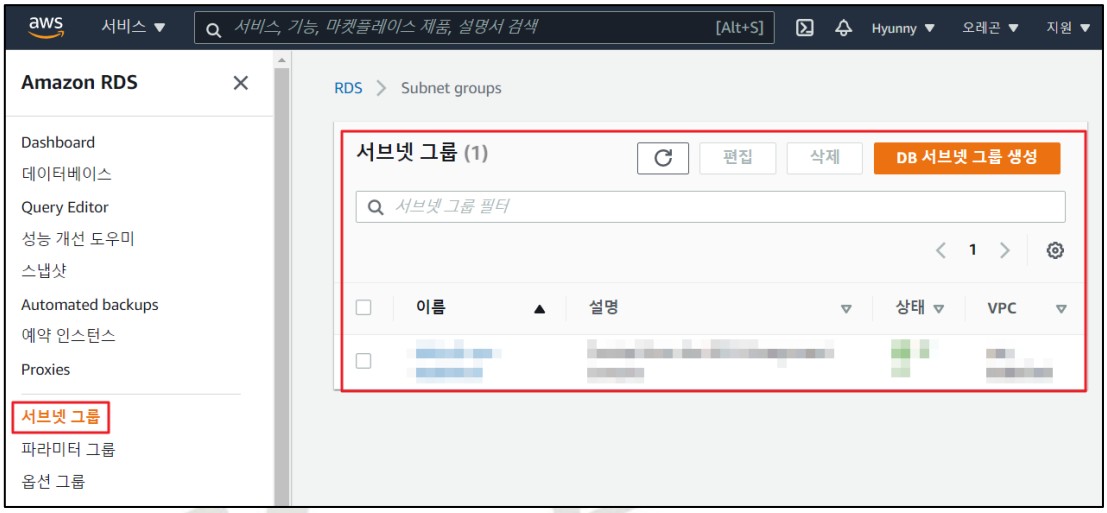
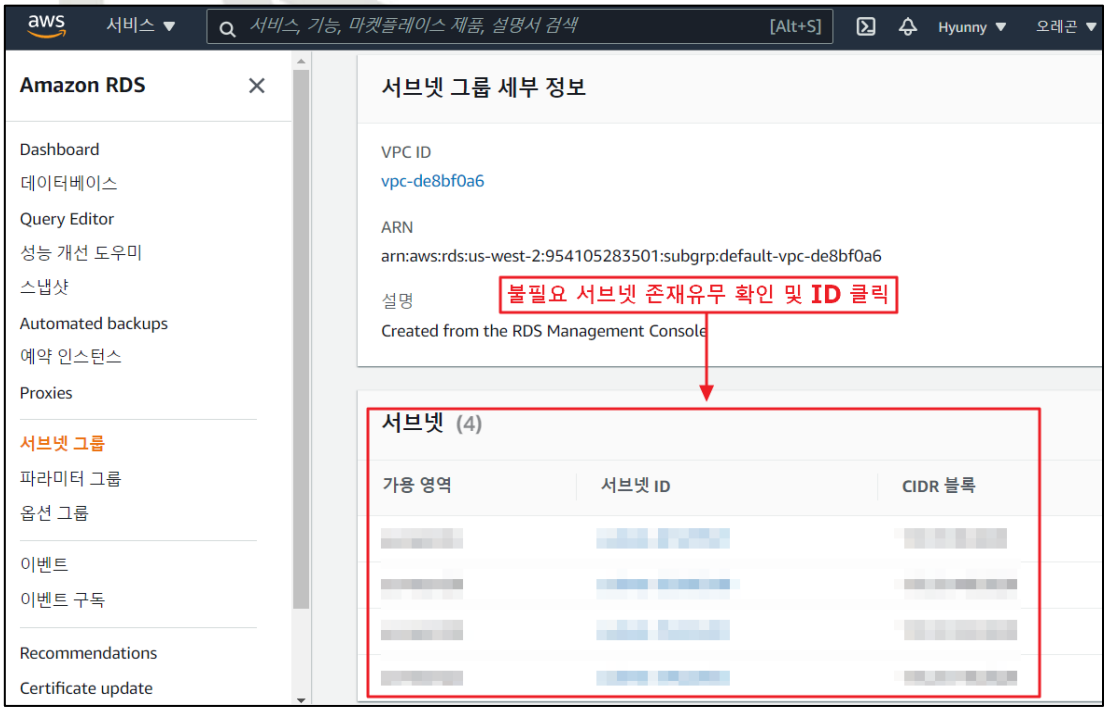
2) 권한 > ACL(액세스 제어 목록) > 편집

3) 불필요 권한 비활성화



진단 기준	**양호기준** : 퍼블릭 액세스 차단이 설정되어 있거나, 퍼블릭 액세스를 허용할 경우 ACL을 버킷 소유자에게만 설정하고 있을 경우 **취약기준** : 퍼블릭 액세스 차단이 설정되어 있지 않고, ACL이 모든 사람, 외부계정 소유자로 설정하고 있을 경우
비고	S3의 버킷/객체 ACL의 소유자 상세 권한은 "읽기", "쓰기"로 구분되어 ACL 상세설정을 확인 후 점검이 필요함

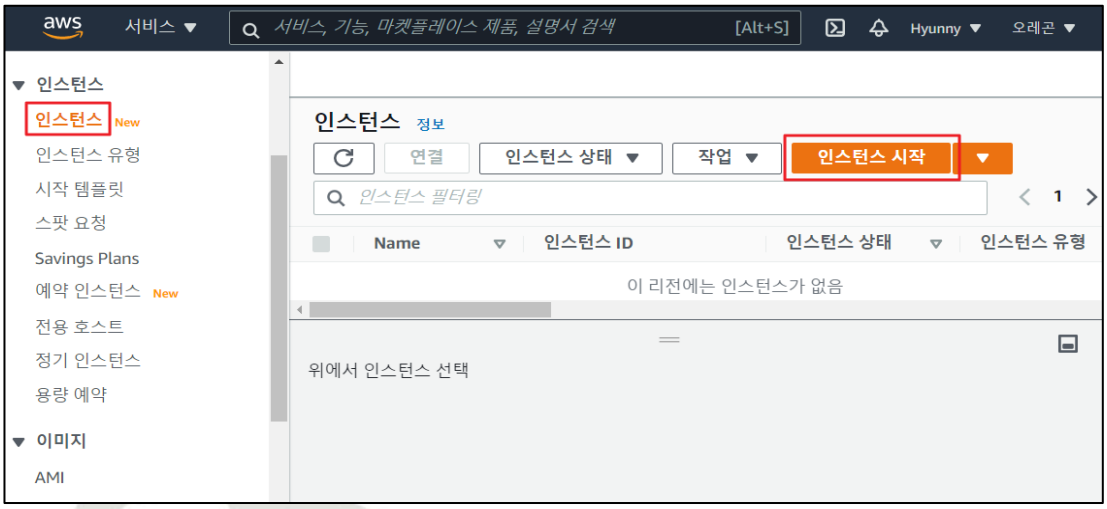
3.8 RDS 서브넷 가용 영역 관리

분류	가상 리소스 관리	중요도	중
항목명	RDS 서브넷 가용 영역 관리		
항목 설명	서브넷이란 하나의 IP 네트워크 주소를 지역적으로 나누어 이 하나의 네트워크 IP 주소가 실제로 여러 개의 서로 연결된 지역 네트워크로 사용할 수 있도록 하는 방법으로 EC2 인스턴스와 RDS 상호 통신 시 필요하나 불필요한 서브넷이 포함되어 있을 경우 보안성 위험을 발생시킬 수 있으므로 불필요한 서브넷의 유무를 관리해야 합니다.		
설정 방법	**가. 서브넷 그룹 설정 확인** 1) 서브넷 그룹 확인  2) 연결된 서브넷 확인 		

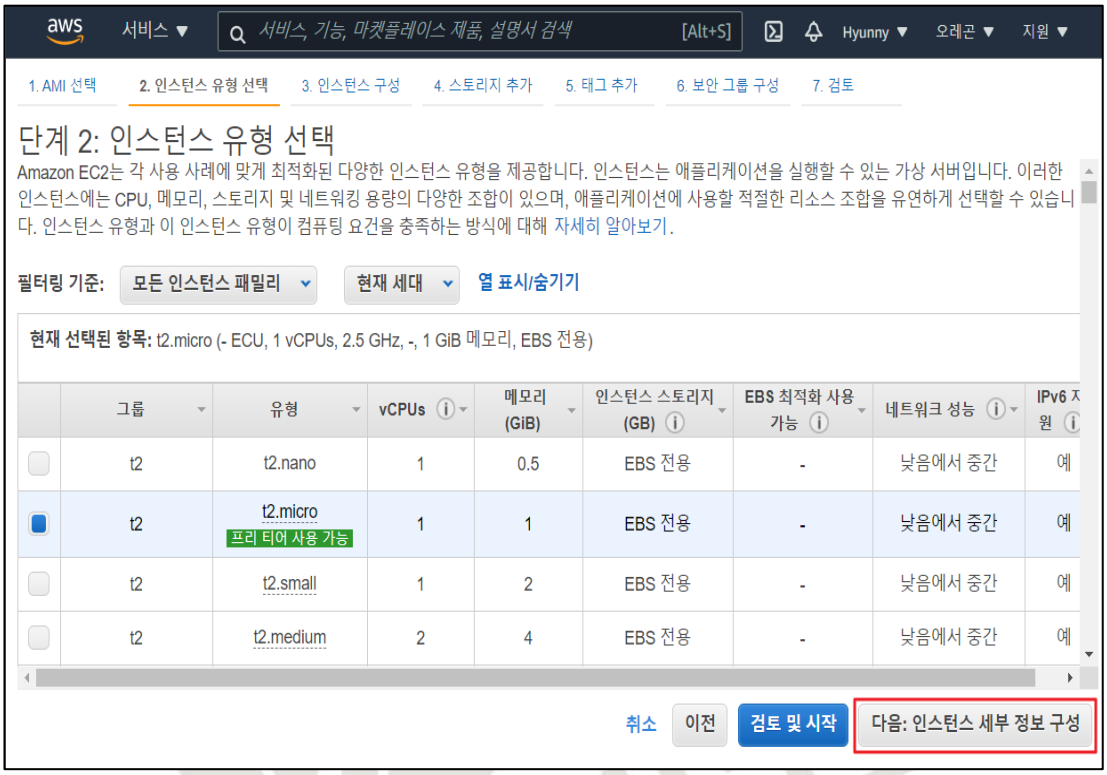
진단 기준	**양호기준** : RDS 서브넷 그룹 내 불필요한 가용영역이 존재하지 않는 경우 **취약기준** : RDS 서브넷 그룹 내 불필요한 가용영역이 존재하는 경우
비고	

4. 운영 관리

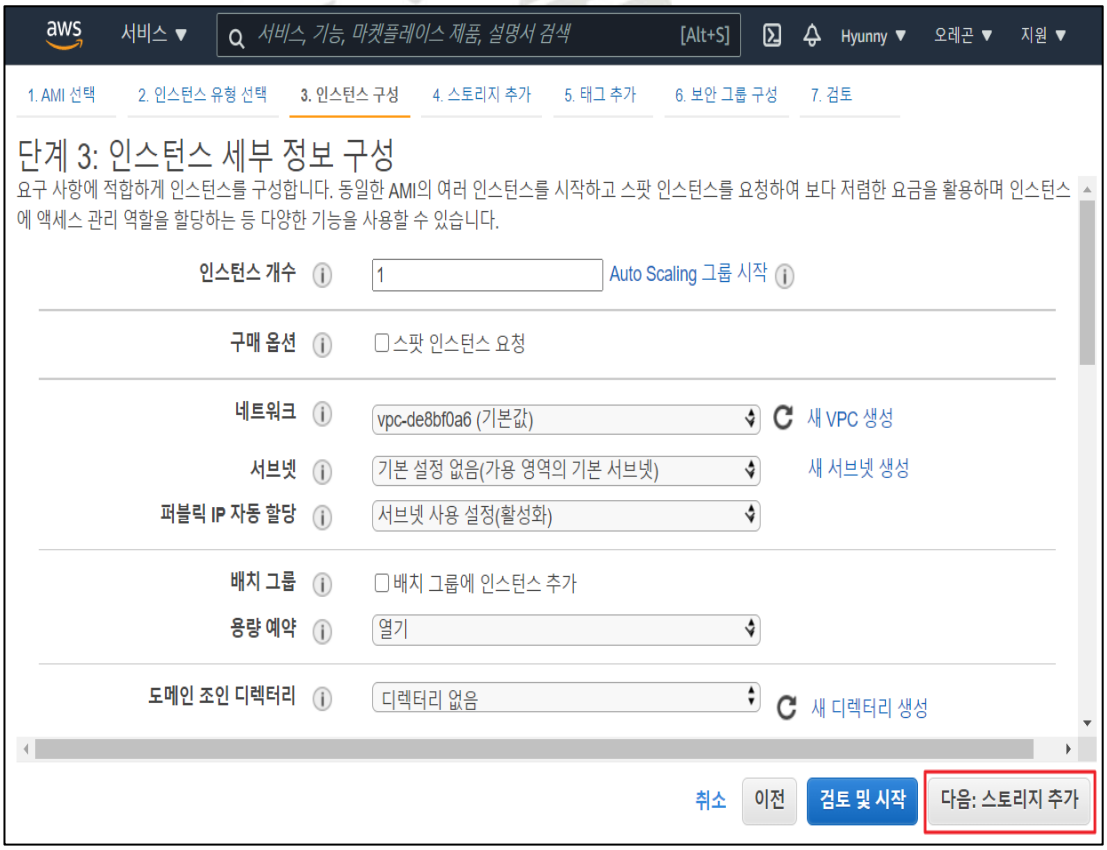
4.1 EBS 및 볼륨 암호화 설정

분류	운영 관리	중요도	중
항목명	EBS 및 볼륨 암호화 설정		
항목 설명	EBS는 EC2 인스턴스 생성 및 이용 시 사용되는 블록 형태의 스토리지 볼륨이며 파일시스템 생성 및 블록 디바이스 사용 등을 할 수 있습니다. 또한 EBS는 AES-256 알고리즘을 사용하여 볼륨 암호화를 지원하며 데이터 및 애플리케이션에 대한 다양한 정보를 안전하게 저장할 수 있게 해줍니다.		
설정 방법	**가. EC2 스토리지 암호화 설정 방법** 1) 인스턴스 시작 클릭  2) AMI 선택 		

