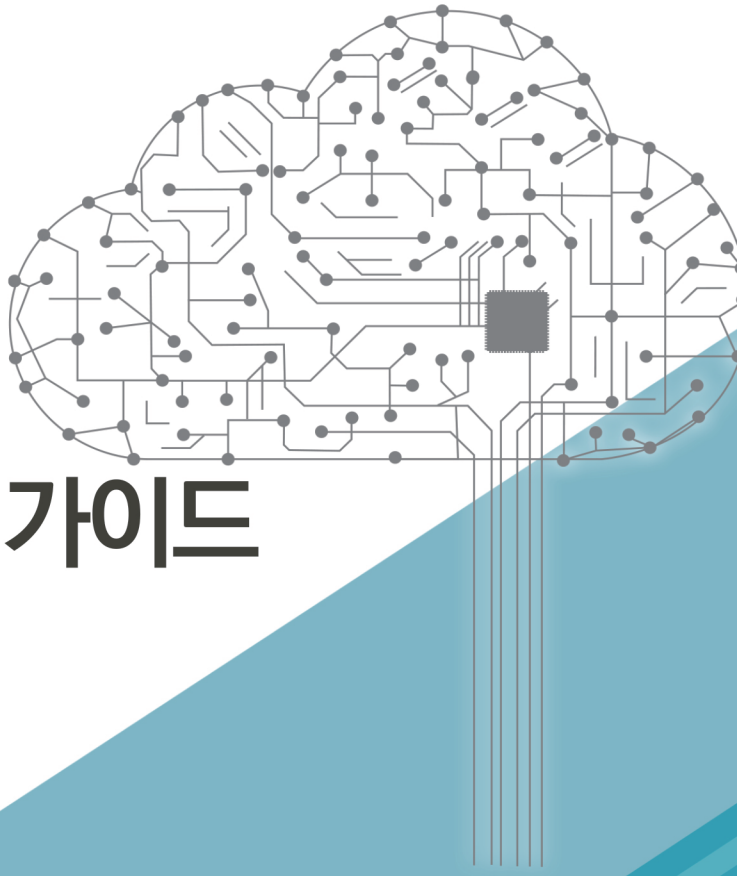
ADT캡스 | infosec



2021 클라우드 보안 가이드

-AWS

클라우드 보안 가이드 2021 발간사

안녕하십니까? ADT캡스 인포섹입니다.
지난 2019년 인포섹의 취약점진단팀은 '클라우드 보안 가이드 - AWS, Cloud Z', '클라우드 보안 가이드(컨테이너 보안) - Docker, Kubernetes', '클라우드 보안 가이드 - Azure, GCP'를 발간했습니다.

그동안 AWS, Azure, GCP는 빠르게 변화했으며, 이러한 트렌드를 분석하고 변화에 대응하고자 올해 '클라우드 보안 가이드 - AWS, Azure, GCP' 3종의 개정판을 발간하게 되었습니다.

매년 클라우드 환경으로 전환하는 기업들이 늘어나고 있으며, 클라우드 도입 및 전환 시 미흡한 환경설정 및 보안정책 설정으로 인한 해킹공격이 발생하고 있습니다.

이번 가이드는 계정 관리, 권한 관리, 데이터 관리, 가상 리소스 관리, 감사/추적 관리 영역으로 분류됐으며, 각 영역별 보안 정책 설정 방법과 점검 방법에 대한 설명을 담고 있습니다. 또한, 취약점 점검 항목을 포함하여 클라우드 운영자가 위협에 대응하고 인증 심사와 컴플라이언스 기준을 충족할 수 있는 기준을 제시했습니다.

앞으로도 ADT캡스 인포섹은 클라우드 운영자가 다양한 환경에 발빠르게 대응할 수 있도록 보안 가이드를 발간할 계획입니다.

더불어, 1년 동안 클라우드 보안 가이드 개선에 많은 시간과 노력을 투자한 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 계정관리(7개 항목), 권한관리(6개 항목), 데이터관리(3개 항목), 가상 리소스 관리(10개 항목), 감사/추적 관리(4개 항목)으로 총 5개 영역에서 30개 항목으로 구성 하였습니다.

[표] 1. AWS 보안진단 체크리스트

영역	항목코드	항목명	중요도
계정관리	1.1	관리자 계정 최소화 관리	상
	1.2	IAM 사용자 계정 단일화 관리	상
	1.3	IAM 사용자 계정 식별 관리	중
	1.4	Key Pair 접근 관리	상
	1.5	Key Pair 보관 관리	상
	1.6	MFA (Multi-Factor Authentication) 설정	중
	1.7	패스워드 정책 관리	중
권한관리	2.1	인스턴스 보안 정책 관리	상
	2.2	RDS 보안 정책 관리	상
	2.3	S3 보안 정책 관리	상
	2.4	Access Key 정책 관리	중
	2.5	Admin Console 관리자 정책 관리	중
	2.6	IAM 사용자 및 그룹 정책 관리	중
데이터관리	3.1	인스턴스 암호화 설정	중
	3.2	RDS 암호화 설정	중
	3.3	S3 암호화 설정	중
가상 리소스 관리	4.1	보안그룹 인/아웃바운드 ANY 설정 관리	중
	4.2	보안그룹 인/아웃바운드 불필요 정책 관리	중
	4.3	ACL 네트워크 인/아웃바운드 트래픽 정책 관리	상
	4.4	라우팅 테이블 정책 관리	중
	4.5	NAT 게이트웨이 연결 관리	중
	4.6	인터넷 게이트웨이 연결 관리	하
	4.7	S3 버킷 접근 관리	중
	4.8	RDS 리소스 액세스 권한 관리	중
	4.9	RDS API 작업 권한 관리	중
	4.10	RDS 서브넷 가용 영역 관리	중
감사/추적 관리	5.1	AWS 사용자 계정 로깅 설정	하
	5.2	가상 인스턴스 로깅 설정	하
	5.3	RDS 로깅 설정	하
	5.4	S3 버킷 로깅 설정	하

2. 위험도 구분

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

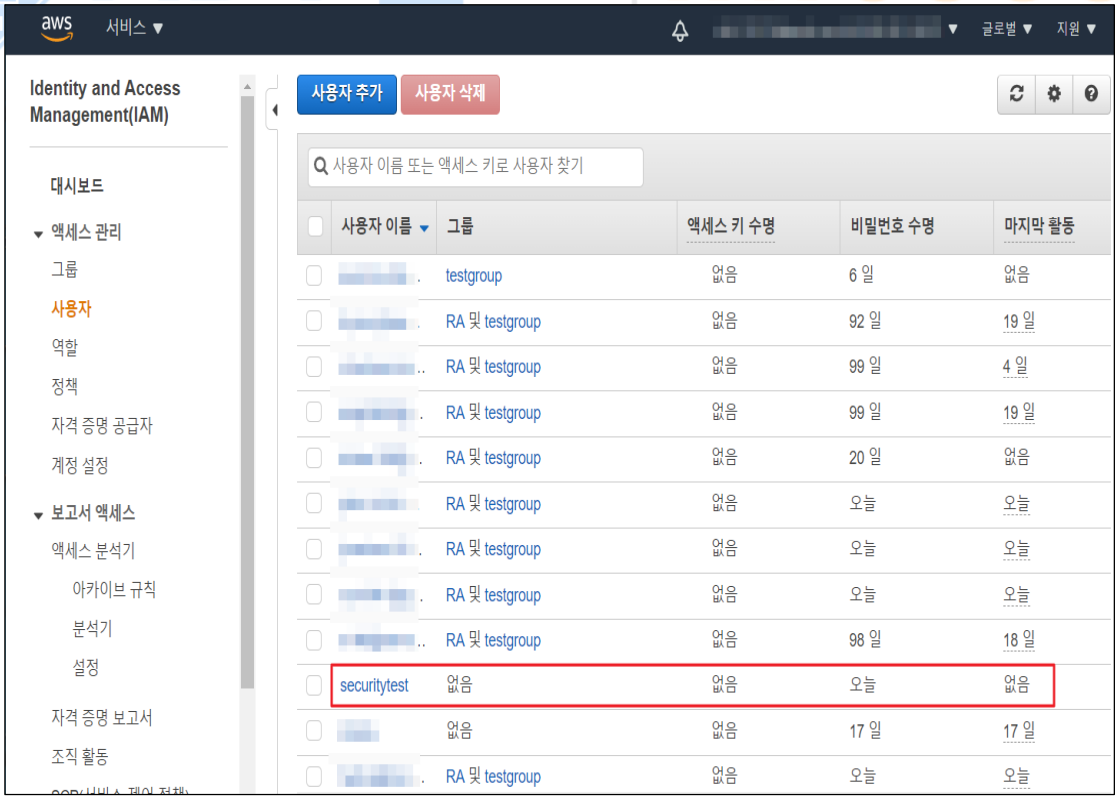
[표] 2. 위험도 구분

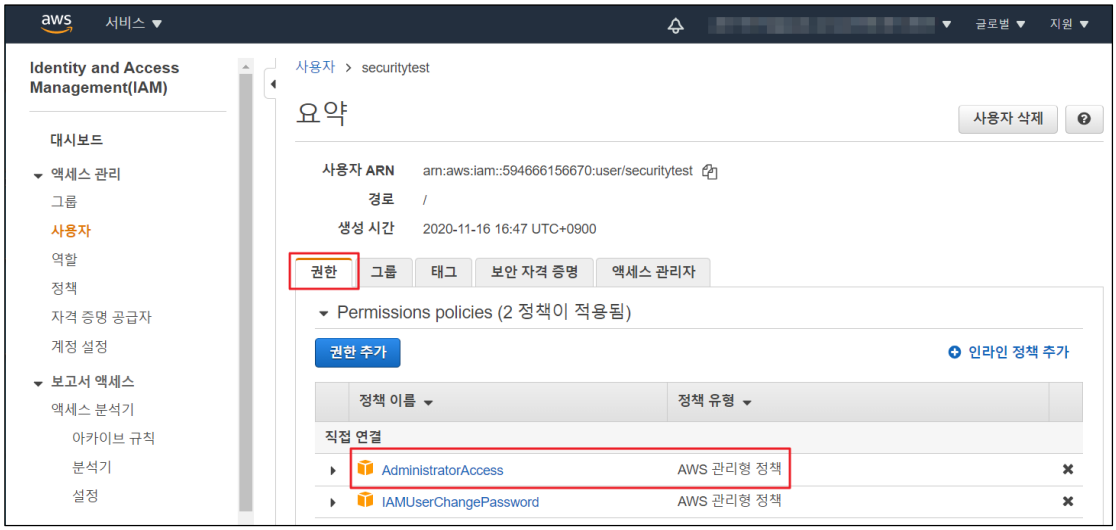
위험도	내 용	비고
상	관리자 계정 및 주요정보 유출로 인한 치명적인 피해 발생	
중	노출된 정보를 통해 서비스/시스템 관련 추가 정보 유출 발생 우려	
하	타 취약점과 연계 가능한 잠재적인 위협 내재	

II. 세부항목 설정

1. 계정관리

1.1 관리자 계정 최소화 관리

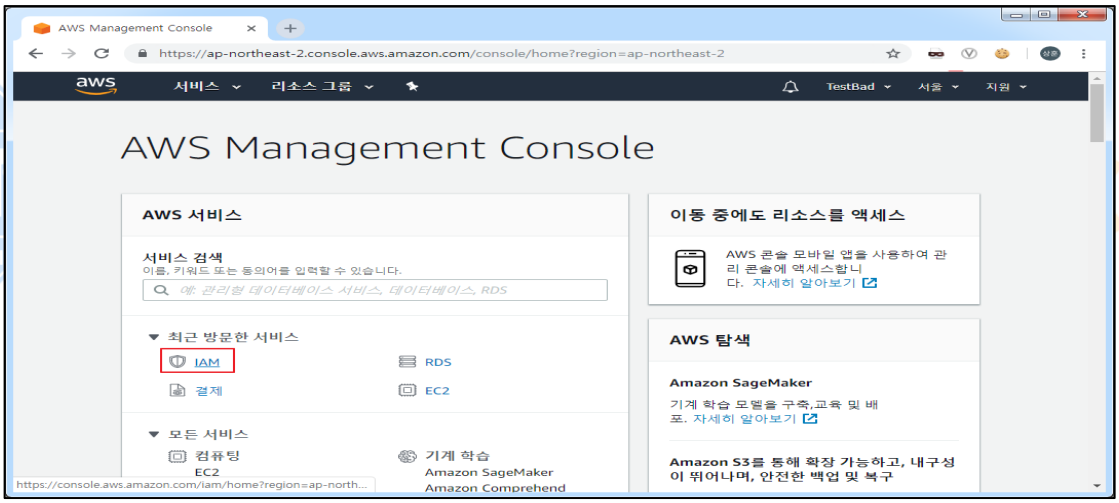
분류	계정관리	중요도	상
항목명	관리자 계정 최소화 관리		
항목 설명	모든 AWS 리소스는 AWS 계정의 소유이고, 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(즉, 사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다. **1) AWS 관리형 정책** 서비스 내 FULL ACCESS 등과 같이 중요도가 높은 AWS 관리형 정책은 EC2 서비스 관리/운영자 및 관련 담당자 외에 다른 IAM 계정에 아래와 같은 권한 할당이 되지 않도록 해야합니다. 그중에서도 AWS Root 관리자 인 **"Administratoraccess"** 권한은 다수의 IAM 계정에 설정되지 않도록 관리조치가 필요합니다. **(*) "Administratoraccess" 및 "Full Access" 권한이 부여된 다수의 계정이 존재할 경우 담당자 확인이 필요함**		
설정 방법	**가. IAM 그룹에 포함되지 않은 단일 사용자 권한 확인** 1) IAM 그룹에 포함되지 않은 단일 사용자 계정 전체 권한 확인  2) 전체 권한 여부 확인		

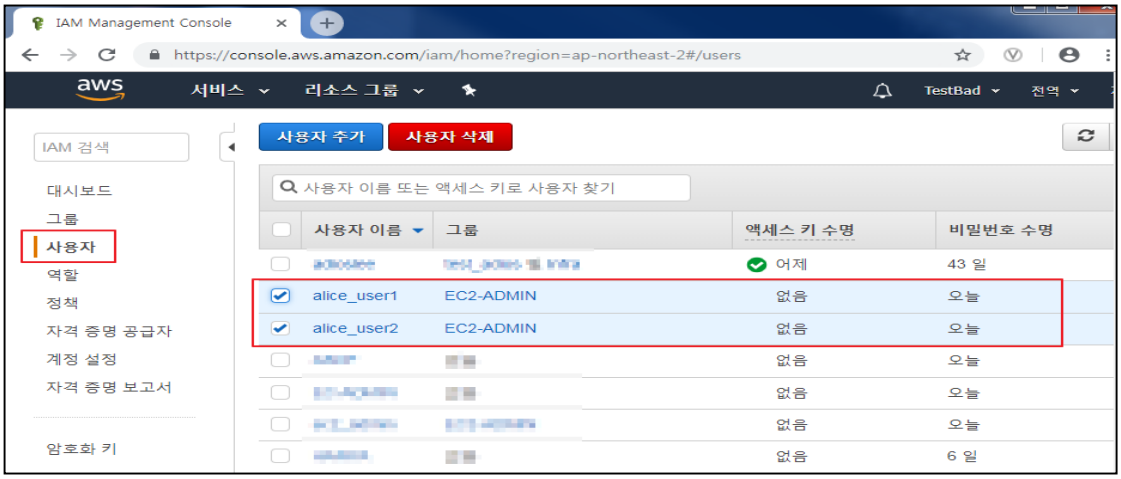
<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단 기준</td><td>양호기준
: 관리자 권한이 사용 목적에 맞게 지정된 사용자가 부여되어 있을 경우

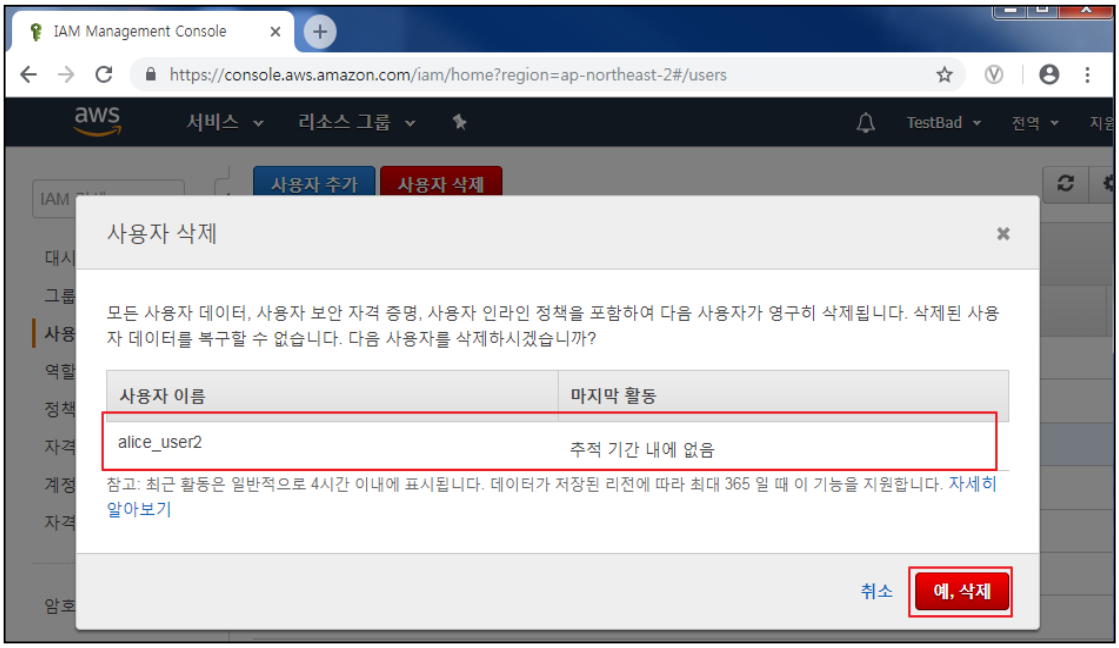
취약기준
: 관리자 권한이 사용 목적에 맞지 않은 사용자에게 불필요하게 부여되어 있을 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

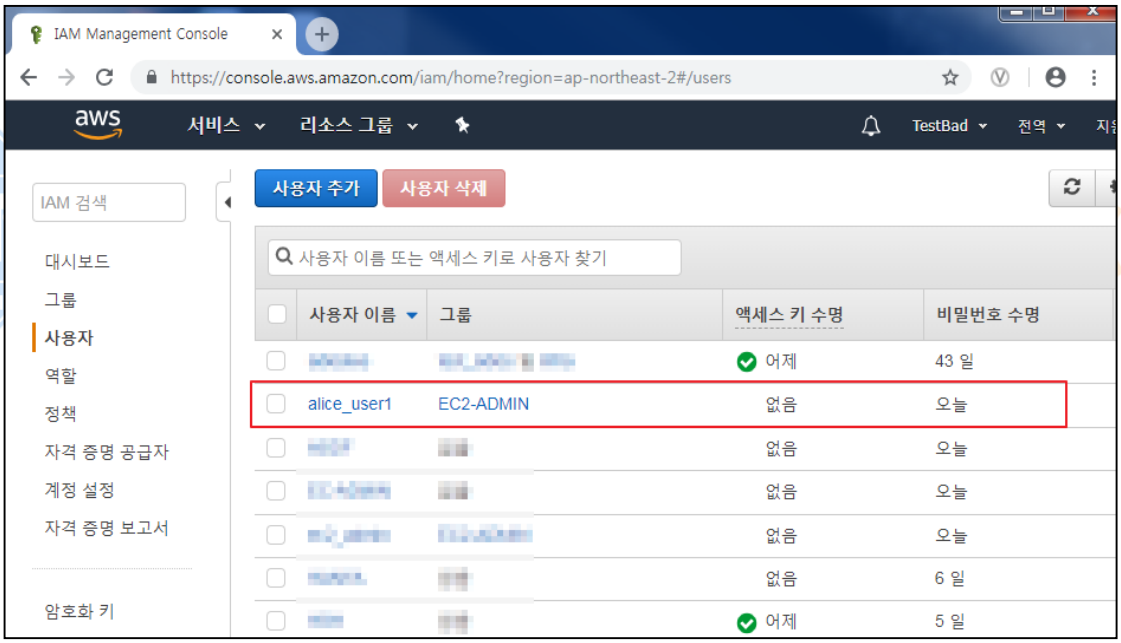
1.2 IAM 사용자 계정 단일화 관리

분류	계정관리	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 IAM 계정 1인 1계정 초과 사용 시 사용자 삭제 [IAM] → [사용자 삭제] → [예, 삭제]		



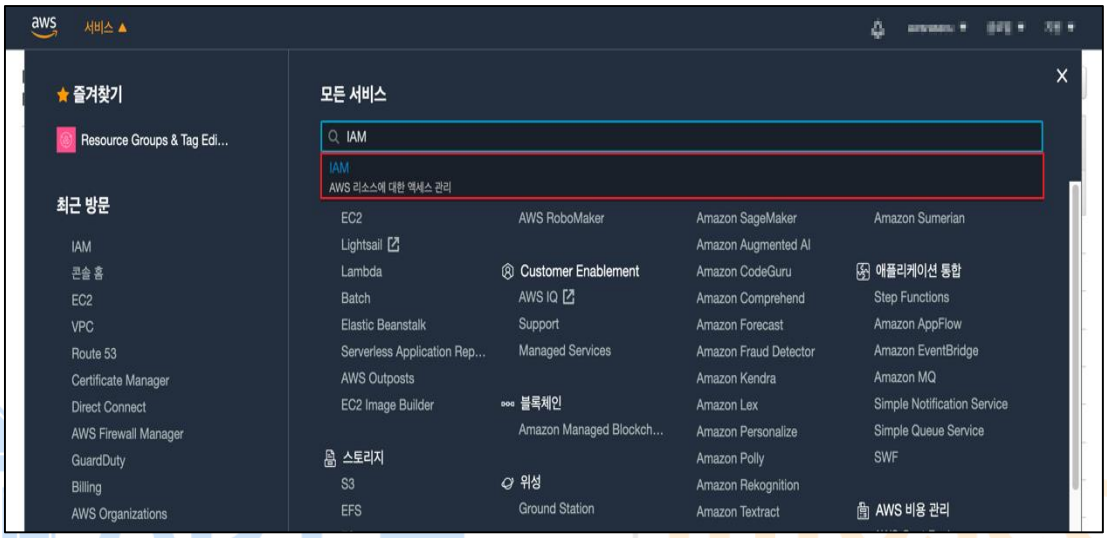
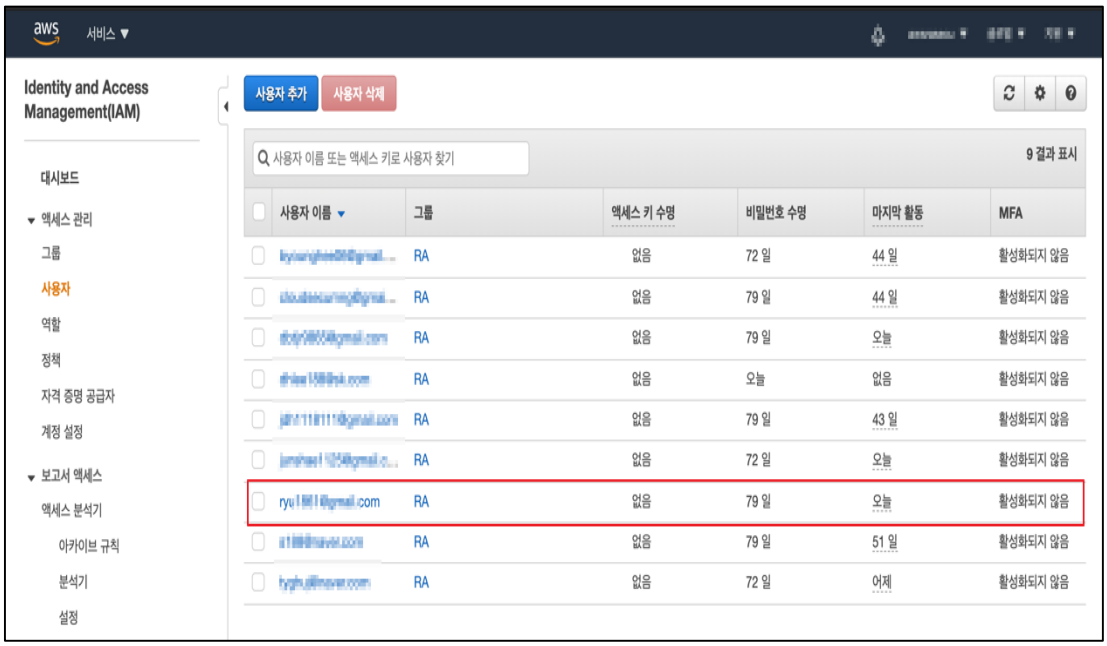


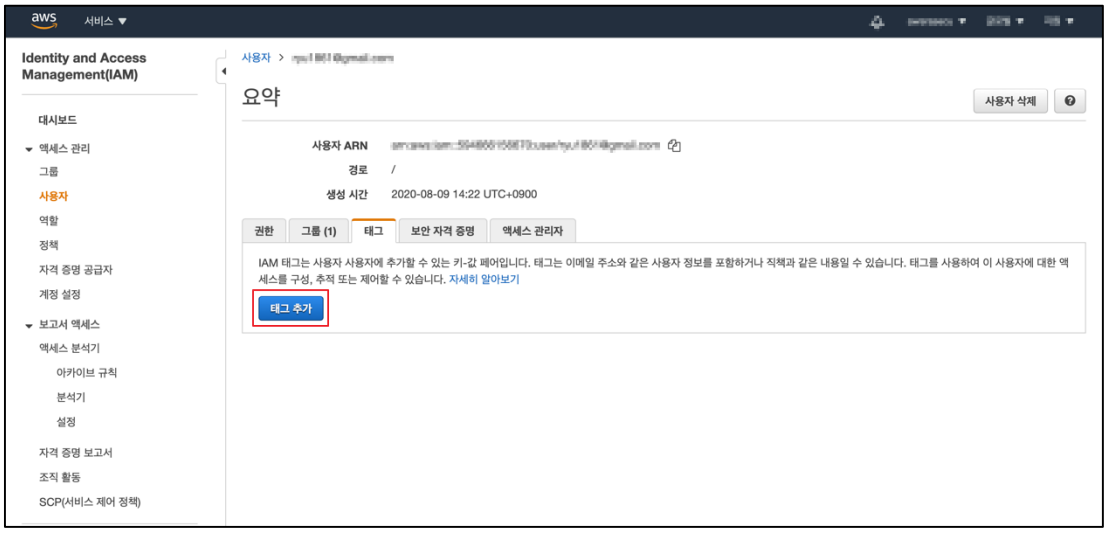




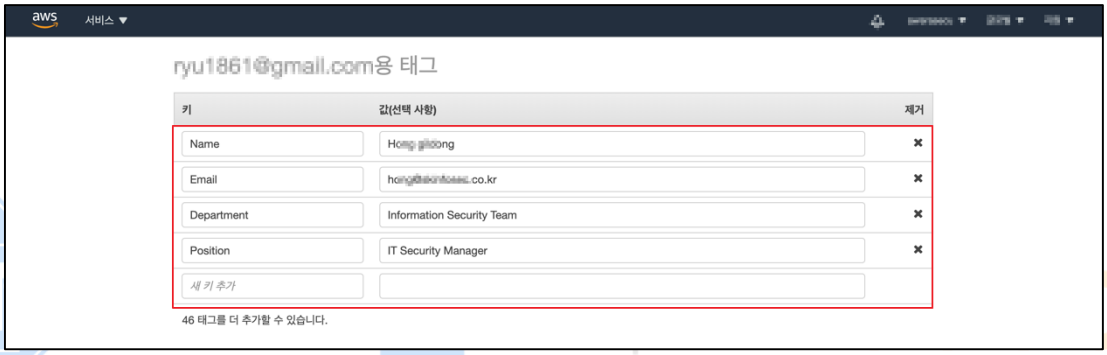
진단 기준	**양호기준** : 단일 사용자가 다수의 IAM 계정을 사용하지 않을 경우 **취약기준** : 단일 사용자가 다수의 IAM 계정을 사용할 경우
비고	

1.3 IAM 사용자 계정 식별 관리

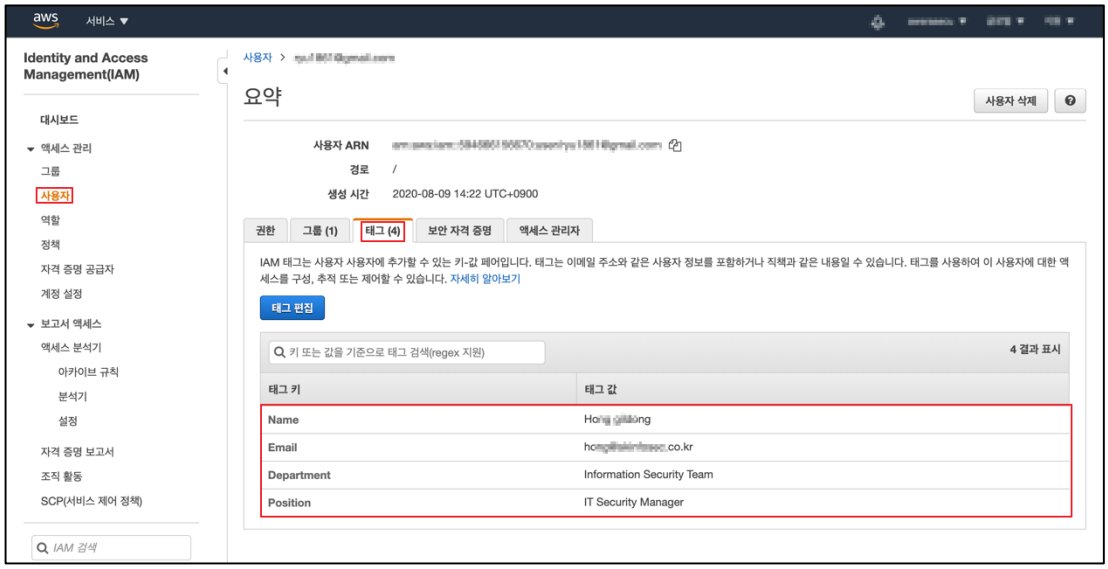
분류	계정관리	중요도	중
항목명	사용자 계정 식별 관리		
항목 설명	IAM 사용자 계정에는 태그를 추가할 수 있으며, 해당 태그 설정은 사용자를 표현하는 정보 및 직책의 내용을 포함할 수 있습니다. 이러한 태그 사용은 IAM 사용자에 대한 액세스 구성, 추정 또는 제어가 가능합니다.		
설정 방법	**가. IAM 사용자 정보 태그 설정 방법** 1) AWS 주요 서비스 중 "IAM" 클릭  2) IAM "사용자" 클릭 및 계정 리스트 확인  3) IAM 사용자 태그 확인 및 태그 추가 버튼 클릭		