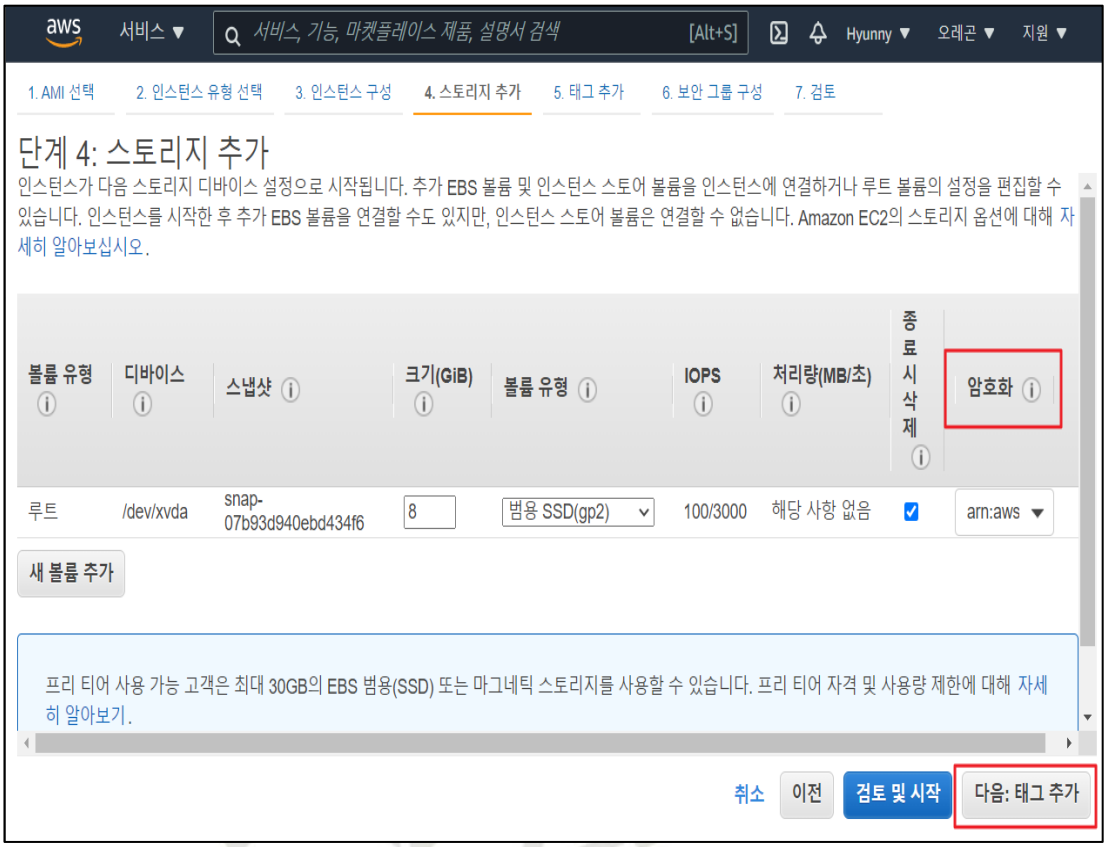
3) 인스턴스 유형 선택



4) 인스턴스 구성



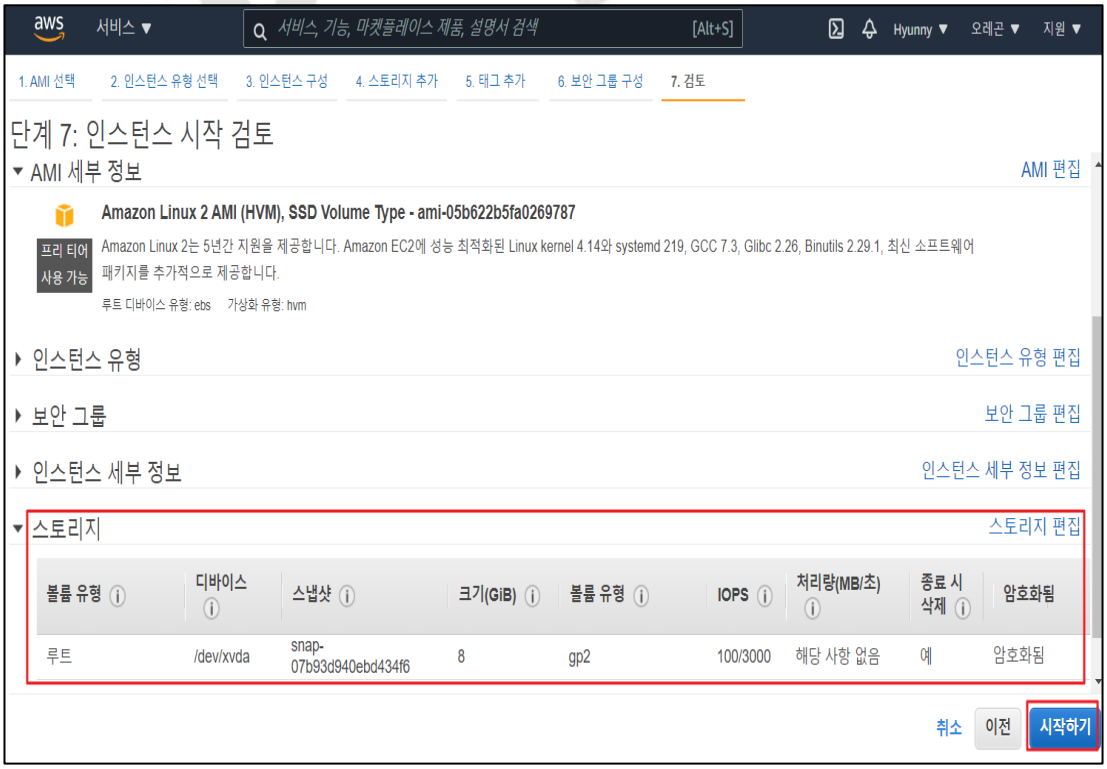
5) 스토리지 추가



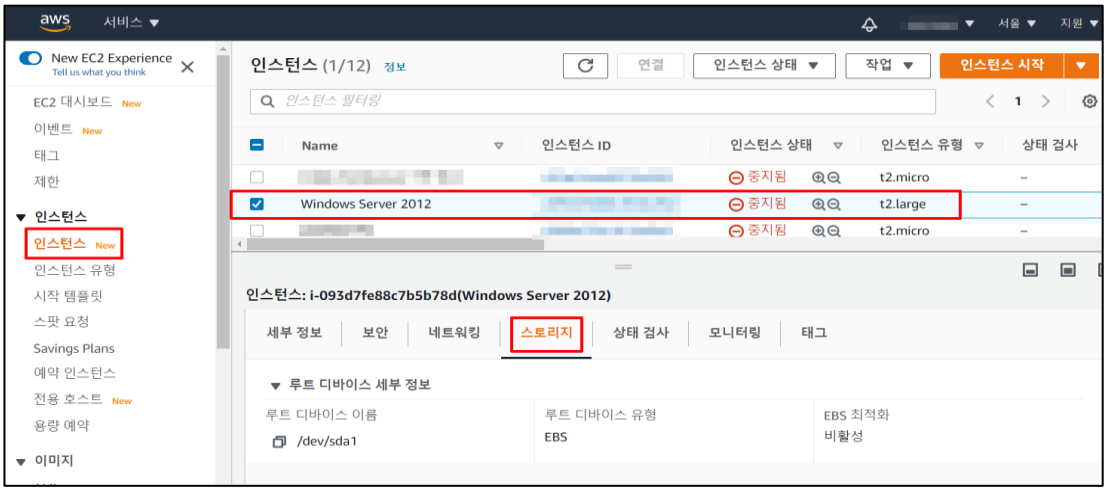
6) 태그 추가

7) 보안 그룹 구성

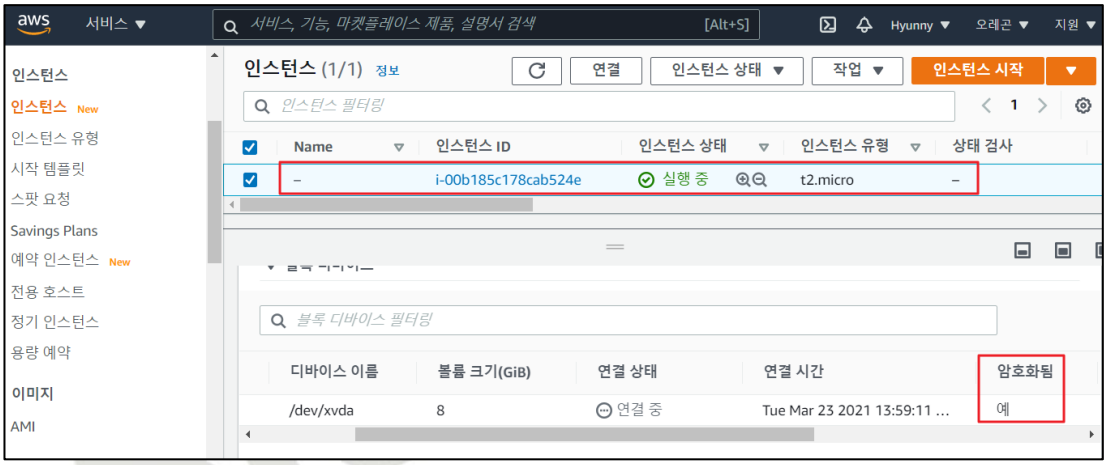
8) 스토리지 암호화 여부 확인



9) EC2 인스턴스 클릭 및 스토리지 클릭

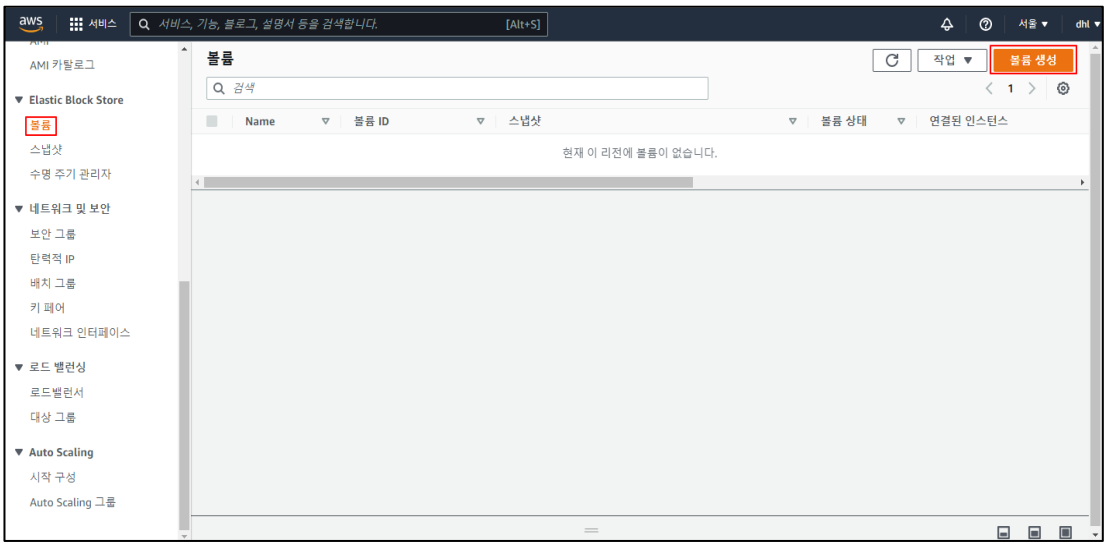


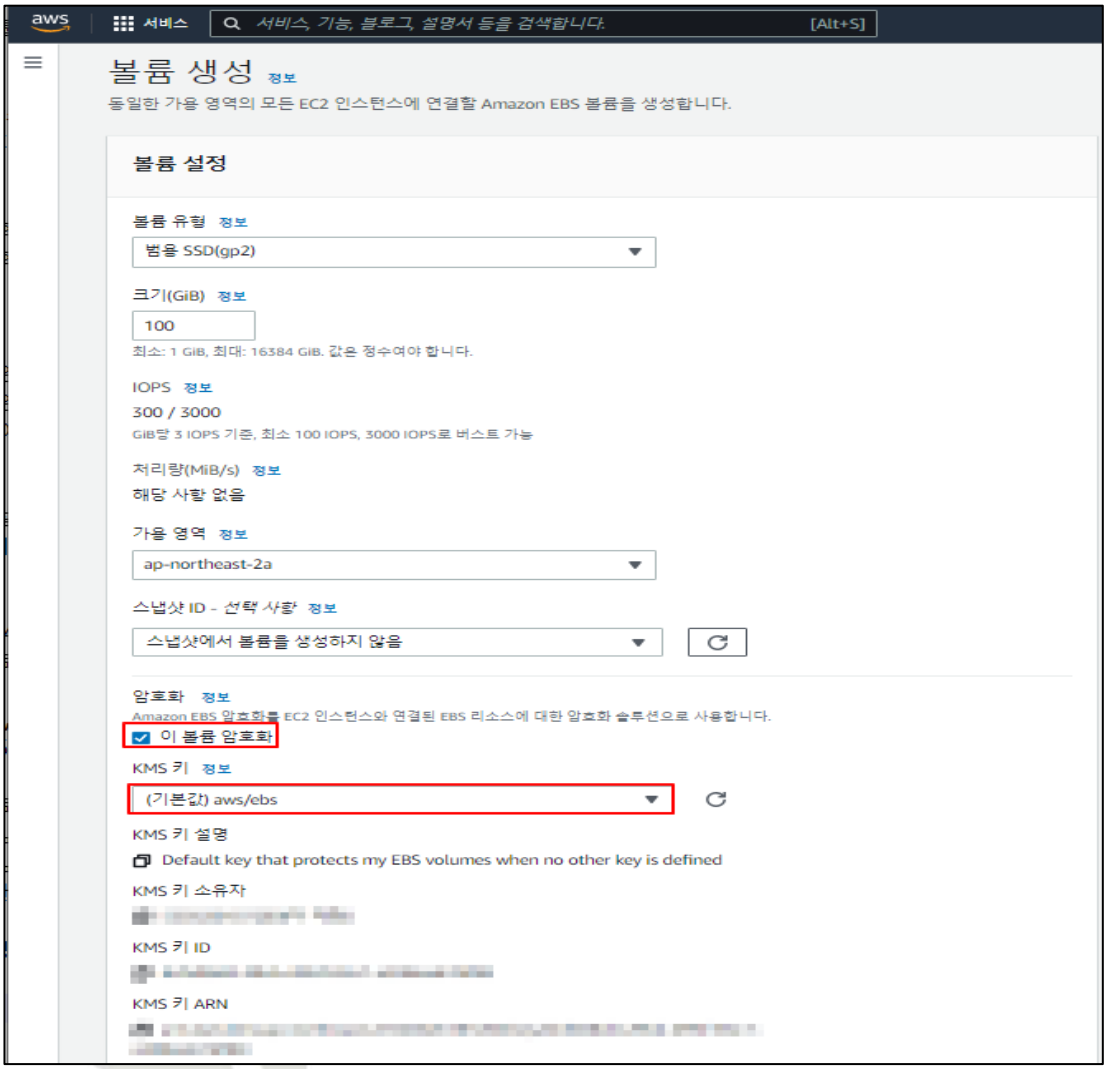
10) 스토리지 암호화 설정여부 확인



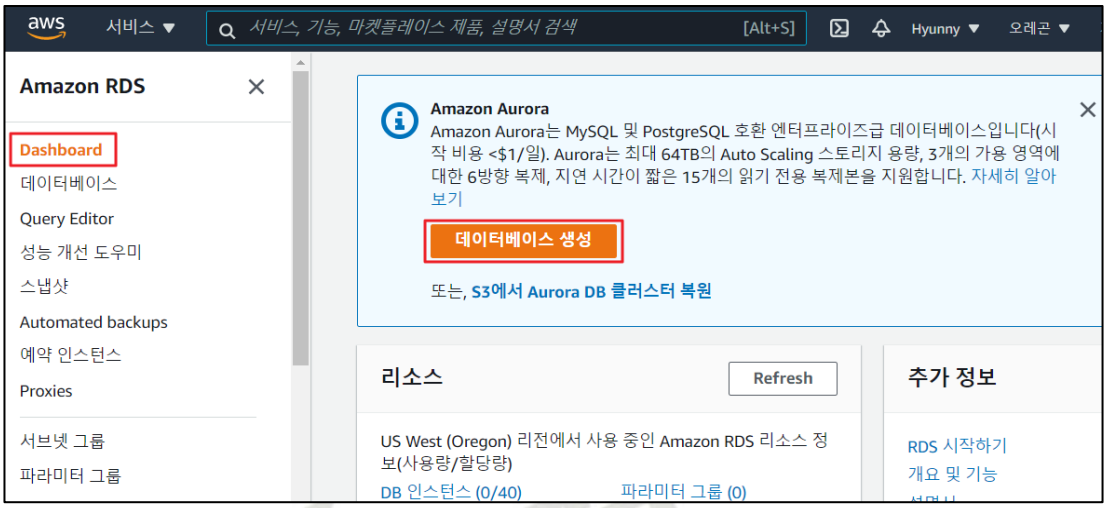
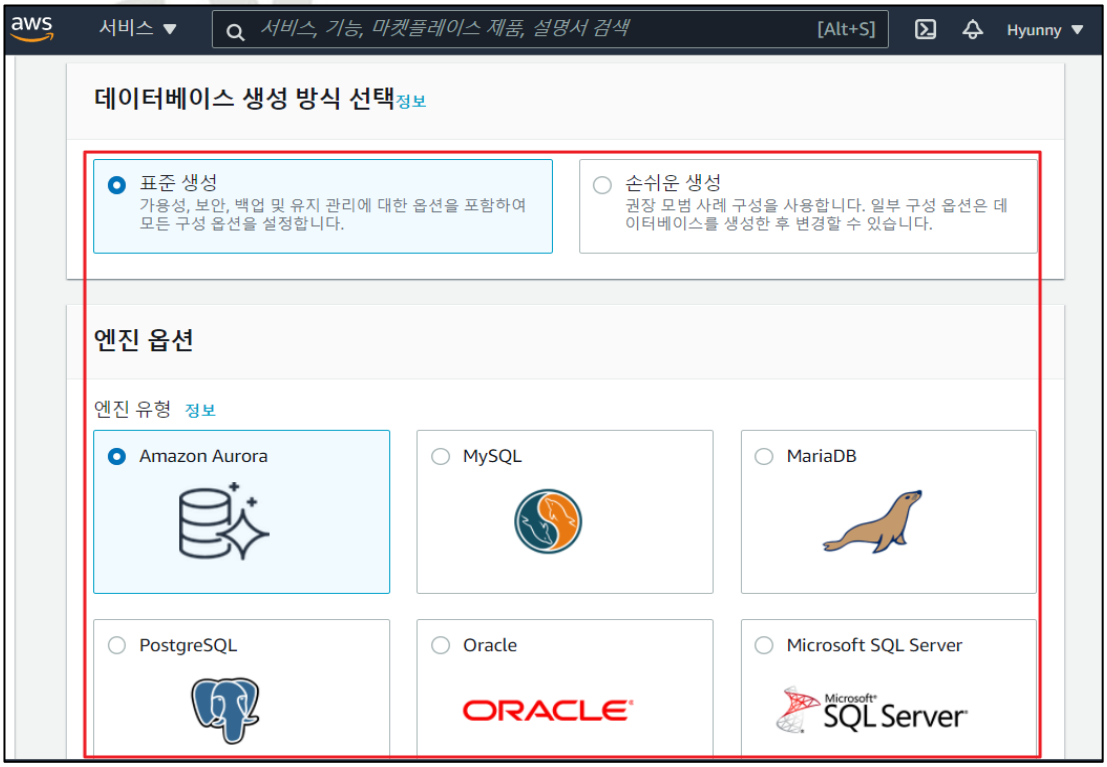
나. EBS 볼륨 암호화 설정 방법

1) Elastic Block Store 메뉴 내 볼륨 기능 선택

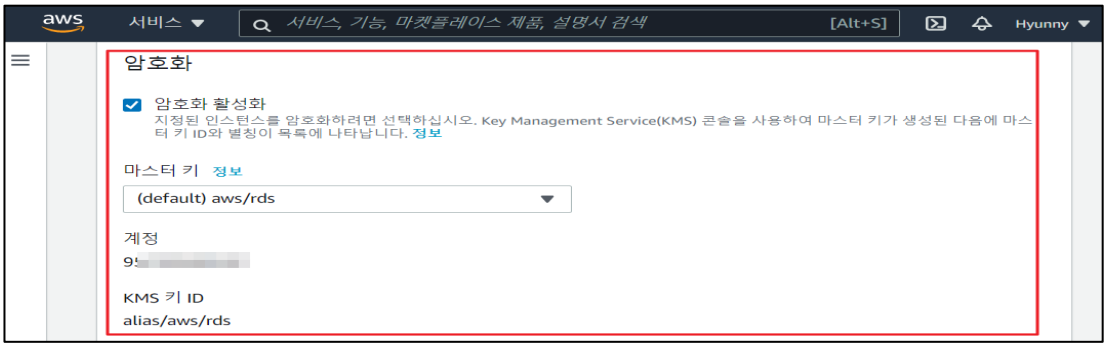


	2) 볼륨 생성 메뉴 내 "암호화" 활성화 후 KMS 키 값을 추가하여 설정해야 함 
진단 기준	**양호기준** : EBS 및 볼륨 리소스에 암호화가 활성화되어 있을 경우 **취약기준** : EBS 및 볼륨 리소스에 암호화가 비활성화되어 있을 경우
비고	

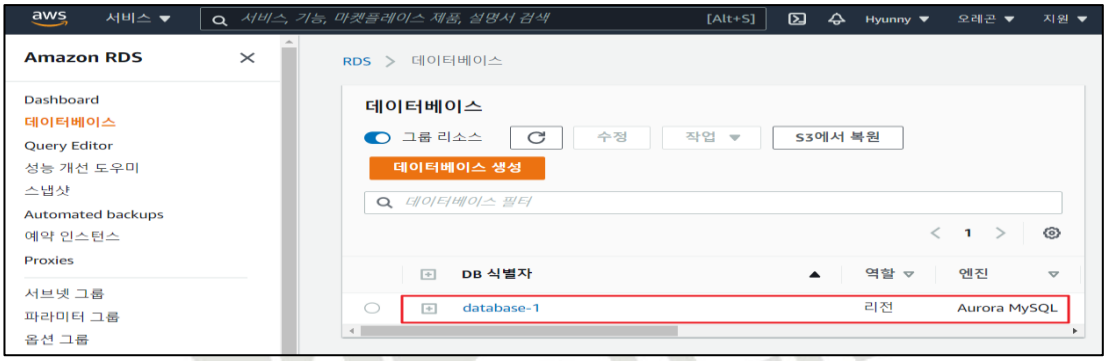
4.2 RDS 암호화 설정

분류	운영 관리	중요도	중
항목명	RDS 암호화 설정		
항목 설명	RDS는 데이터 보호를 위해 DB 인스턴스에서 암호화 옵션 기능을 제공하며 암호화 시 AES-256 암호화 알고리즘을 이용하여 DB 인스턴스의 모든 로그, 백업 및 스냅샷 암호화가 가능합니다.		
설정 방법	**가. RDS 데이터베이스 암호화 설정 확인** 1) 데이터베이스 클릭  2) DB 생성 방식 및 엔진 등 설정 		