4) IAM 사용자 태그 입력 칸 내 계정 정보 입력 후 저장



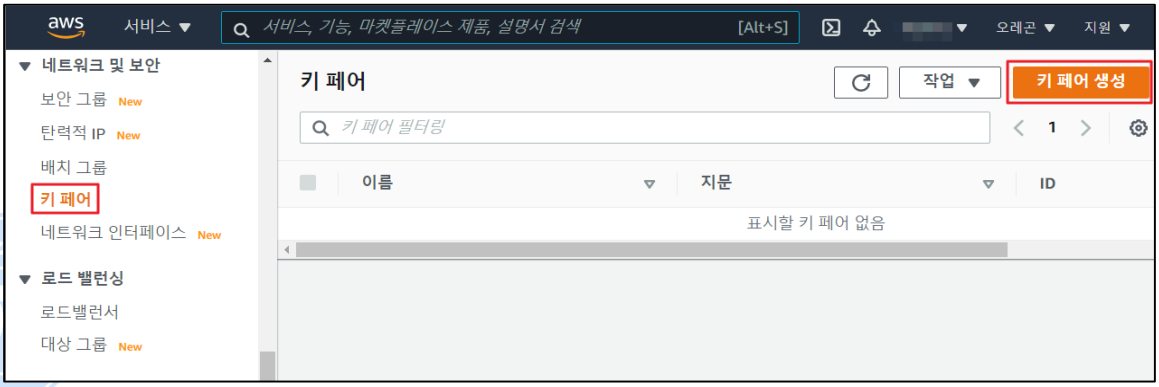
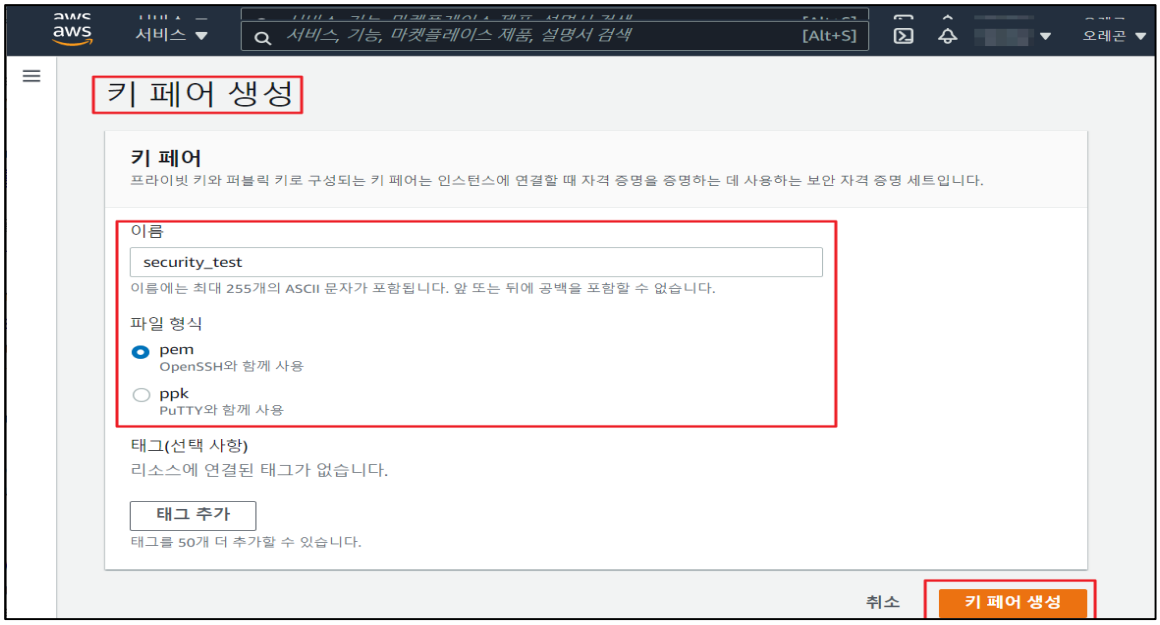
5) IAM 사용자 태그 계정정보 확인

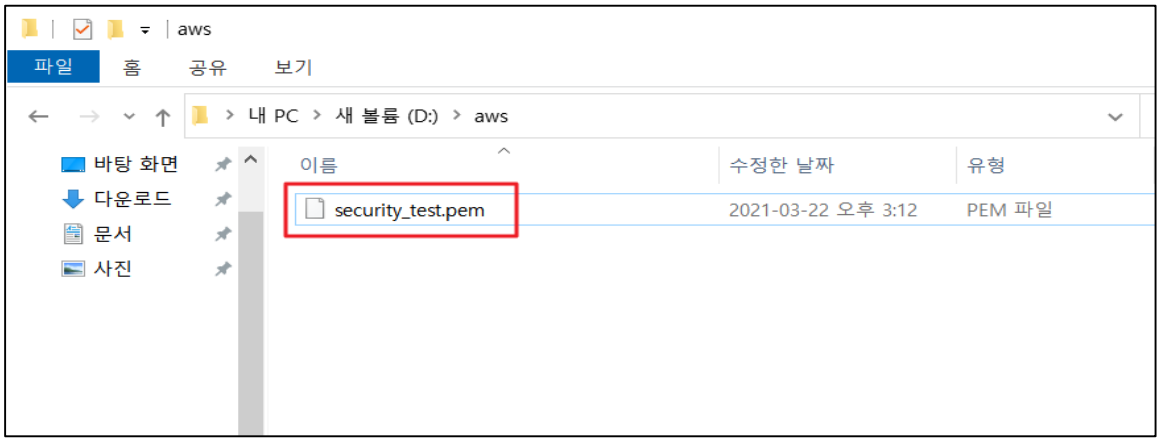


진단 기준	**양호기준** : 사용자 정보(이름, 이메일, 부서 등)가 IAM 사용자 태그에 설정되어 있을 경우

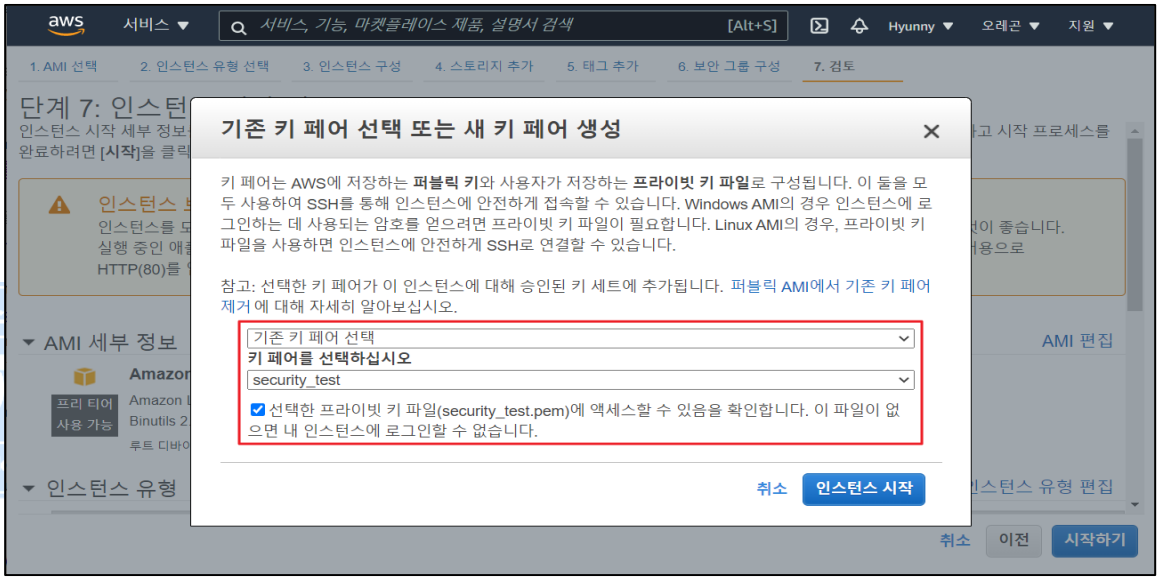
	취약기준 : 사용자 정보(이름, 이메일, 부서 등)가 IAM 사용자 태그에 설정되어 있지 않을 경우
비고	

1.4 Key Pair 접근 관리

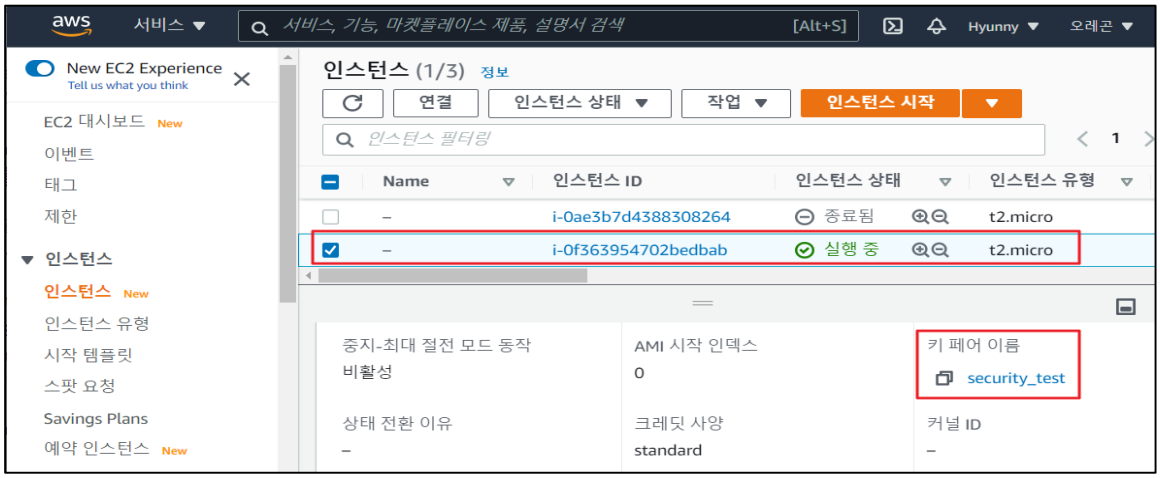
분류	계정관리	중요도	상
항목명	Key Pair 접근 관리		
항목 설명	EC2는 키(Key)를 이용한 암호화 기법을 제공합니다. 해당 기법은 퍼블릭/프라이빗 키를 통해 각각 데이터의 암호화 및 해독을하는 방식으로 여기에 사용되는 키를 '키페어' 라고 하며, 해당 암호화 기법을 사용할 시 EC2의 보안성을 향상시킬 수 있으므로 EC2 인스턴스 생성 시 Key Pair 등록을 권장합니다. 또한, Amazone EC2에 사용되는 키는 '2048비트 SSH-2 RSA 키'이며, 키 페어는 리전당 최대 5천 개까지 보유할 수 있습니다.		
설정 방법	**가. 키 생성 및 등록 방법** 1) 콘솔을 통한 키 생성: 네트워크 및 보안 → 키 페어 → 키 페어 생성  2) 키 페어 생성  3) 생성된 키 페어 파일을 쉽게 유추 및 접근할 수 없는 공간에 보관		



4) 인스턴스 생성 시 생성된 키 페어 등록

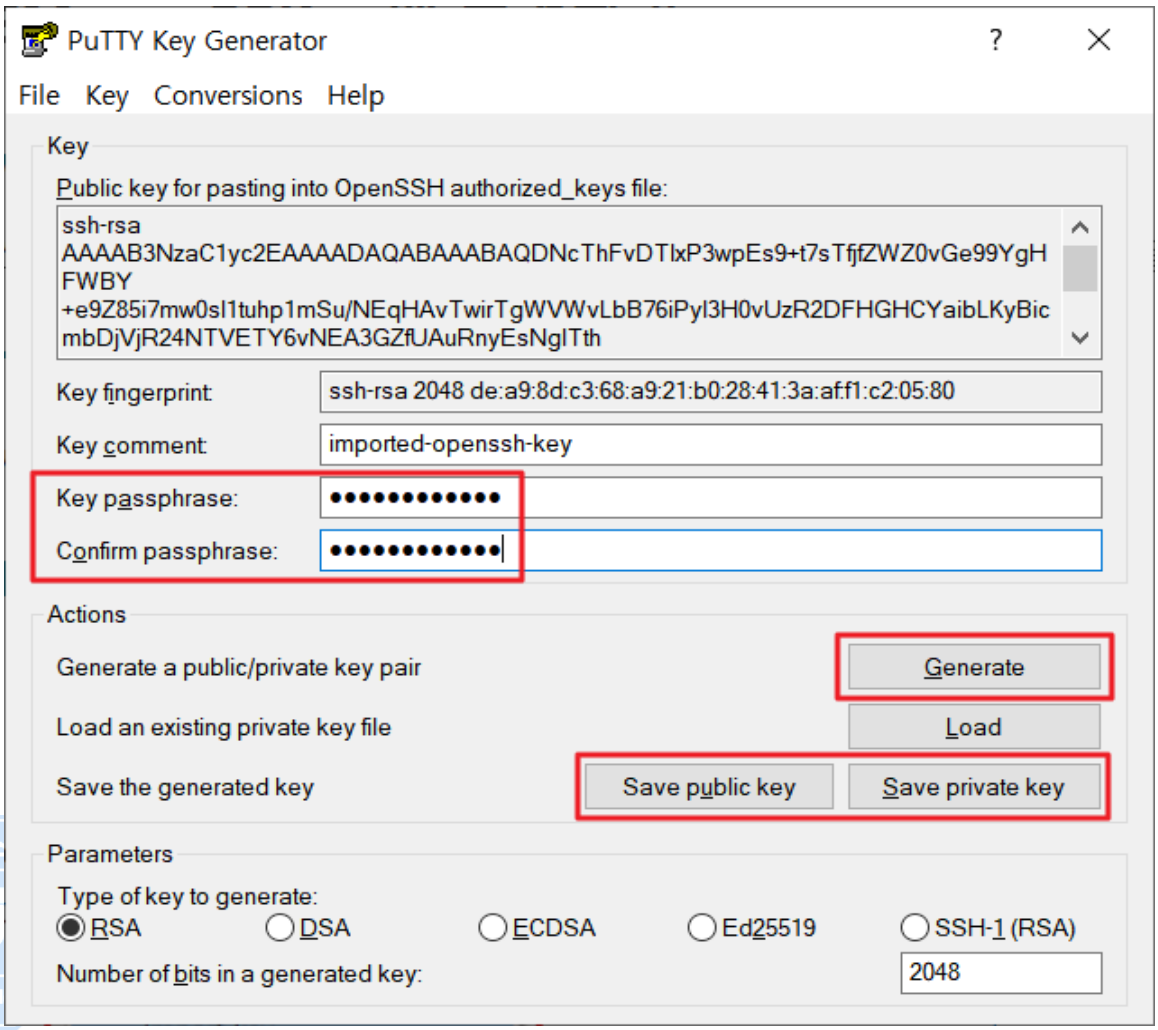


5) 인스턴트 생성 완료 시 키 페어 정상 등록여부 확인

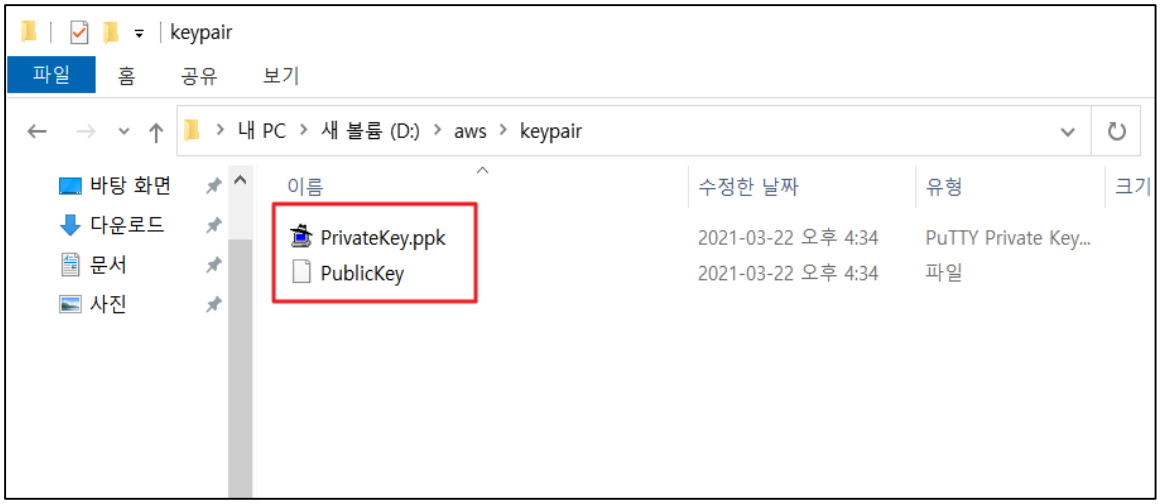


6) PuTTY-Gen을 통한 키 생성

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

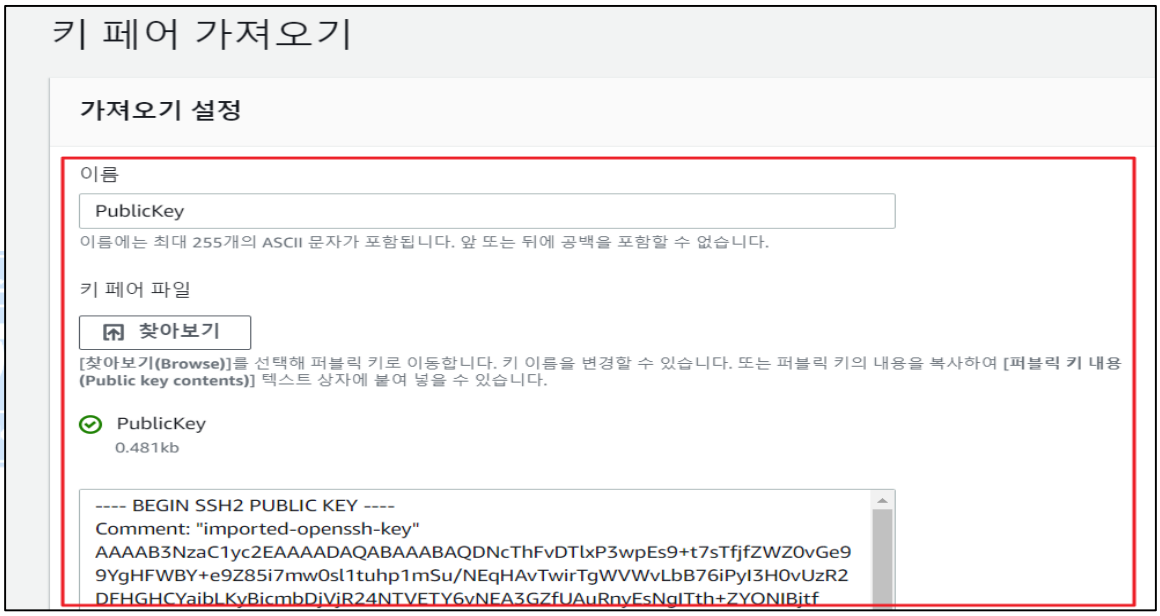


7) 생성된 키 페어 파일을 쉽게 유추 및 접근할 수 없는 공간에 보관

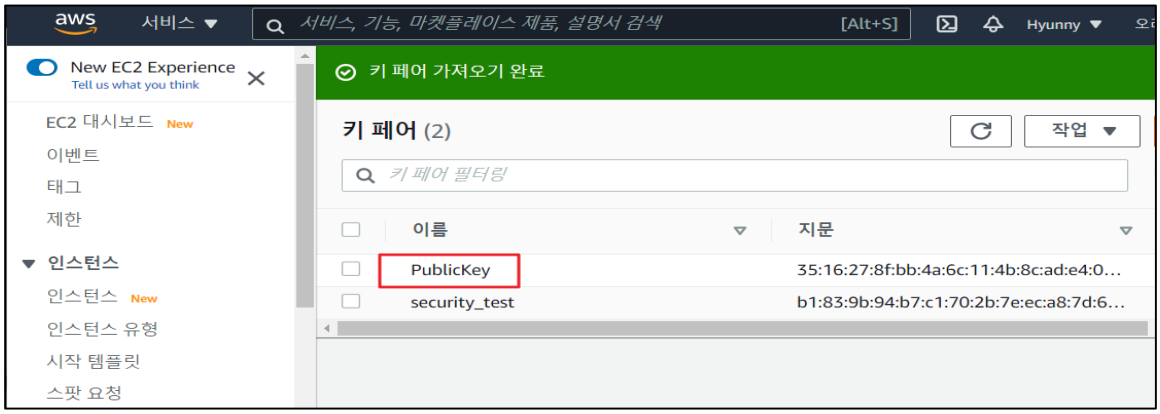


8) 생성된 키 콘솔로 가져오기: 네트워크 및 보안 → 키페어 → 키 페어 가져오기

9) 가져오기 설정



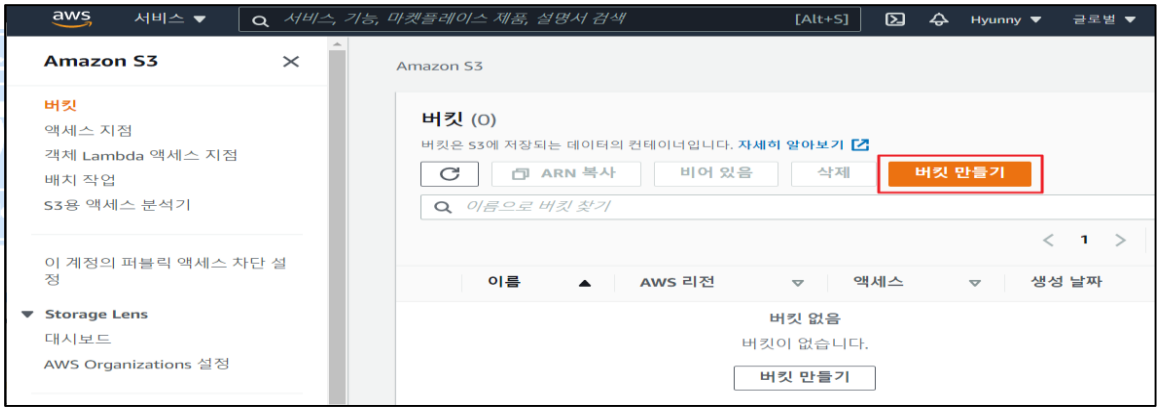
10) 생성된 키가 콘솔에 정상적으로 등록되었는지 확인

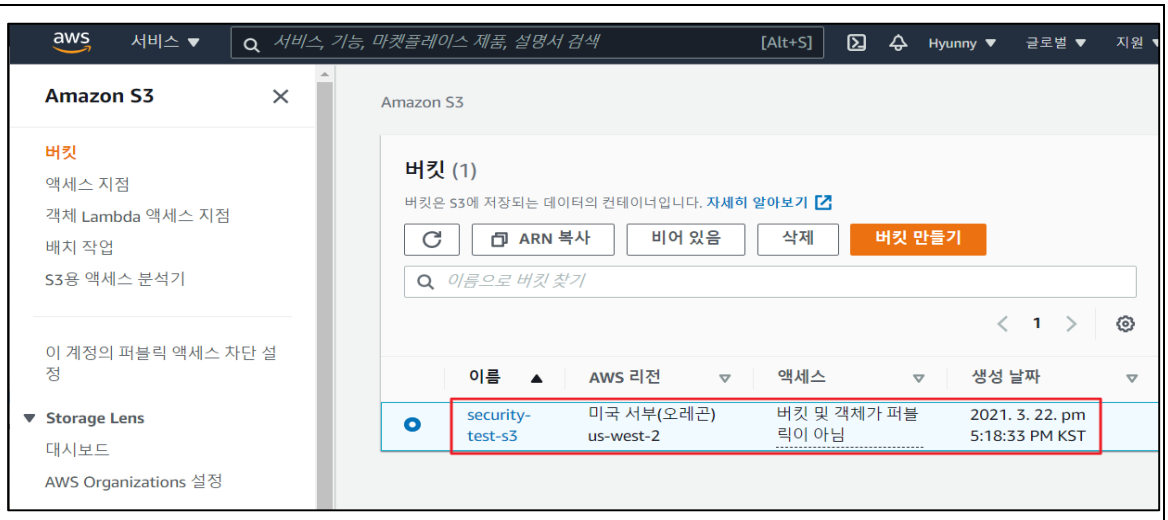


진단 기준	**양호기준** : Key Pair(PEM)를 통해 EC2 인스턴스에 접근할 경우

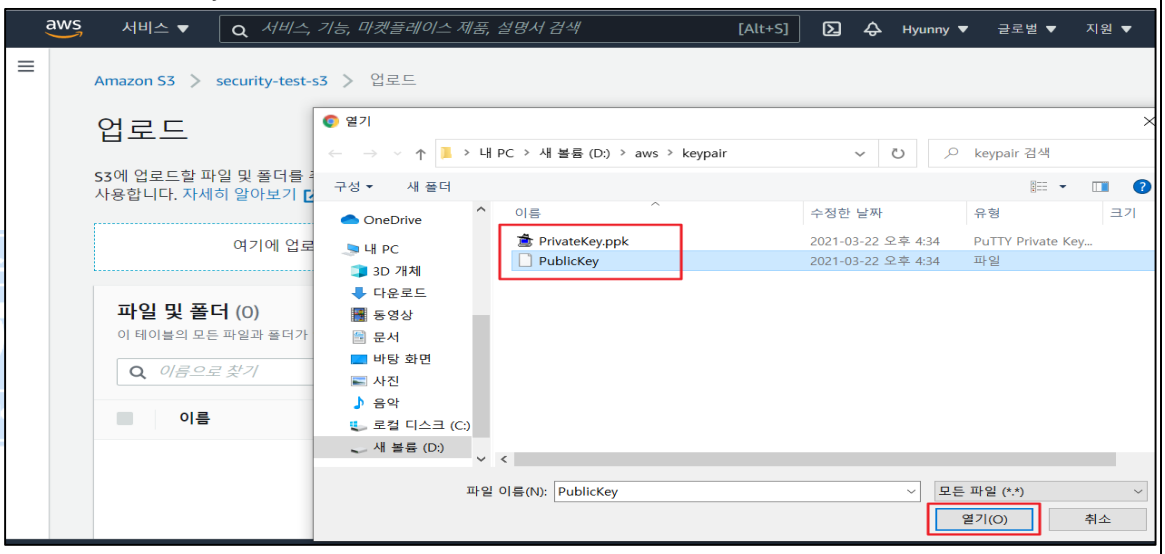
	취약기준 : Key Pair(PEM)가 아닌 일반 패스워드로 EC2 인스턴스에 접근할 경우
비고	

1.5 Key Pair 보관 관리

분류	계정관리	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 해독을하는 방식으로 여기에 사용되는 키를 '키페어' 라고 하며, 해당 암호화 기법을 사용할 시 EC2의 보안성을 향상시킬 수 있으므로 EC2 인스턴스 생성 시 Key Pair 등록을 권장합니다. 또한, Amazone EC2에 사용되는 키는 '2048비트 SSH-2 RSA 키'이며, 키 페어는 리전당 최대 5천 개까지 보유할 수 있습니다. **※ Key Pair 는 타 사용자가 확인이 가능한 공개된 위치에 보관하게 될 경우 EC2 Instance 에 무단으로 접근이 가능해지므로 비인가자가 쉽게 유추 및 접근이 불가능한 장소에 보관해야 합니다.**		
설정 방법	**가. S3 버킷 내 키 페어 관리하기** 1) 버킷 접근  2) 버킷 생성하기  3) 생성된 버킷 확인		

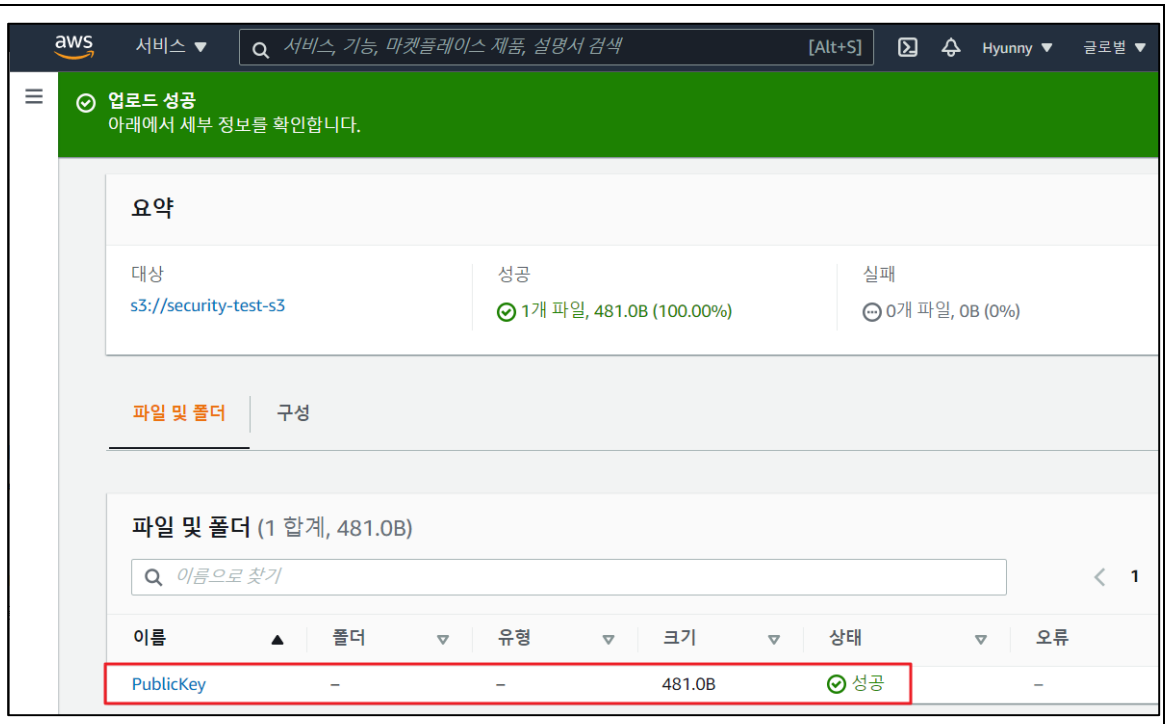


4) S3 버킷 내 KeyPair 업로드



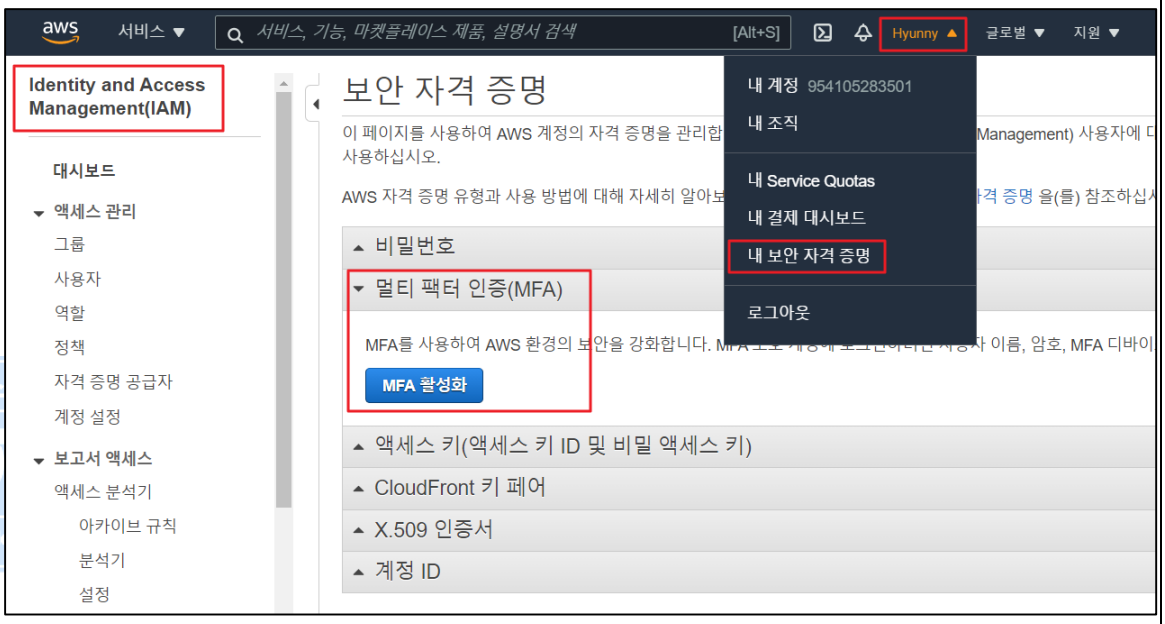
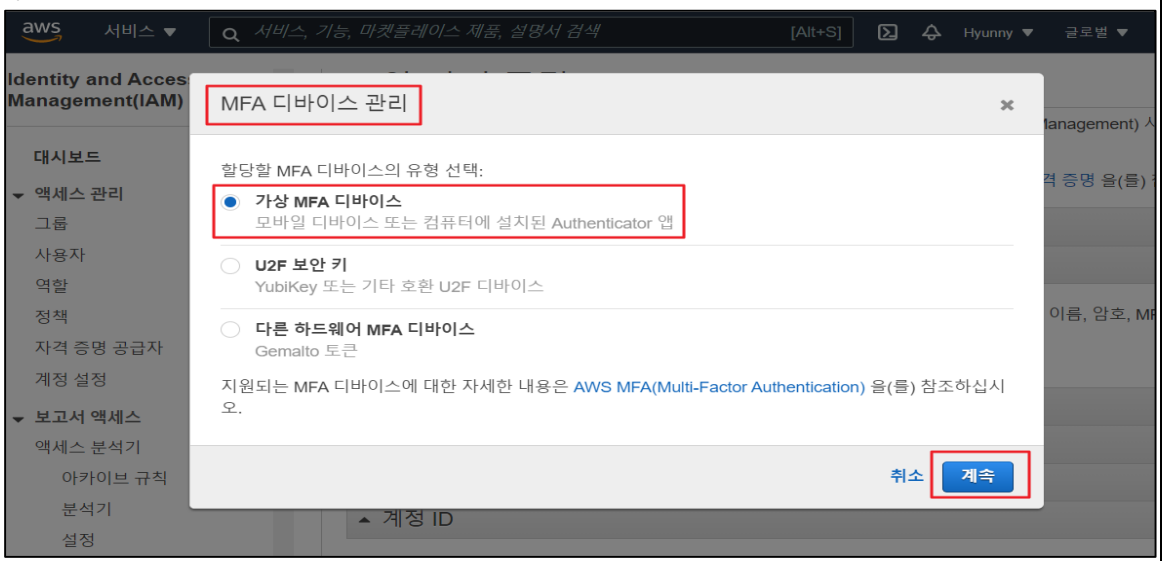
5) 업로드 된 KeyPair 확인

6) Key Pair 보관 확인(Private S3 버킷)

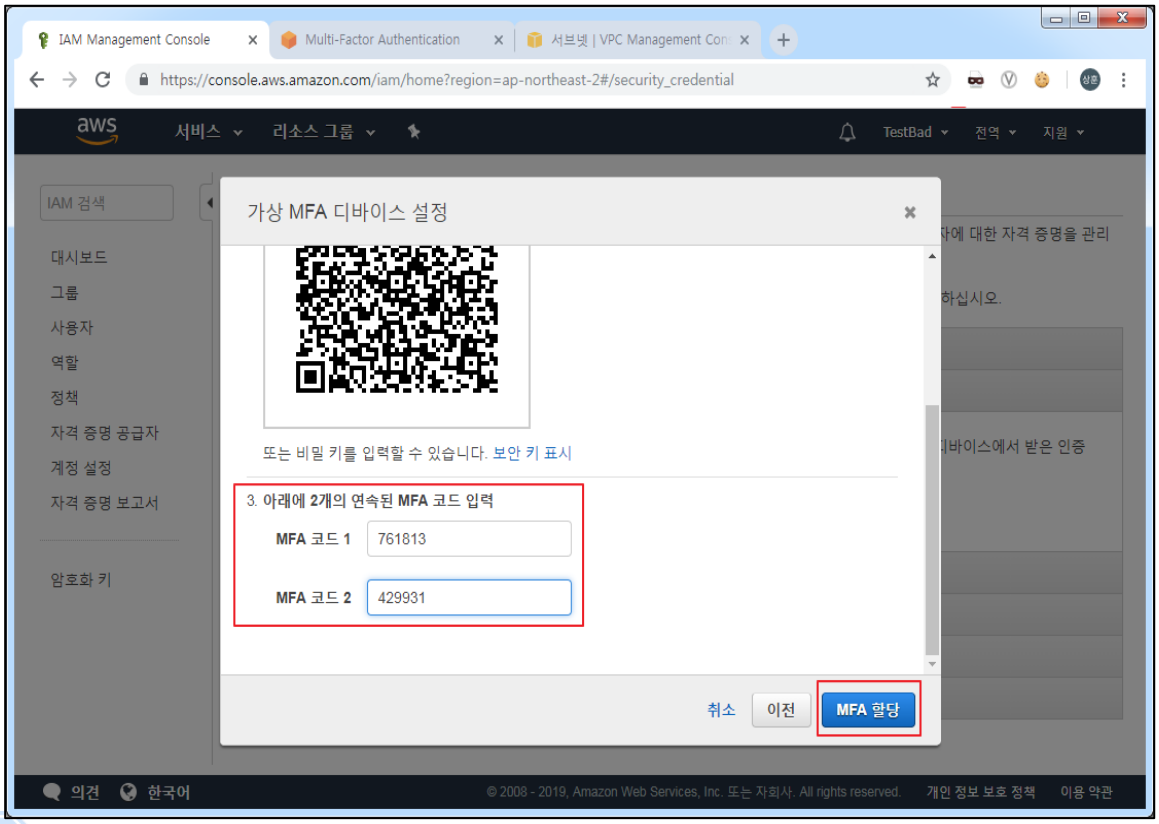
<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단
기준</td><td>양호기준
: Key Pair(PEM) File의 보관 위치가 쉽게 유추할 수 없는 공간에 보관되어 있을 경우

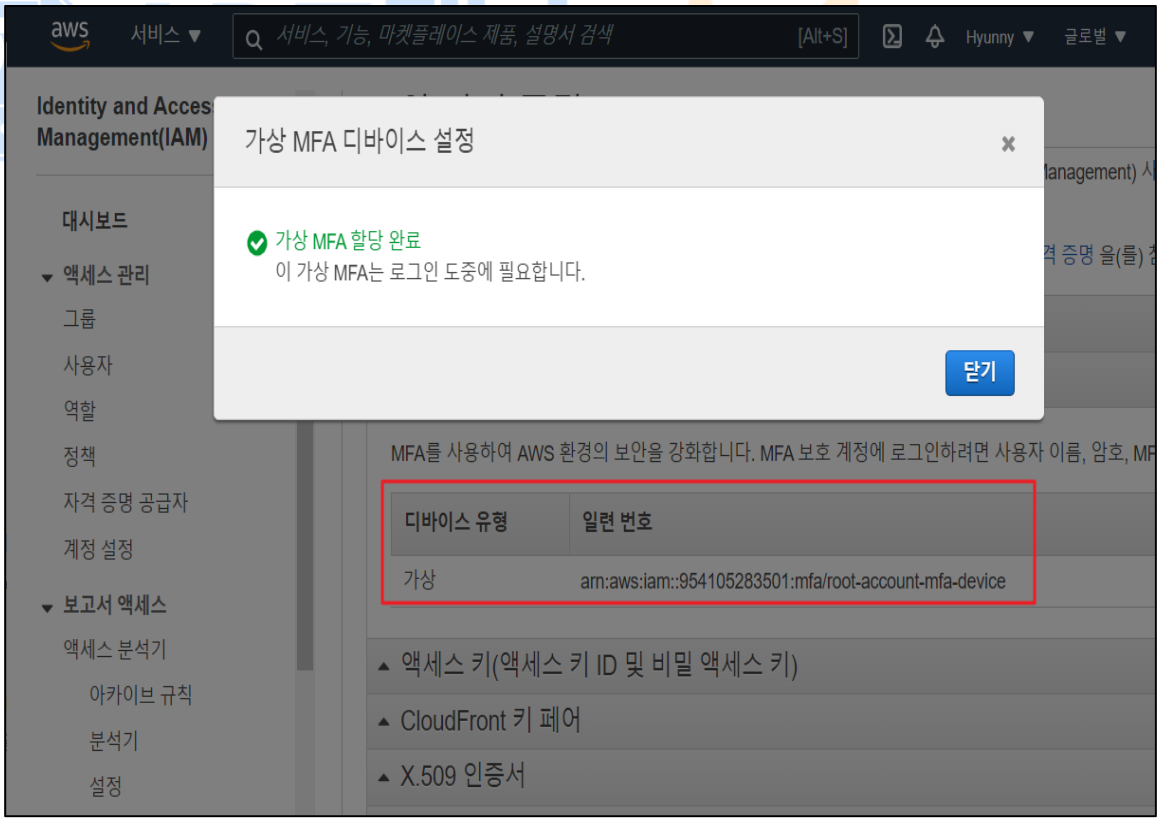
취약기준
: Key Pair(PEM) File의 보관 위치가 다수 접근이 가능한 공용공간(Public S3, EC2 “root(/)” 디렉토리등)에 보관되어 있을 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

1.6 MFA (Multi-Factor Authentication) 설정

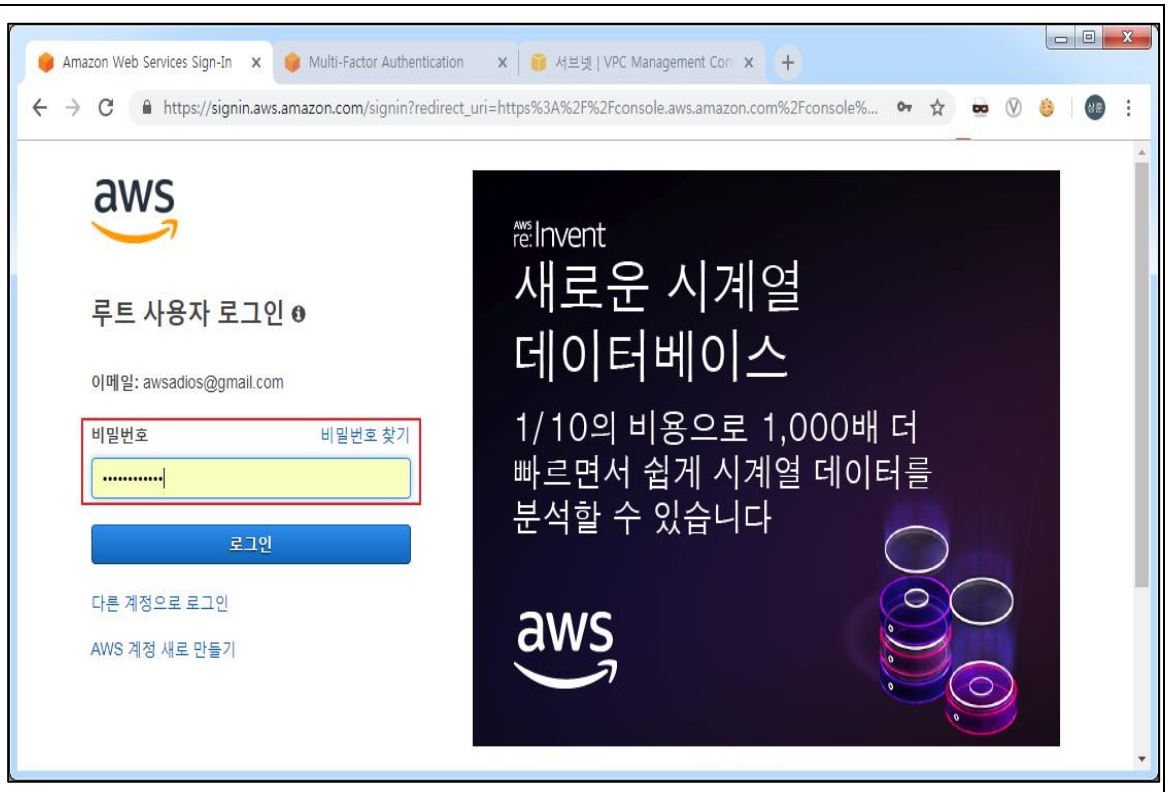
분류	계정관리	중요도	중
항목명	MFA (Multi-Factor Authentication) 설정		
항목 설명	AWS Multi-Factor Authentication(MFA)은 사용자 이름과 암호 외에 보안을 한층 더 강화할 수 있는 방법으로 MFA를 활성화하면 사용자가 AWS 웹 사이트에 로그인할 때 사용자 이름과 암호뿐만 아니라 AWS MFA 디바이스의 인증 응답을 입력하라는 메시지가 표시됩니다. 이러한 다중 요소를 통해 AWS 계정 설정 및 리소스에 대한 보안을 높일 수 있습니다.		
설정 방법	**가. MFA 인증 설정 및 확인** 1) IAM 메인 → 우측상단 계정 → 내 보안 자격 증명 → 멀티 팩터 인증 → MFA 활성화  3) MFA 디바이스 관리 → 가상 MFA 디바이스선택 → 계속  4) Google OTP 어플 설치 → '+' 버튼 → 바코드 스캔 → 나타난 QR코드를 어플에서 스캔		

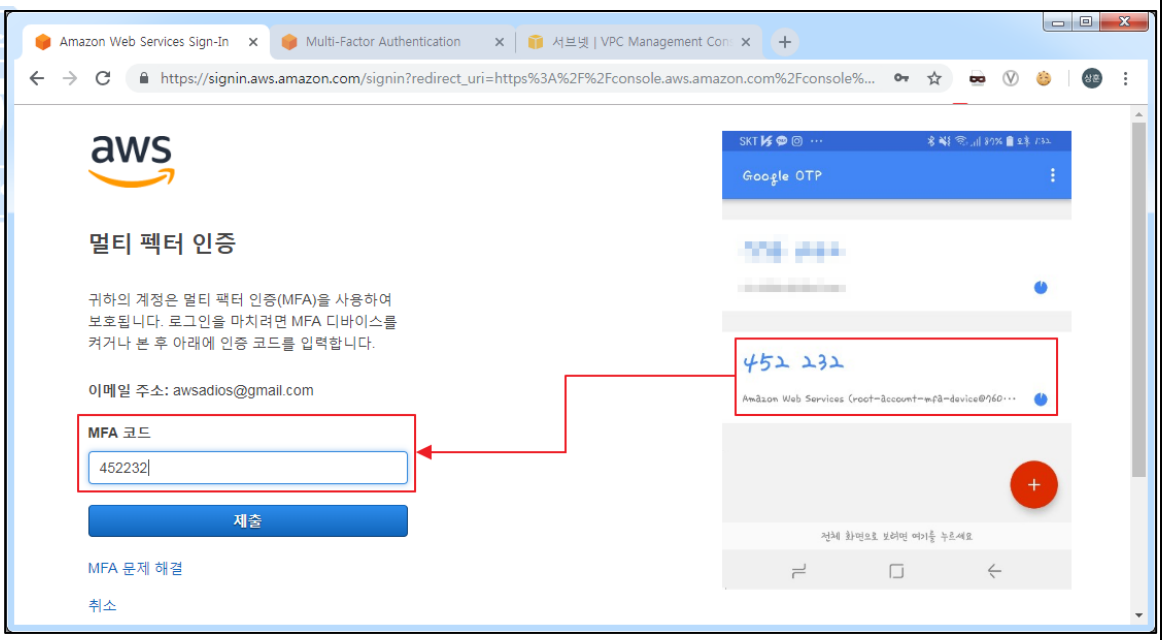
5) 스캔 후 나타난 숫자 MFA 코드 1 입력 → 재생성된 숫자 MFA 코드 2 입력

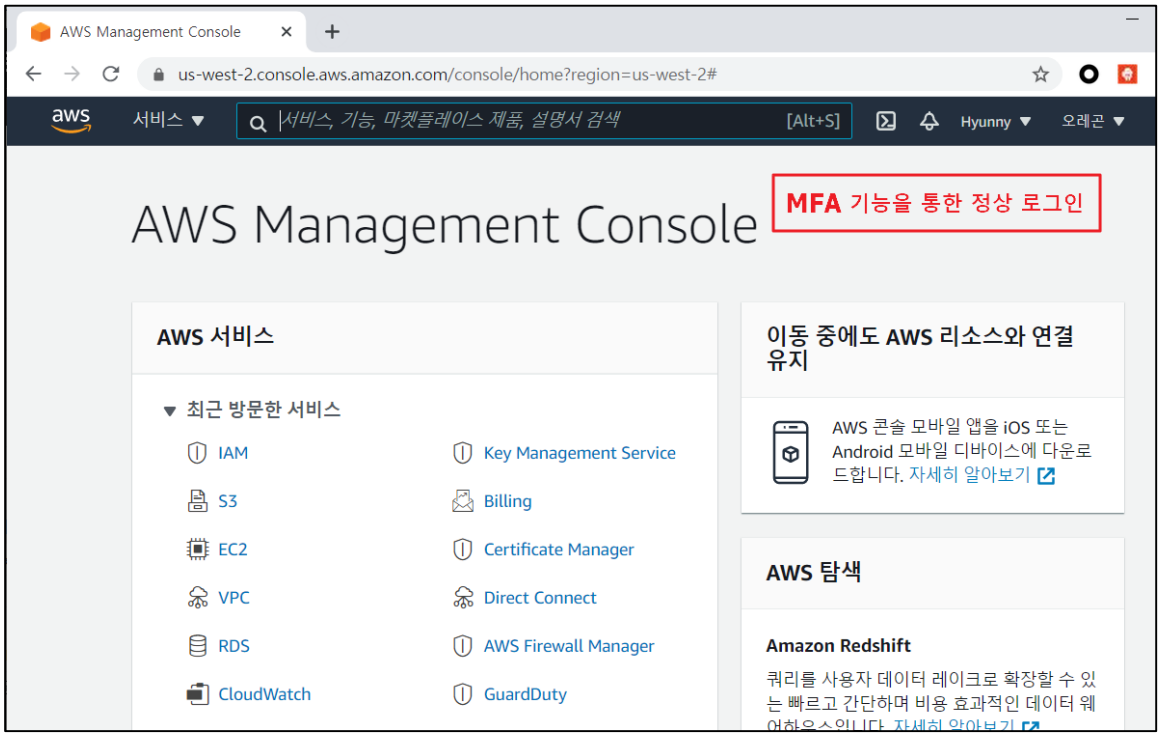




6) 로그인 시 비밀번호 입력 → Google OTP 번호 입력 후 로그인 시도





<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단 기준</td><td>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</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

1.7 AWS 계정 패스워드 정책 관리

분류	계정관리	중요도	중
항목명	AWS 계정 패스워드 정책 관리		

항목 설명

AWS Root Account 계정 및 IAM 사용자 계정의 암호 설정 시 일반적으로 유추하기 쉬운 암호를 설정하는 경우 비인가된 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>

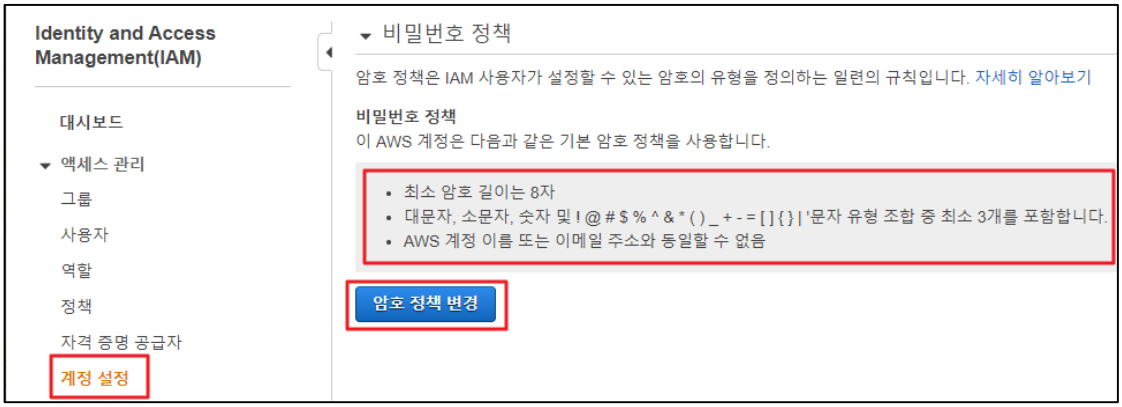
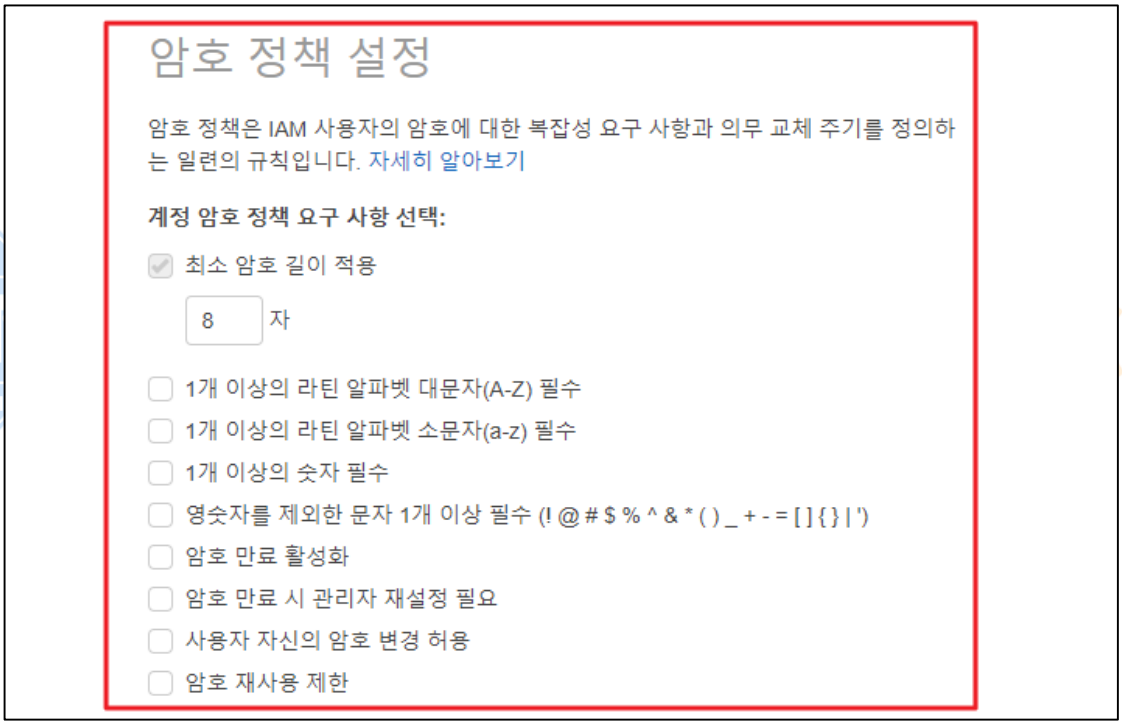
1) Null 패스워드 사용 금지
2) 문자 또는 숫자만으로 구성 금지
3) 사용자 ID와 동일한 패스워드 금지
4) 연속적인 문자 및 숫자 사용 금지
5) 주기성 패스워드 사용 금지
6) 전화번호, 생일, 게정명, hostname과 같이 추측하기 쉬운 패스워드 사용 금지

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

설정 방법	**가. IAM 계정 비밀번호 정책 확인** 1) 계정 설정 확인  2) 암호 정책 설정 확인 
진단 기준	**양호기준** : Admin Console 및 IAM 계정의 패스워드가 복잡성 기준을 준수하였을 경우 **취약기준** : Admin Console 및 IAM 계정의 패스워드가 복잡성 기준을 준수하지 않을 경우
비고	

2. 권한관리

2.1 인스턴스 보안 정책 관리

분류	권한관리	중요도	상
항목명	인스턴스 보안 정책 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) 인스턴스 관리형 정책

- 인스턴스 관리형 정책은 AWS에서 생성 및 관리하는 정책으로 여러 가지 직무 및 일반 사용 사례에서 권한을 제공할 목적으로 설계된 정책입니다.

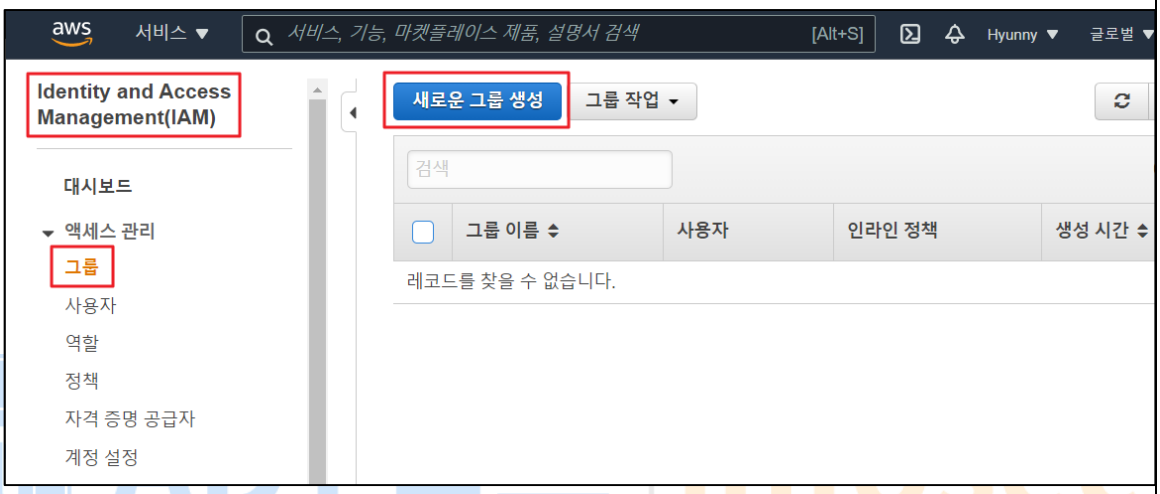
※ 인스턴스 서비스 내 FULL ACCESS 등과 같이 중요도가 높은 AWS 관리형 정책은 EC2 서비스 관리/운영자 및 관련 담당자 외에 다른 IAM 계정에 아래와 같은 권한 할당이 되지 않도록 해야합니다.

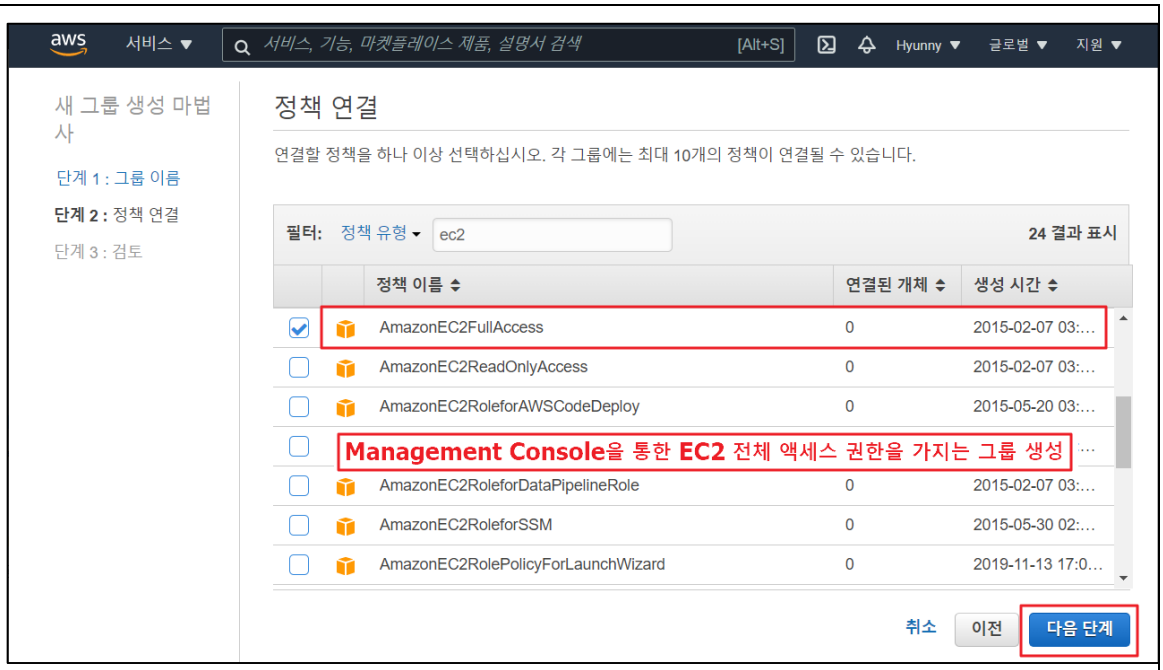
2) 인스턴스 역할별 권한 관리 (예시)

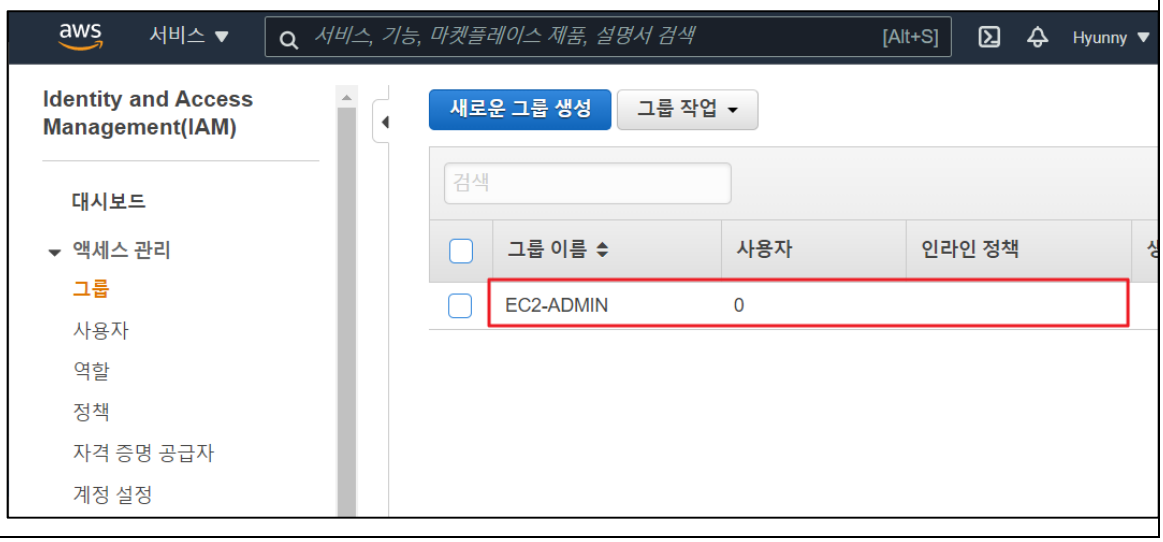
역할	관리형 정책명
AWS Root 관리자	* ALL FULL ACCESS *, AdministratorAccess
Infra 운영/관리자 및 담당자	Amazon EC2 / ECR / ECS *FullAccess*
Application 운영/관리자 및 담당자	Amazon EC2 / ECR / ECS *ReadOnlyAccess* / *Poweruser* / *Role* / CloudWatchActionsEC2Access
개발 관리자 및 담당자	Amazon EC2 / ECR / ECS *ReadOnlyAccess* / *Poweruser* / *Role* / CloudWatchActionsEC2Access
재무 / 비용 관리자 및 담당자	Amazon EC2 / ECR / ECS 중요도 "하" Access

3) IAM 관리형 정책 권한 관리 List (예시)

역할	계정 관리 (그룹 및 계정명)	AWS 관리형 정책	취약 유/무
AWS Root 관리자	Ex)EC2_Admin (admin_accout)	Ex) EC2_Admin (AmazonEC2FullAcces)	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

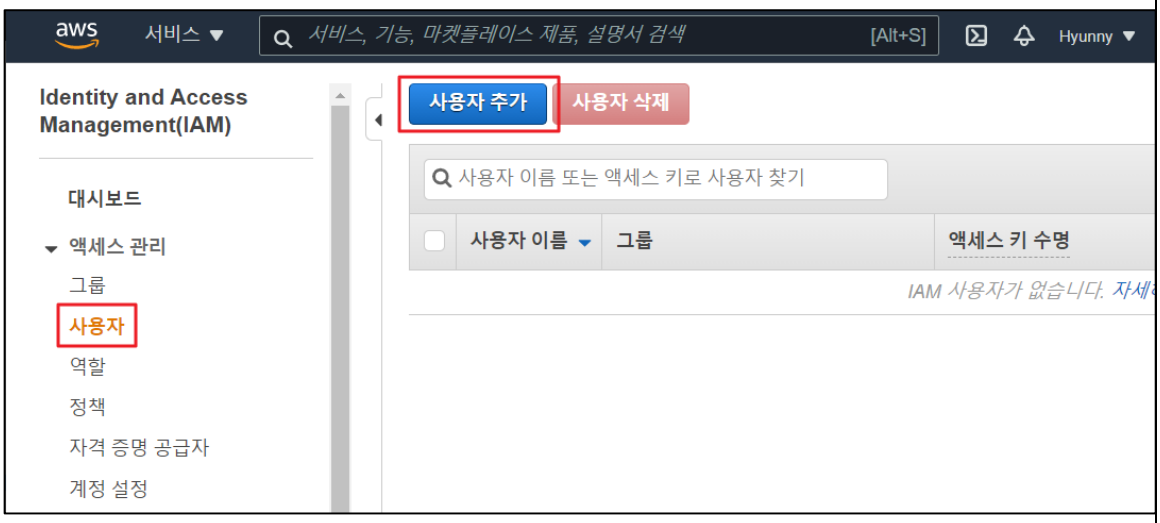
설정 방법	**가. 인스턴스 IAM 관리자/운영자 권한 그룹 생성 및 사용자 추가** - 인스턴스 서비스의 운영/관리를 위한 IAM 그룹 생성 및 사용자 추가 **1) IAM 그룹 생성** [IAM] → [그룹] → [새로운 그룹 생성] → [그룹 이름 설정] → [IAM 계정 권한에 맞는 정책 연결] → [그룹 생성] **※ 인스턴스 운영/관리에 필요한 IAM FULL Access 등의 권한과 같이 중요도가 높은 권한은 Infra 운영/관리자 및 담당자에게만 정책이 되도록 해야하며 최소한의 계정 수가 유지되야함**  