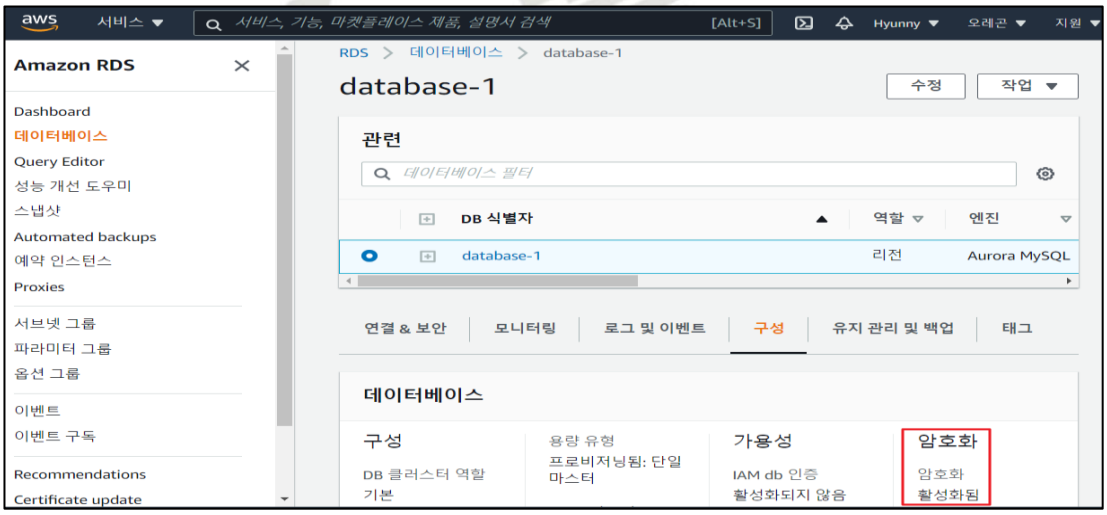
3) 데이터베이스 암호화 설정



4) 데이터베이스 생성 확인



5) 데이터베이스 암호화 확인



진단 기준

양호기준

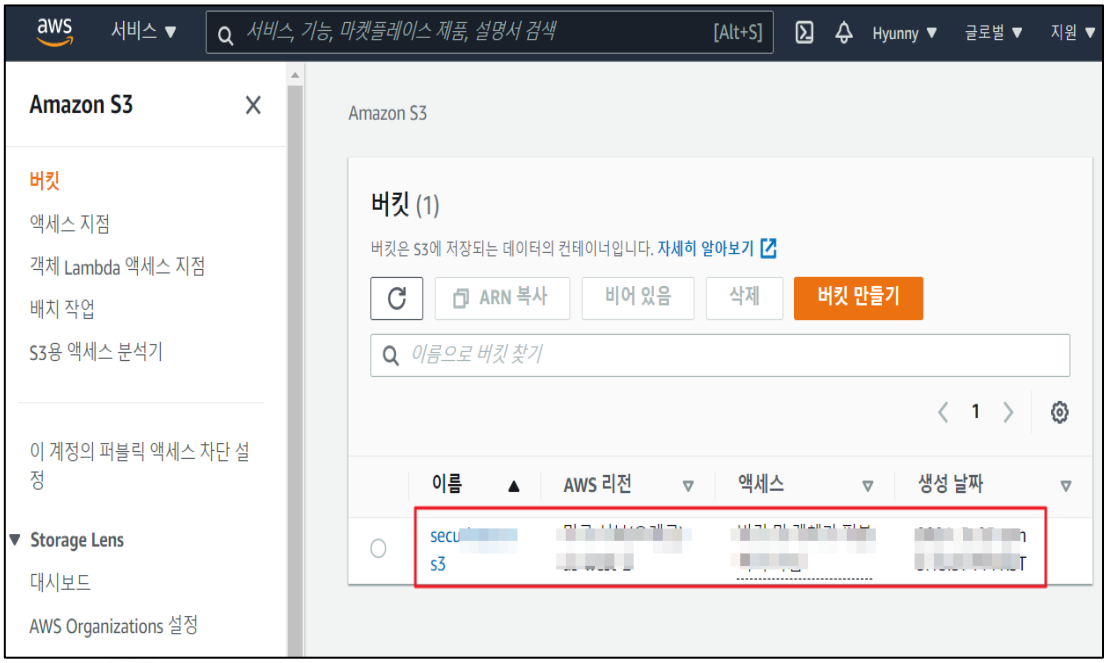
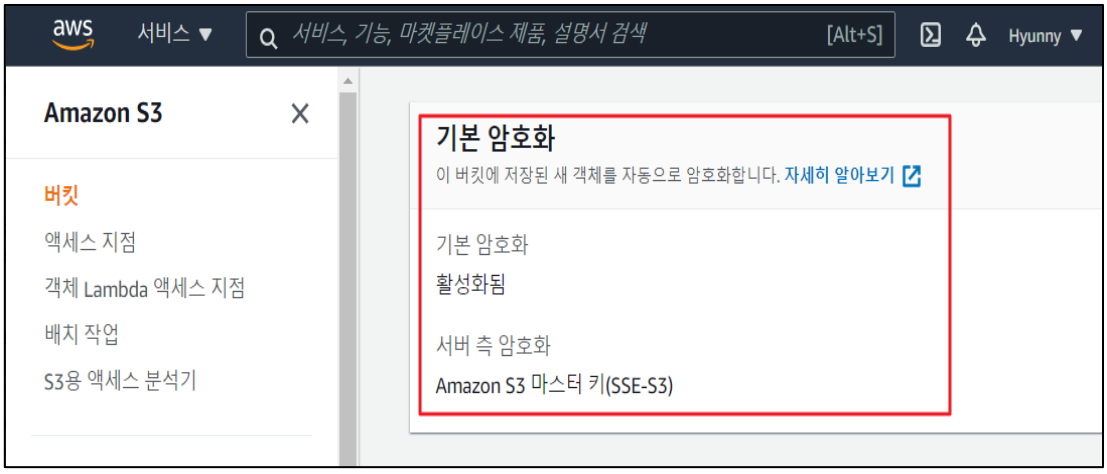
: RDS 데이터베이스 암호화가 활성화되어 있을 경우

취약기준

: RDS 데이터베이스 암호화가 비활성화되어 있을 경우

비고

4.3 S3 암호화 설정

분류	운영 관리	중요도	중
항목명	S3 암호화 설정		
항목 설명	버킷 기본 암호화 설정은 S3 버킷에 저장되는 모든 객체를 암호화 되도록 하는 설정이며 Amazon S3 관리형 키(SSE-S3) 또는 AWS KMS 관리형 키(SSE-KMS)로 서버 측 암호화를 사용하여 객체를 암호화합니다. **※ S3 버킷 신규 생성 시 기본 암호화 (SSE-S3, SSE-KMS)를 설정할 수 있으며, 버킷에 기본 암호화가 적용된 상태에서 객체가 저장될 경우 하위 객체까지 자동으로 암호화 설정이 가능함**		
설정 방법	**가. S3 버킷 기본 암호화 설정 확인** 1) S3 버킷 선택  2) S3 버킷 속성 확인 		

진단 기준	**양호기준** : Amazon S3 키(SSE-S3)로 서버 측 암호화 사용 또는 SSE-KMS로 서버 측 암호화가 설정되어 있을 경우 **취약기준** : Amazon S3 키(SSE-S3)로 서버 측 암호화 사용 또는 SSE-KMS 로 서버 측 암호화가 설정되어 있지 않을 경우
비고	

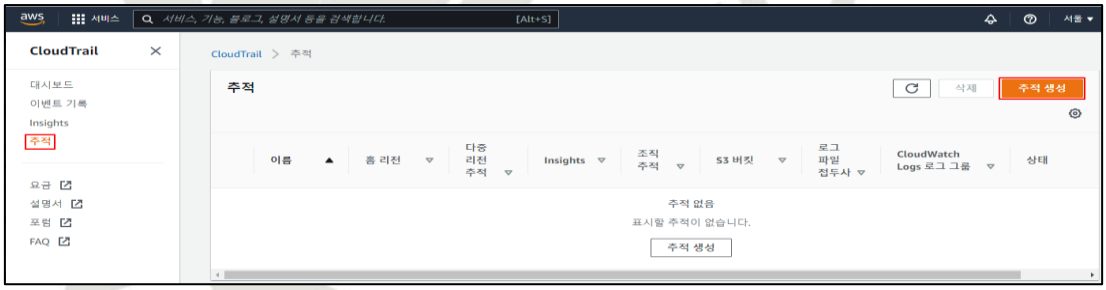
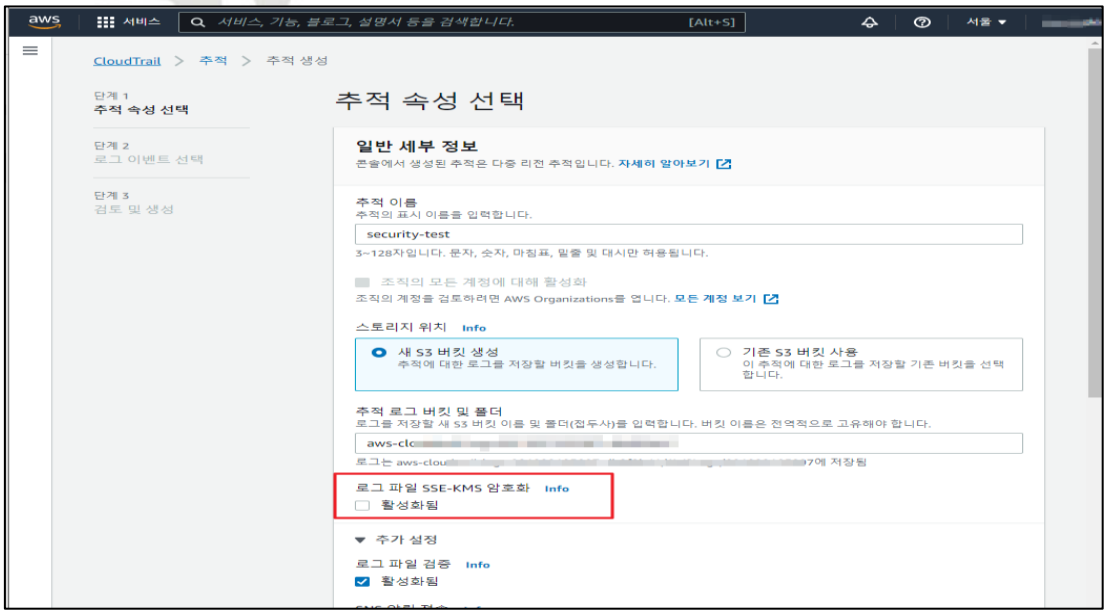
4.4 통신구간 암호화 설정

<table>
<tr><td>분류</td><td>운영 관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">통신구간 암호화 설정</td></tr>
<tr><td>항목
설명</td><td colspan="3">클라우드 리소스를 통해 대/내외 서비스에서 정보를 송, 수신 하는 경우 중간에서 공격자가 패킷을 가로채어 공격에 활용할 수 없도록 통신구간을 암호화하여 설정하여야 합니다.</td></tr>
<tr><td>설정
방법</td><td colspan="3">
가. 중요정보 전송 시 암호화 정책 수립
1) 중요정보 전송 시 이동구간 암호화
- 암호화된 통신 채널 사용
- 서버 원격 접근 시 암호화된 통신수단(VPN, SSH등)을 사용
- 공공기관 데이터이관 시 VPN을 통해 이관
- 기타 관리를 위한 접근 시 OpenSSH 및 OpenSSL(TLS V1.2) 사용

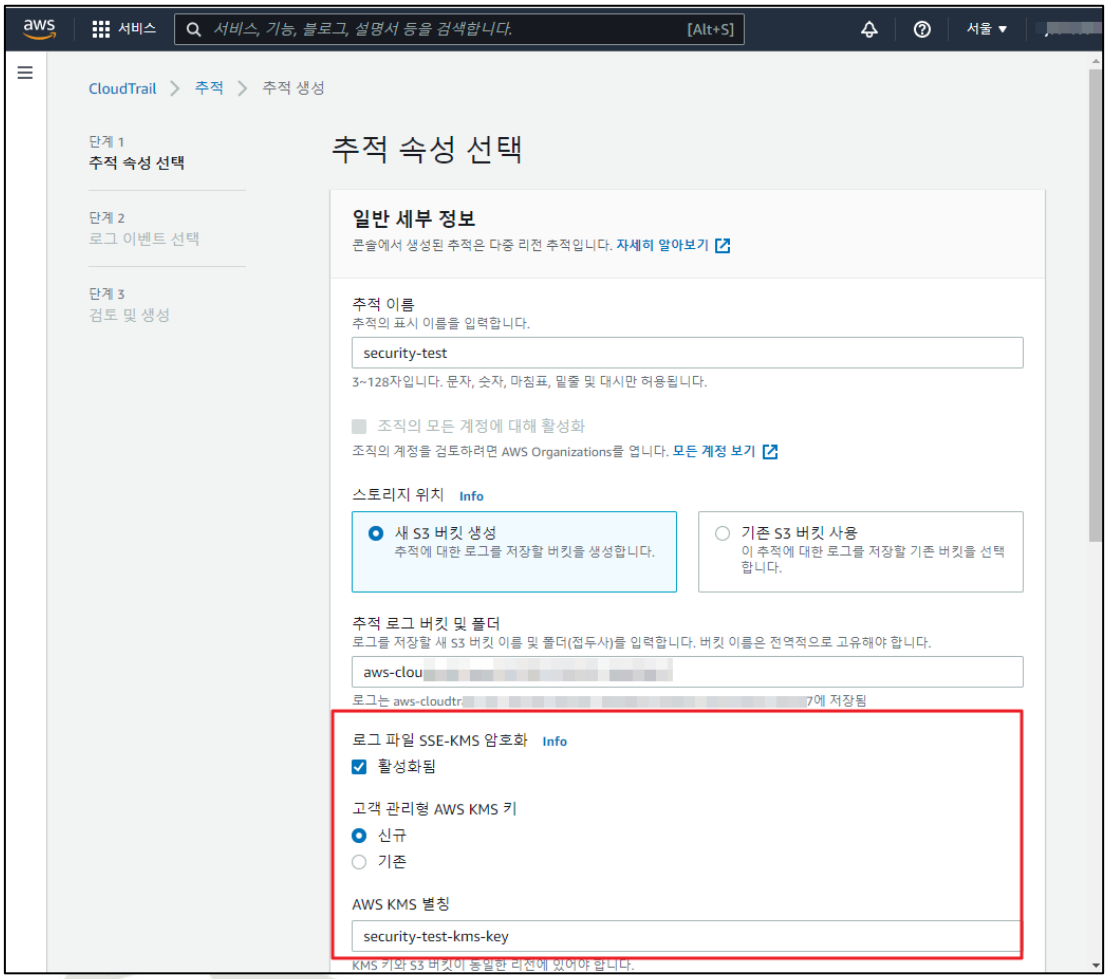
(*) 중요 정보 전송 및 저장 시 암호화 방안 예시
<table>
<tr><th>구분</th><th>암호화 방안</th></tr>
<tr><td>서버와 클라이언트 간 전송</td><td>SSL 방식
응용프로그램</td></tr>
<tr><td>개인정보처리시스템 간 전송</td><td>IPSec 방식, SSL 방식, SSH 방식</td></tr>
<tr><td>개인정보처리시스템 암호화 방식</td><td>응용프로그램 자체 암호화
DB 서버 암호화
DBMS 자체 암호화
DBMS 암호화 기능 호출
운영체제 암호화</td></tr>
<tr><td>업무용 컴퓨터
보조저장매체 암호화 방식</td><td>문서 도구 자체 암호화
암호 유틸리티 이용 암호화
DRM
디스크 암호화</td></tr>
</table>
※ 클라우드서비스 보안인증제도(IaaS) 평가기준 해설서의 “11.1.4 네트워크 암호화 및 12.3.1 암호 정책 수립“ 항목 참고
</td></tr>
<tr><td>진단
기준</td><td colspan="3">
양호기준
: 클라우드 리소스 통신 구간 내 암호화 설정이 되어 있는 경우

취약기준
: 클라우드 리소스 통신 구간 내 암호화 설정이 되어 있지 않는 경우
</td></tr>
<tr><td>비고</td><td colspan="3"></td></tr>
</table>

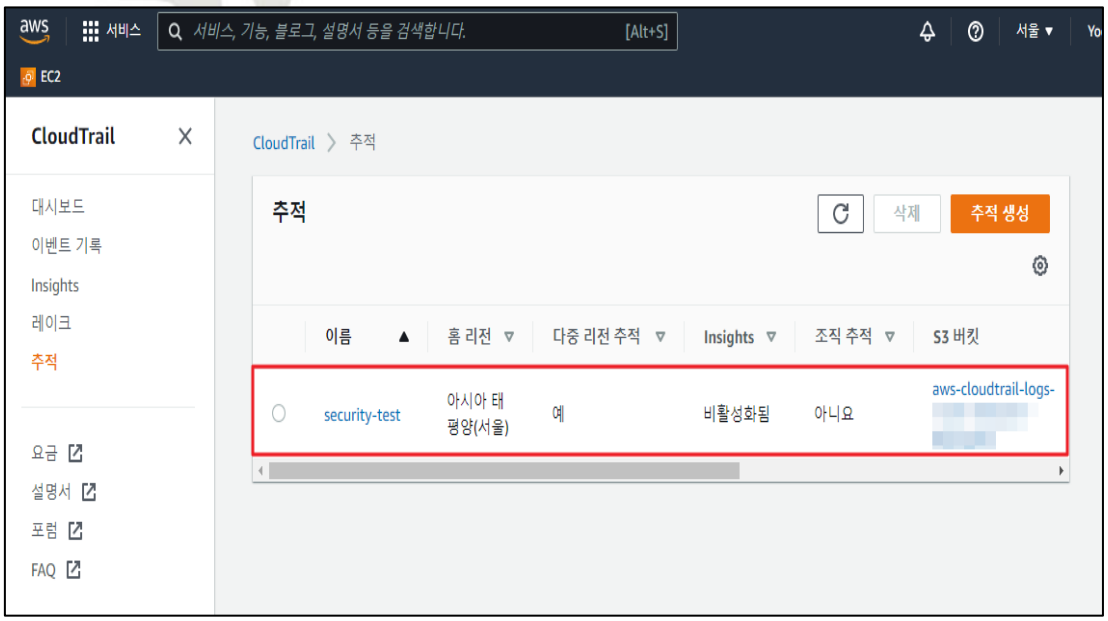
4.5 CloudTrail 암호화 설정

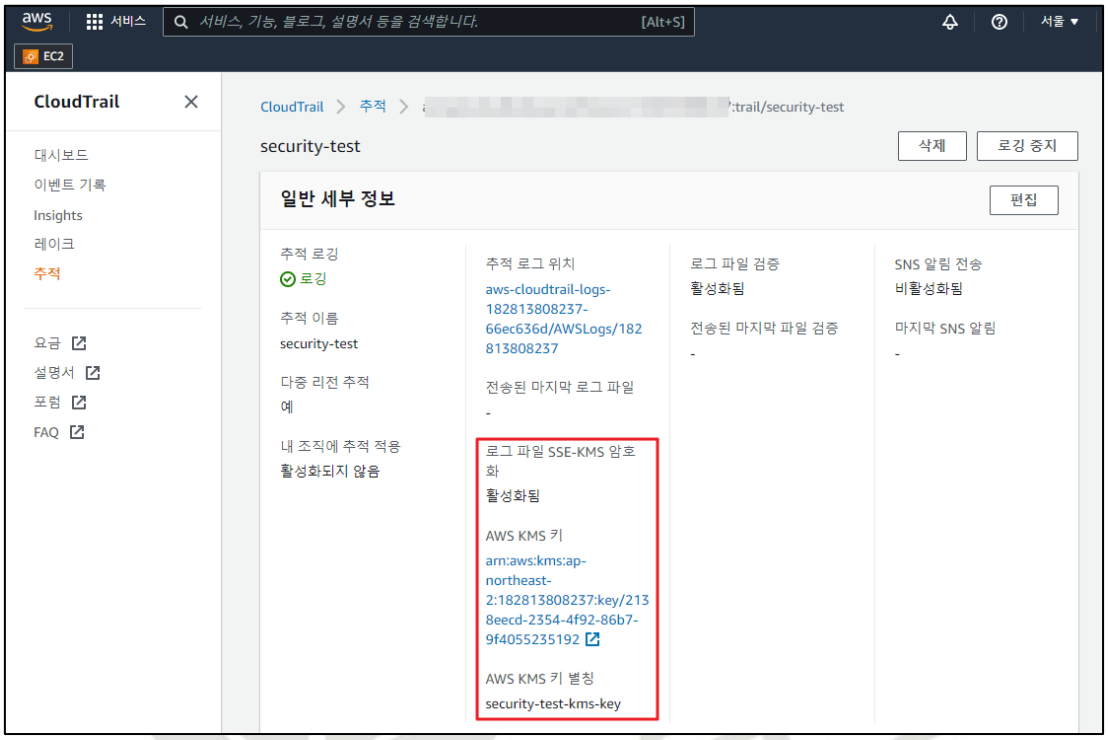
분류	운영 관리	중요도	중
항목명	CloudTrail 암호화 설정		
항목 설명	CloudTrail 이 버킷에 제공하는 로그 파일은 Amazon S3 가 관리하는 암호화 키(SSE-S3)를 사용하는 서버 측 암호화를 사용하여 암호화됩니다. 직접 관리할 수 있는 보안 계층을 제공하려면 CloudTrail 로그 파일에 대한 AWS KMS 관리형 키(SSE-KMS)를 사용하는 서버 측 암호화를 대신 사용하면 됩니다. **(*) 암호화 대상 기준** - 개인정보, 고유식별정보, 비밀번호, 생체인식정보, 금융 거래 정보 등 **※ ISMS-P 인증기준 안내서 내 "2.7 암호화 적용" 세부 설명 참고 바랍니다.** **※ 사내 정책 따른 중요/주요 정보에 대한 암호화 기준이 별도 존재하는 경우 해당 정보에 대해서도 암호화를 적용해 시스템을 운용해야 합니다.**		
설정 방법	**가. CloudTrail 추적 생성 방법** 1) CloudTrail 추적 생성  2) CloudTrail 추적 속성 비활성화 상태  		