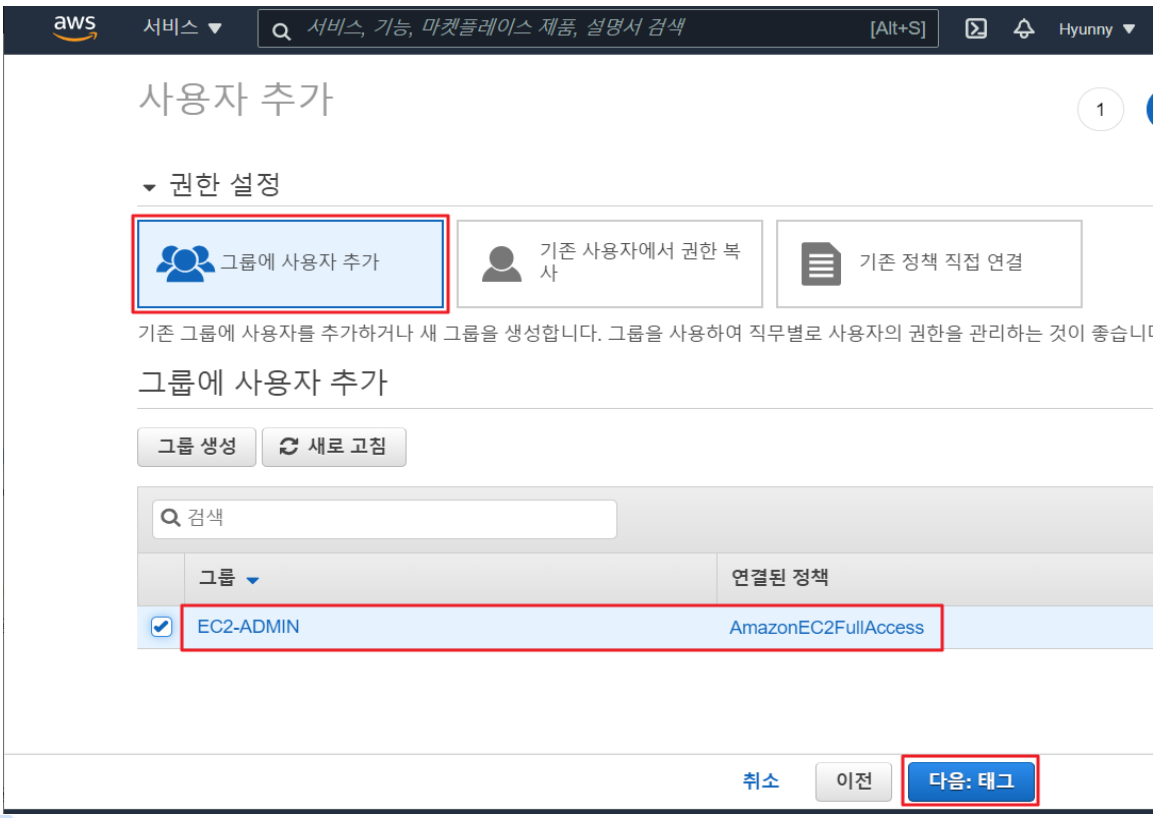


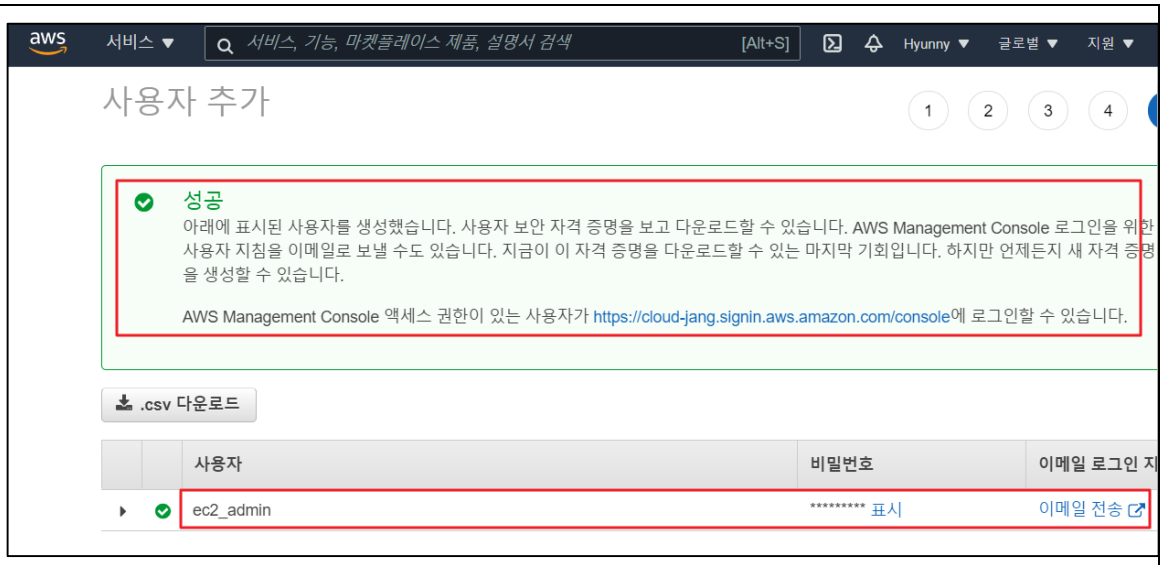


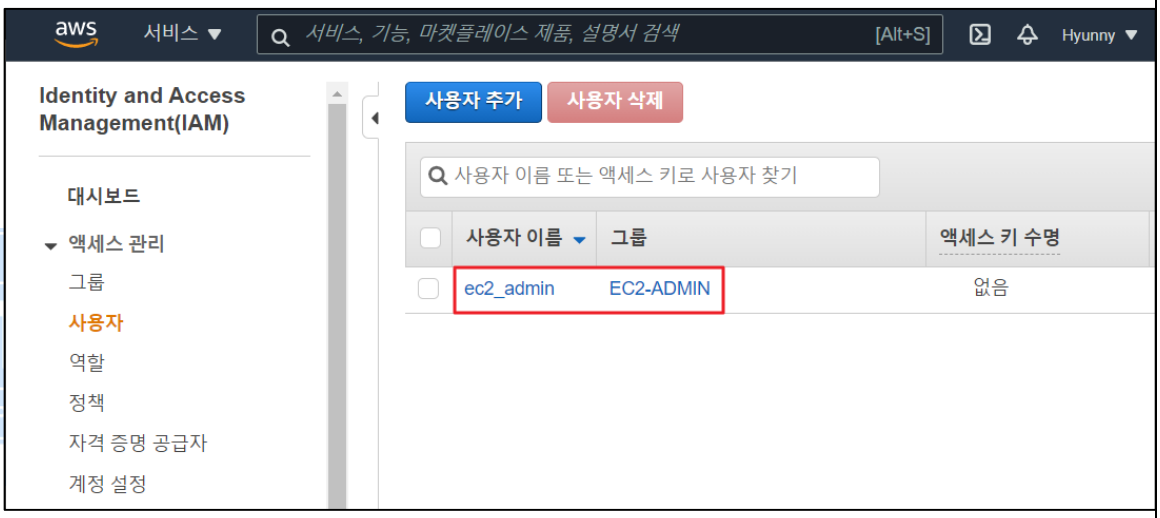
2) IAM 사용자 생성 및 그룹 지정

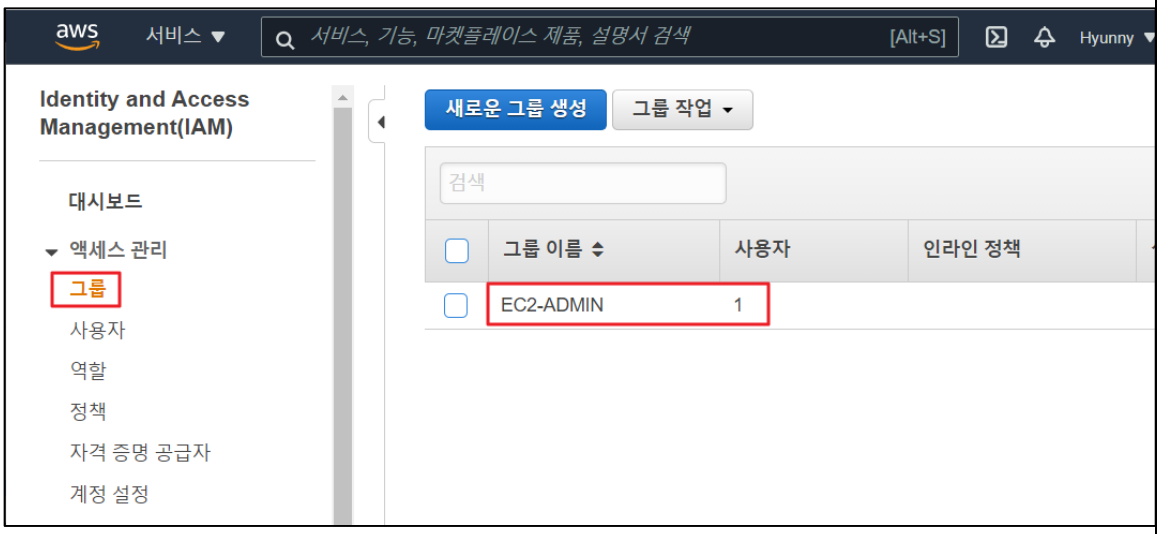
[IAM] → [사용자] → [사용자 추가] → [사용자 세부정보 지정] → [권한 설정 (그룹에 사용자를 추가)] → [사용자 만들기]

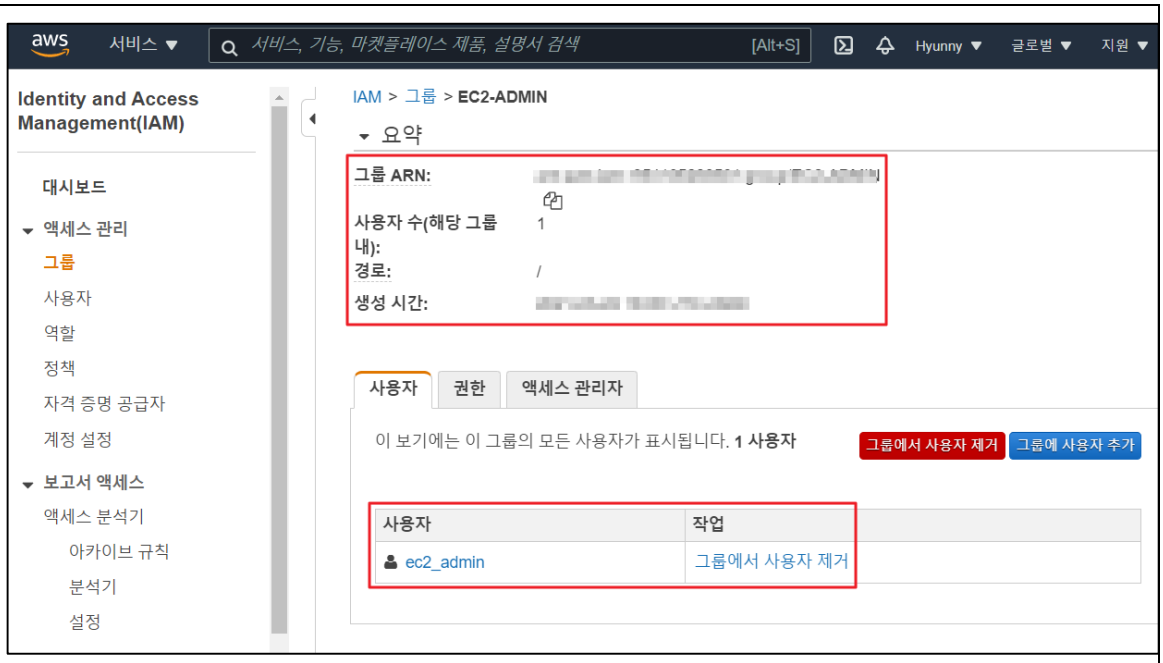










<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단 기준</td><td>양호기준
: 인스턴스 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있을 경우

취약기준
: 인스턴스 서비스 IAM 사용 권한이 각각 서비스 역할에 맞지 않게 설정되어 있을 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

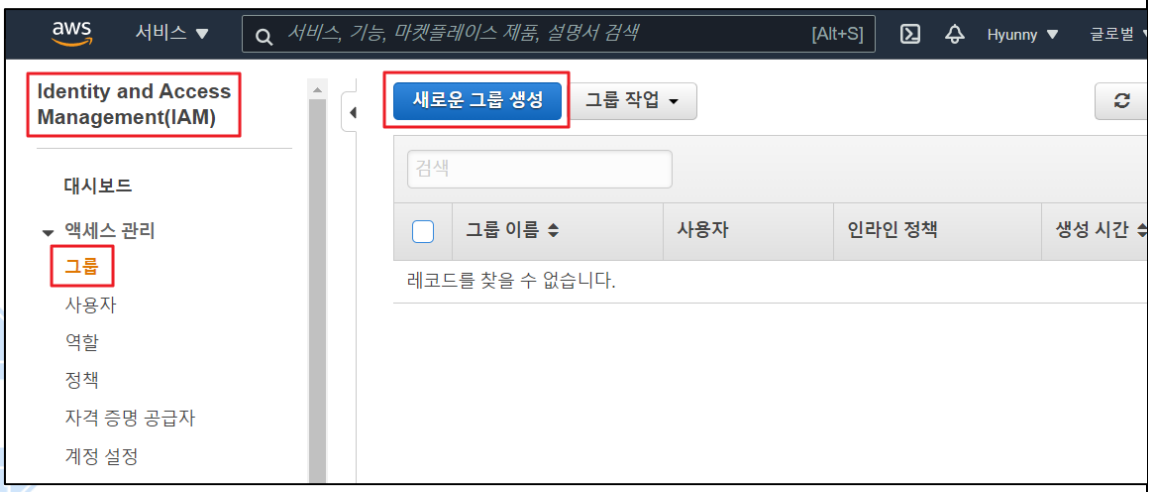
2.2 RDS 보안 정책 관리

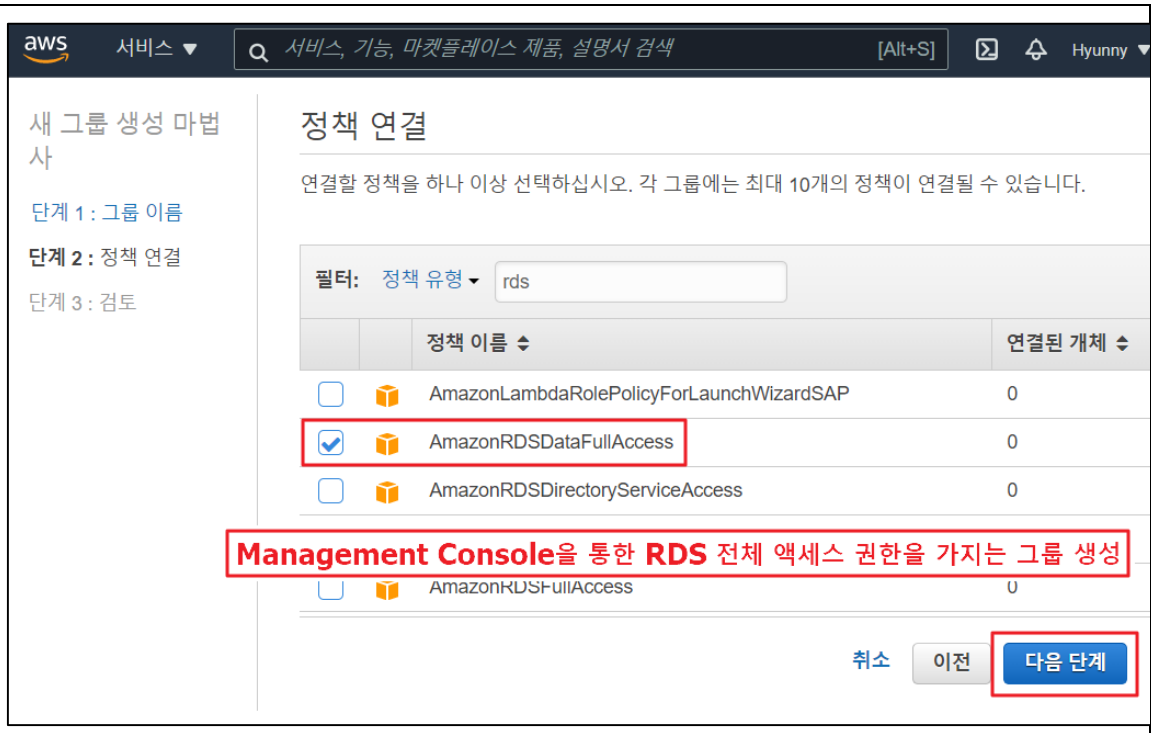
<table>
<tr><td>분류</td><td>권한관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">RDS 보안 정책 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">
모든 AWS 리소스는 AWS 계정의 소유이고, 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(즉, 사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다.

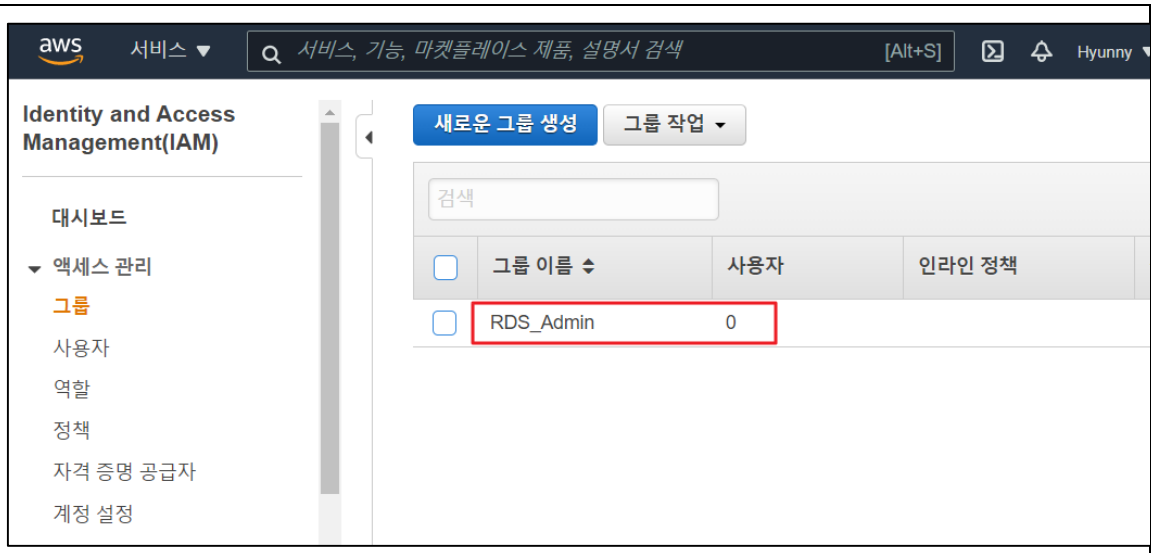
1) RDS 관리형 정책
- RDS 관리형 정책은 AWS에서 생성 및 관리하는 정책으로 여러 가지 직무 및 일반 사용 사례에서 권한을 제공할 목적으로 설계된 정책입니다.

※ RDS 서비스 내 "AmazonRDSFullAccess" 등과 같이 중요도가 높은 AWS 관리형 정책은 RDS 서비스 관리/운영자 및 관련 담당자 외에 다른 IAM 계정에 아래와 같은 권한 할당이 되지 않도록 해야합니다.

2) RDS 역할별 권한 관리 (예시)
<table>
<tr><th>역할</th><th>관리형 정책명</th></tr>
<tr><td>AWS Root 관리자</td><td>* ALL FULL ACCESS *, AdministratorAccess</td></tr>
<tr><td>Infra 운영/관리자 및 담당자</td><td>Amazon RDS *FullAccess*</td></tr>
<tr><td>Application 운영/관리자 및 담당자</td><td>Amazon RDS / AmazonRDSDataFullAccess / *ReadOnlyAccess* / *Role* / 중요도 "하" Access</td></tr>
<tr><td>개발 관리자 및 담당자</td><td>Amazon RDS / AmazonRDSDataFullAccess / *ReadOnlyAccess* / *Role* / 중요도 "하" Access</td></tr>
<tr><td>재무 / 비용 관리자 및 담당자</td><td>Amazon RDS 중요도 "하" Access</td></tr>
</table>
3) IAM 관리형 정책 권한 관리 List (예시)
<table>
<tr><th>역할</th><th>계정 관리
(그룹 및 계정명)</th><th>AWS 관리형 정책</th><th>취약
유/무</th></tr>
<tr><td>AWS Root 관리자</td><td>Ex)RDS_Admin
(admin_accout)</td><td>Ex) RDS_Admin
(AmazonRDSFullAccess)</td><td></td></tr>
<tr><td>Infra 운영/관리자 및 담당자</td><td></td><td></td><td></td></tr>
<tr><td>Application 운영/관리자 및 담당자</td><td></td><td></td><td></td></tr>
<tr><td>개발 관리자 및 담당자</td><td></td><td></td><td></td></tr>
<tr><td>재무 / 비용 관리자 및 담당자</td><td></td><td></td><td></td></tr>
</table>
</td></tr>
</table>

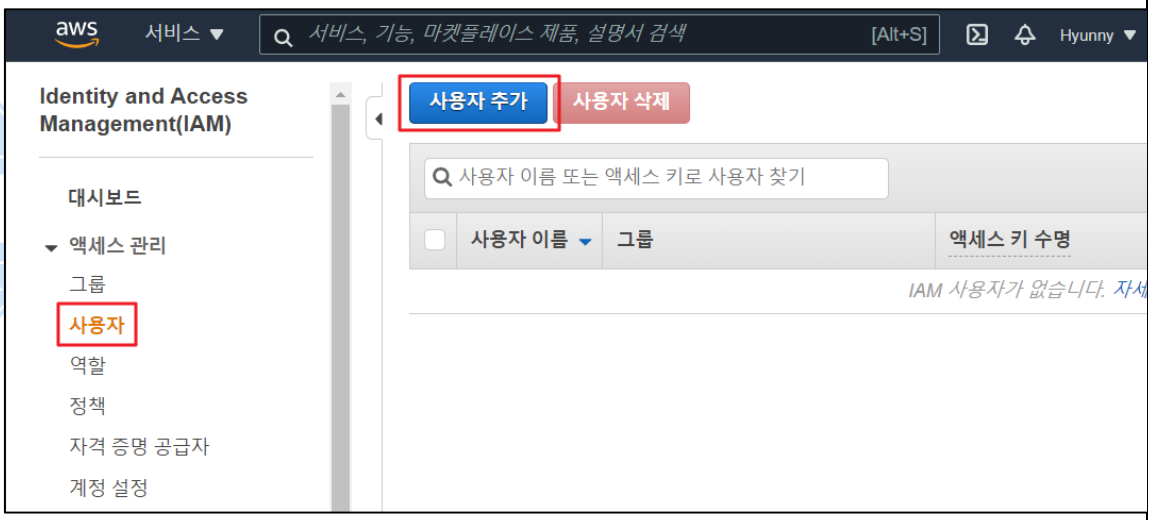
설정 방법	**가. RDS IAM 관리자/운영자 권한 그룹 생성 및 사용자 추가** - RDS 서비스의 운영/관리를 위한 IAM 그룹 생성 및 사용자 추가 **1) IAM 그룹 생성** [IAM] → [그룹] → [새로운 그룹 생성] → [그룹 이름 설정] → [IAM 계정 권한에 맞는 정책 연결] → [그룹 생성] **※ RDS 운영/관리에 필요한 IAM FULL Access 등의 권한과 같이 중요도가 높은 권한은 Infra 운영/관리자 및 담당자에게만 정책이 되도록 해야하며 최소한의 계정 수가 유지되야함**  

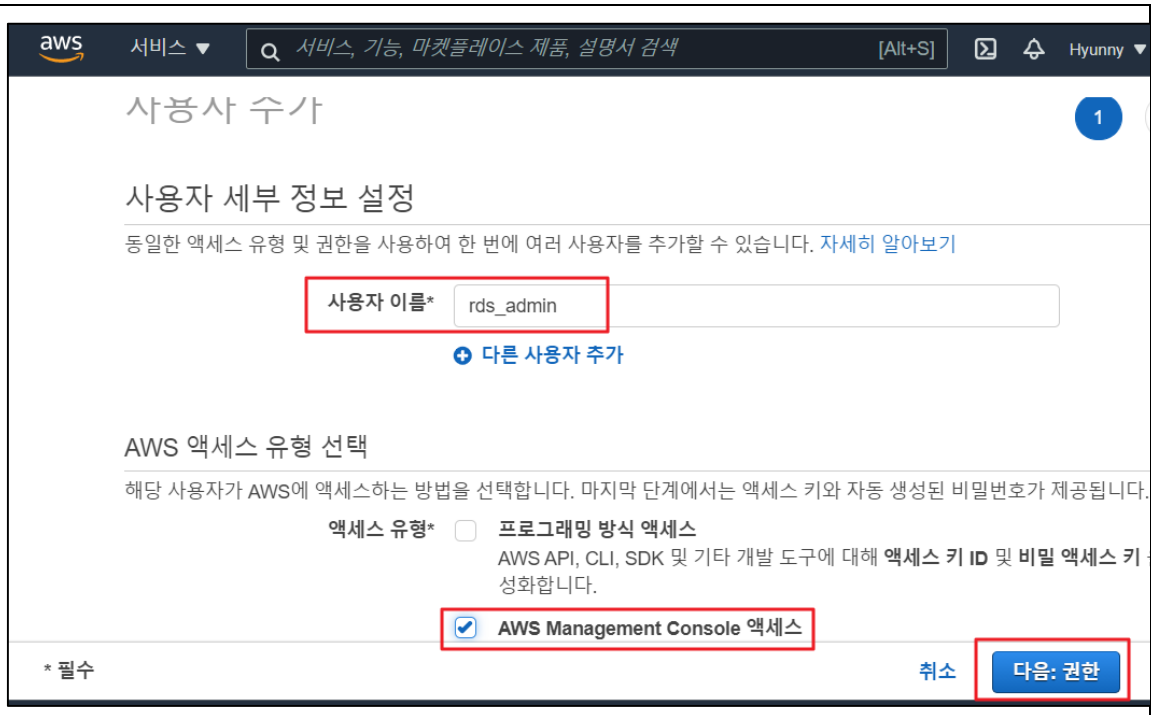


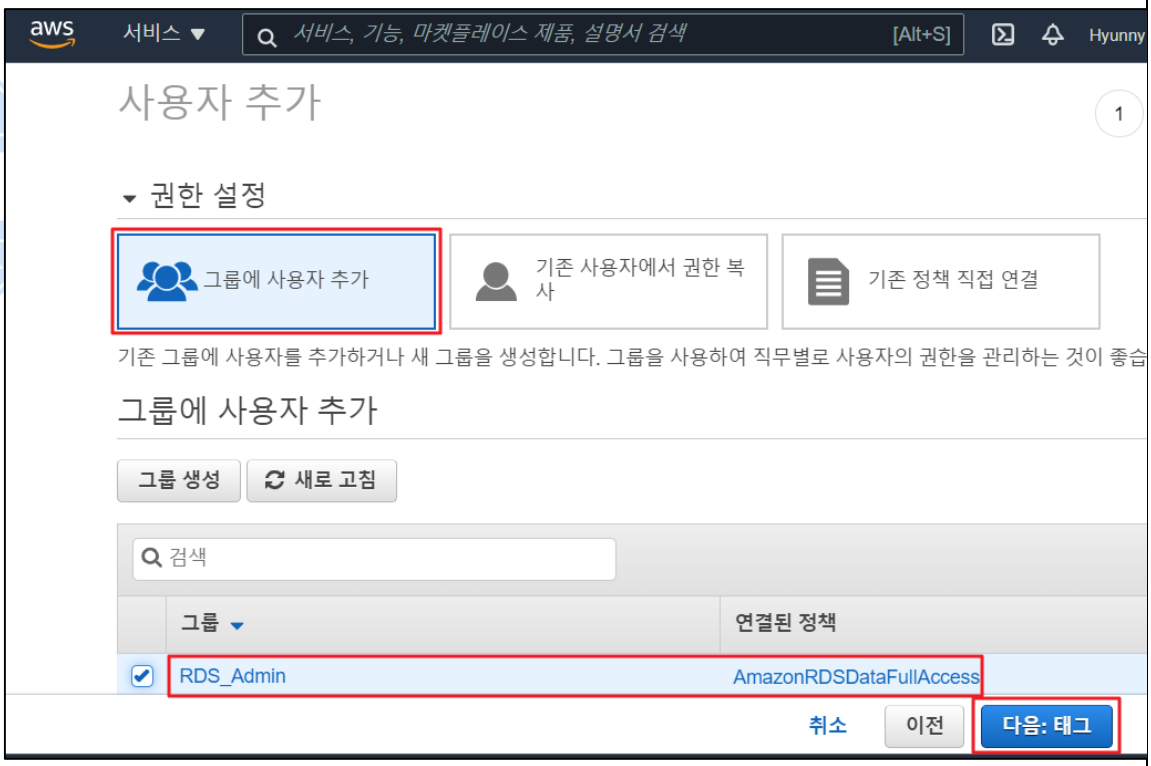


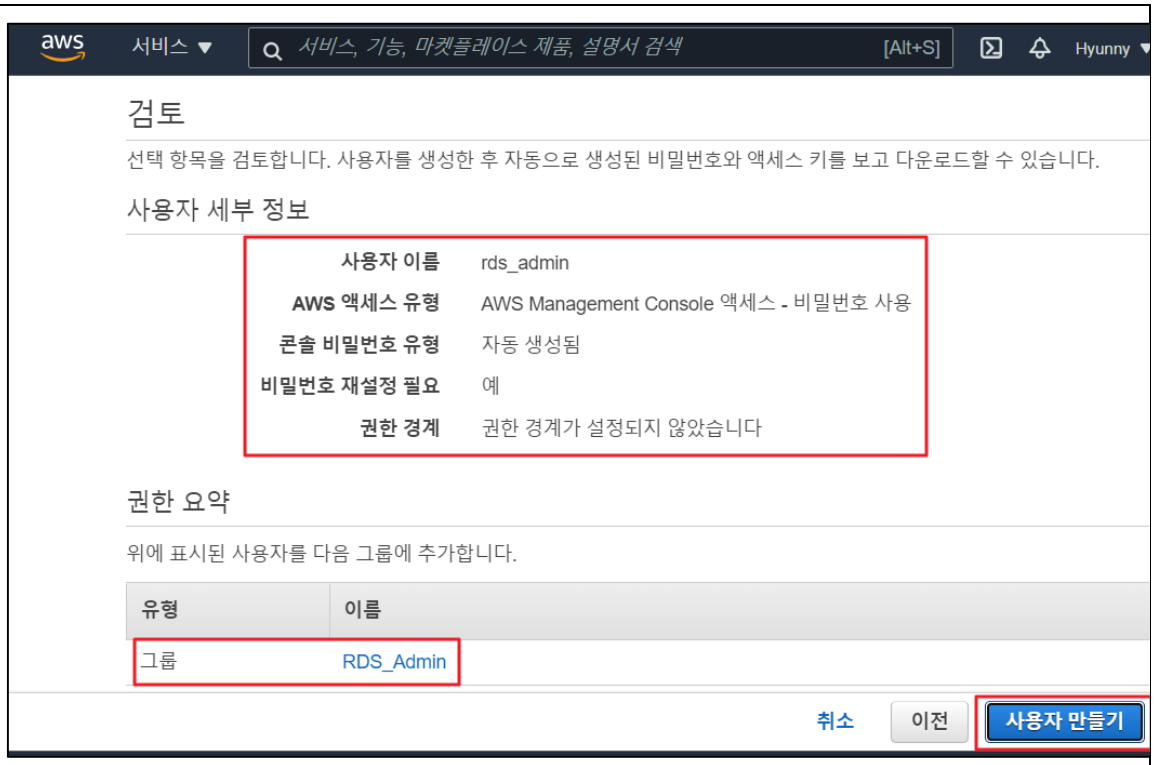
2) IAM 사용자 생성 및 그룹 지정

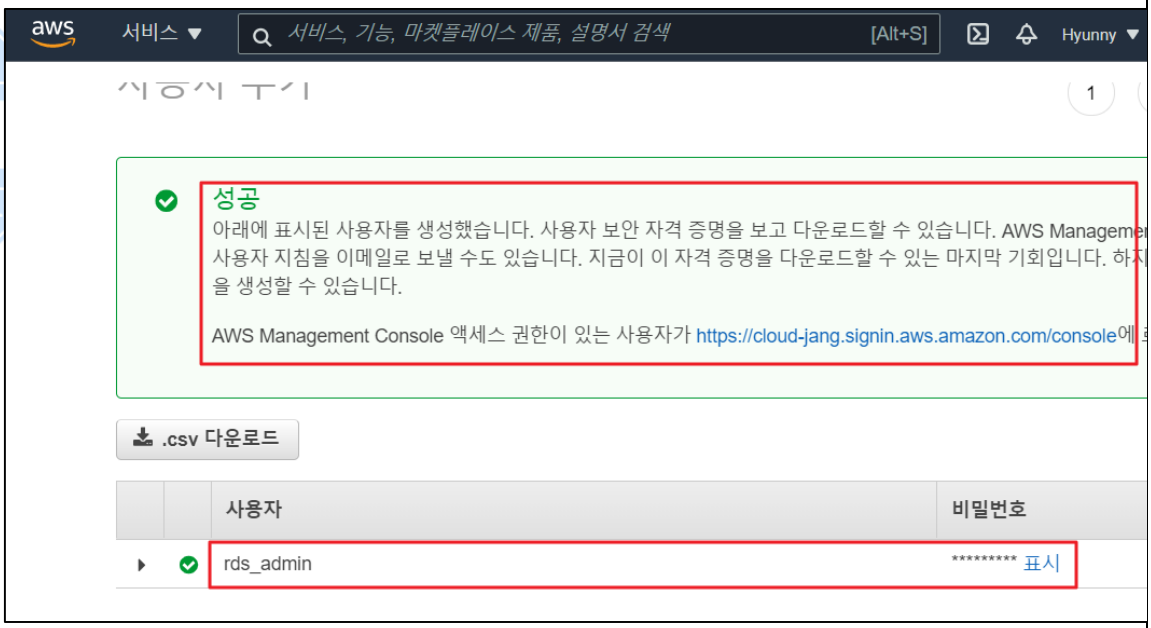
[IAM] → [사용자] → [사용자 추가] → [사용자 세부정보 지정] → [권한 설정 (그룹에 사용자를 추가)] → [사용자 만들기]