3) CloudTrail 추적 속성 활성화 후 "고객 관리형 AWS KMS 키" 추가 설정

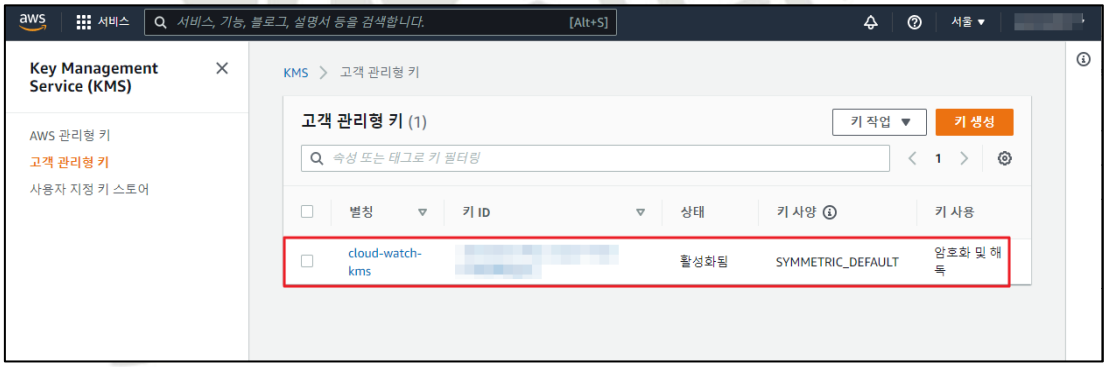
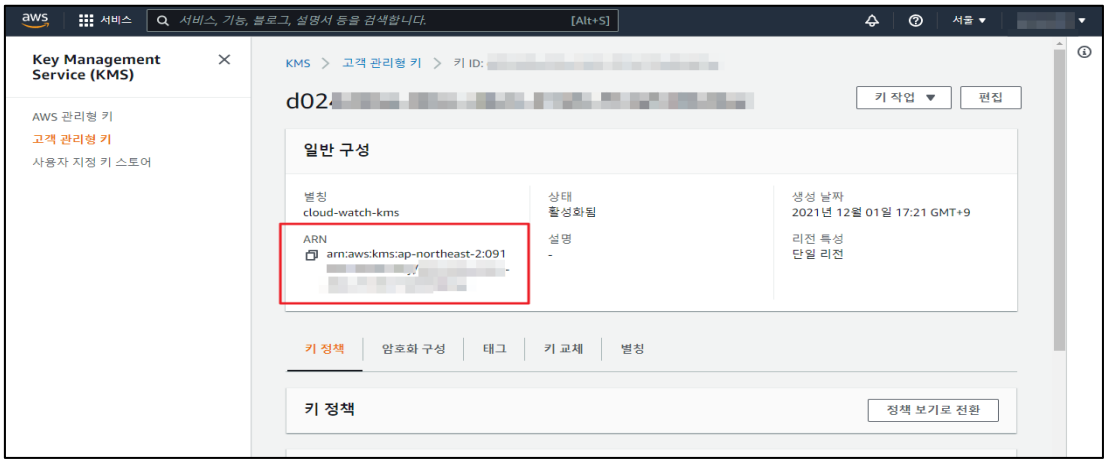


4) CloudTrail 추적 생성 완료



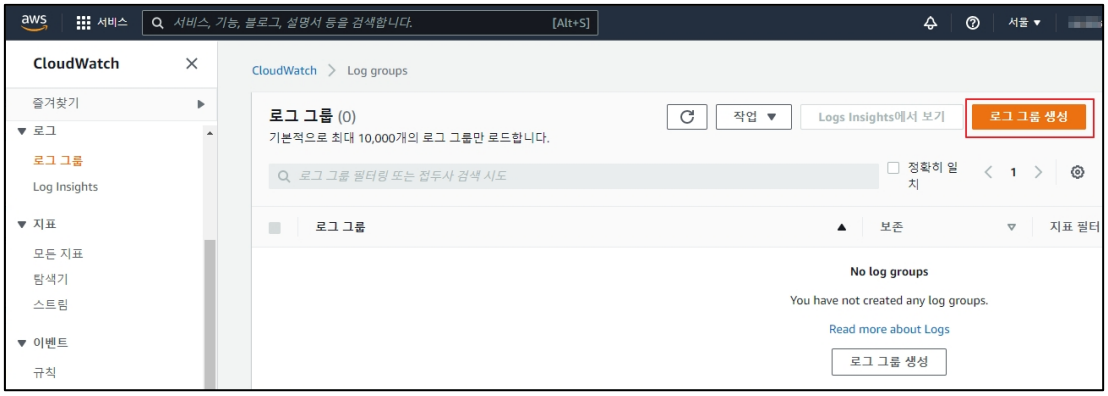
	5) CloudTrail 암호화 설정 확인 
진단 기준	**양호기준** : CloudTrail 관련 로그 파일에 SSE-KMS 암호화 설정이 되어있을 경우 **취약기준** : CloudTrail 관련 로그 파일에 SSE-KMS 암호화 설정이 되어있지 않을 경우
비고	

4.6 CloudWatch 암호화 설정

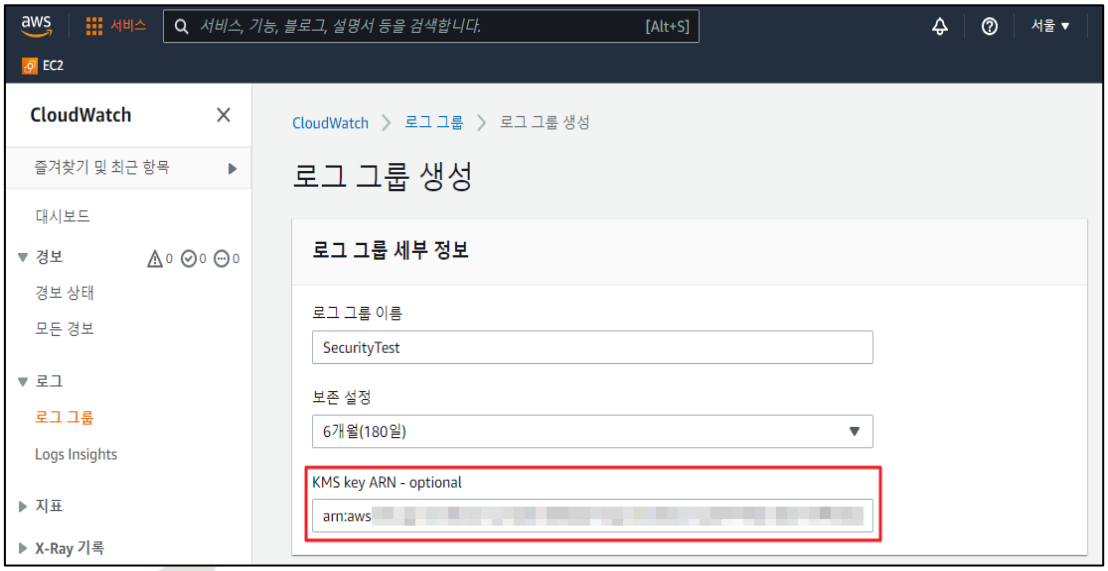
분류	운영 관리	중요도	중
항목명	CloudWatch 암호화 설정		
항목 설명	Amazon CloudWatch 는 Key Management Service(KMS)와 사용자 지정 마스터 키(CMK)를 통해 관리되는 키를 사용하여 로그를 암호화할 수 있습니다. 로그 그룹을 생성할 때나 로그 그룹이 존재하는 경우에는 CMK 를 로그 그룹에 연결하면 로그 그룹 수준에서 암호화가 활성화됩니다. CMK 를 로그 그룹에 연결하고 나면 로그 데이터에서 새로 수집된 모든 데이터를 CMK 를 사용해 암호화할 수 있습니다. 이 데이터는 보존 기간 전반에 걸쳐 암호화된 형식으로 저장됩니다. **(*) 암호화 대상 기준** - 개인정보, 고유식별정보, 비밀번호, 생체인식정보, 금융 거래 정보 등 **※ ISMS-P 인증기준 안내서 내 "2.7 암호화 적용" 세부 설명 참고 바랍니다.** **※ 사내 정책 따른 중요/주요 정보에 대한 암호화 기준이 별도 존재하는 경우 해당 정보에 대해서도 암호화를 적용해 시스템을 운용해야 합니다.**		
설정 방법	**가. KMS Key ARN 확인 방법** 1) 서비스 > KMS > 고객 관리형 키 접근  2) 고객 관리형 키 > ARN 값 확인 		

나. CloudWatch 로그 그룹 생성 및 KMS key ARN 설정 방법

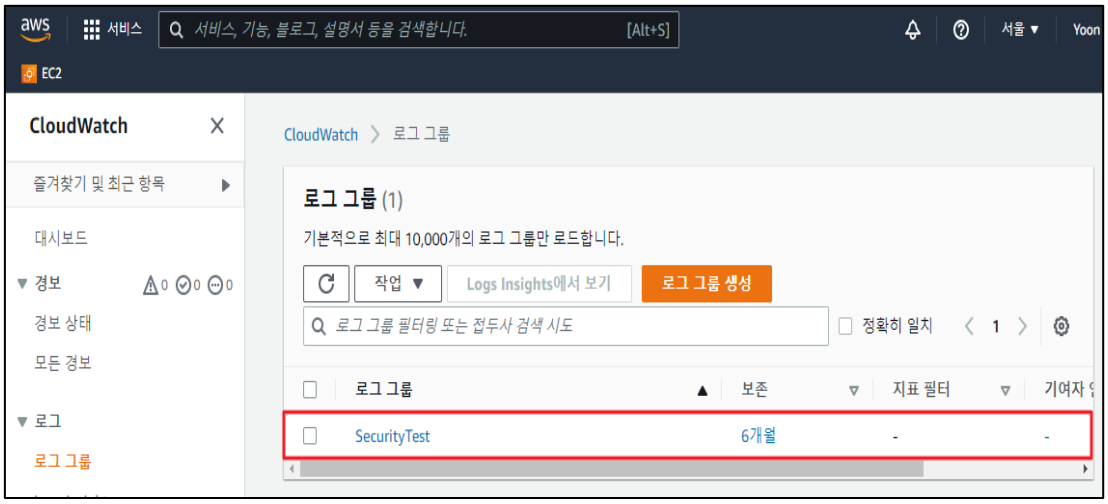
1) 서비스 > CloudWatch 로그 그룹 생성



2) 로그 그룹 생성 시 사전 확인된 KMS key ARN 값 설정 필요

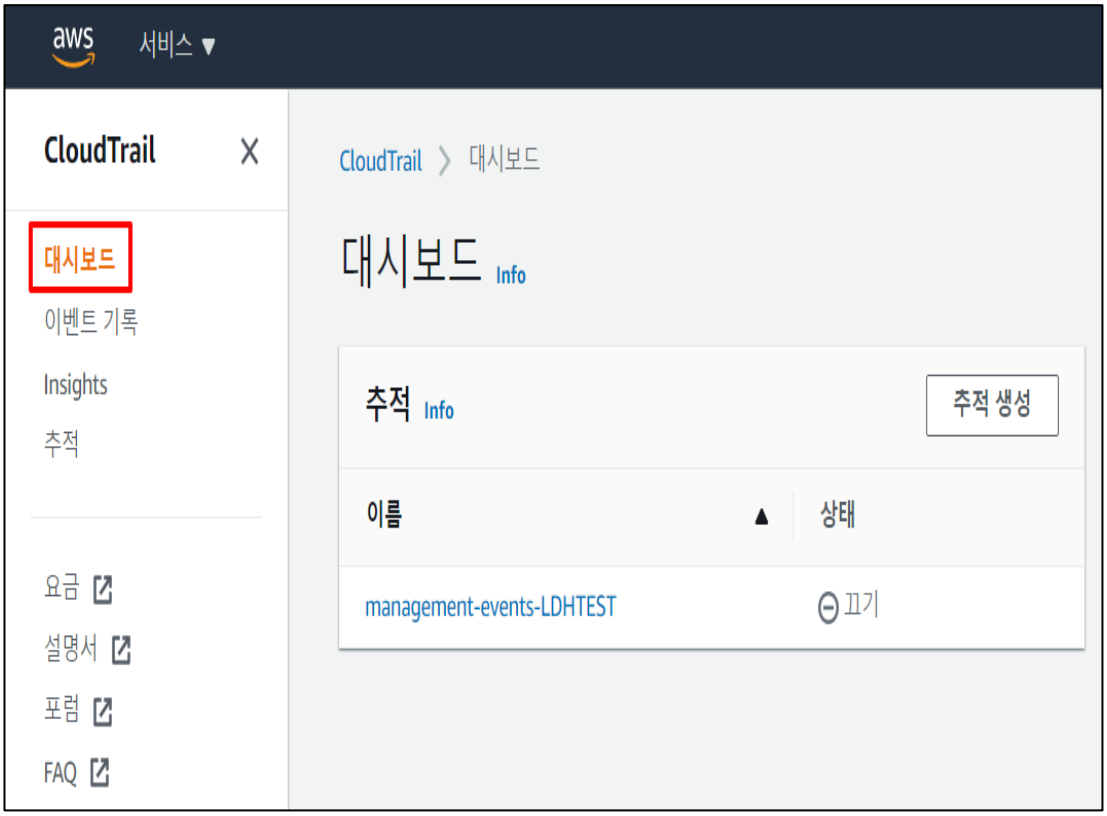
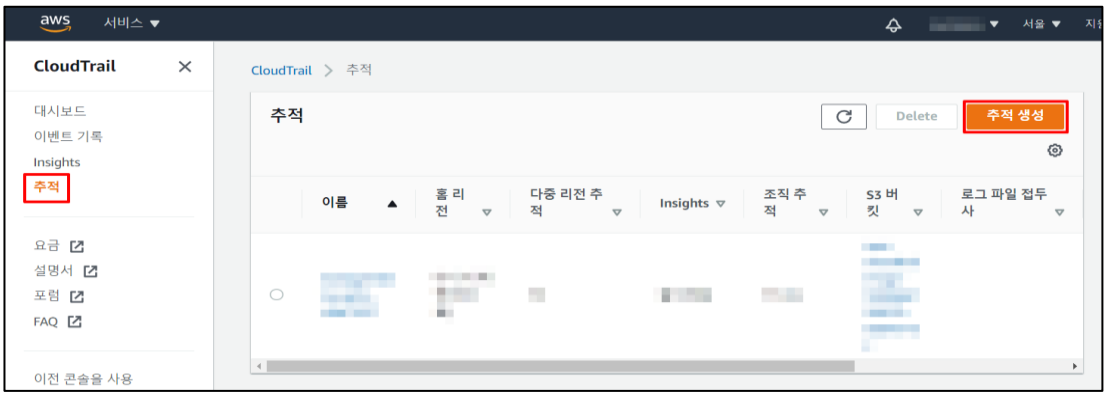


3) 로그 그룹 생성 완료

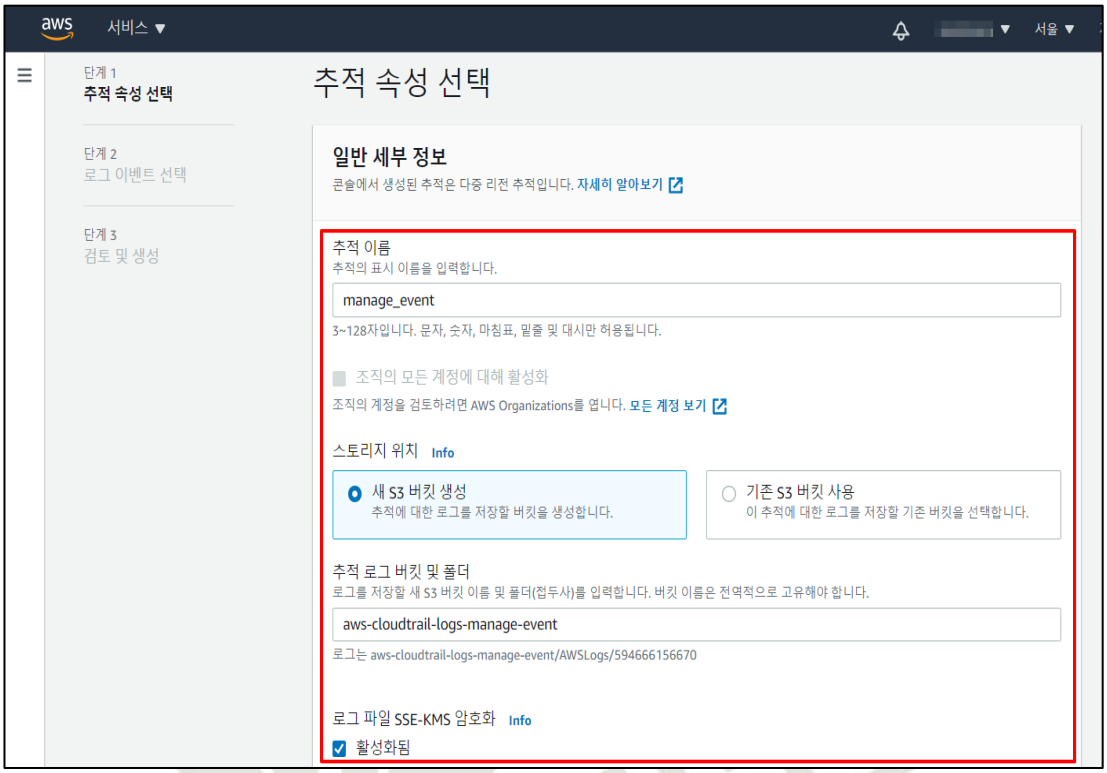


진단 기준	**양호기준** : 로그 그룹 생성 시 "KMS key ARN" 을 설정하여 사용하고 있는 경우 **취약기준** : 로그 그룹 생성 시 "KMS key ARN" 을 설정하여 사용하고 있지 않는 경우
비고	

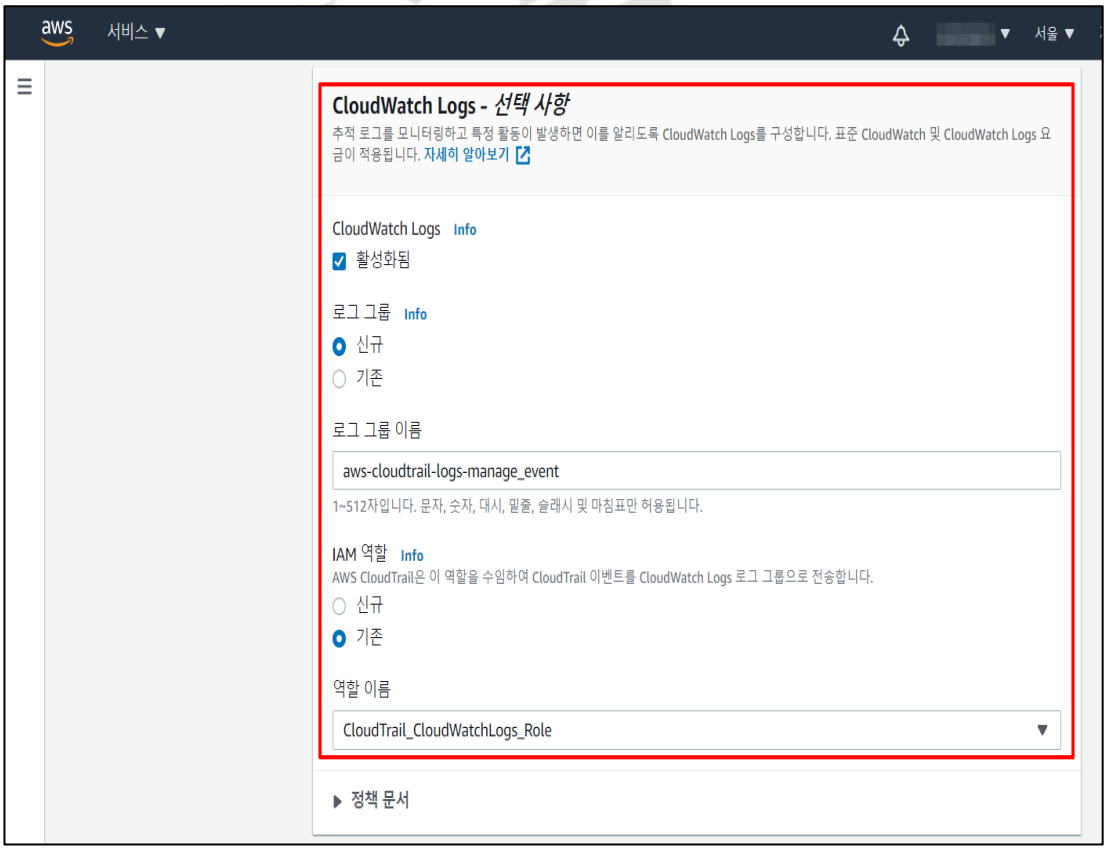
4.7 AWS 사용자 계정 로깅 설정

분류	운영 관리	중요도	상
항목명	AWS 사용자 계정 로깅 설정		
항목 설명	AWS CloudTrail 은 계정의 거버넌스, 규정 준수, 운영 및 위험 감사를 활성화하도록 도와주는 서비스로서 사용자, 역할 또는 AWS 서비스가 수행하는 작업들의 이벤트가 기록됩니다. 또한 CloudTrail 은 생성 시 AWS 계정에서 활성화됩니다. 활동이 AWS 계정에서 이루어지면 해당 활동이 CloudTrail 이벤트에 기록됩니다.		
설정 방법	**가. CloudTrail 및 CloudWatch 관리 이벤트 설정 방법** 1) CloudTrail 대시보드 진입 및 관리 이벤트 추적 확인  2) CloudTrail 추적 생성 버튼 클릭 		