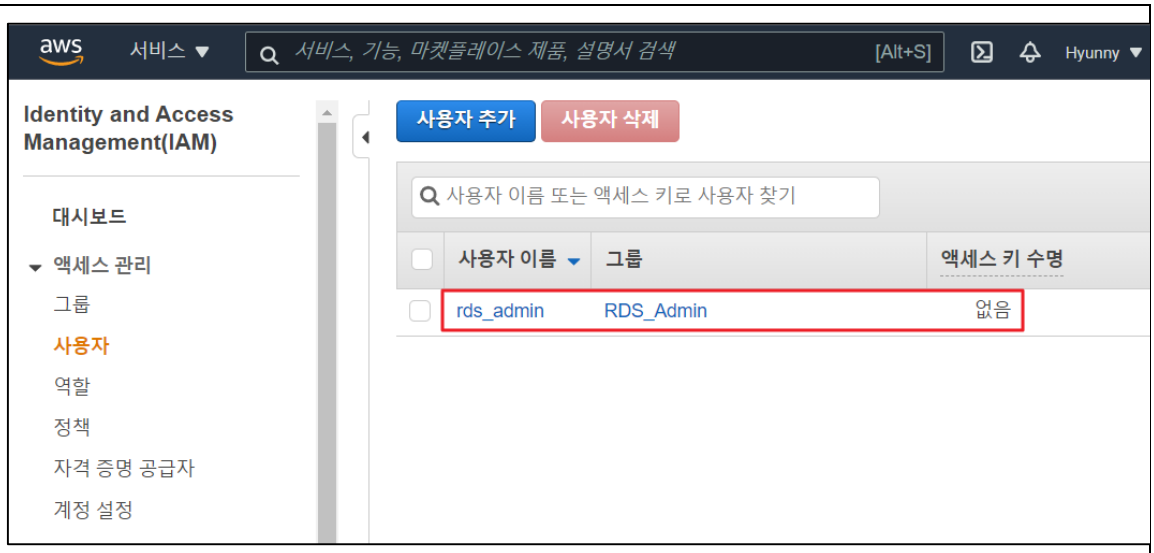


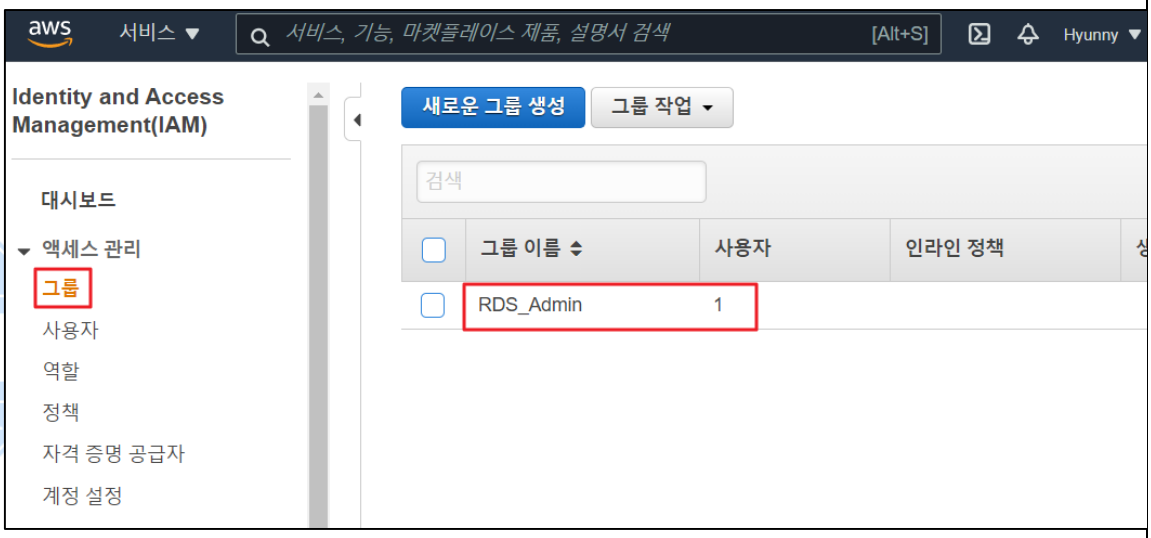












진단	양호기준

기준	: RDS 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있을 경우 **취약기준** : RDS 서비스 IAM 사용 권한이 각각 서비스 역할에 맞지 않게 설정되어 있을 경우
비고	

2.3 S3 보안 정책 관리

<table>
<tr><td>분류</td><td>권한관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">S3 보안 정책 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.

1) AWS 관리형 정책 (S3)
- AWS 관리형 정책은 AWS에서 생성 및 관리하는 정책으로 여러 가지 직무 및 일반 사용 사례에서 권한을 제공할 목적으로 설계된 정책입니다.

※ S3 서비스 내 FULL ACCESS 등과 같이 중요도가 높은 AWS 관리형 정책은 S3 서비스 관리/운영자 및 관련 담당자 외에 다른 IAM 계정에 아래와 같은 권한 할당이 되지 않도록 해야합니다.

2) S3 역할별 권한 관리 (예시)
<table>
<tr><th>역할</th><th>관리형 정책명</th></tr>
<tr><td>AWS Root 관리자</td><td>* ALL FULL ACCESS *, AdministratorAccess</td></tr>
<tr><td>Infra 운영/관리자 및 담당자</td><td>AmazonS3FullAccess</td></tr>
<tr><td>Application 운영/관리자 및 담당자</td><td>Amazon S3 / AmazonDMSRedshiftS3Role / AmazonS3ReadOnlyAccess</td></tr>
<tr><td>개발 관리자 및 담당자</td><td>Amazon S3 / AmazonDMSRedshiftS3Role / AmazonS3ReadOnlyAccess</td></tr>
<tr><td>재무 / 비용 관리자 및 담당자</td><td>Amazon S3 / AmazonS3ReadOnlyAccess / QuickSightAccessForS3StorageManagement AnalyticsReadOnly</td></tr>
</table>
3) IAM 관리형 정책 권한 관리 List (예시)
<table>
<tr><th>역할</th><th>계정 관리
(그룹 및 계정명)</th><th>AWS 고객관리형 정책</th><th>취약
유/무</th></tr>
<tr><td>AWS Root 관리자</td><td>Ex)S3_Admin
(admin_accout)</td><td>Ex) S3_Admin
(CustomS3FullAccess)</td><td></td></tr>
<tr><td>Infra 운영/관리자 및 담당자</td><td></td><td></td><td></td></tr>
<tr><td>Application 운영/관리자 및 담당자</td><td></td><td></td><td></td></tr>
<tr><td>개발 관리자 및 담당자</td><td></td><td></td><td></td></tr>
</table>
</td></tr>
</table>

재무 / 비용 관리자 및 담당자	

설정 방법

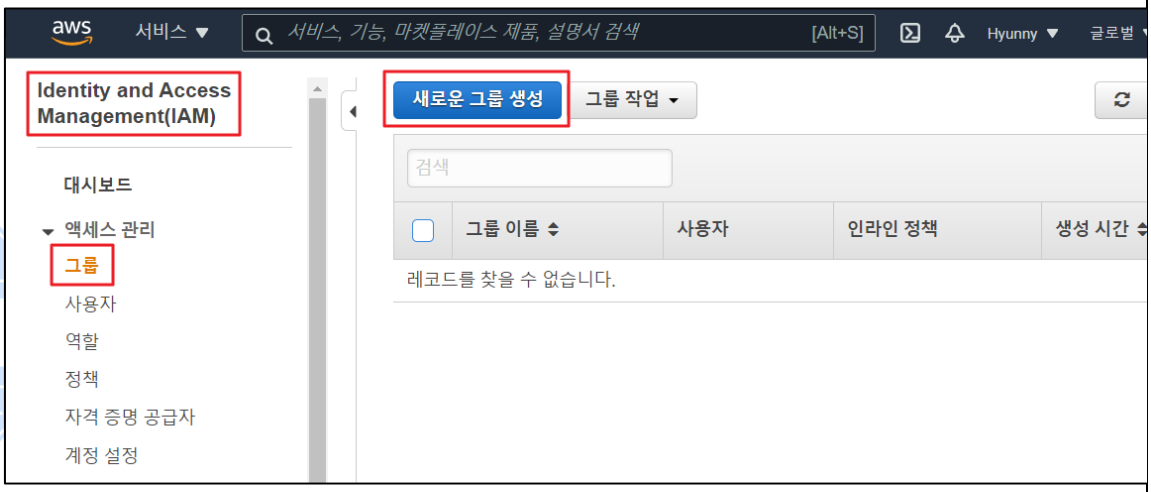
가. S3 IAM 관리자/운영자 권한 그룹 생성 및 사용자 추가

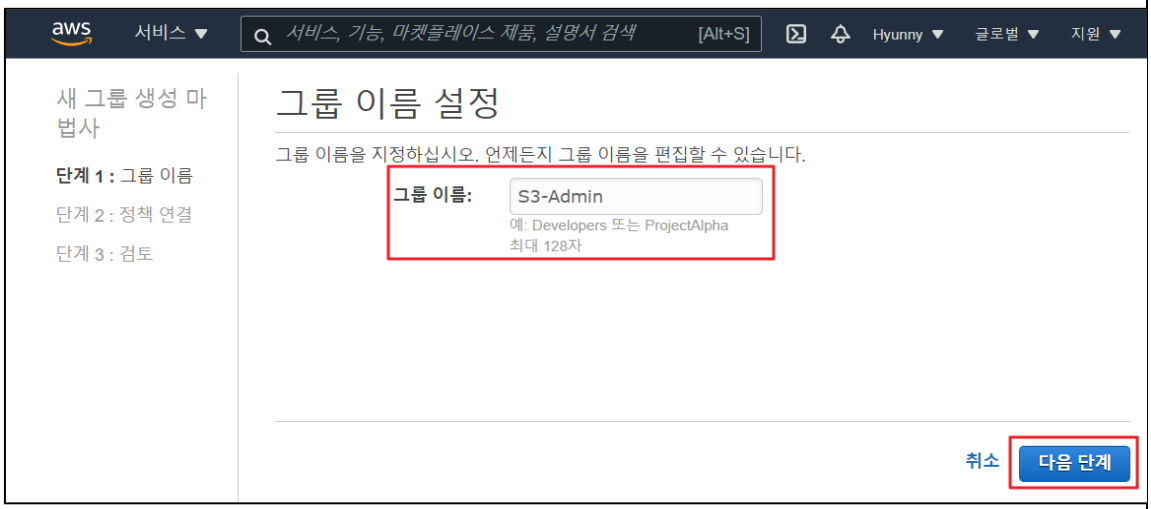
- S3 서비스의 운영/관리를 위한 IAM 그룹 생성 및 사용자 추가

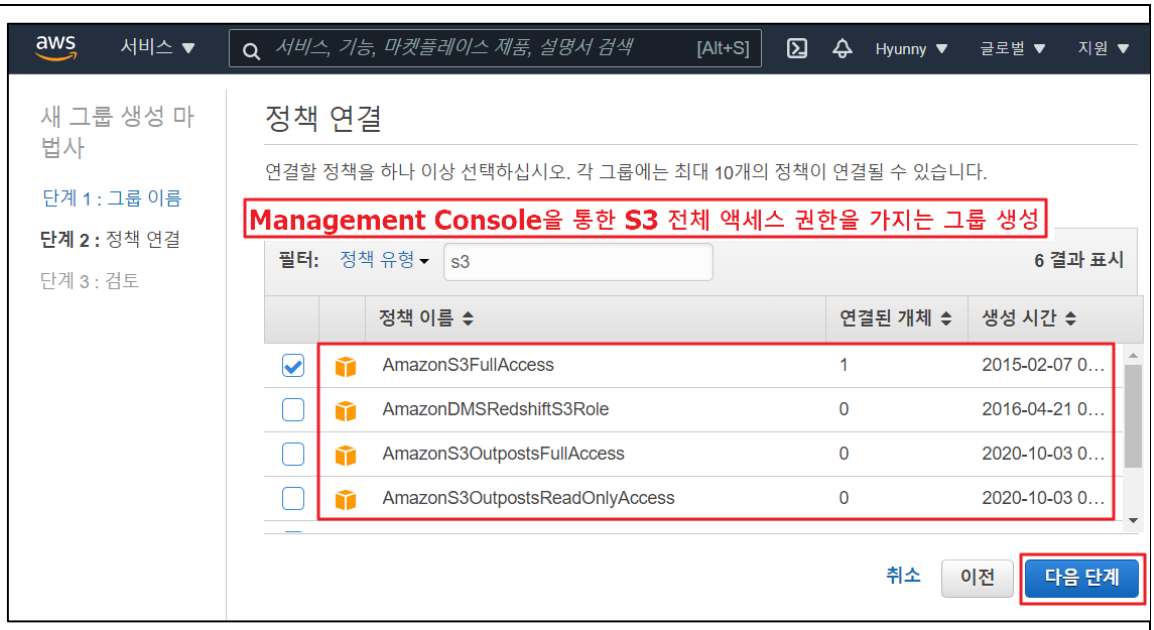
1) IAM 그룹 생성

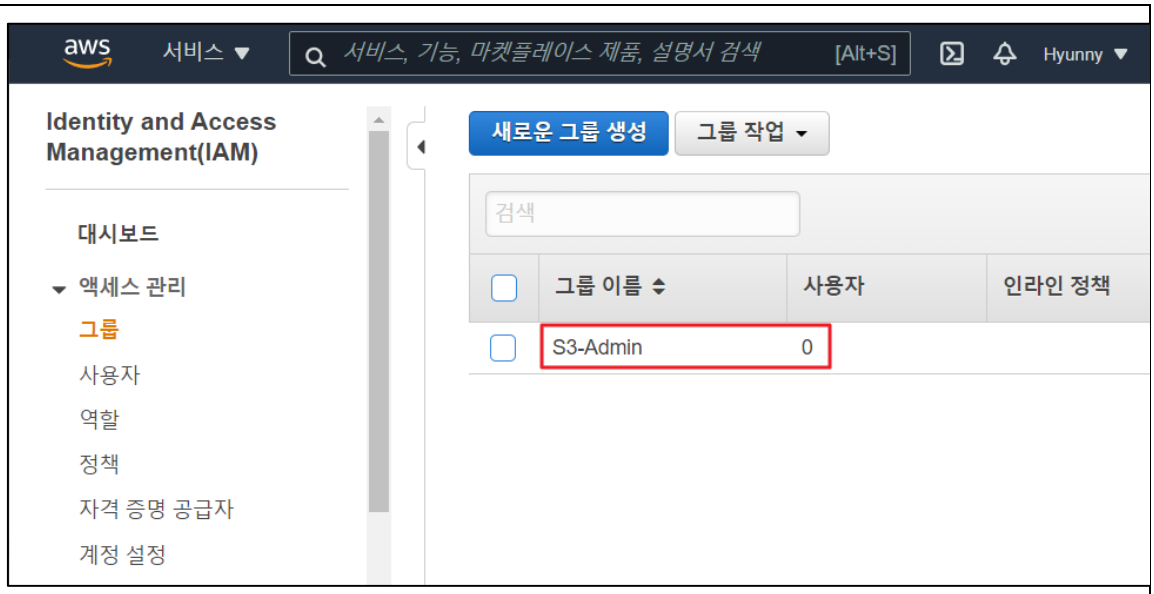
[IAM] → [그룹] → [새로운 그룹 생성] → [그룹 이름 설정] → [IAM 계정 권한에 맞는 정책 연결] → [그룹 생성]

※ S3 운영/관리에 필요한 IAM FULL Access 등의 권한과 같이 중요도가 높은 권한은 Infra 운영/관리자 및 담당자에게만 정책이 되도록 해야하며 최소한의 계정 수가 유지되야함



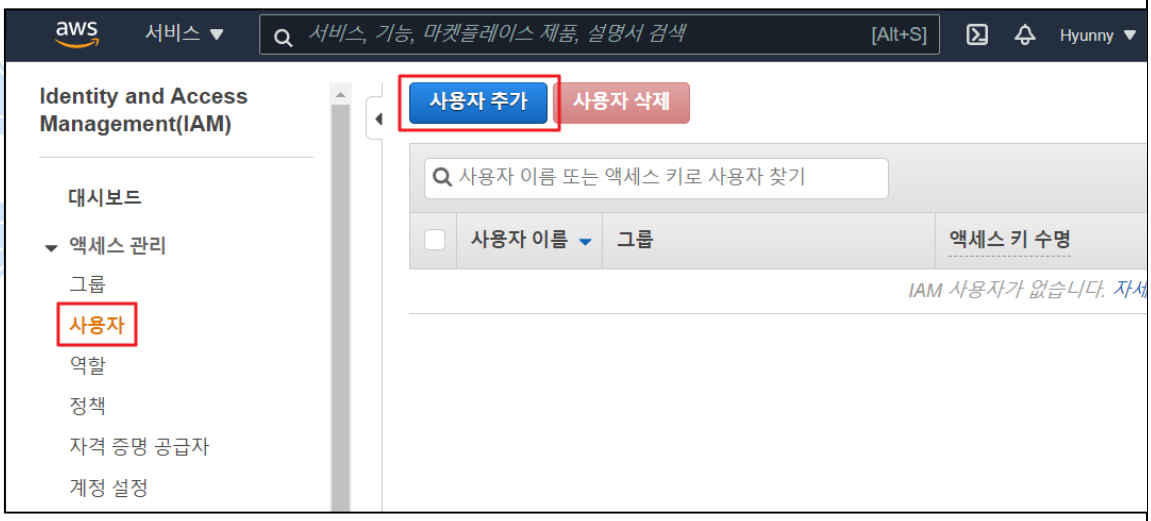


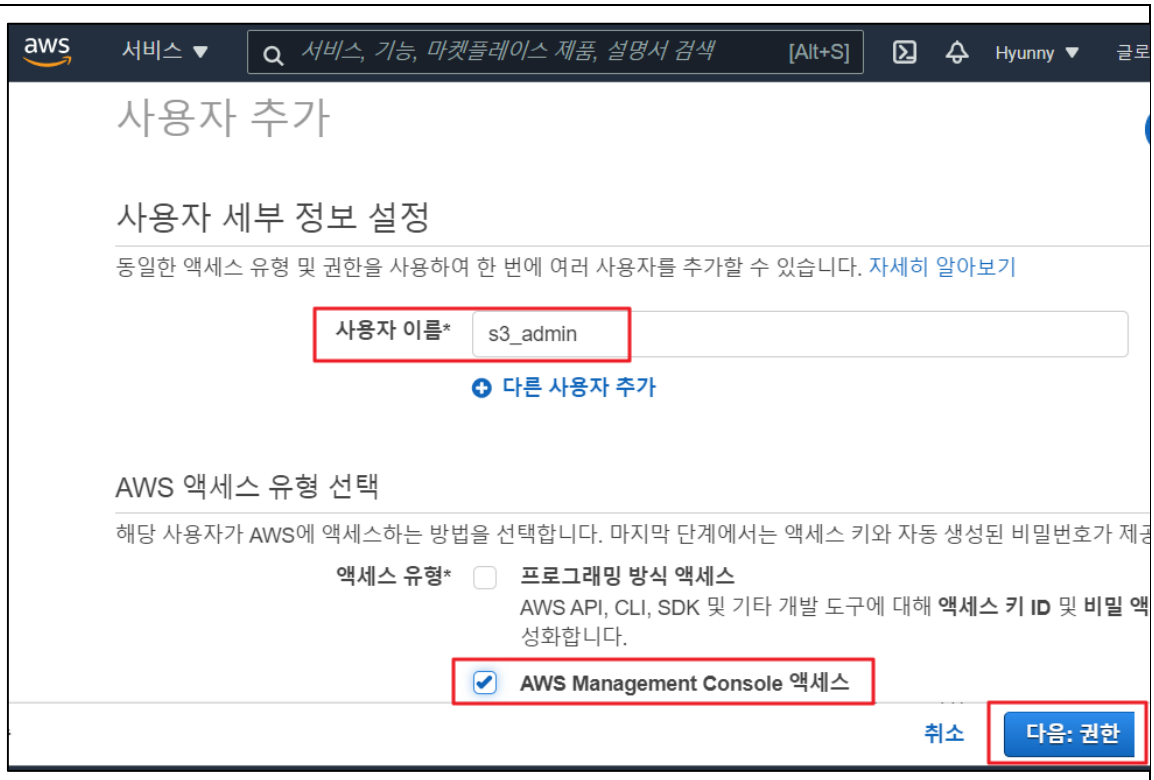


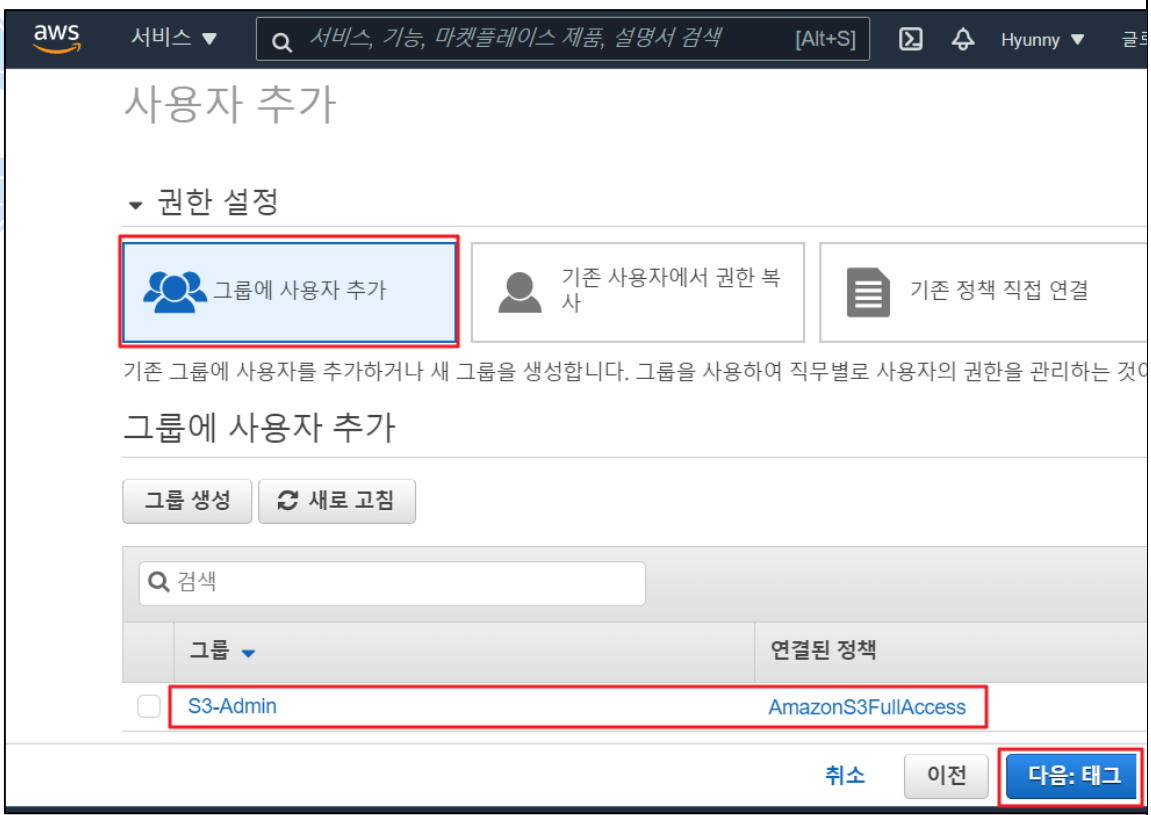


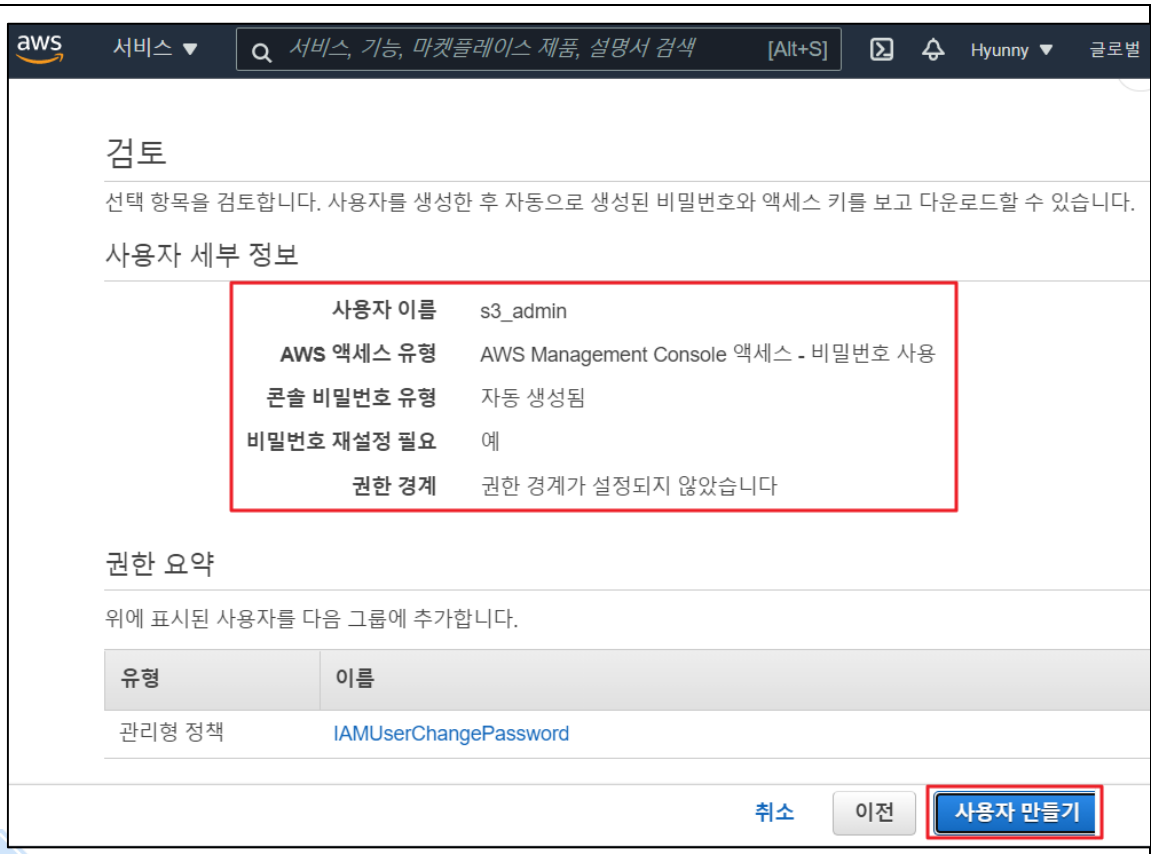
2) IAM 사용자 생성 및 그룹 지정

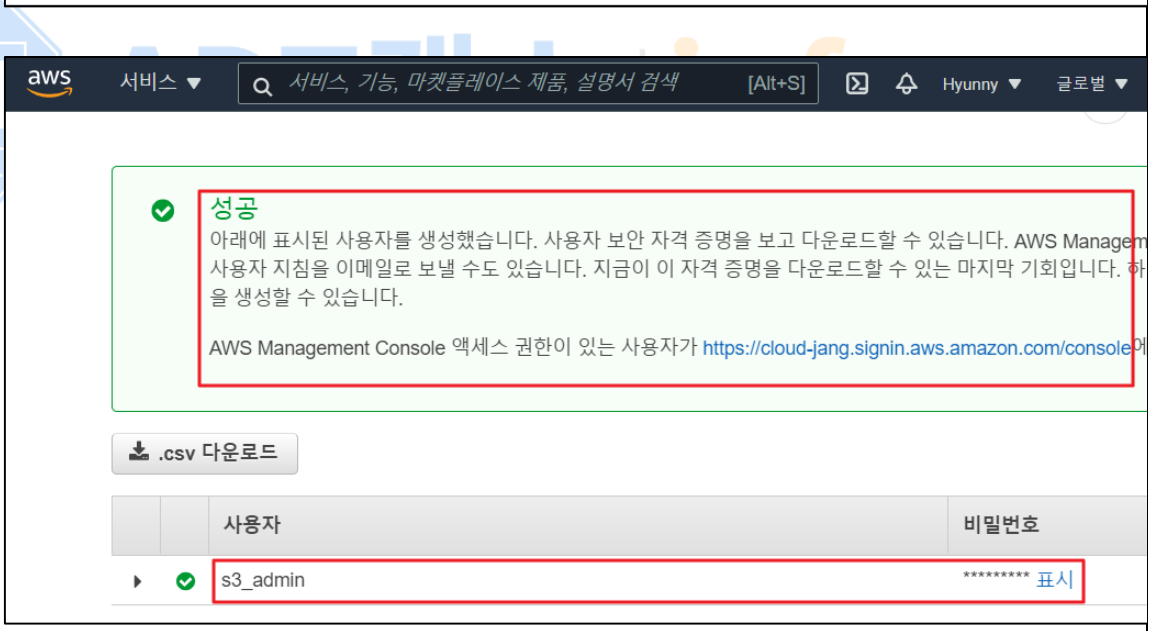
[IAM] → [사용자] → [사용자 추가] → [사용자 세부정보 지정] → [권한 설정 (그룹에 사용자를 추가)] → [사용자 만들기]