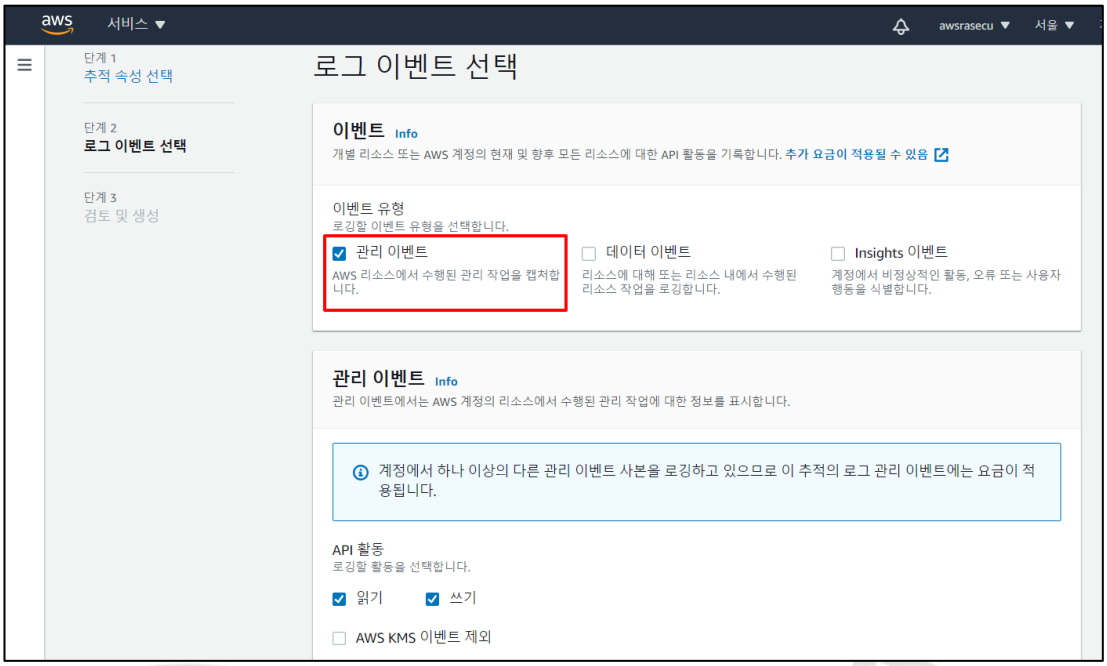
3) CloudTrail 추적 속성 설정



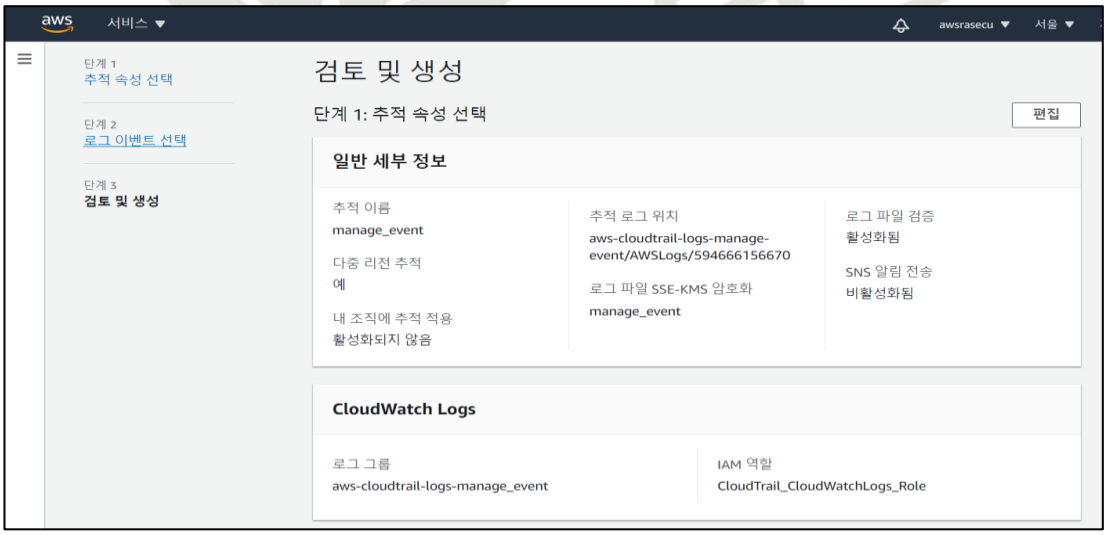
4) CloudTrail CloudWatch Logs 설정



5) 로그 이벤트 선택 – 관리 이벤트

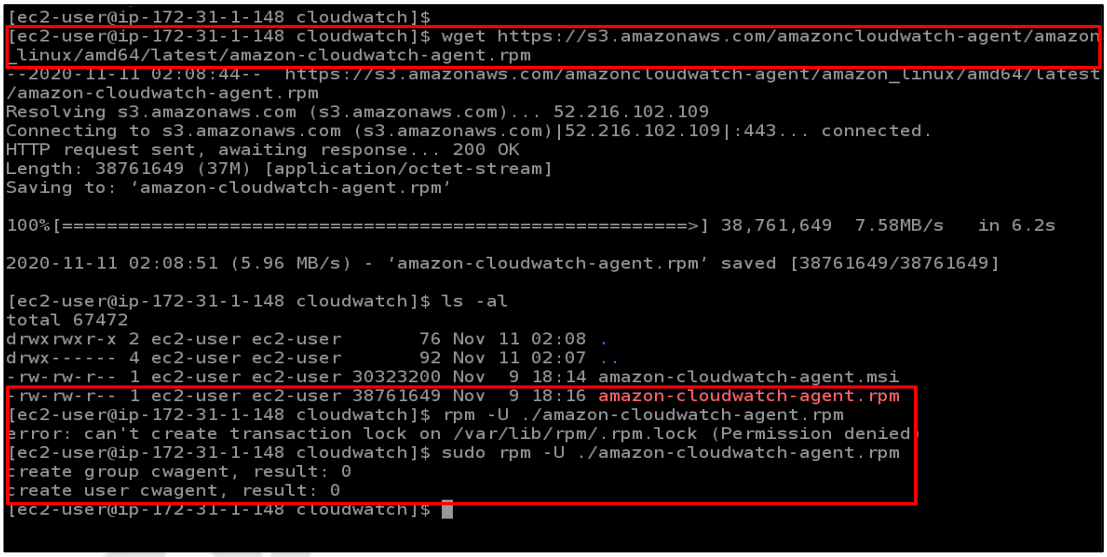
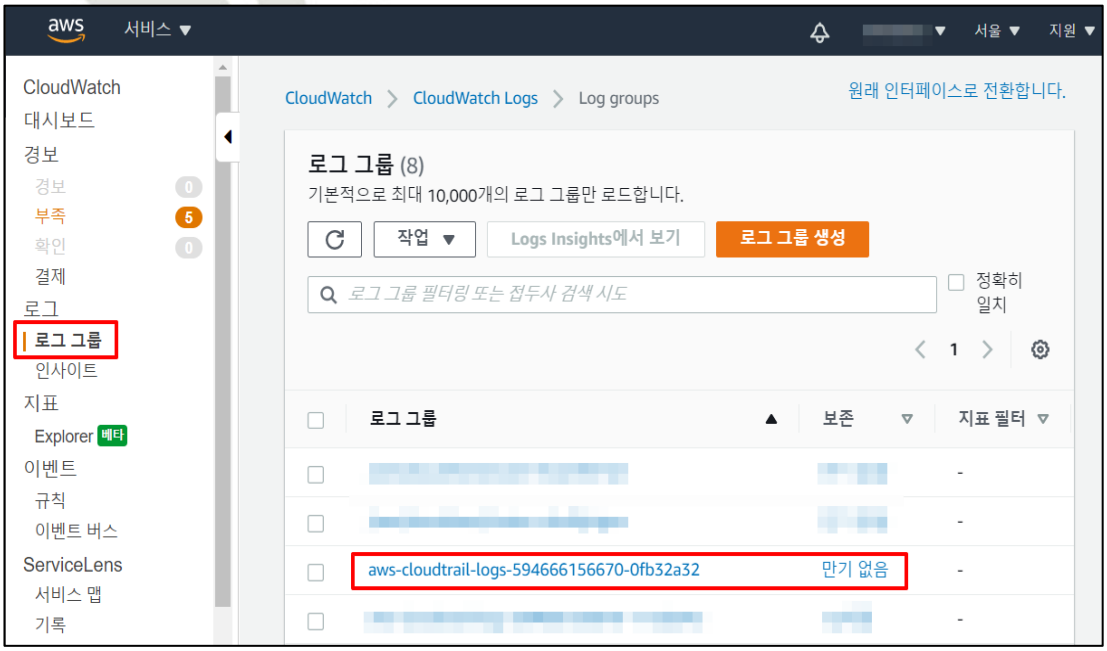


6) CloudTrail 검토 및 생성 내용 확인

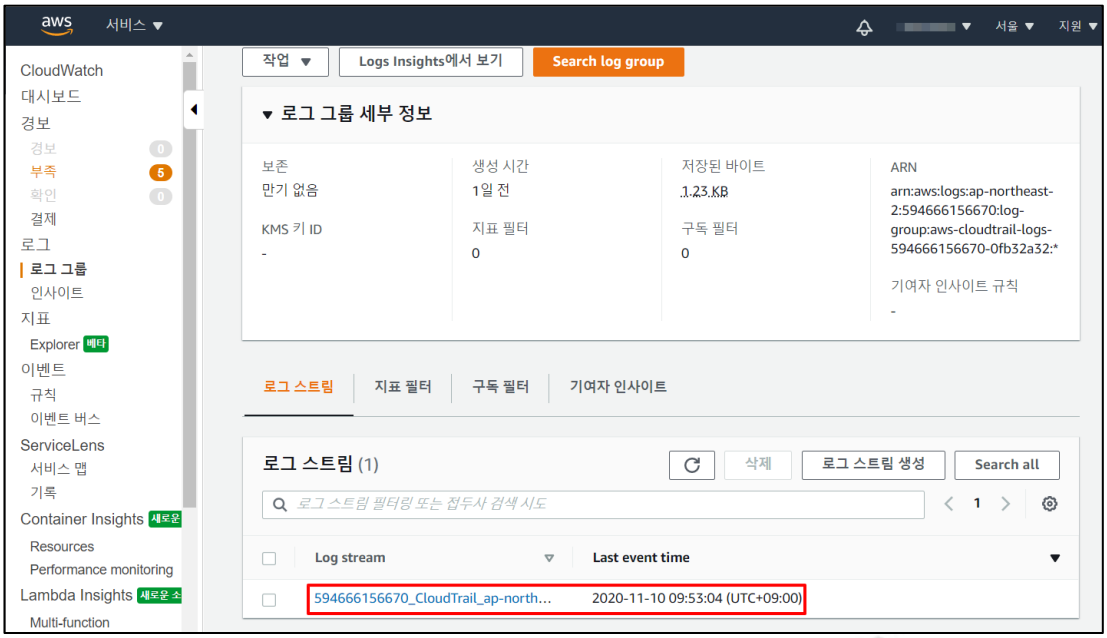


진단 기준	**양호기준** : AWS 사용자 계정(Console, IAM)의 로깅이 설정되어 있는 경우 **취약기준** : AWS 사용자 계정(Console, IAM)의 로깅이 설정되어 있지 않은 경우
비고	

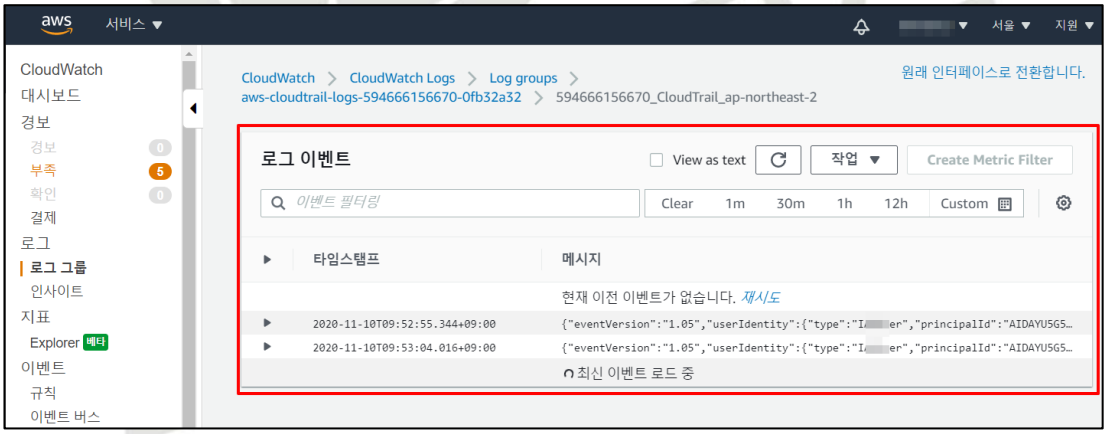
4.8 인스턴스 로깅 설정

분류	운영 관리	중요도	중
항목명	인스턴스 로깅 설정		
항목 설명	Amazon CloudWatch Logs 는 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.		
설정 방법	**가. 로그 그룹 및 로그 스트림 내 EC2 로깅 확인 방법** 1) EC2 내 CloudWatch 에이전트 설치  2) CloudWatch 내 로그 그룹 확인 		

3) 로그 그룹 내 로그 스트림 확인



4) 로그 스트림 내 로깅 확인



진단 기준

양호기준

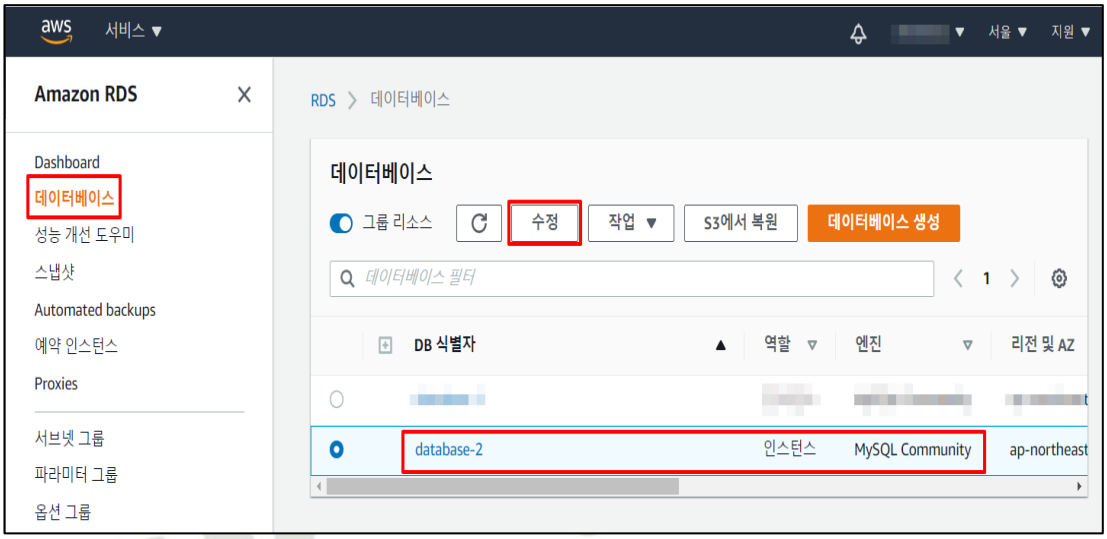
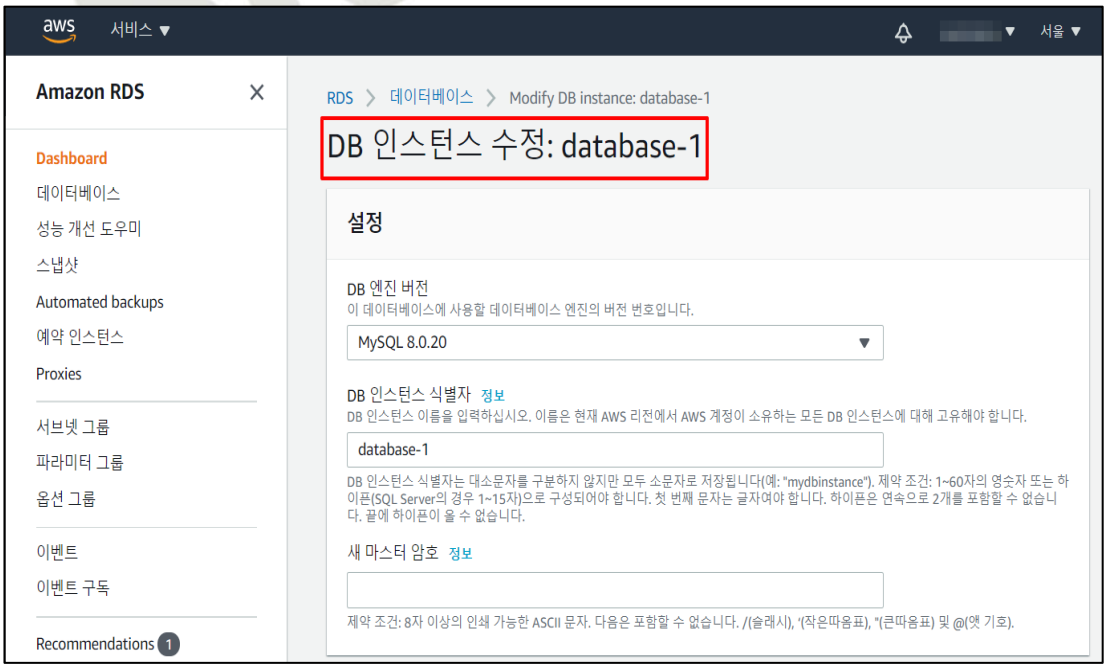
: CloudWatch 로그 스트림으로 보관하고 있는 경우