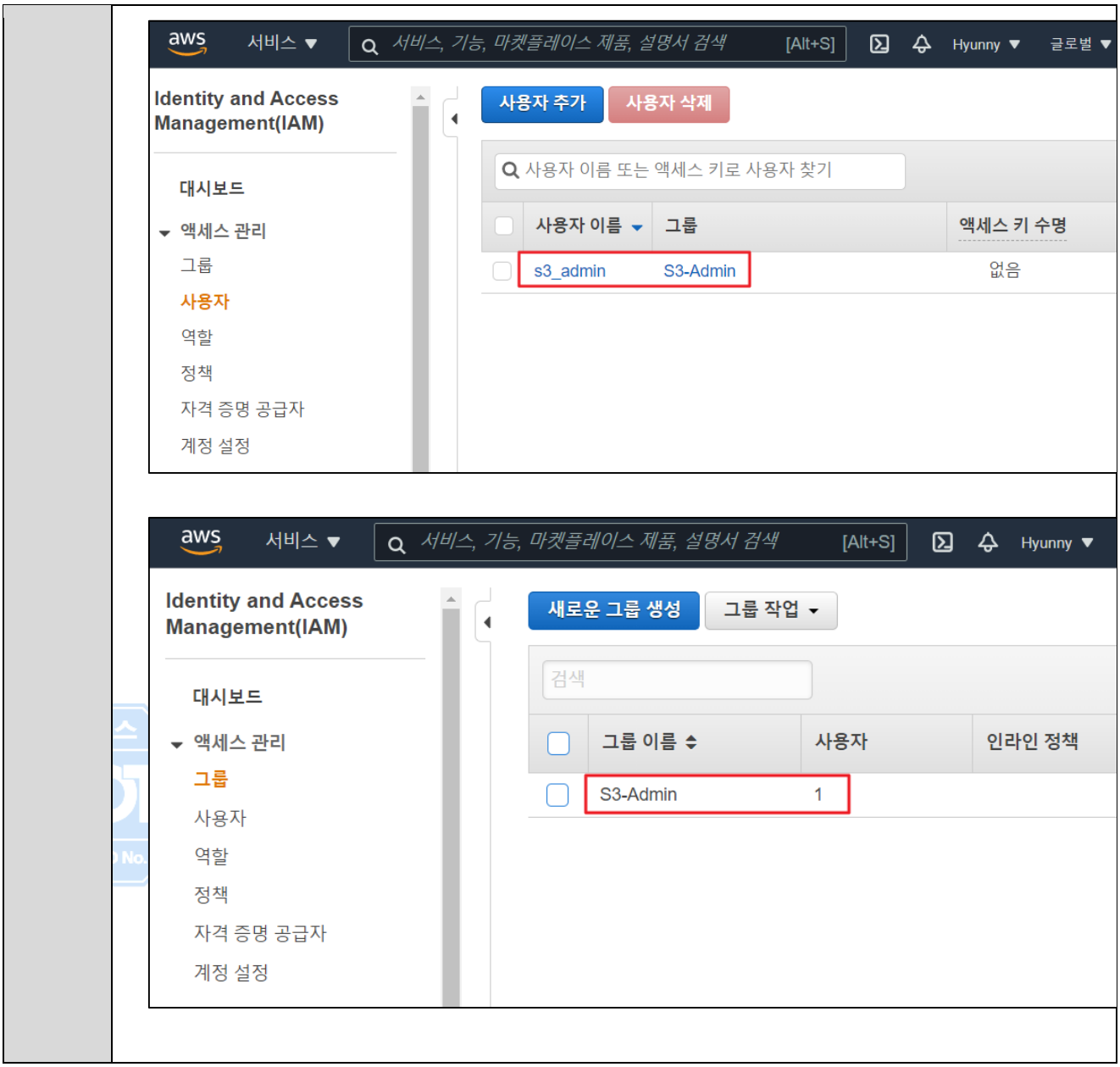








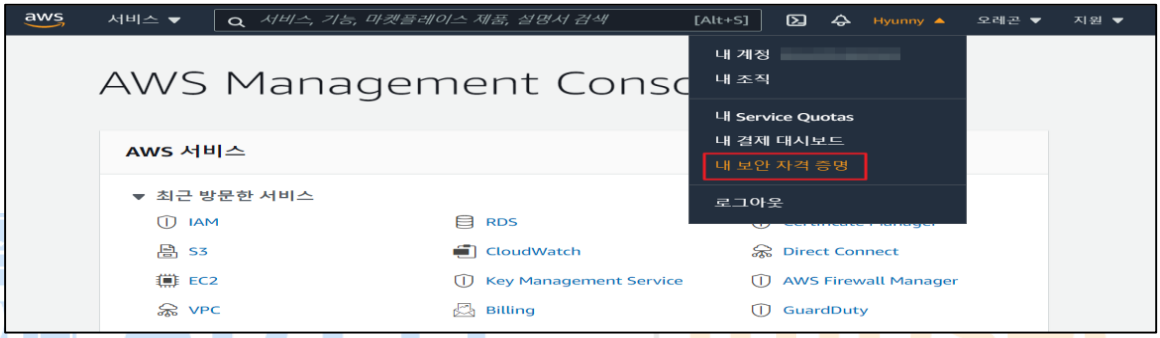
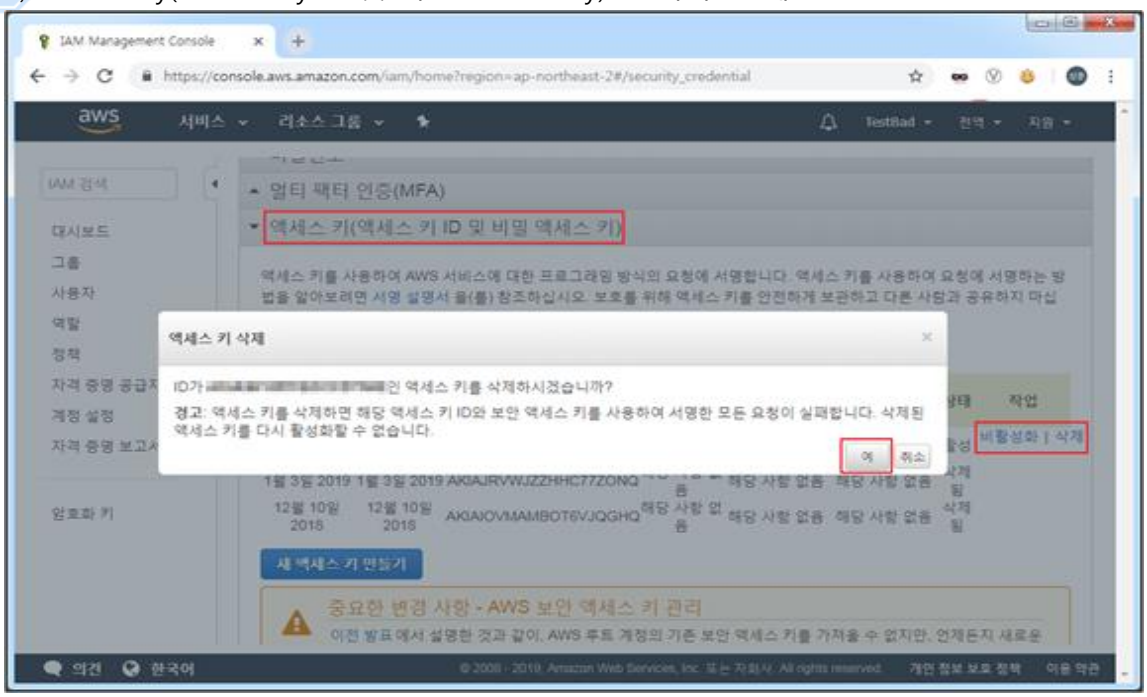




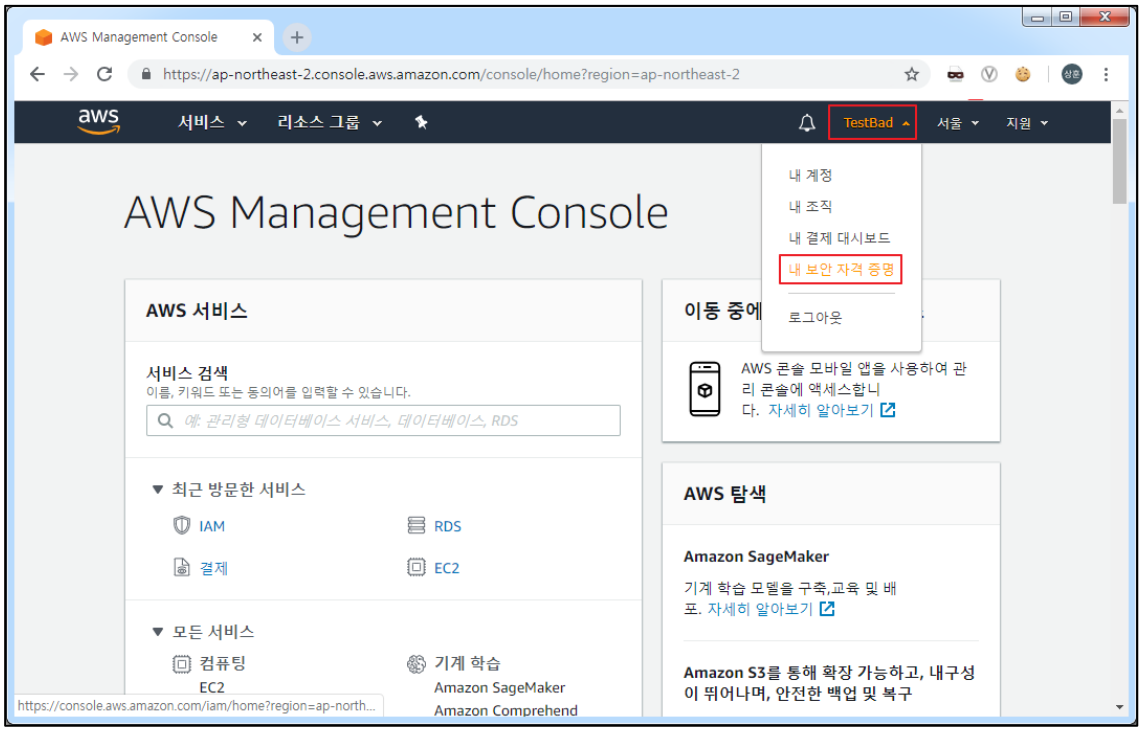
<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단 기준</td><td>양호기준
: S3 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있을 경우

취약기준
: S3 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있지 않을 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

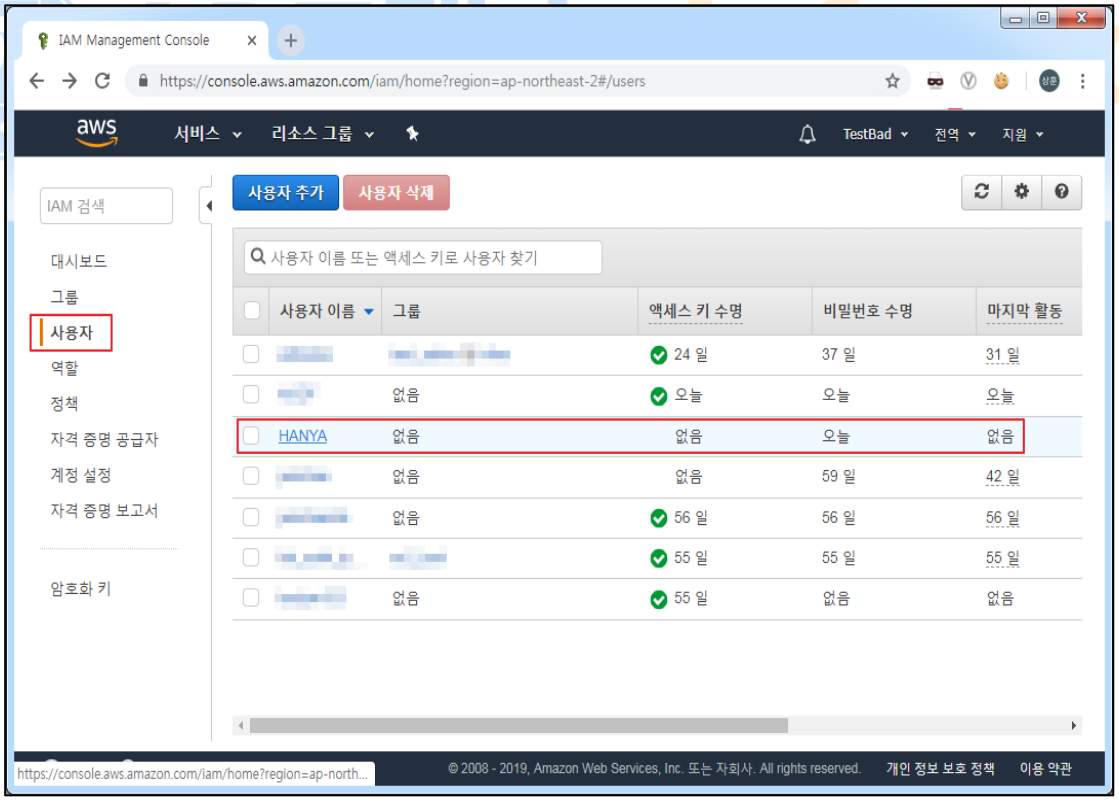
2.4 Access Key 정책 관리

분류	권한관리	중요도	중
항목명	Access Key 정책 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 Root 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 Root 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**		

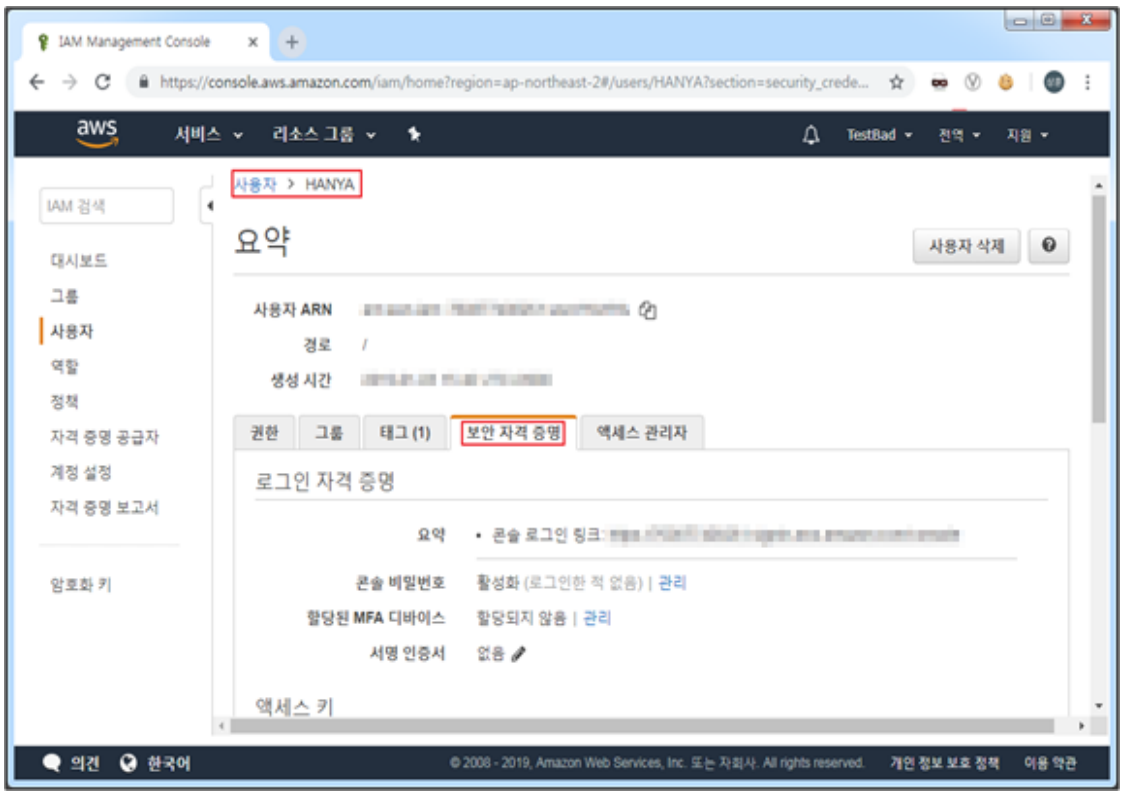
1) 메인 우측 상단 계정 → 내 보안 자격 증명



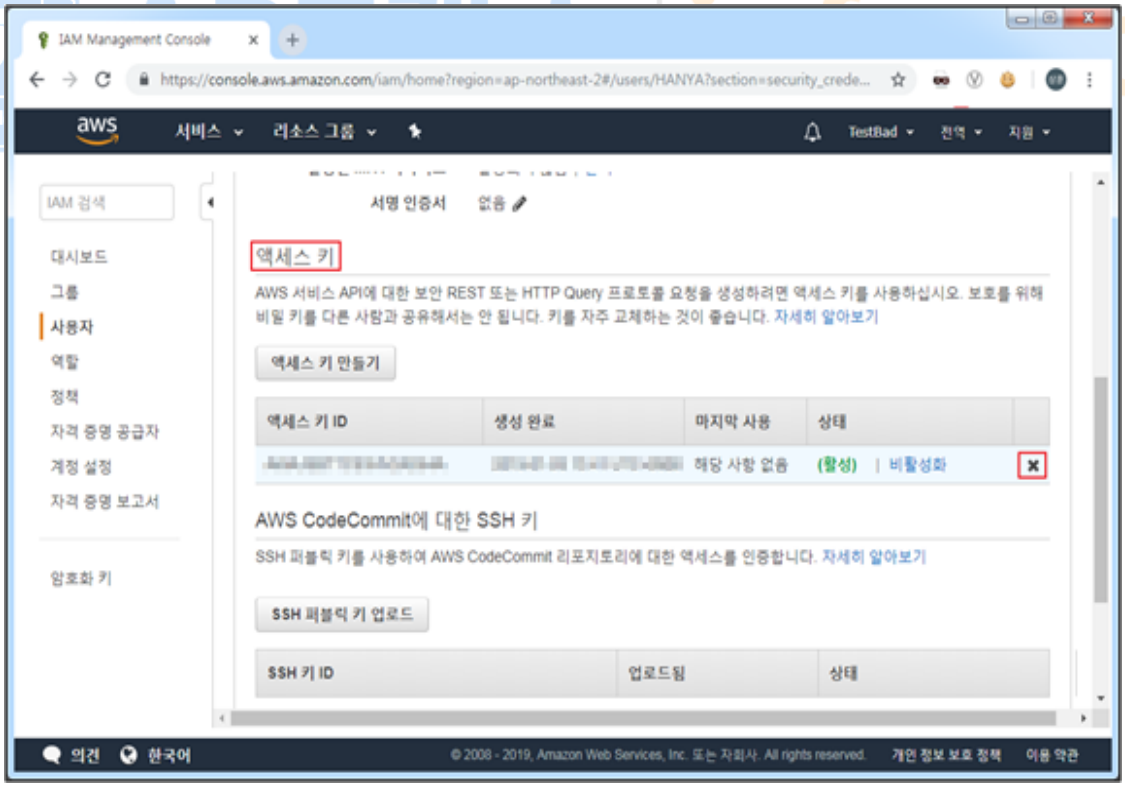
2) 사용자 → Aceess Key를 삭제할 계정 선택



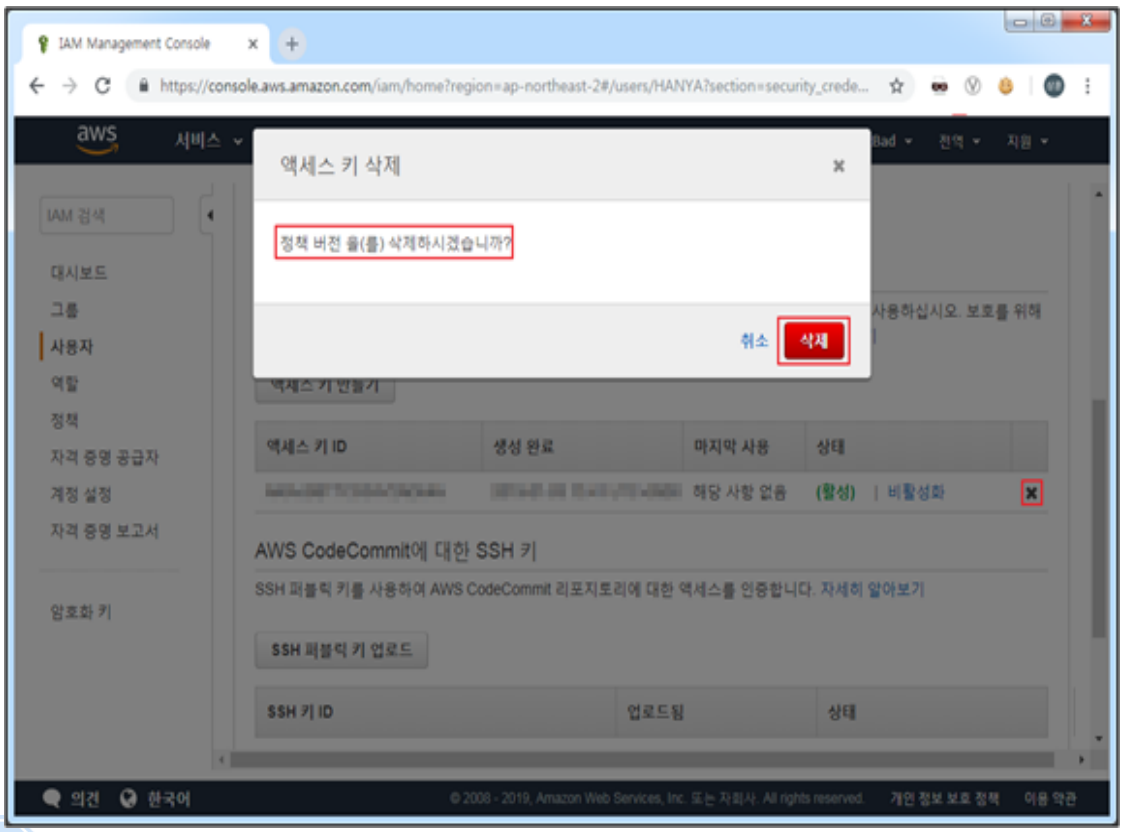
3) 요약 → 보안 자격 증명 탭



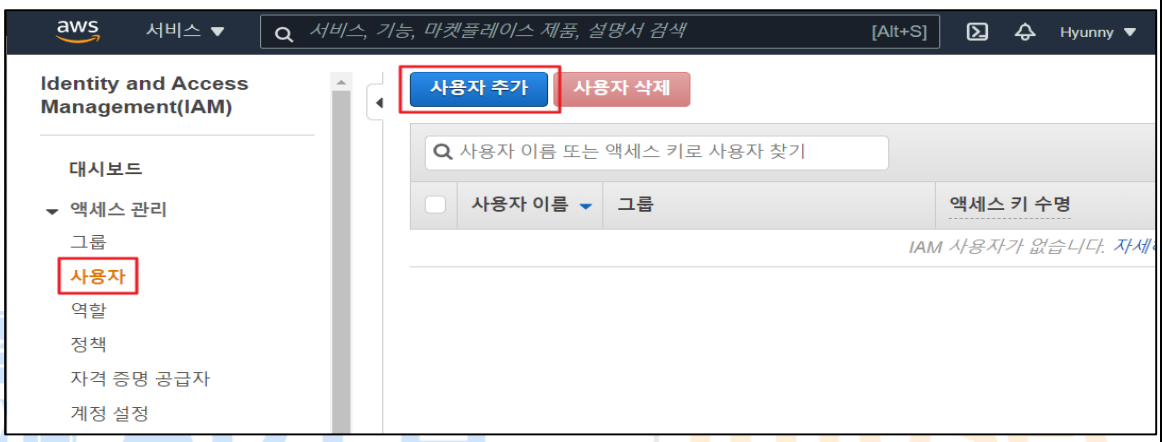
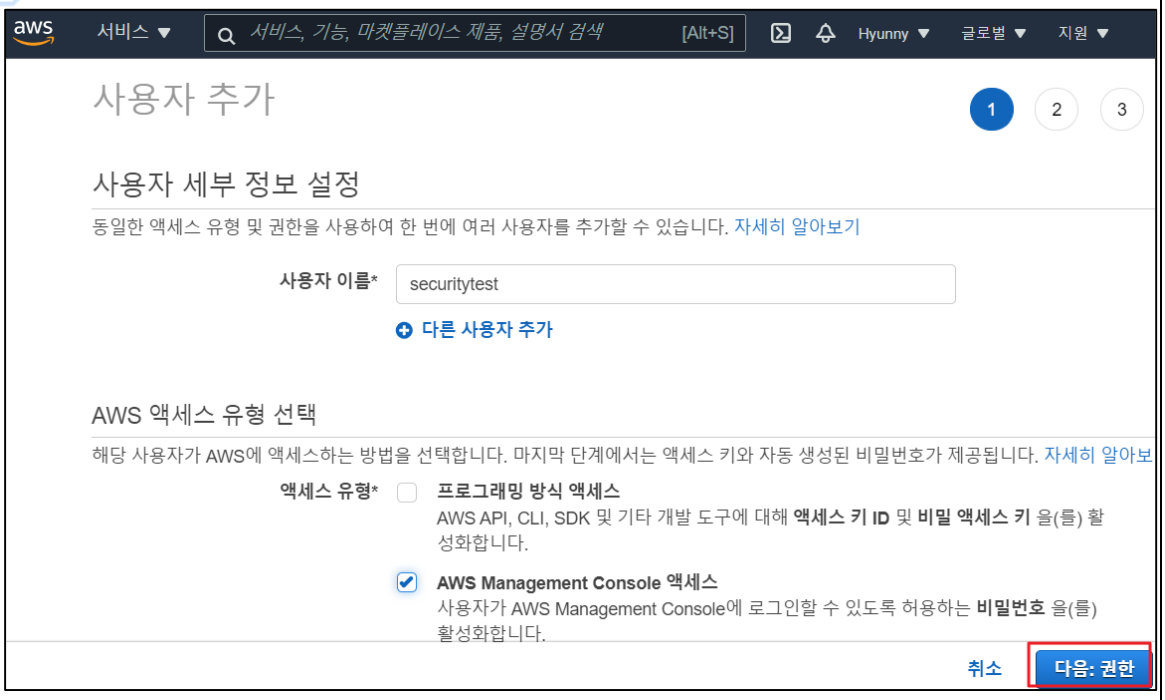
4) Access Key → Access Key ID → 'X'(삭제) 버튼

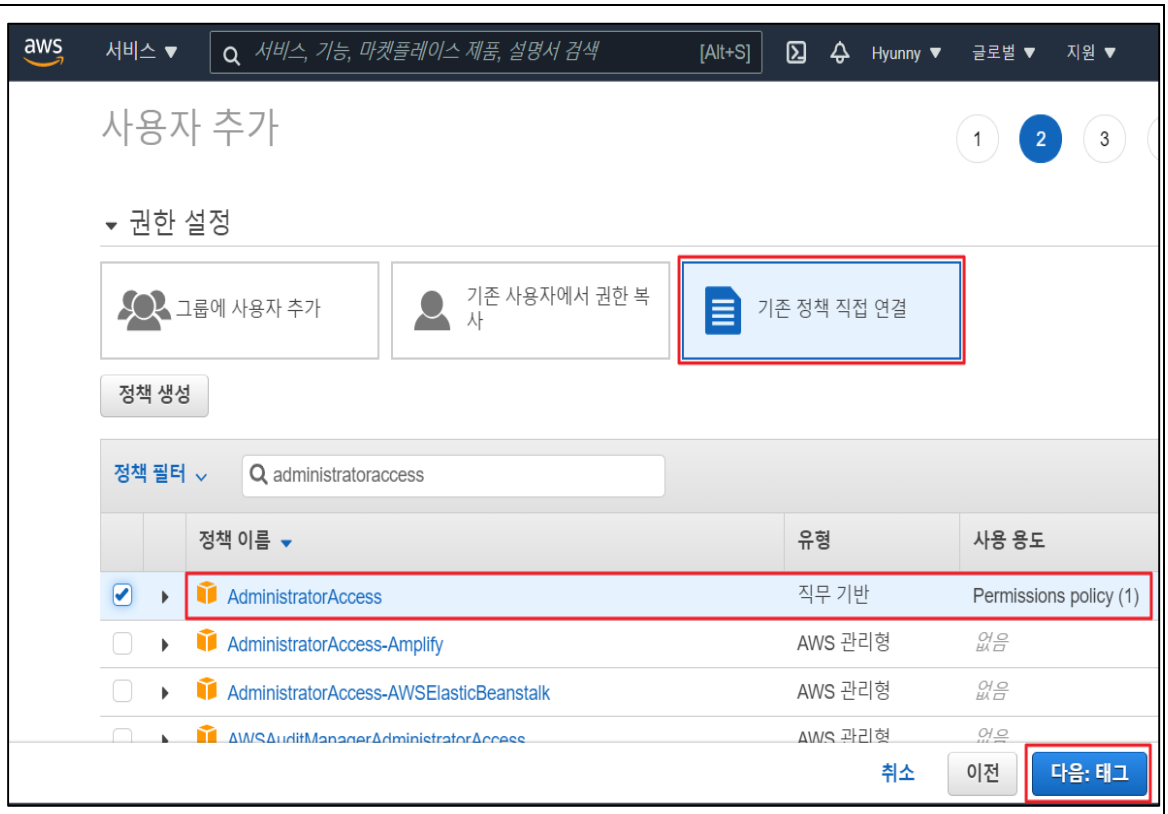


5) Access Key 삭제 → 삭제

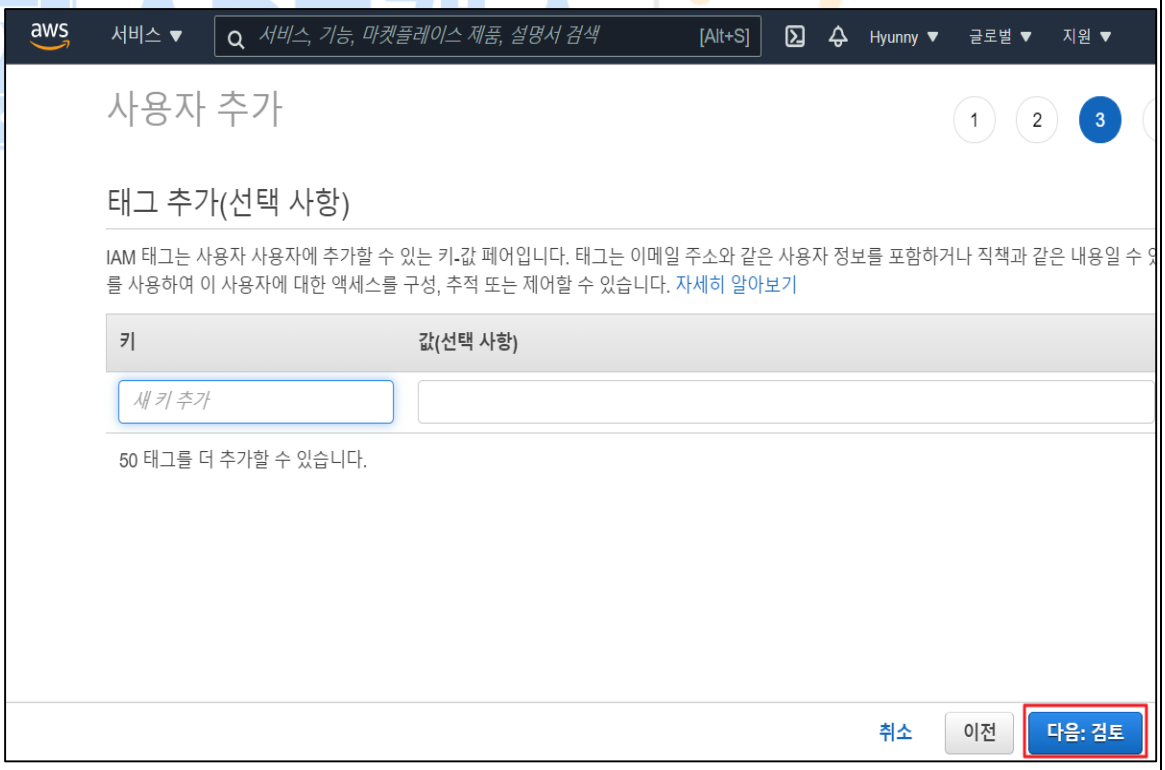
	
진단 기준	**양호기준** : AWS Root 및 IAM 사용자 계정에 Access Key가 존재하지 않을 경우 **취약기준** : AWS Root 및 IAM 사용자 계정에 Access Key가 존재 할 경우
비고	

2.5 Admin Console 관리자 정책 관리

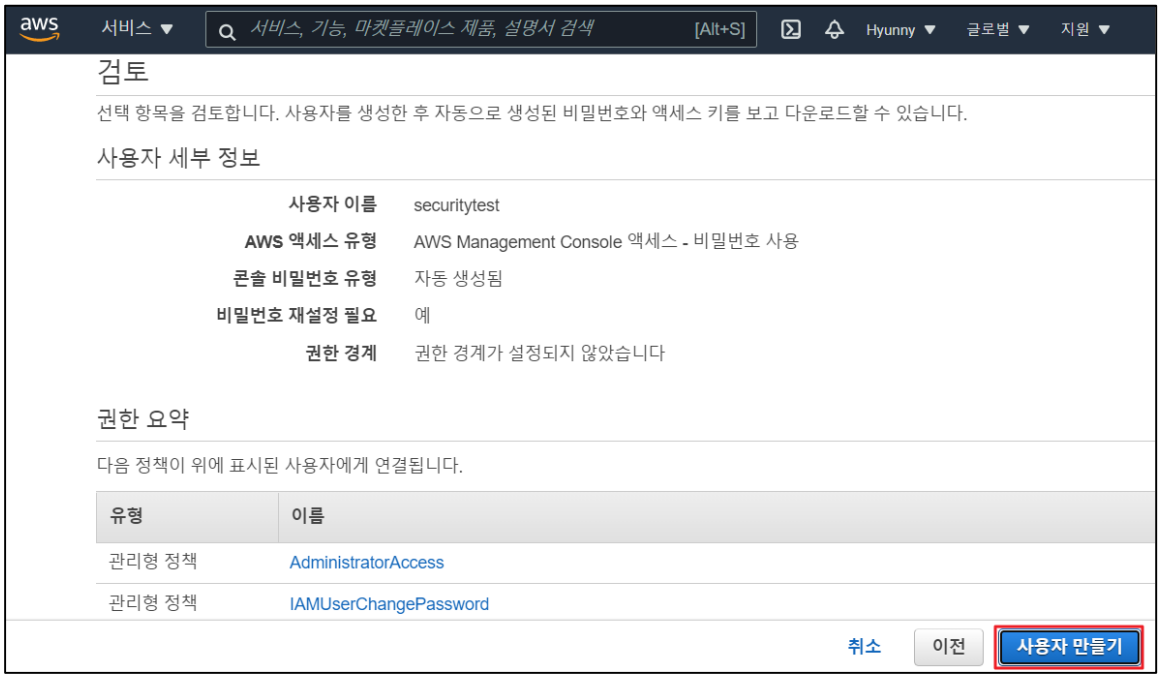
분류	권한관리	중요도	중
항목명	Admin Console 관리자 정책 관리		
항목 설명	AWS Cloud 사용을 위해 처음 발급한 계정은 IAM 사용자 계정과 달리 모든 서비스에 접근할 수 있는 최고 관리자 계정입니다. Cloud 서비스 특성 상 인터넷 연결이 가능한 망에서 계정정보를 입력하여 WEB Console에 접근하게 됩니다. 이는 최고 권한을 보유하고 있는 관리자 계정이 아닌 권한이 조정된 IAM 사용자 계정을 기본으로 사용해야 보다 안전한 접근이 이뤄질 수 있습니다.		
설정 방법	**가. IAM 사용자 계정 생성** 1) 사용자 추가 버튼 클릭  2) 사용자 추가 (기본설정 - 이름, 액세스 유형 선택)  3) 사용자 추가 (기존 정책 직접 연결하기)		



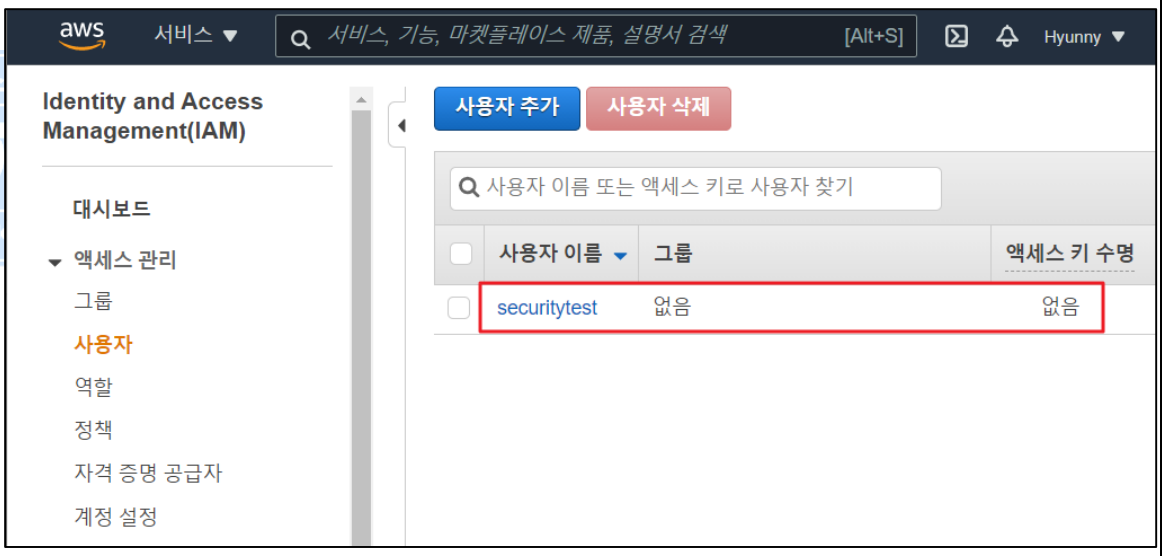
4) 사용자 추가 (태그 계정 정보 입력)

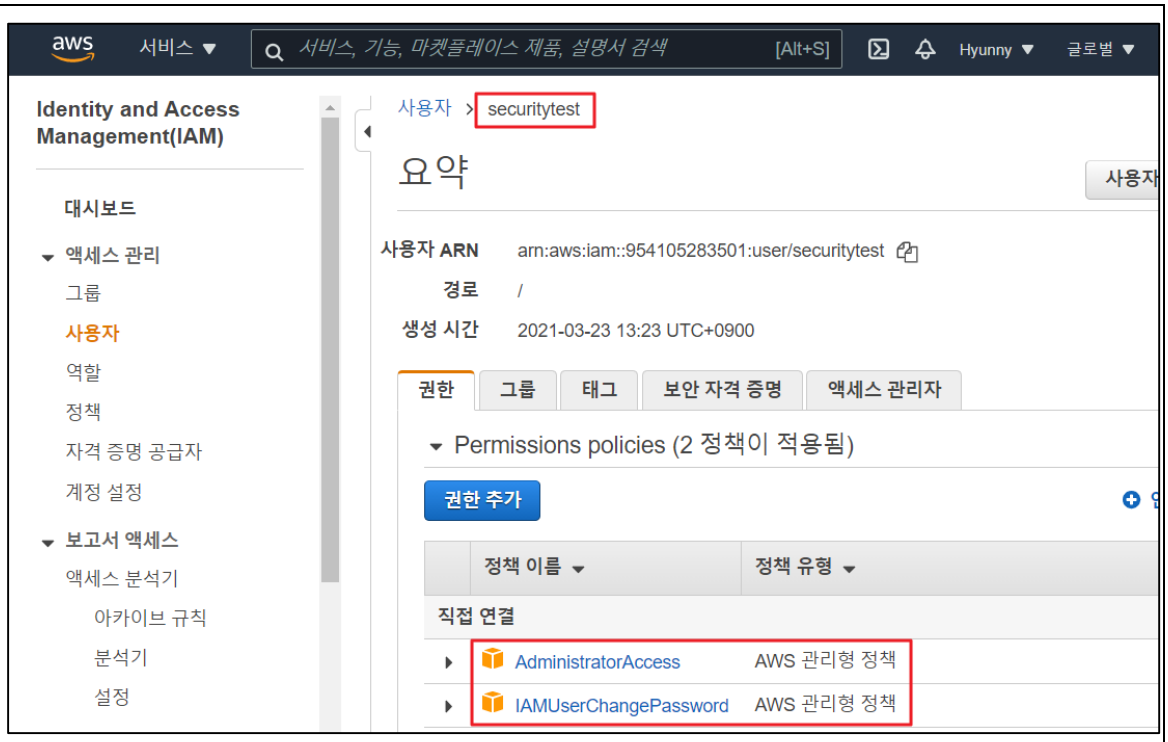


5) 사용자 추가 (검토하기)



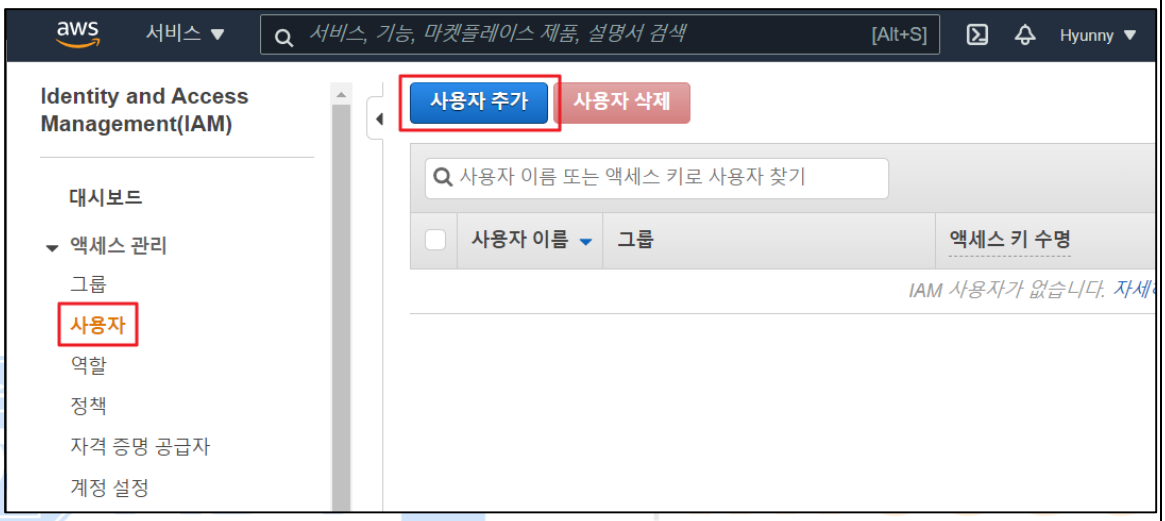
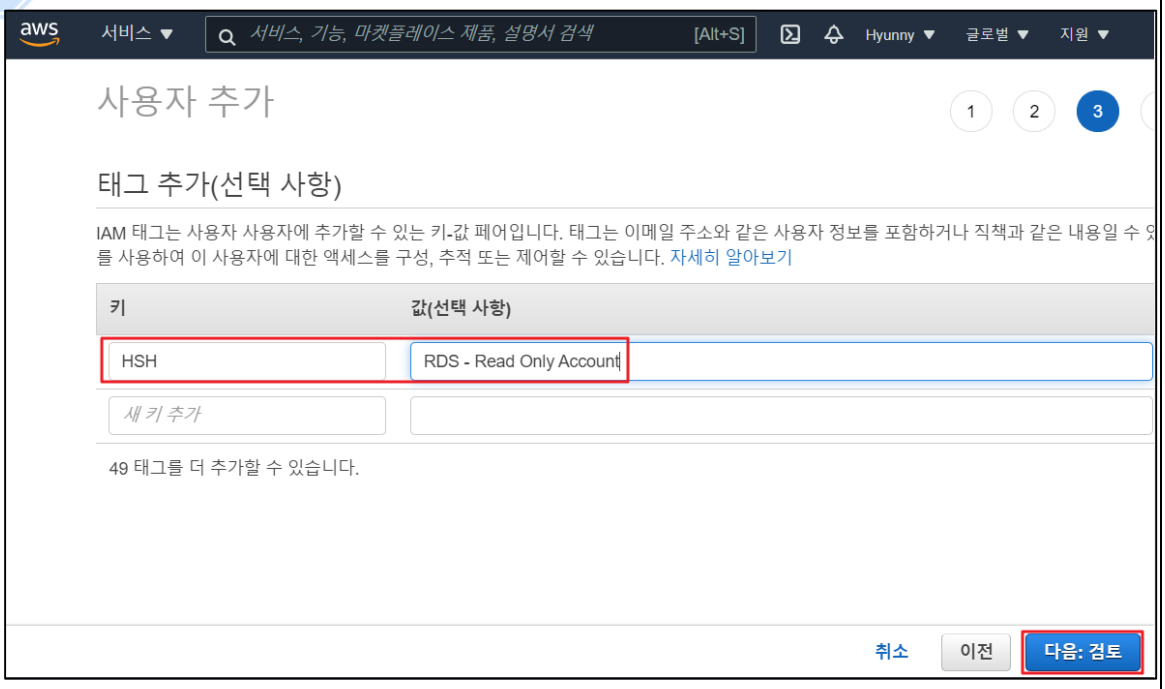
6) IAM 사용자에 추가된 신규 사용자 확인

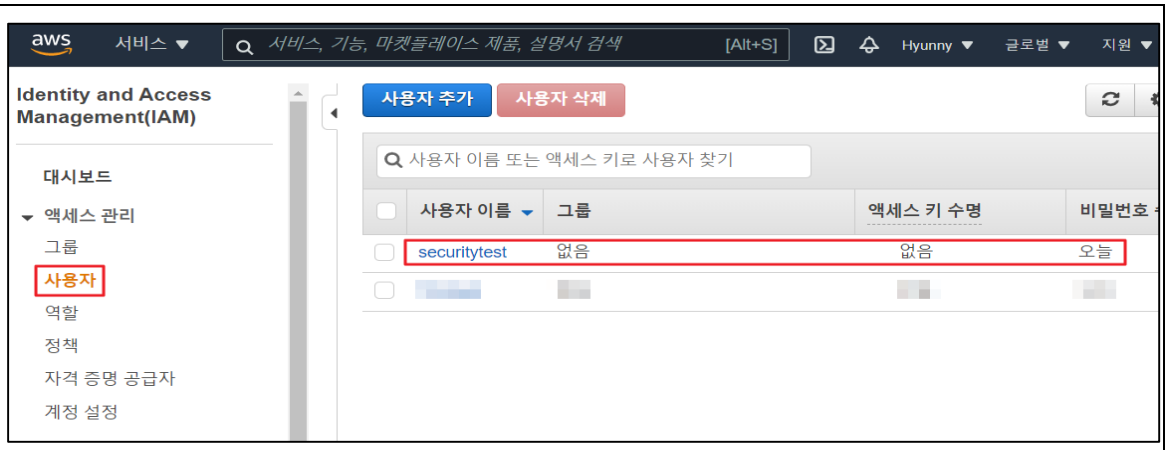


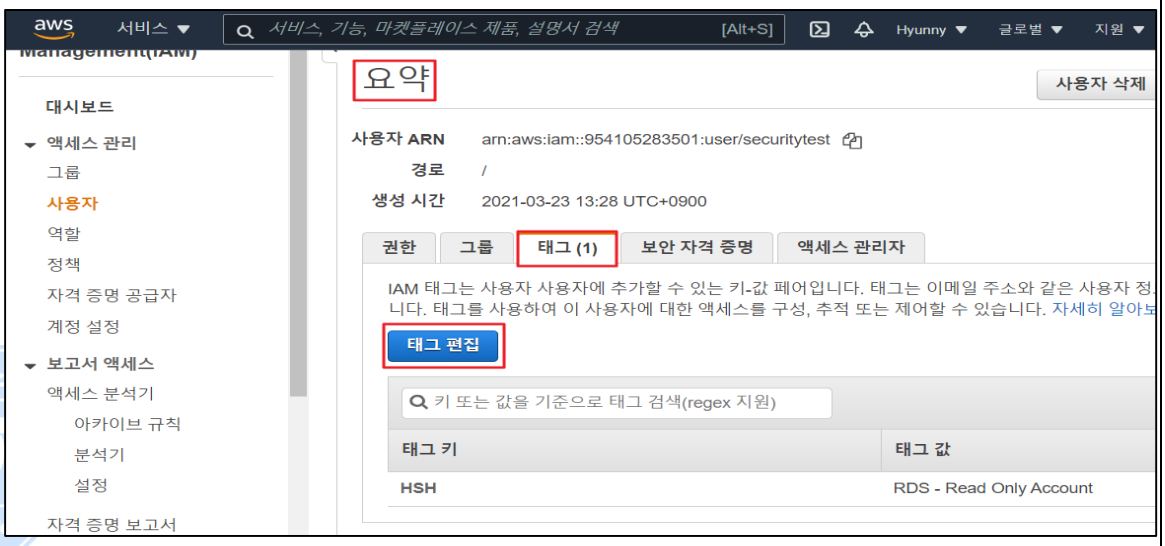
<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단 기준</td><td>양호기준
: AWS 회원가입 시 처음 발급한 Admin 계정을 서비스 용도로 사용하지 않을 경우

취약기준
: AWS 회원가입 시 처음 발급한 Admin 계정을 서비스 용도로 사용할 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

2.6. IAM 사용자 및 그룹 정책 관리

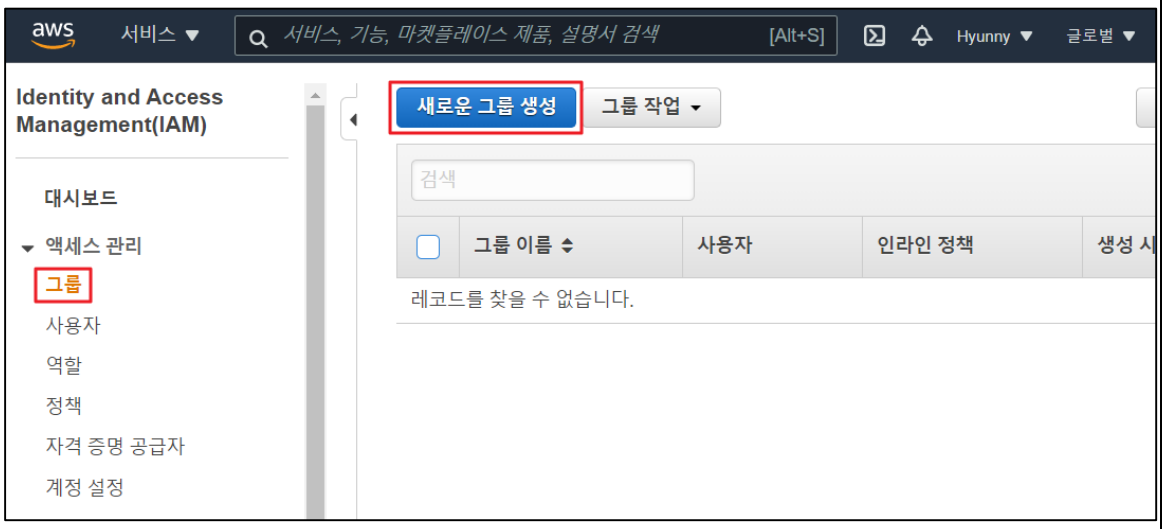
분류	권한관리	중요도	중
항목명	IAM 사용자 및 그룹 정책 관리		
항목 설명	AWS IAM(Identity and Access Management)은 AWS 리소스에 대한 접근 및 사용권한을 부여하여 관리하는 자격 증명 기반 정책 서비스로 무분별한 IAM 계정 생성 및 유추하기 쉬운 계정명(test, user, adm, abcd 등) 사용 시 보안상 위험을 발생 시킬 수 있으므로 계정 생성 시 사용자 식별 및 유추하기가 쉽지 않은 계정명을 사용해야 합니다.		
설정 방법	**가. 계정 정보 입력/수정 방법** 1) 계정 생성 시 태그 입력: IAM → 사용자 추가 → 생성 도중 태그 추가 → 정보입력   2) 기존 생성 계정 태그 추가/수정: IAM → 사용자 선택 → 요약 → 태그 → 태그 편집		

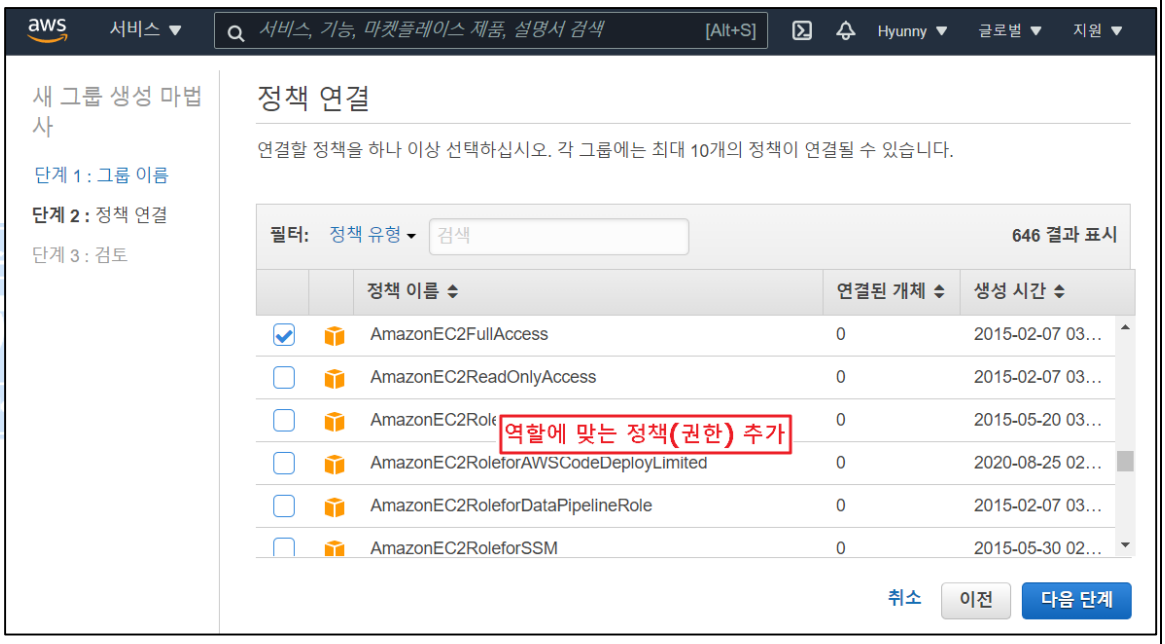




나. IAM Group 설정 방법

1) IAM → 그룹 → 새로운 그룹 생성 → 이름설정 → 정책(권한) 연결 → 생성 및 권한 확인

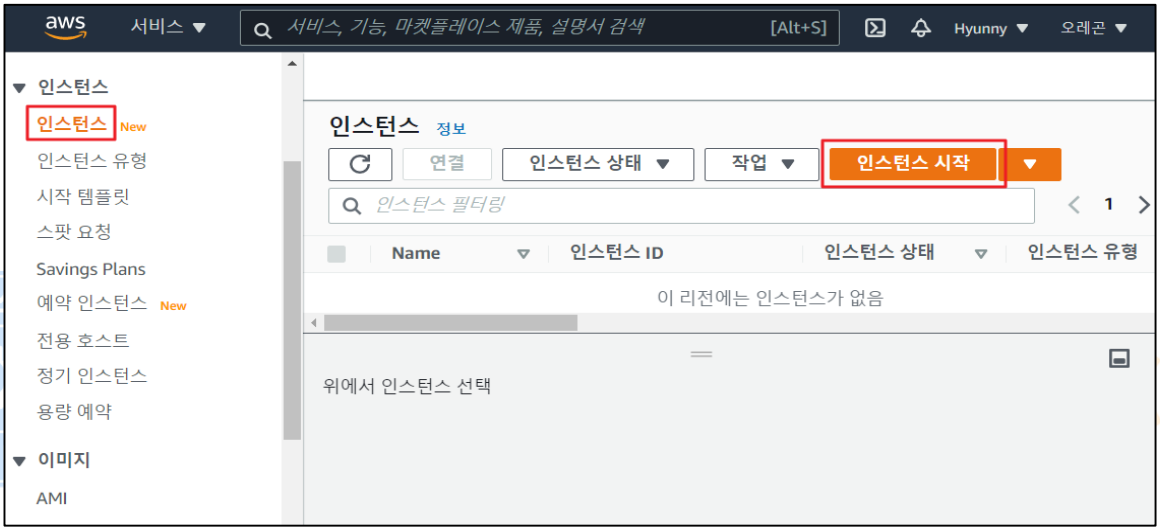
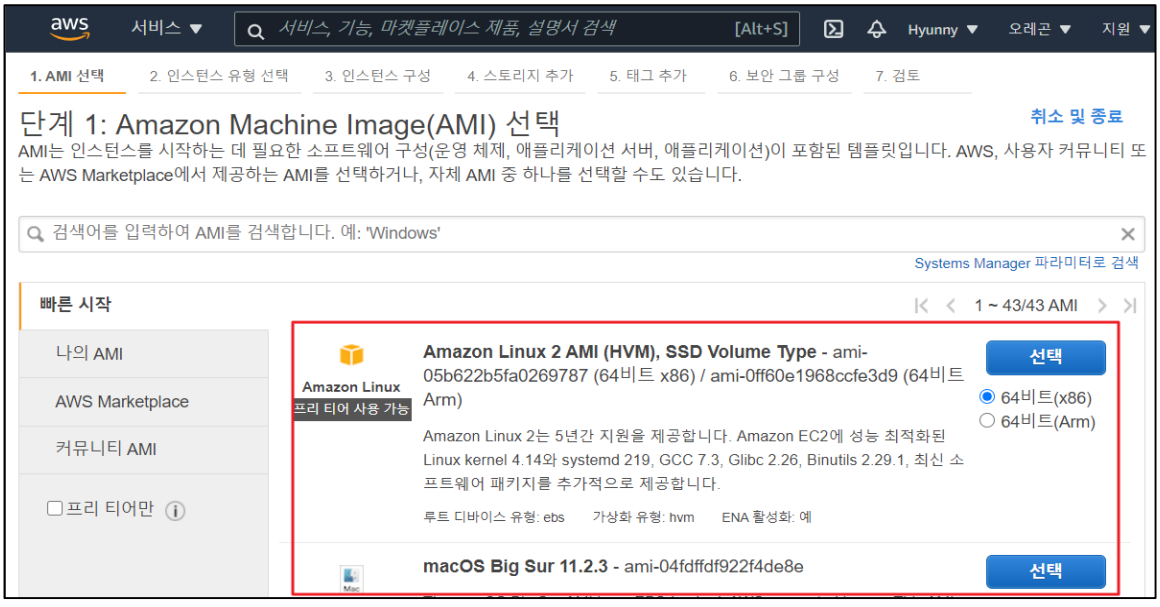


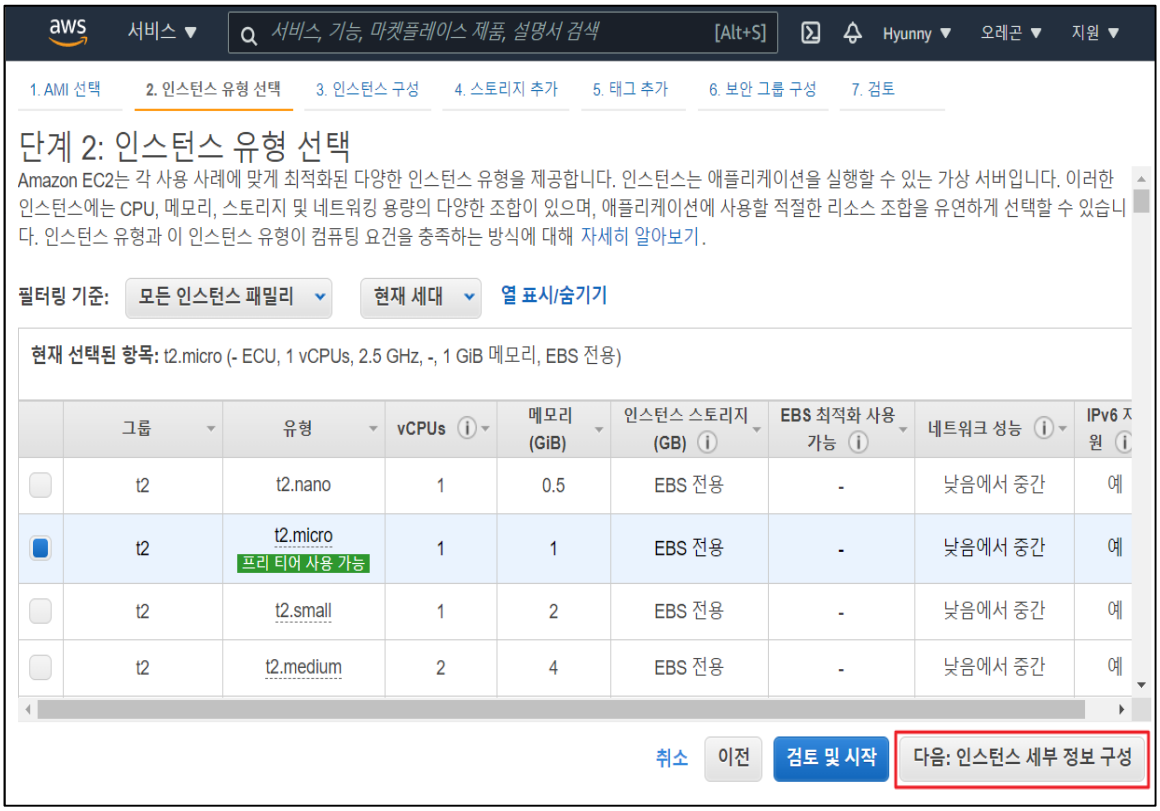


<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단 기준</td><td>양호기준
: IAM 그룹에 포함된 사용자 계정 중 불필요한 계정이 존재하지 않을 경우
취약기준
: IAM 그룹에 포함된 사용자 계정 중 불필요한 계정이 존재할 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