취약기준

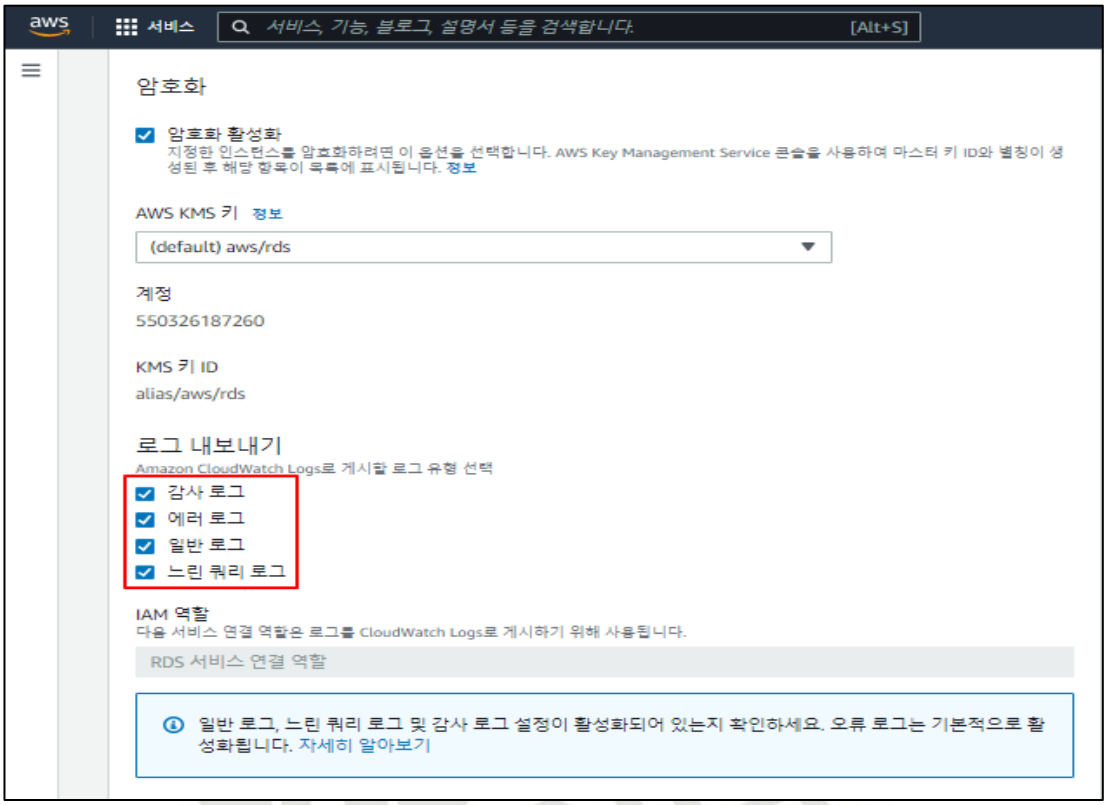
: CloudWatch 로그 스트림으로 보관하고 있지 않은 경우

비고

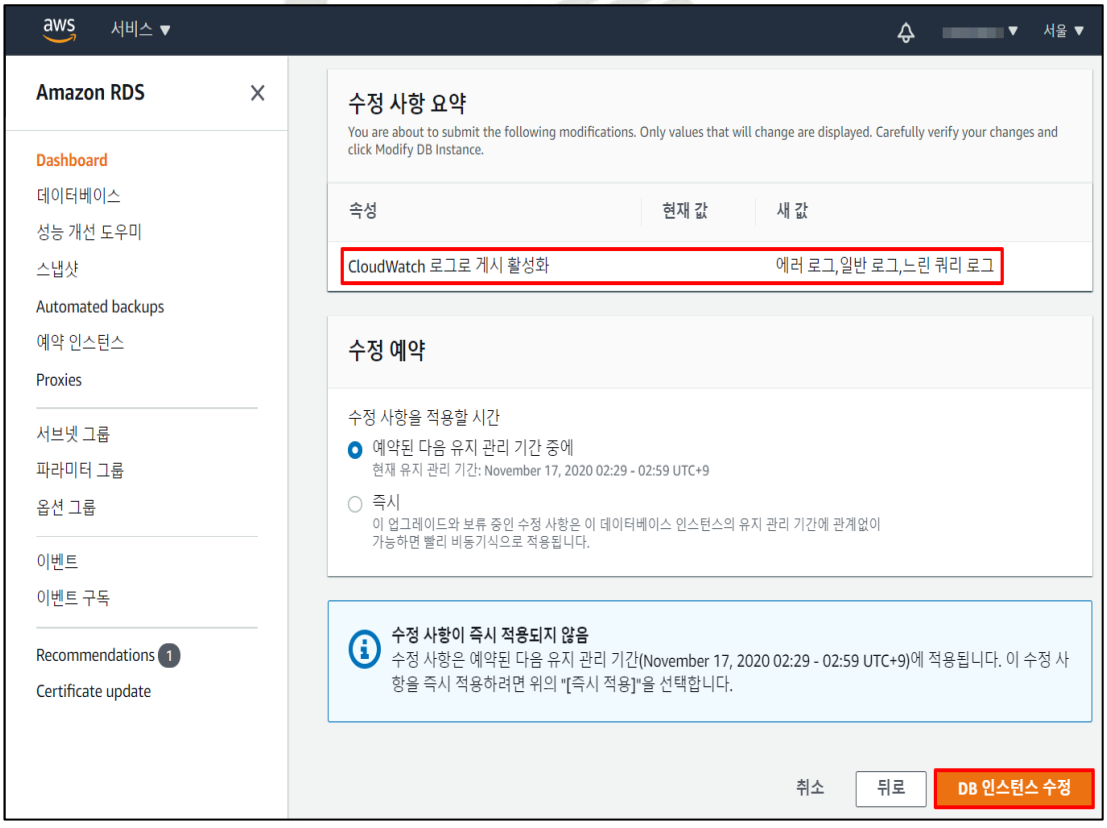
4.9 RDS 로깅 설정

분류	운영 관리	중요도	중
항목명	RDS 로깅 설정		
항목 설명	Amazon CloudWatch Logs 는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스, AWS CloudTrail, Route 53 및 기타 소스에서 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다. 또한, 데이터베이스 옵션(로그 내보내기)을 수정하여 로그 그룹에 등록된 로그 스트림을 통해 RDS 로그를 확인할 수 있습니다.		
설정 방법	**가. 로그 그룹 및 로그 스트림 내 RDS 로깅 확인 방법** 1) RDS 내 데이터베이스 수정  2) 데이터베이스 수정 페이지 접근  		

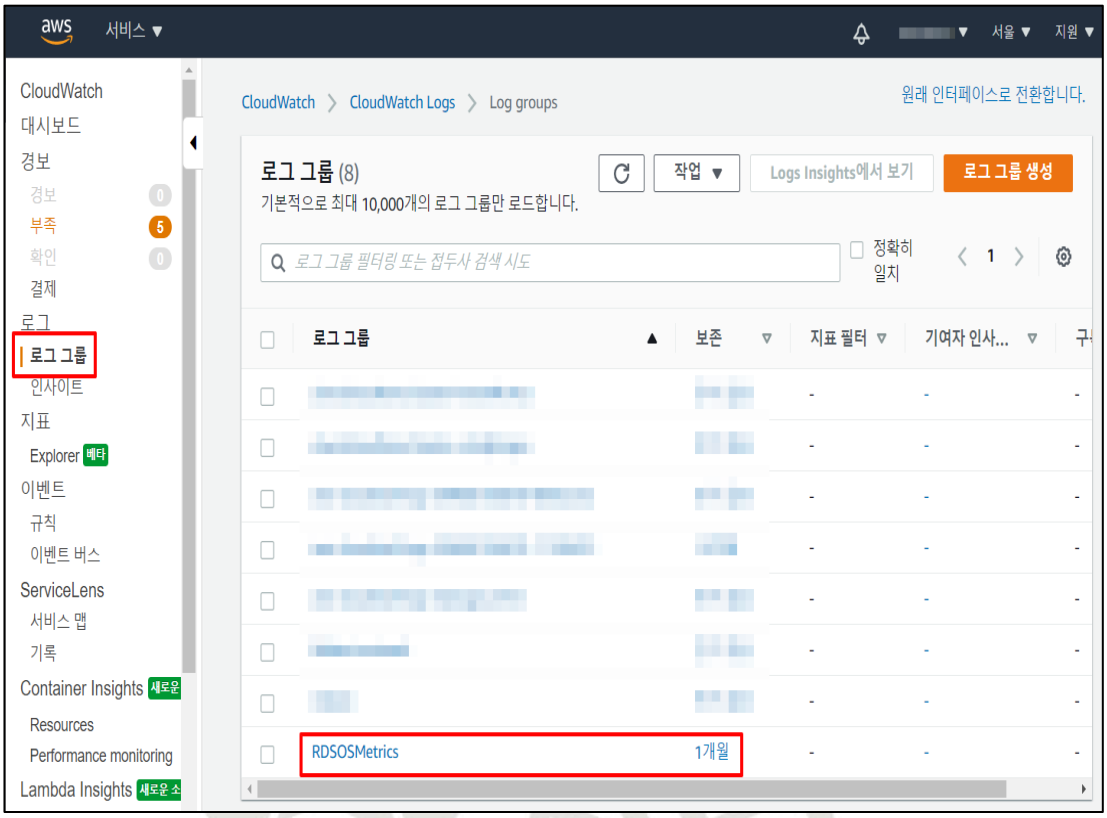
3) 로그 내보내기 옵션 선택



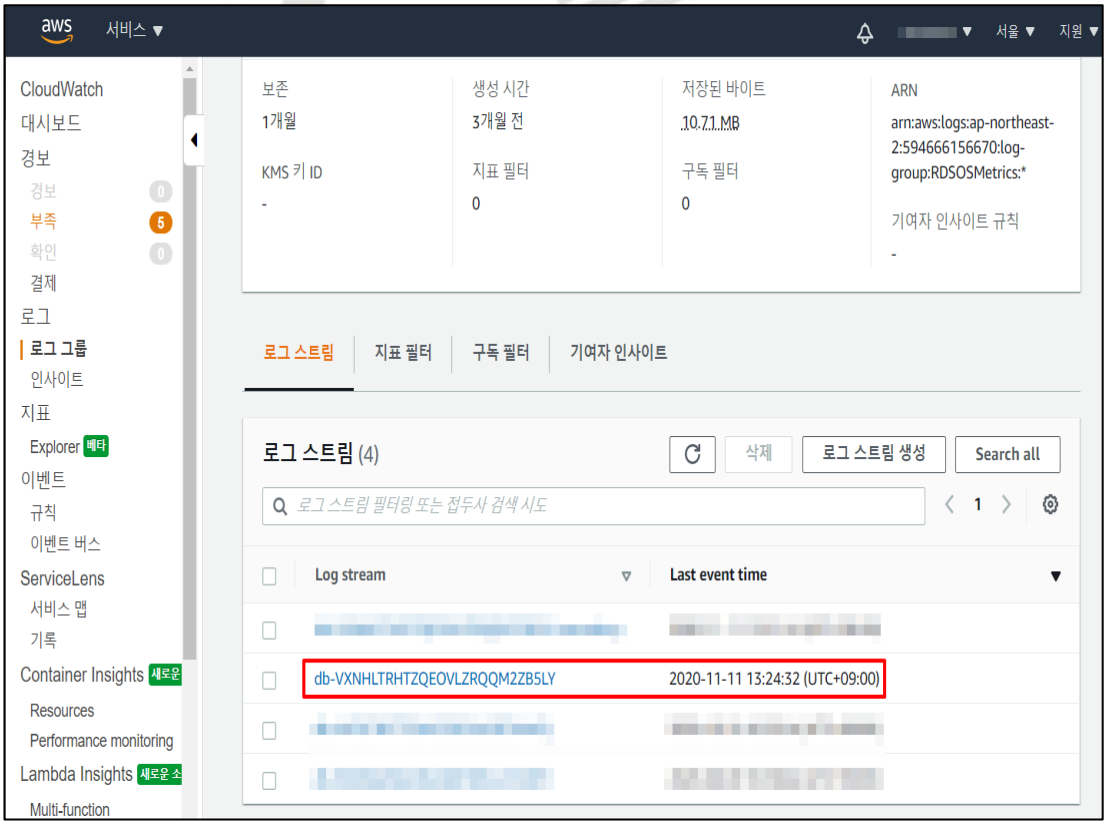
4) DB 인스턴스 수정 클릭

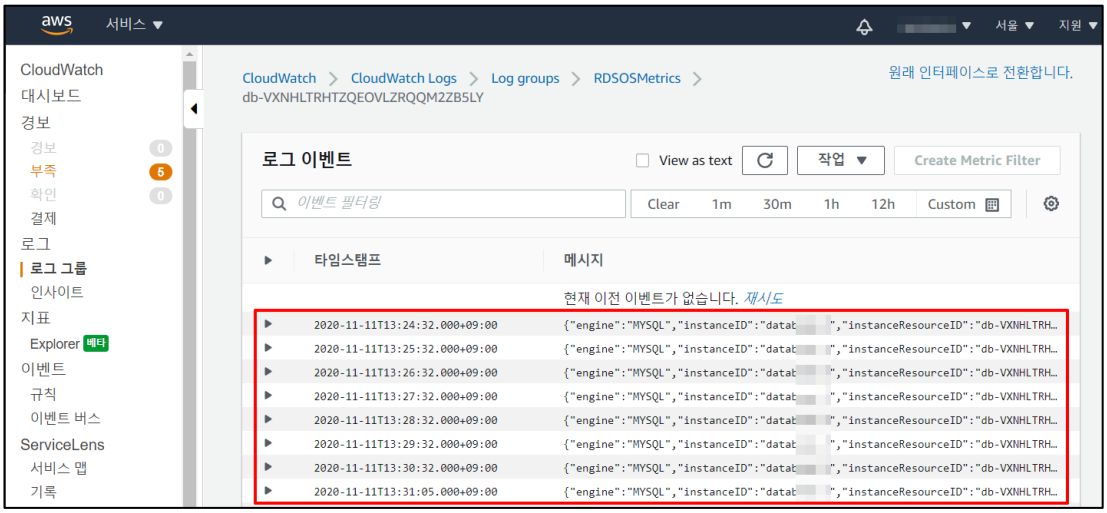


5) 로그 그룹 확인 및 클릭

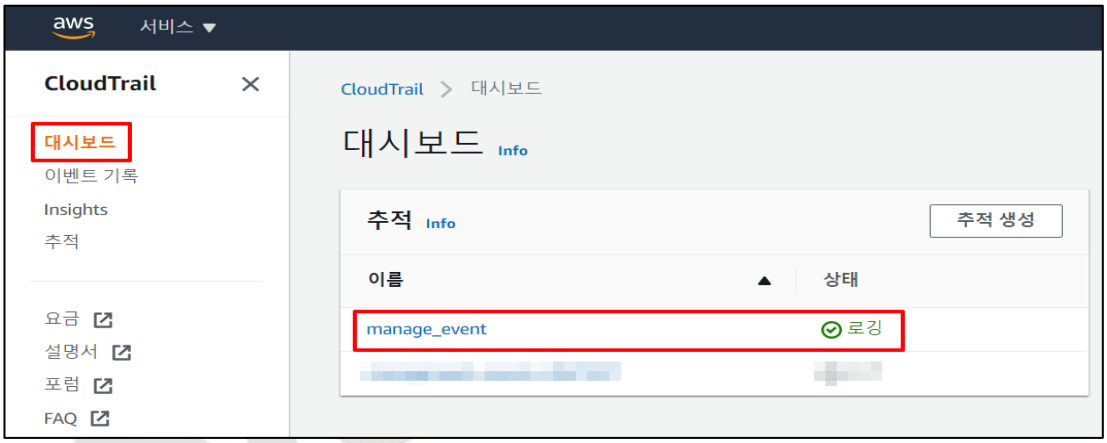
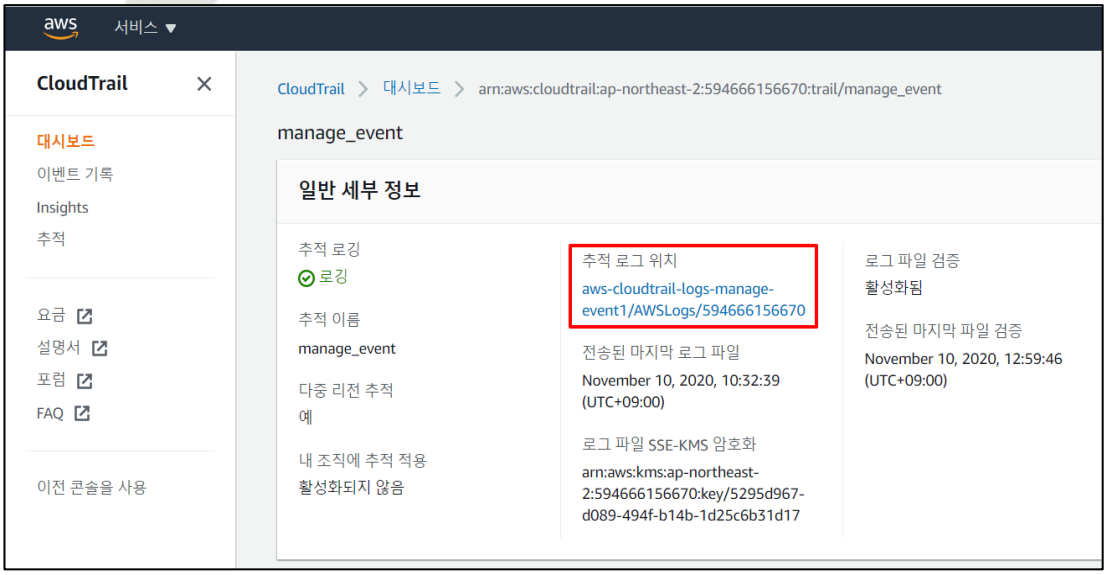


6) 로그 스트림 확인 및 클릭

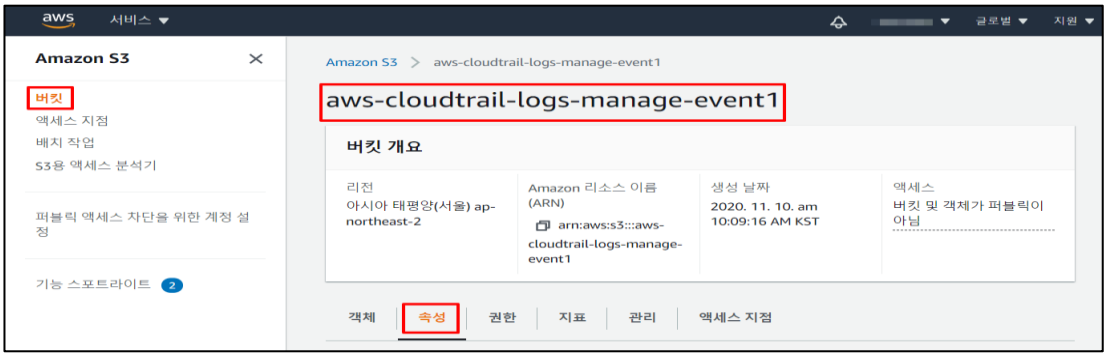


	7) 로그 스트림 내 RDS 로깅 확인 
진단 기준	**양호기준** : CloudWatch 로그 스트림으로 보관하고 있는 경우 **취약기준** : CloudWatch 로그 스트림으로 보관하고 있지 않은 경우
비고	

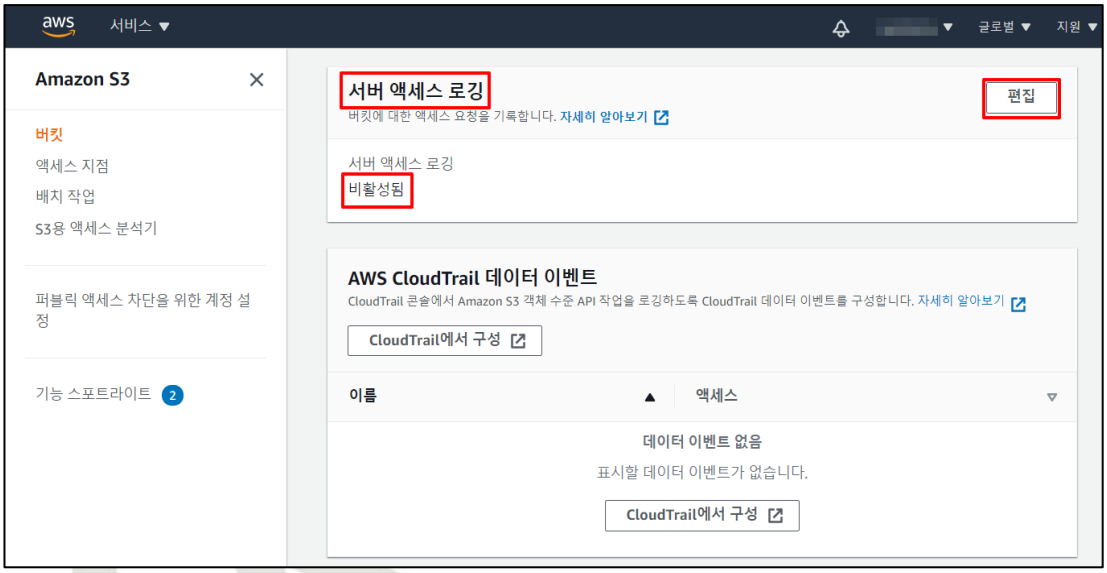
4.10 S3 버킷 로깅 설정

분류	운영 관리	중요도	중
항목명	S3 버킷 로깅 설정		
항목 설명	S3(Simple Storage Service)는 기본적으로 서버 액세스 로그를 수집하지 않으며, AWS Management 콘솔을 통해 S3 버킷에 대한 서버 액세스 로깅을 활성화시킬 수 있습니다. 로깅을 활성화하면 S3 액세스 로그를 사용자가 선택한 대상 버킷에 전달되며, 액세스 로그 레코드에는 요청 유형, 요청에 지정된 리소스, 요청을 처리한 날짜 및 시간 등이 포함됩니다. 대상 버킷은 원본 버킷과 동일한 AWS 리전에 존재해야 하며, 서버 액세스 로깅을 활성화 시 설정이 적용될 때까지 몇 시간이 소요될 수 있습니다.		
설정 방법	**가. CloudTrail 서버 액세스 로그 설정 방법** 1) CloudTrail 대시보드 진입 및 로깅 내용 확인  2) CloudTrail 추적 로그 위치 확인 		

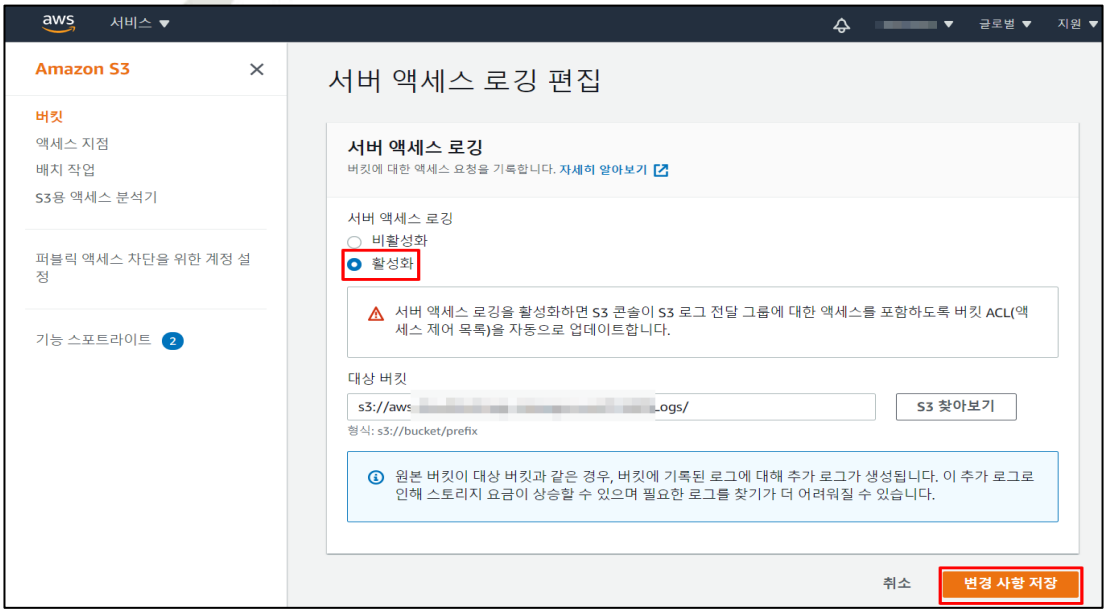
3) CloudTrail 추적 로그 S3 버킷 위치 접근

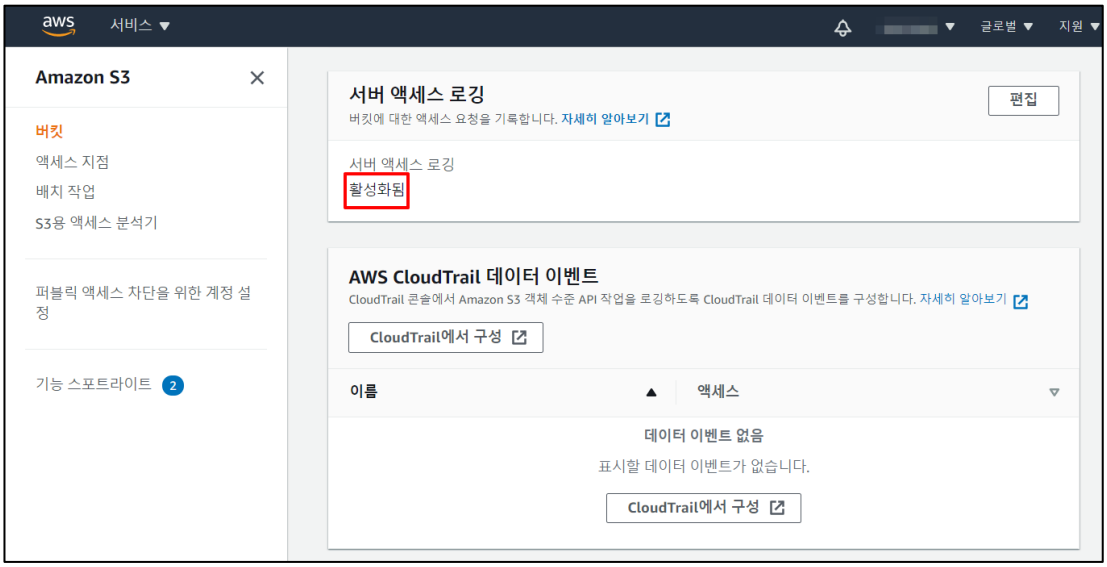


4) S3 버킷 서버 액세스 로깅 비활성화 확인 및 편집 버튼 클릭

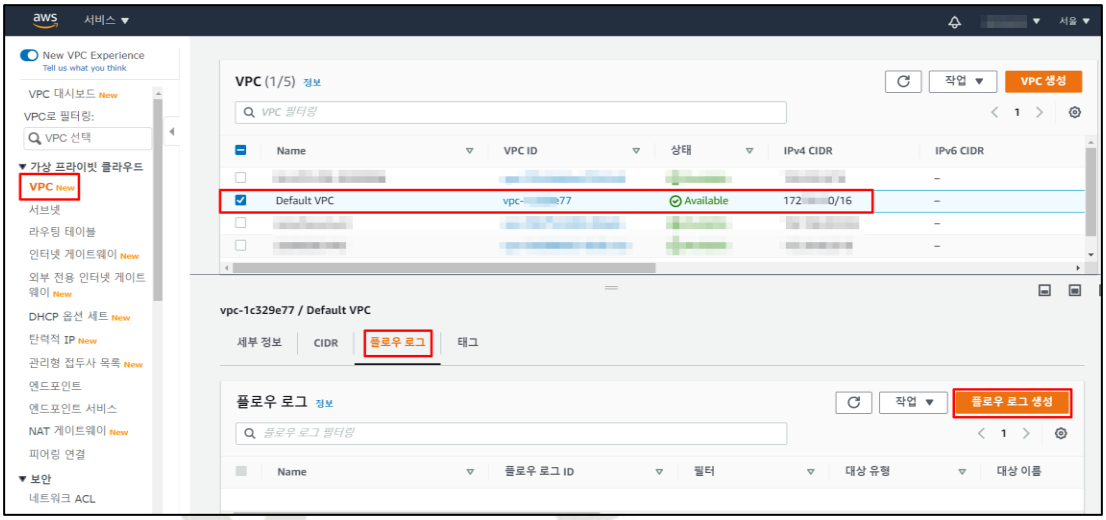
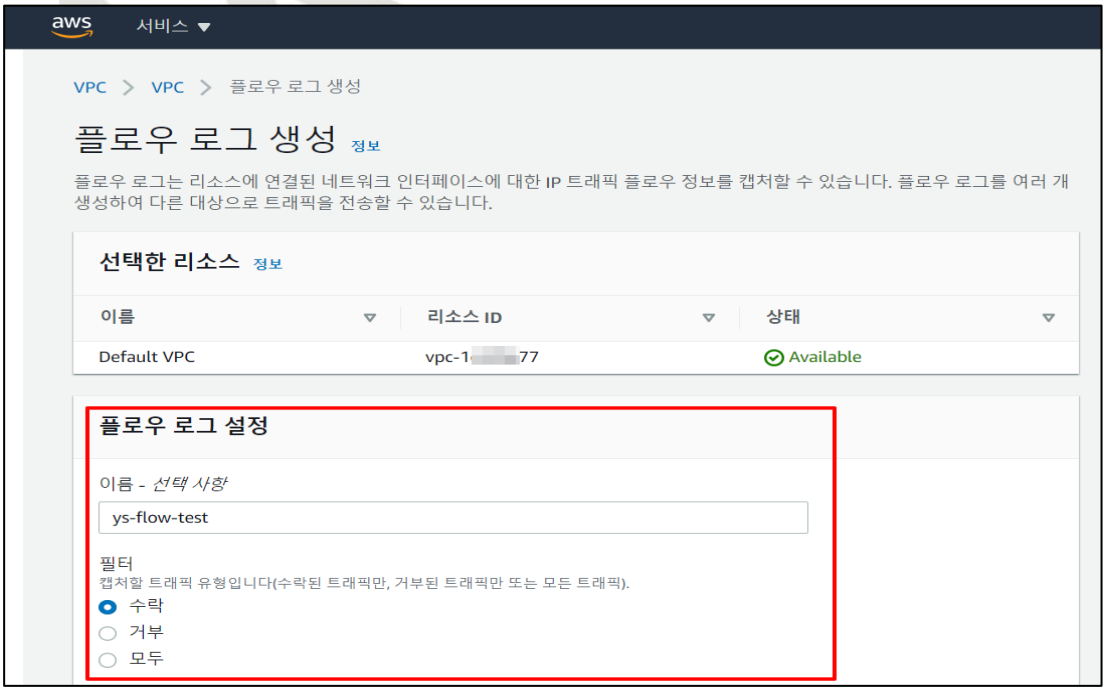


5) S3 버킷 서버 액세스 로깅 활성화

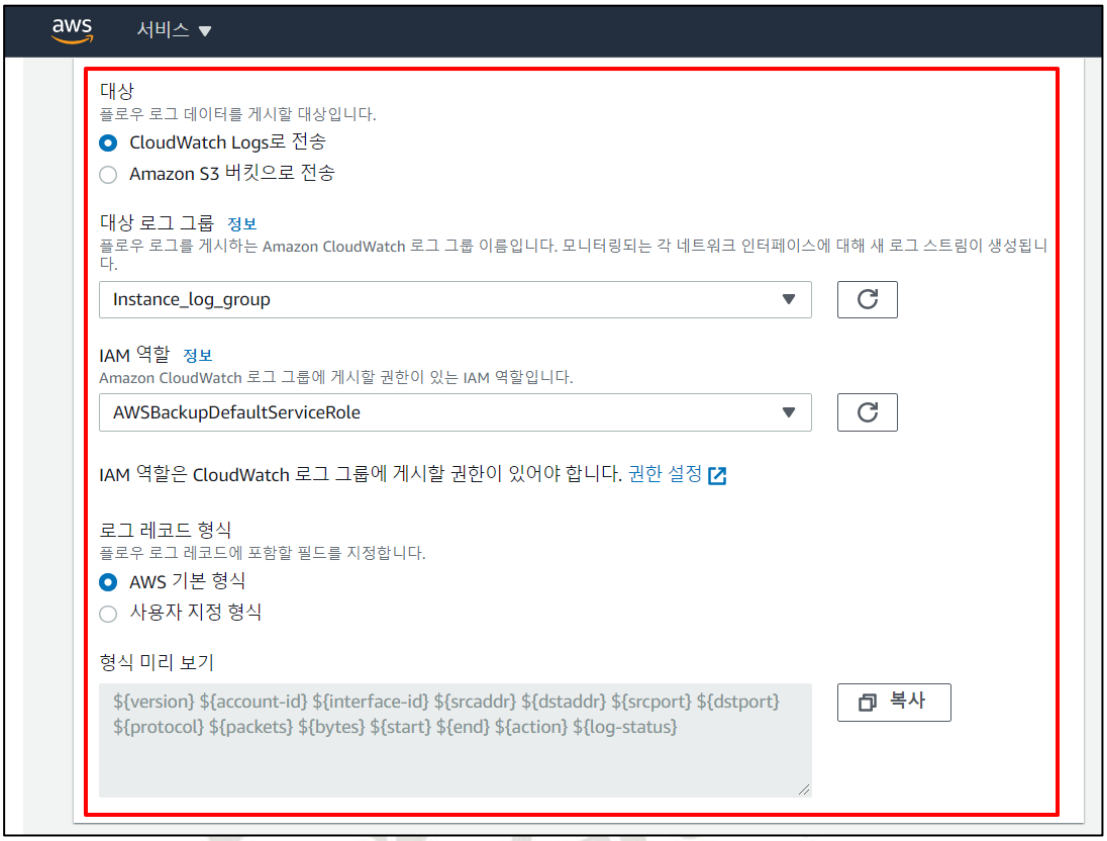


	6) S3 버킷 서버 액세스 로깅 활성화 확인 
진단 기준	**양호기준** : 로그를 보관하고 있는 버킷의 "서버 액세스 로깅"이 설정되어 있는 경우 **취약기준** : 로그를 보관하고 있는 버킷의 "서버 액세스 로깅"이 설정되어 있지 않은 경우
비고	

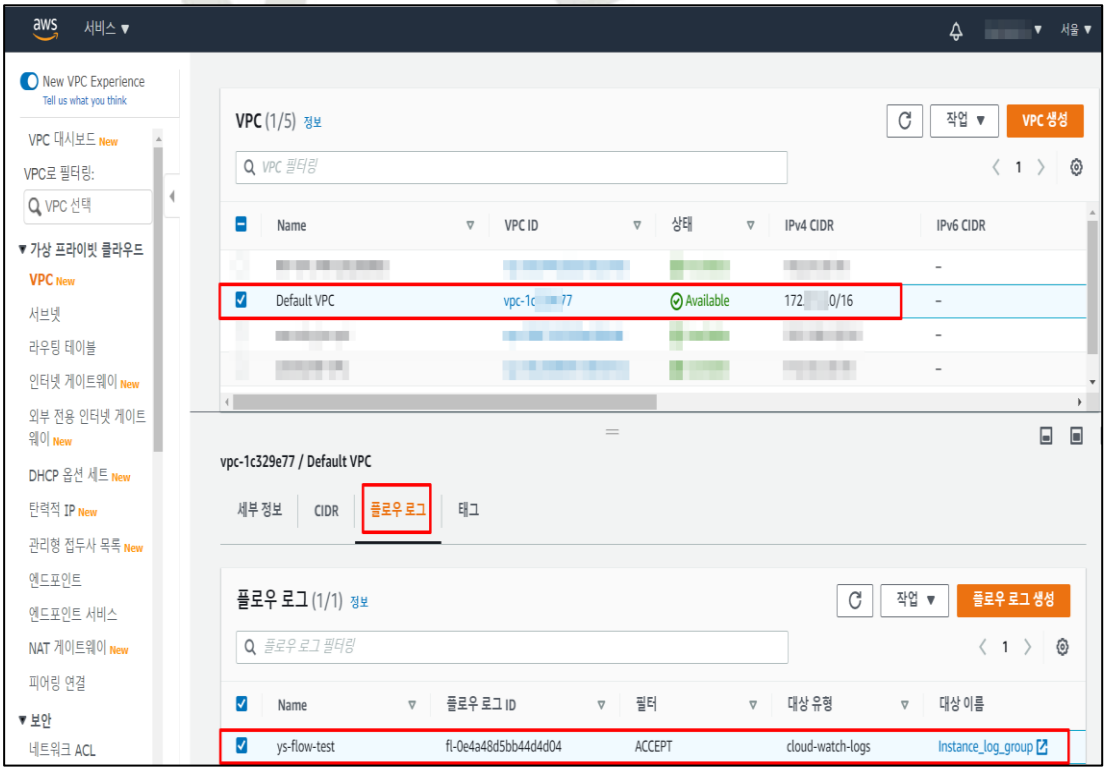
4.11 VPC 플로우 로깅 설정

분류	운영 관리	중요도	중
항목명	VPC 플로우 로깅 설정		
항목 설명	VPC 플로우 로그는 VPC의 네트워크 인터페이스에서 송·수신되는 IP 트래픽에 대한 정보를 수집할 수 있는 기능으로 VPC, 서브넷 또는 네트워크 인터페이스에 생성할 수 있습니다. 플로우 로그는 AWS Management 콘솔의 [VPC] - [플로우 로그] 항목에서 설정 가능하며, 수집된 로그 데이터는 CloudWatch Logs 또는 S3로 저장할 수 있습니다.		
설정 방법	**가. VPC 플로우 로그 CloudWatch 전송 방법** 1) VPC 플로우 로그 설정여부 확인  2) VPC 플로우 로그 이름, 필터 설정 		

3) VPC 플로우 로그 대상(CloudWatch), 로그 그룹, IAM 역할 및 로그 레코드 형식 설정

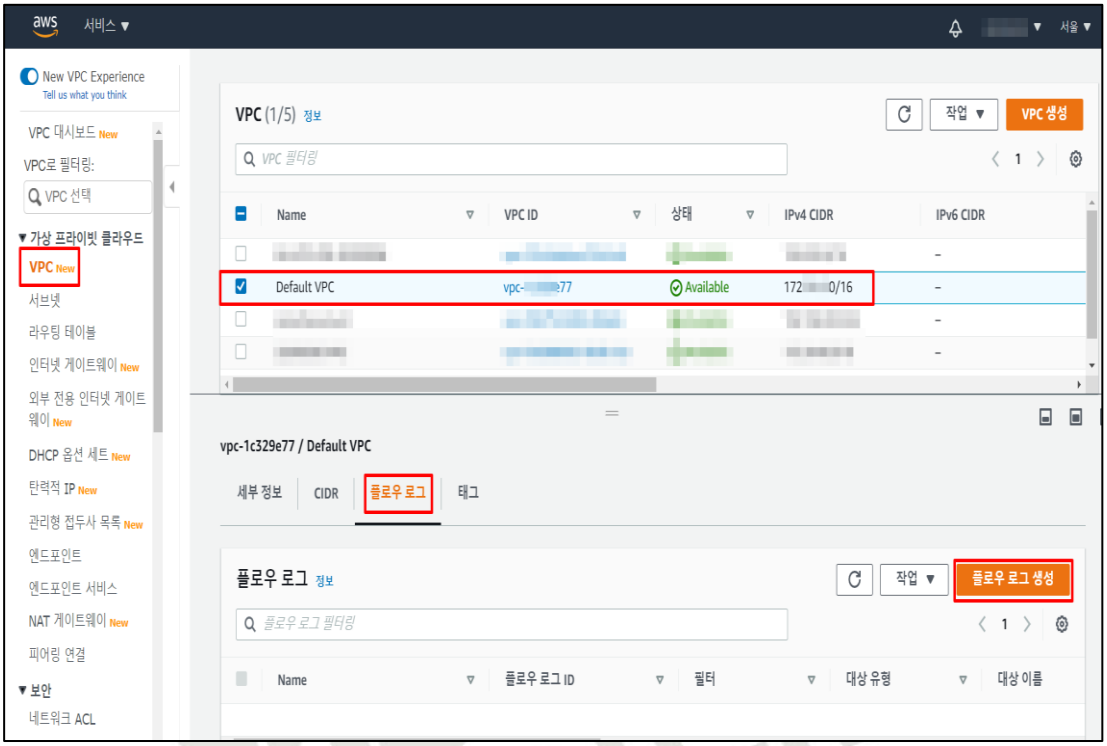


4) VPC 플로우 로그 설정 확인

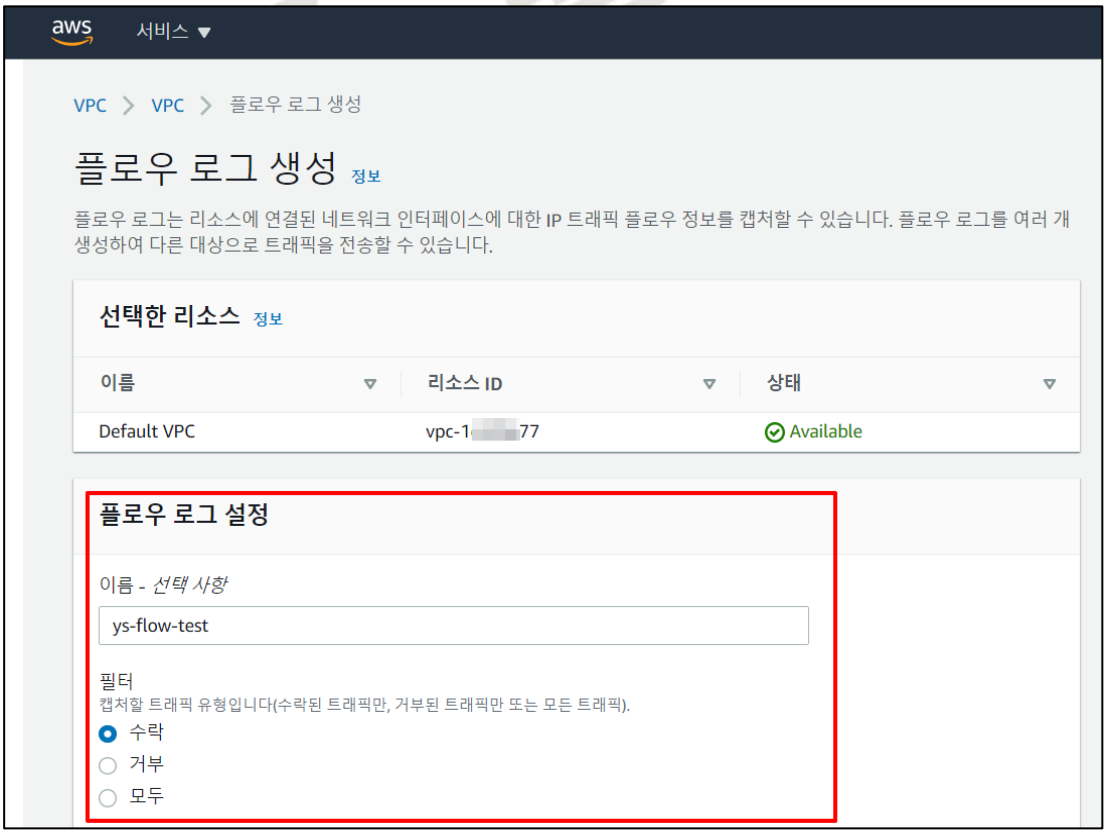


나. VPC 플로우 로그 S3 전송 방법

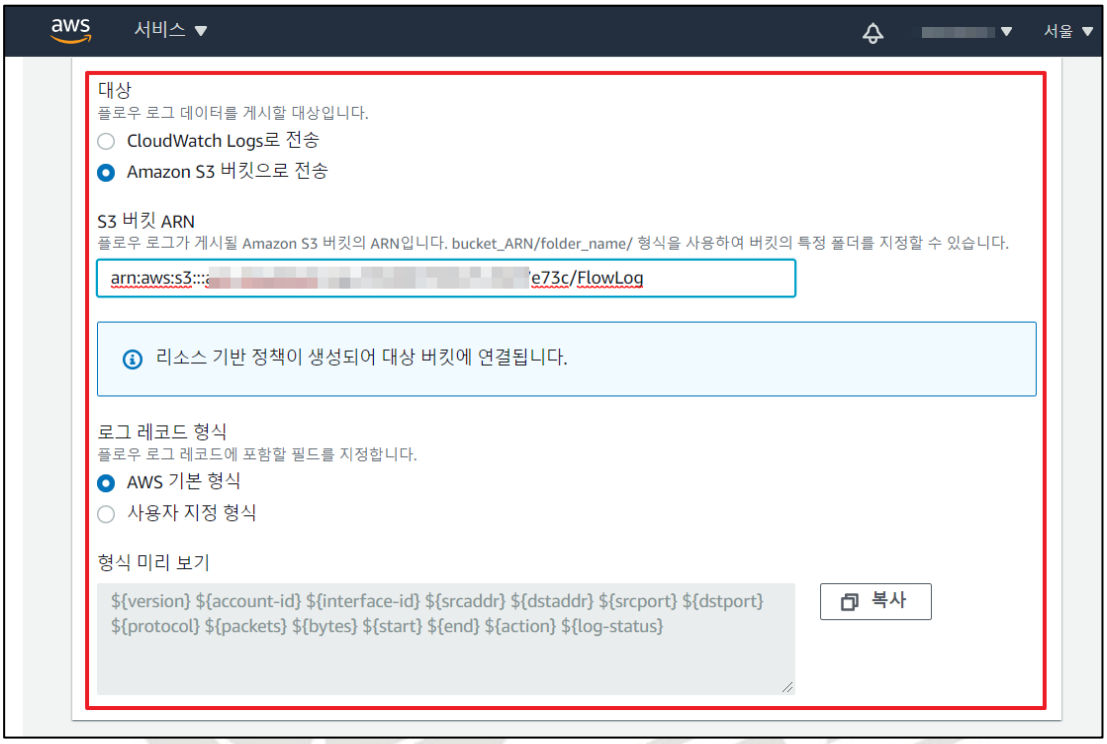
1) VPC 플로우 로그 설정여부 확인



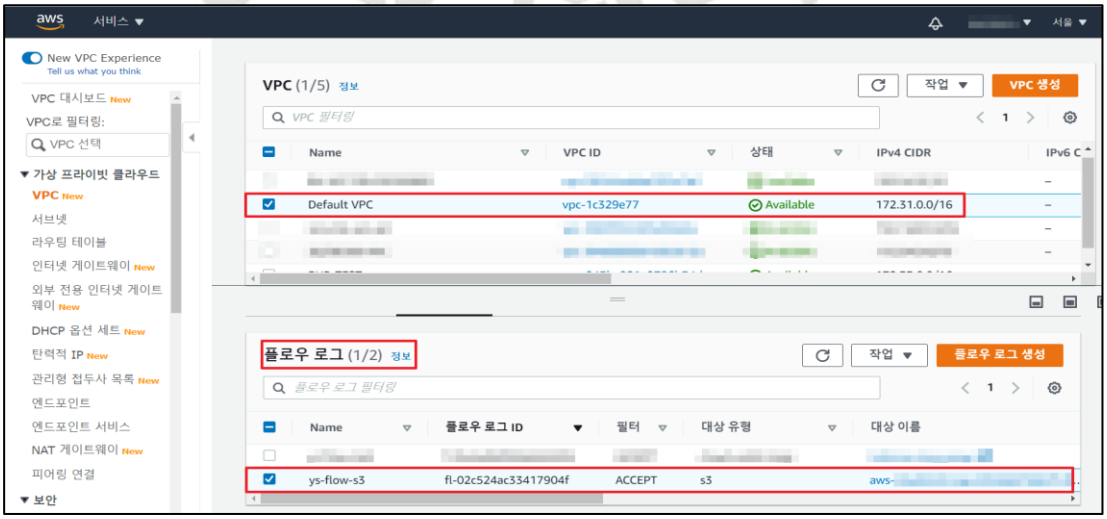
2) VPC 플로우 로그 이름, 필터 설정



3) 플로우 로그 대상(S3), 로그 그룹, IAM 역할 및 로그 레코드 형식 설정



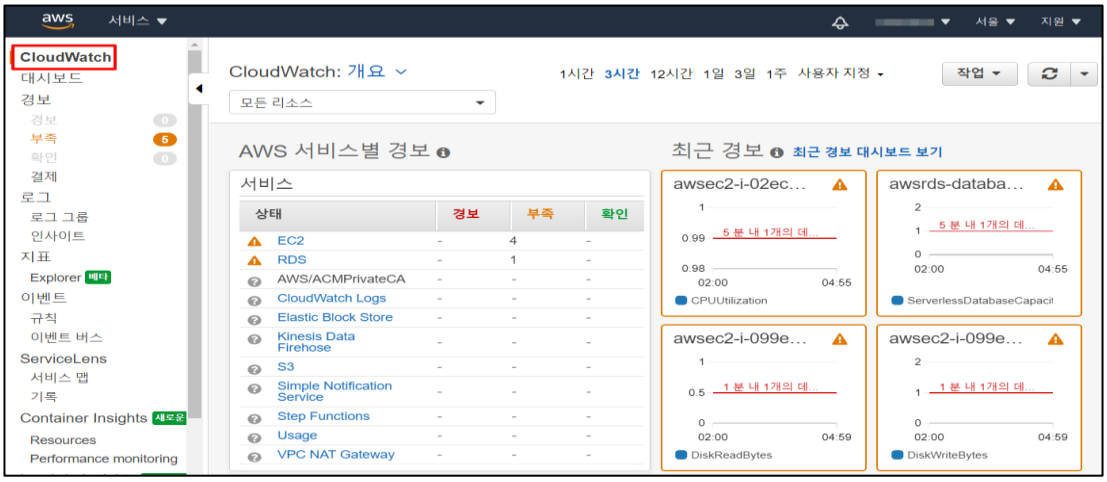
4) VPC 플로우 로그 설정 확인



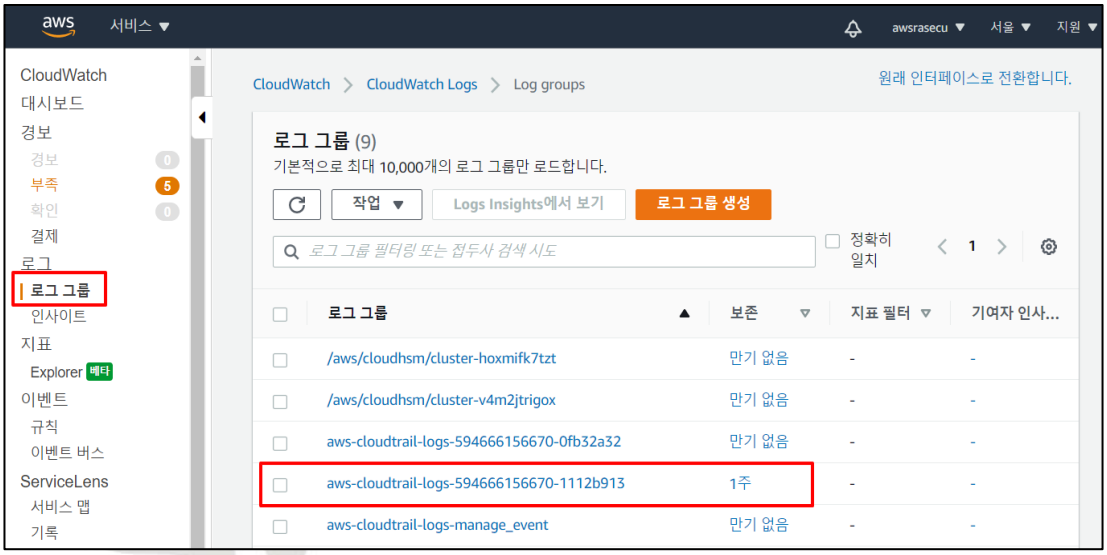
진단 기준	**양호기준** : VPC 플로우 로그 설정이 존재하는 경우 **취약기준** : VPC 플로우 로그 설정이 존재하지 않을 경우
비고	

4.12 로그 보관 기간 설정

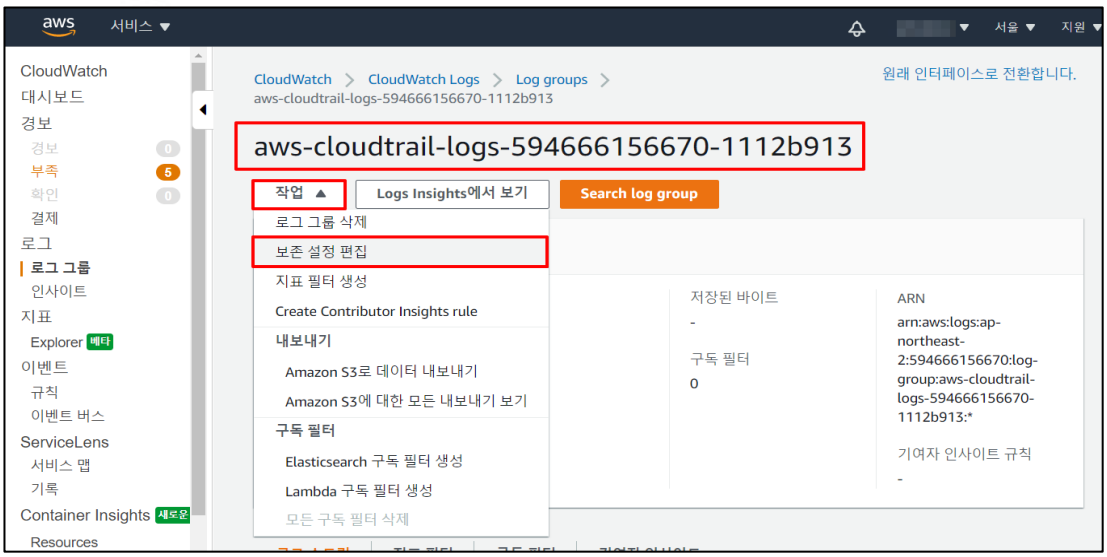
분류	운영 관리	중요도	중
항목명	로그 보관 기간 설정		
항목 설명	CloudWatch Logs에 저장되는 로그 데이터는 기본적으로 무기한 저장되므로, 기업 내부 정책 및 컴플라이언스 준수 등에 부합하도록 로그 데이터 저장 기간을 설정해주어야 하며, AWS Management 콘솔의 CloudWatch 로그 그룹에서 저장 기간 설정이 가능합니다. 국내에서 시행 중인 클라우드 보안인증제에서 보안감사 로그(접근기록 등)는 1년 이상 보존하도록 되어 있으며, 개인정보의 안전성 확보 조치 기준 8조(19.6, 행안부)에서도 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하도록 명시되어 있습니다. **(*) 로그 분류** 1) 개인정보처리시스템 접근 기록 고객 주요 정보, 임직원 주요 정보 등 관련 서비스: S3, RDS, EFS, EBS, FSX, DynamoDB 등 2) 보안관련 감사 로그 사용자 접속 기록, 인증 성공/실패, 계정 생성/삭제 등 관련 서비스: CloudTrail, S3 등 3) 시스템 이벤트 로그 운영체제 구성요소에 의해 발생되는 로그(시스템 시작, 종료, 상태, 에러코드 등) 주요 서버, 네트워크, 보안 장비 등의 로그(접근기록 및 이벤트 로그 등) 관련 서비스: S3, CloudWatch 등 **※ 법적 근거** **국가정보보안기본지침 제55조(로그기록 유지) - 2019/03** **개인정보의 안전성 확보조치 기준 제8조(접속 기록의 보관 및 점검) - 2019/06**		
설정 방법	**가. CloudTrail 로그 보존 기간 설정 방법** 1) CloudTrail 대시보드 진입		



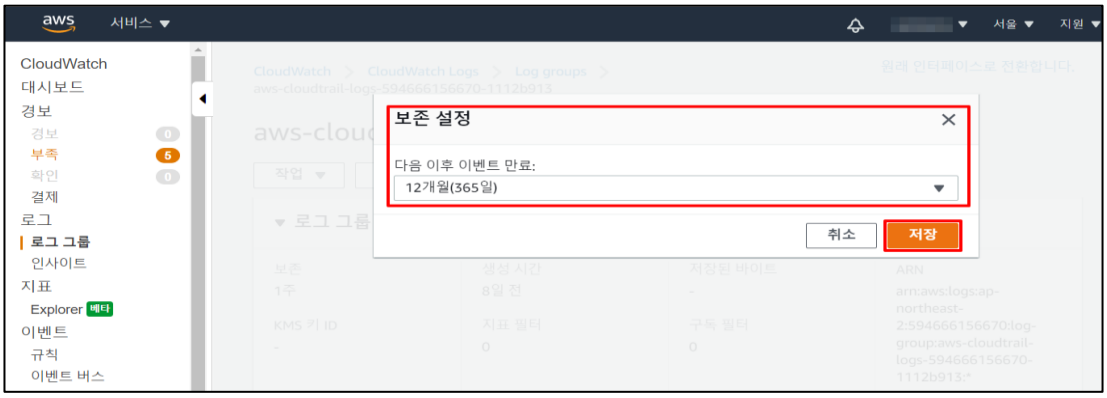
2) CloudTrail 로그 그룹 진입 및 보존 기간 확인



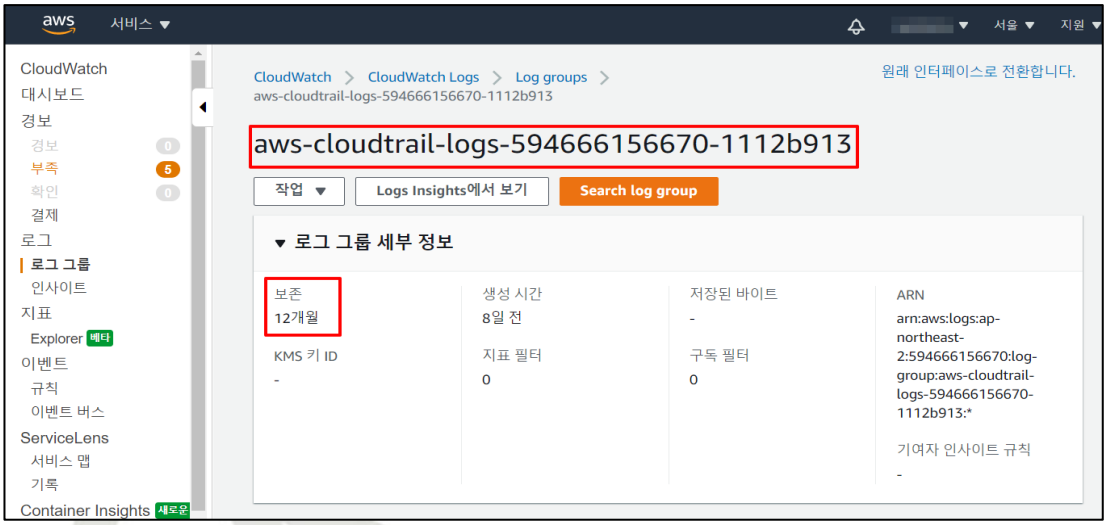
3) CloudTrail 보존 설정 편집 버튼 클릭



4) CloudTrail 보존 설정 기간 설정



5) CloudTrail 보존 설정 기간 정책에 맞게 설정 완료



진단 기준

양호기준

: AWS 서비스 로그를 기준(최소 1년 이상)에 맞게 보관하고 있는 경우

취약기준

: AWS 서비스 로그를 기준(최소 1년 이상)에 맞게 보관하고 있지 않은 경우

비고

4.13 백업 사용 여부

분류	운영 관리	중요도	중
항목명	백업 사용 여부		
항목 설명	운영중인 클라우드 리소스에 대한 시스템 충돌, 장애 발생, 인적 재해 등 기업의 사업 연속성을 해치는 모든 상황에 대비하기 위해 백업 서비스를 구성해야 데이터를 안전하게 보관할 수 있습니다. 이에 보안 담당자 및 관리자는 클라우드 리소스에 대한 백업을 설정하여 데이터 손실을 방지 할 수 있도록 정책을 수립하고 관리하여야 합니다.		
설정 방법	**가. 백업 및 복구 절차 수립** 1) 백업 및 복구 절차 수립, 담당자 지정 - 백업대상(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 **※ 클라우드서비스 보안인증제도(IaaS) 평가기준 해설서의 "6.2 서비스 가용성" 항목 참고**		
진단 기준	**양호기준** : 클라우드 리소스 백업 정책이 존재하는 경우 **취약기준** : 클라우드 리소스 백업 정책이 존재하지 않는 경우		
비고			

2023 클라우드 보안 가이드
- AWS

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 취약점진단팀
제　작 : SK쉴더스 커뮤니케이션그룹