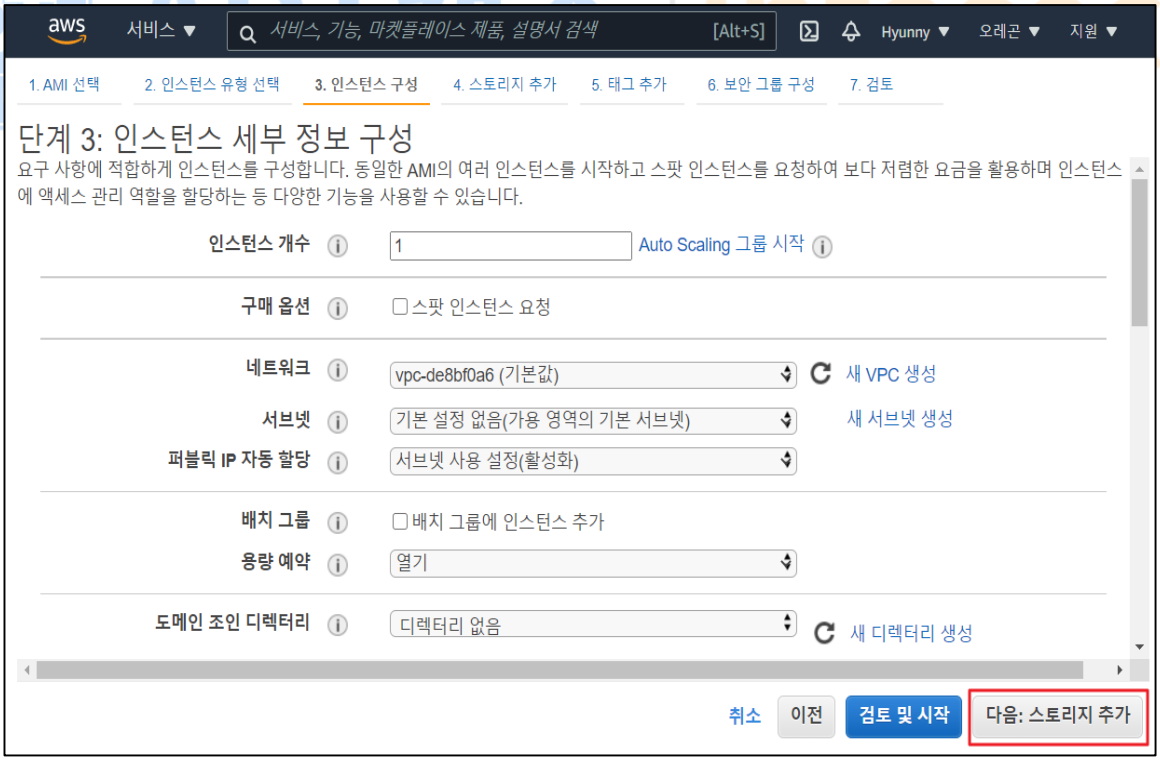
3. 데이터관리

3.1 인스턴스 암호화 설정

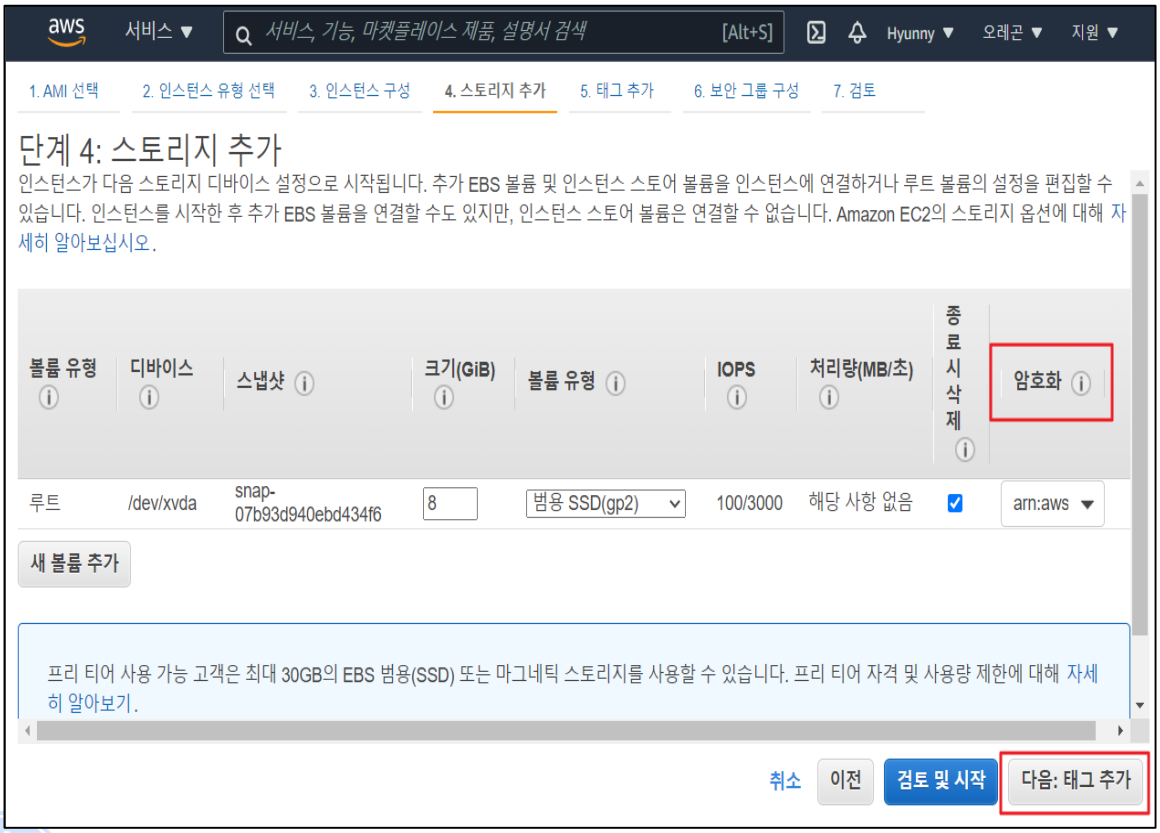
분류	데이터관리	중요도	중
항목명	인스턴스 암호화 설정		
항목 설명	EBS는 EC2 인스턴스 생성 및 이용 시 사용되는 블록 형태의 스토리지 볼륨이며 파일시스템 생성 및 블록 디바이스 사용 등을 할 수 있습니다. 또한 EBS는 AES-256 알고리즘을 사용하여 볼륨 암호화를 지원하며 데이터 및 애플리케이션에 대한 다양한 정보를 안전하게 저장할 수 있게 해줍니다.		
설정 방법	**가. EC2 스토리지 암호화 설정 방법** 1) 인스턴스 시작 클릭  2) AMI 선택  3) 인스턴스 유형 선택		



4) 인스턴스 구성

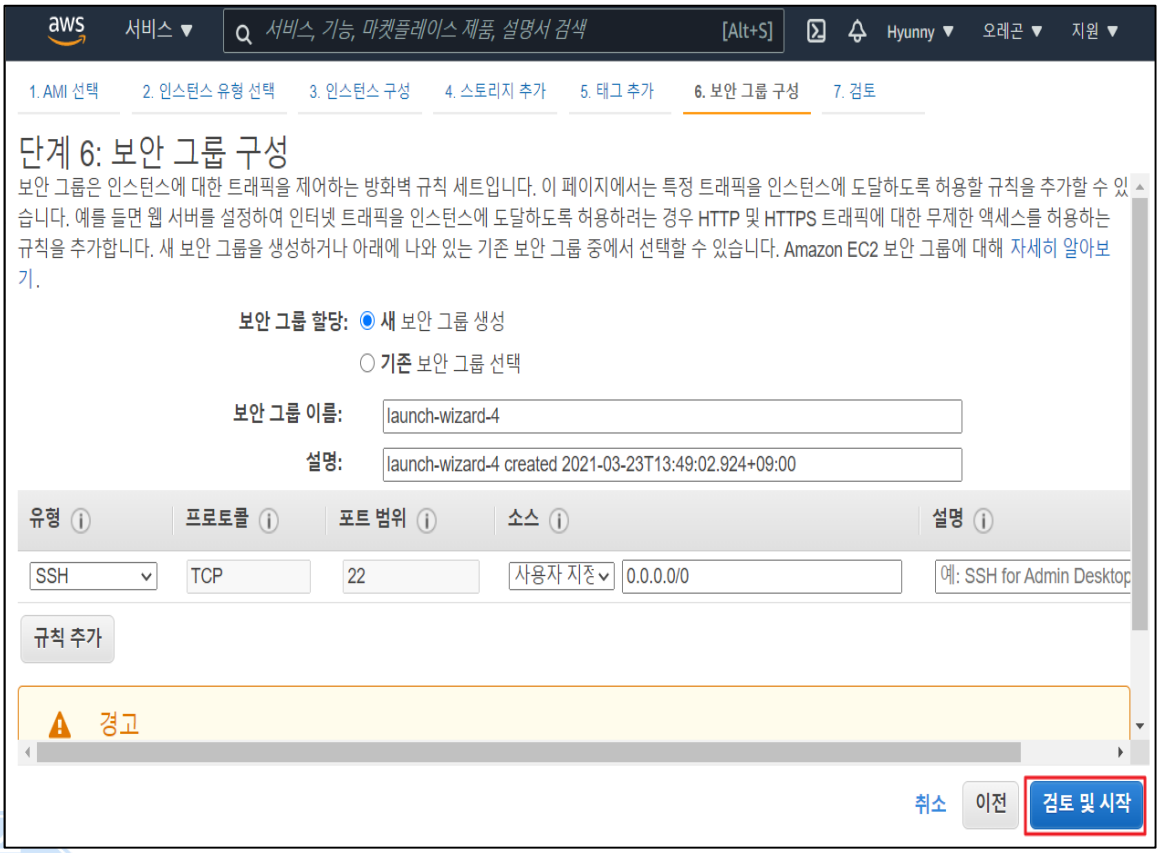


5) 스토리지 추가



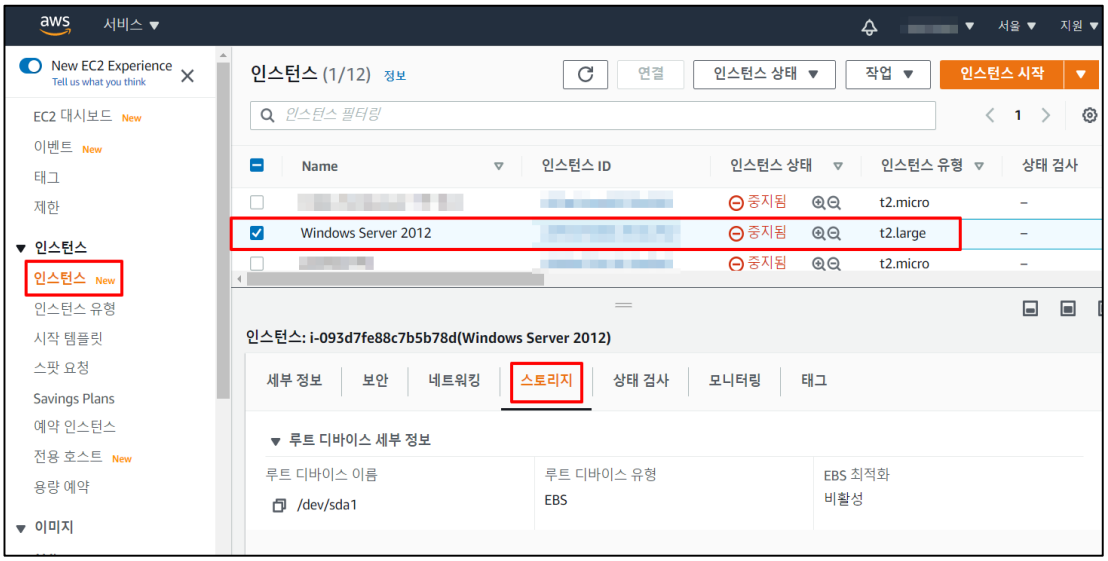
6) 태그추가

7) 보안 그룹 구성

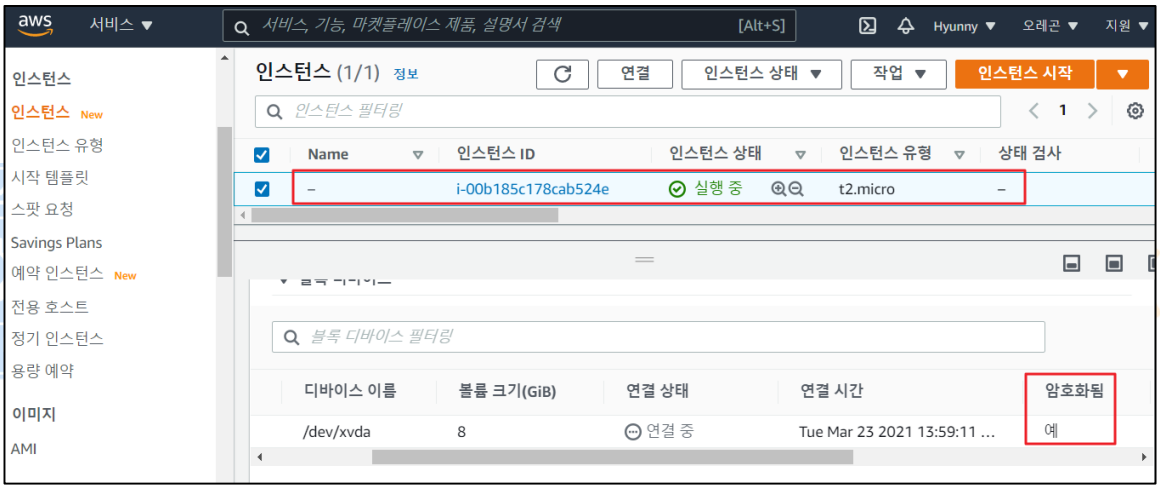


8) 스토리지 암호화 여부 확인

9) EC2 인스턴스 클릭 및 스토리지 클릭

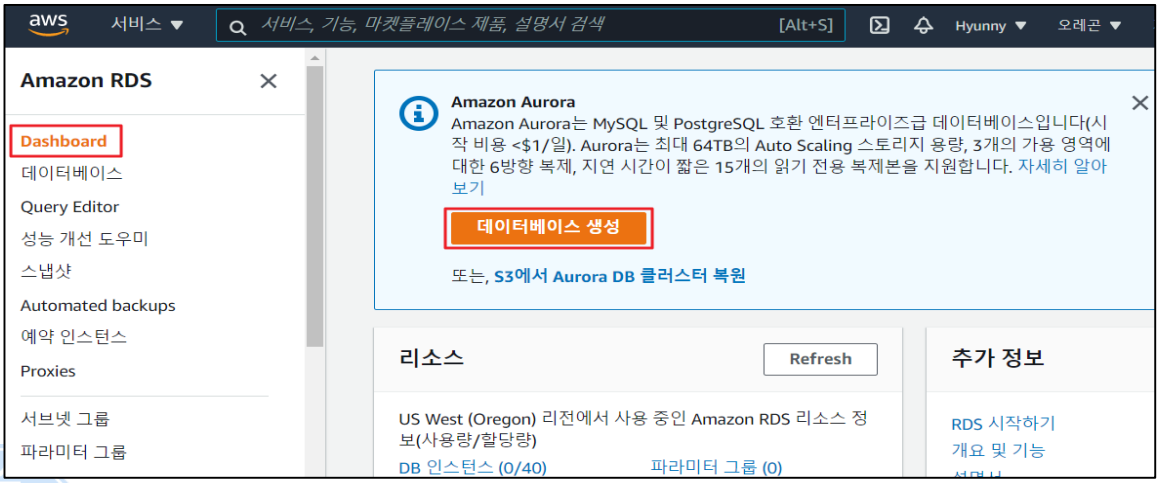
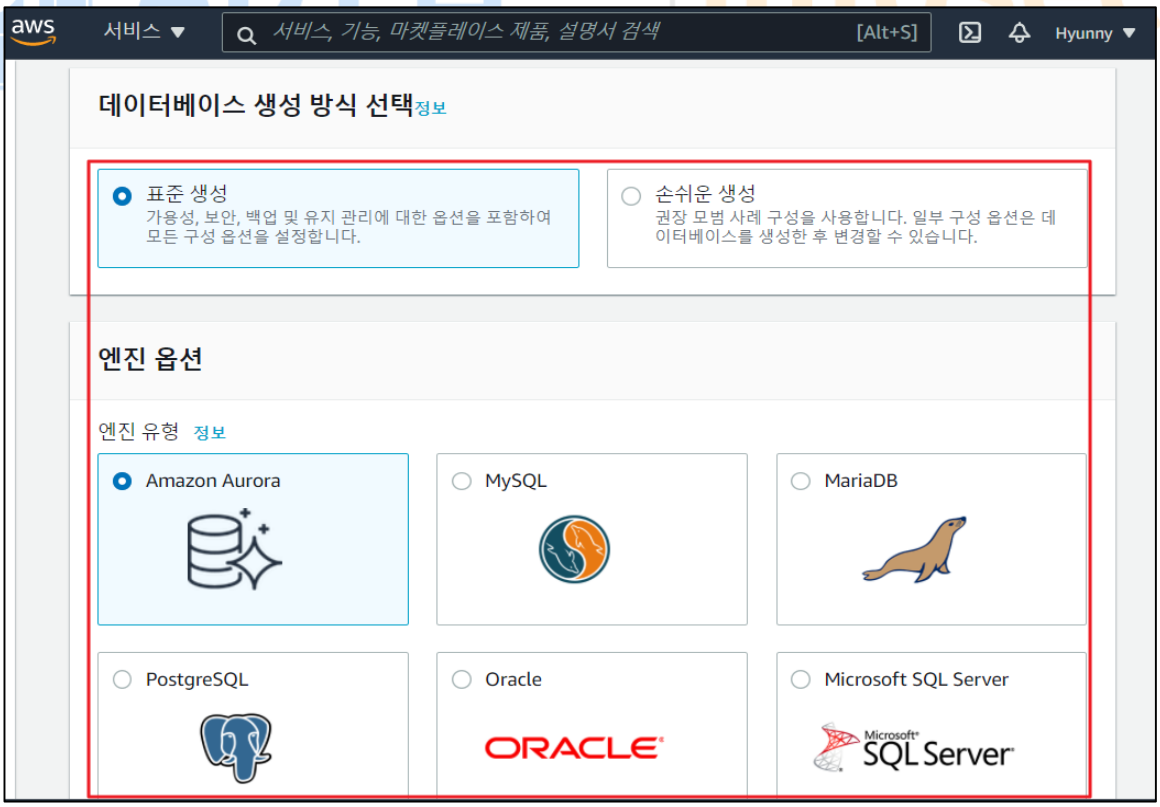


10) 스토리지 암호화 설정여부 확인

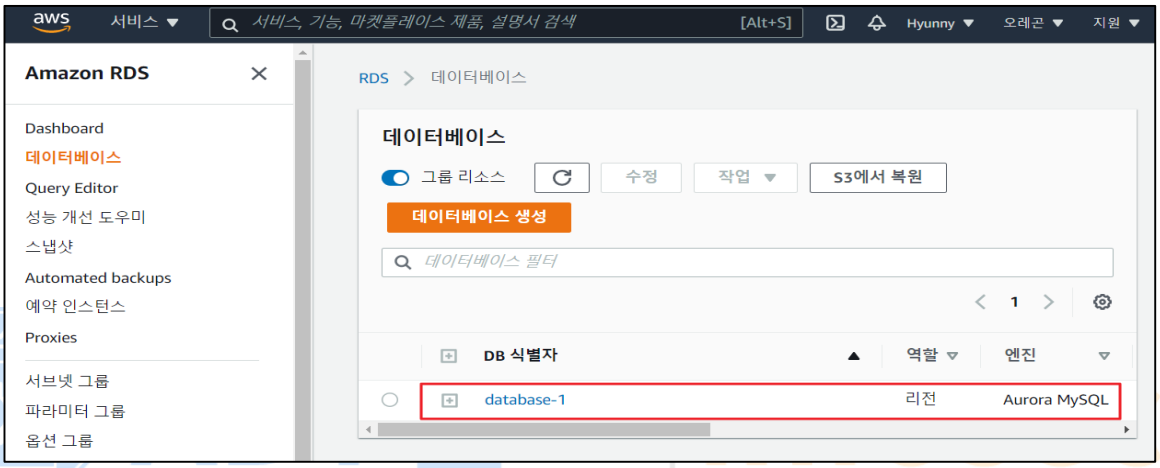


진단 기준	**양호기준** : EC2 인스턴스 스토리지 내 블록 디바이스 암호화가 활성화되어 있을 경우 **취약기준** : EC2 인스턴스 스토리지 내 블록 디바이스 암호화가 비활성화되어 있을 경우
비고	

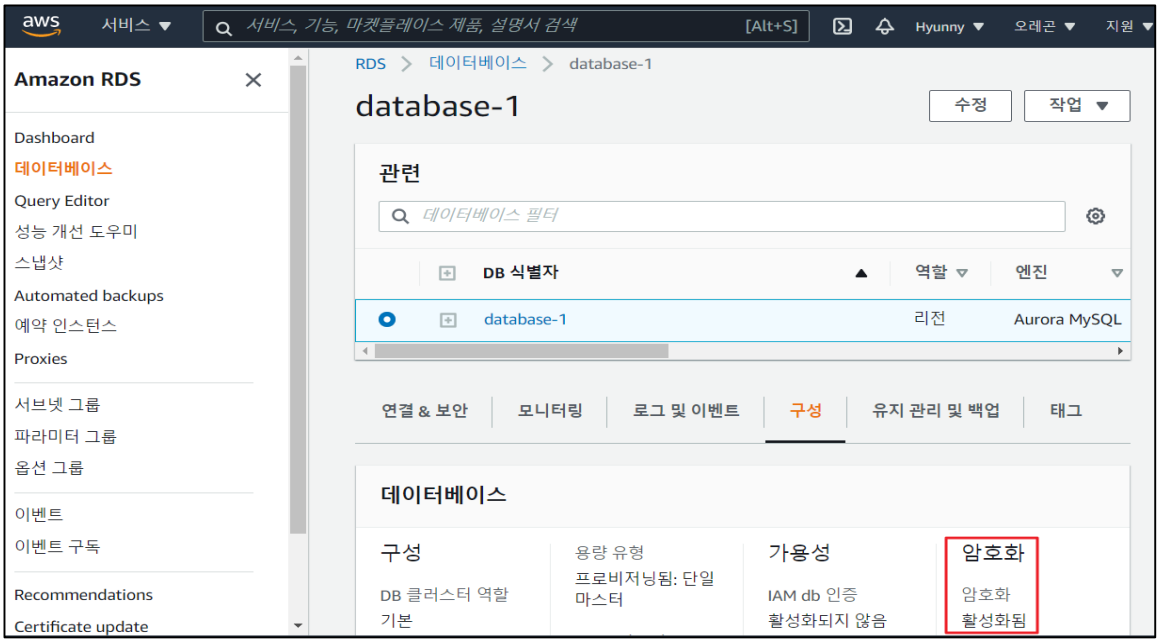
3.2 RDS 암호화 설정

분류	데이터관리	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 스토리지 암호화 설정 확인** 1) 데이터베이스 클릭  2) DB 생성 방식 및 엔진 등 설정  3) 데이터베이스 암호화 설정		

4) 데이터베이스 생성 확인



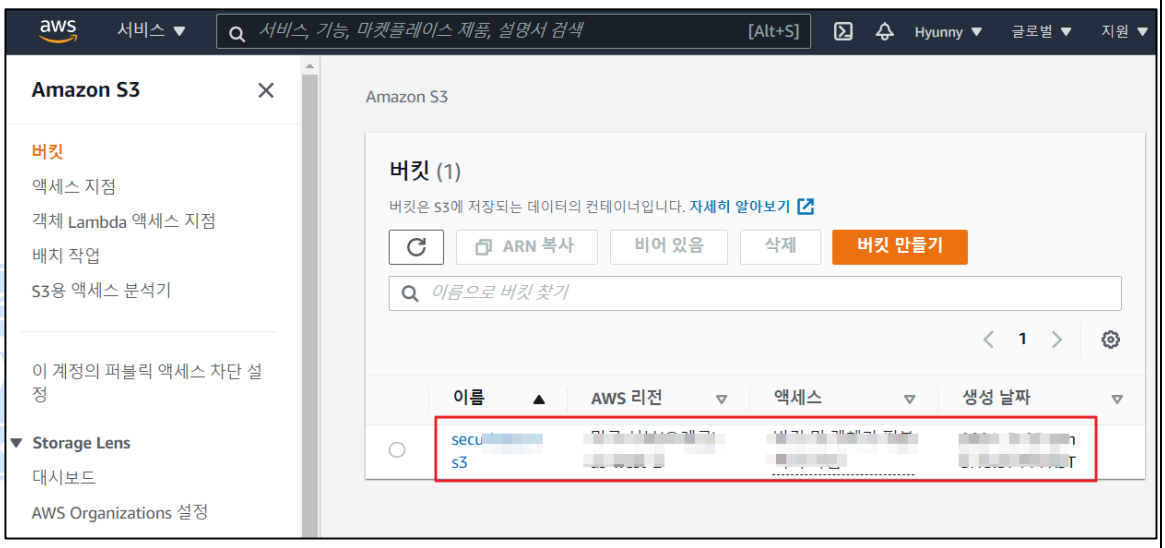
5) 데이터베이스 암호화 확인



진단 기준	**양호기준** : RDS 스토리지 암호화가 활성화되어 있을 경우

	취약기준 : RDS 스토리지 암호화가 비활성화되어 있을 경우
비고	

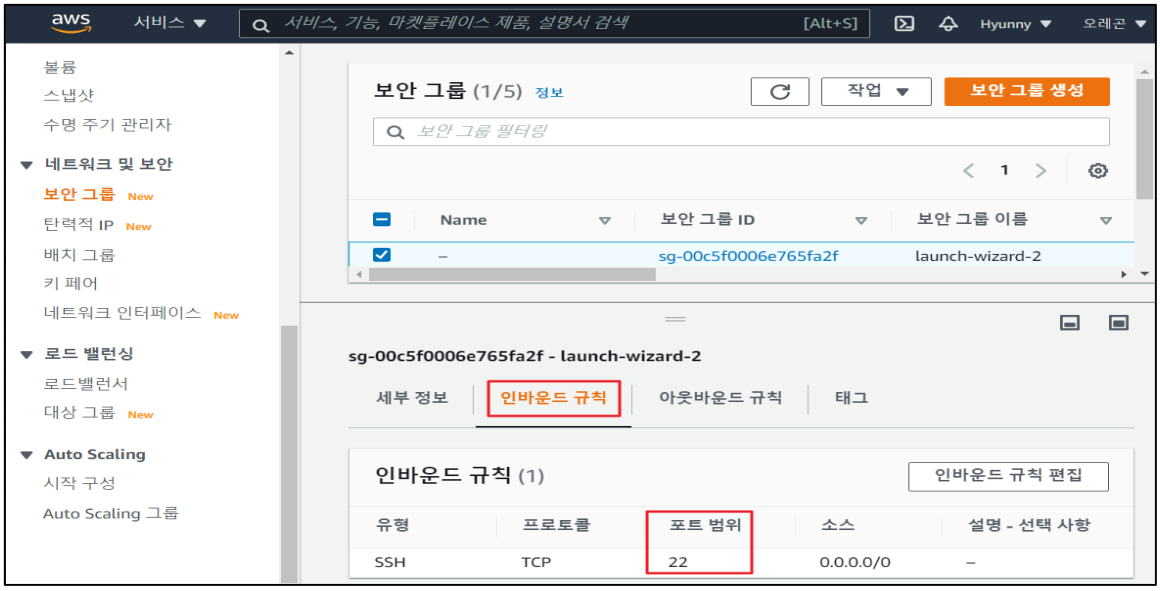
3.3 S3 암호화 설정

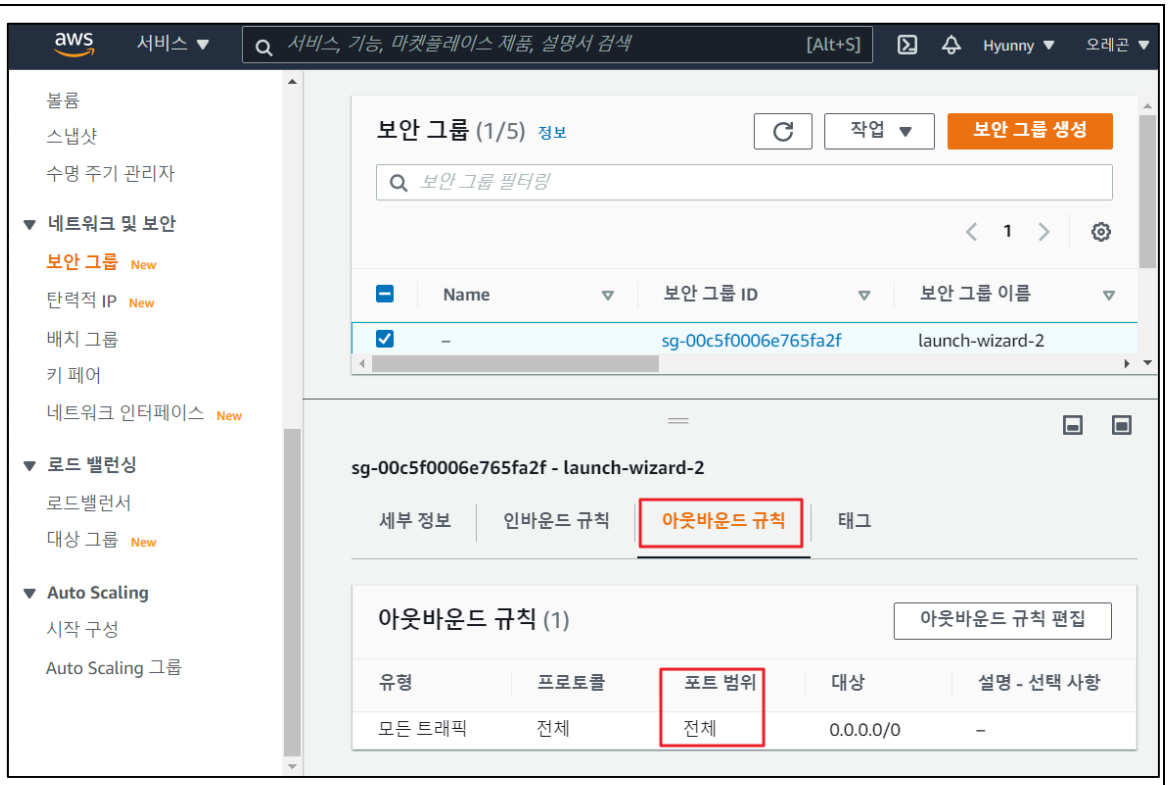
분류	데이터관리	중요도	중
항목명	S3 암호화 설정		
항목 설명	버킷 기본 암호화 설정은 S3 버킷에 저장되는 모든 객체를 암호화 되도록 하는 설정이며 Amazon S3 관리형 키(SSE-S3) 또는 AWS KMS 관리형 키(SSE-KMS)로 서버 측 암호화를 사용하여 객체를 암호화합니다. **※ S3 버킷 신규 생성 시 기본 암호화 (SSE-S3, SSE-KMS)를 설정할 수 있으며, 버킷에 기본 암호화가 적용된 상태에서 객체가 저장될 경우 하위 객체까지 자동으로 암호화 설정이 가능함**		
설정 방법	**가. S3 버킷 기본 암호화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

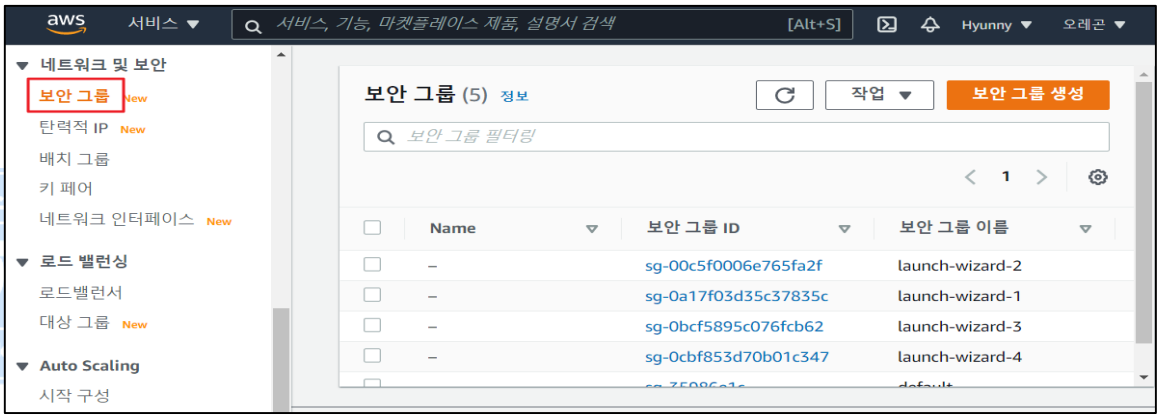
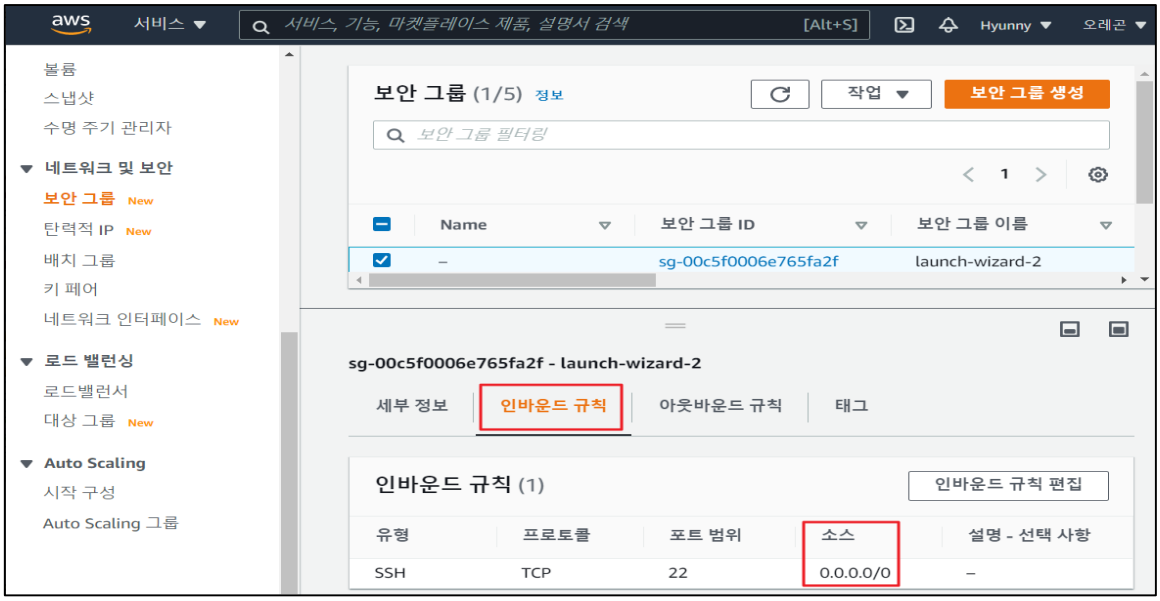
4. 가상 리소스 관리

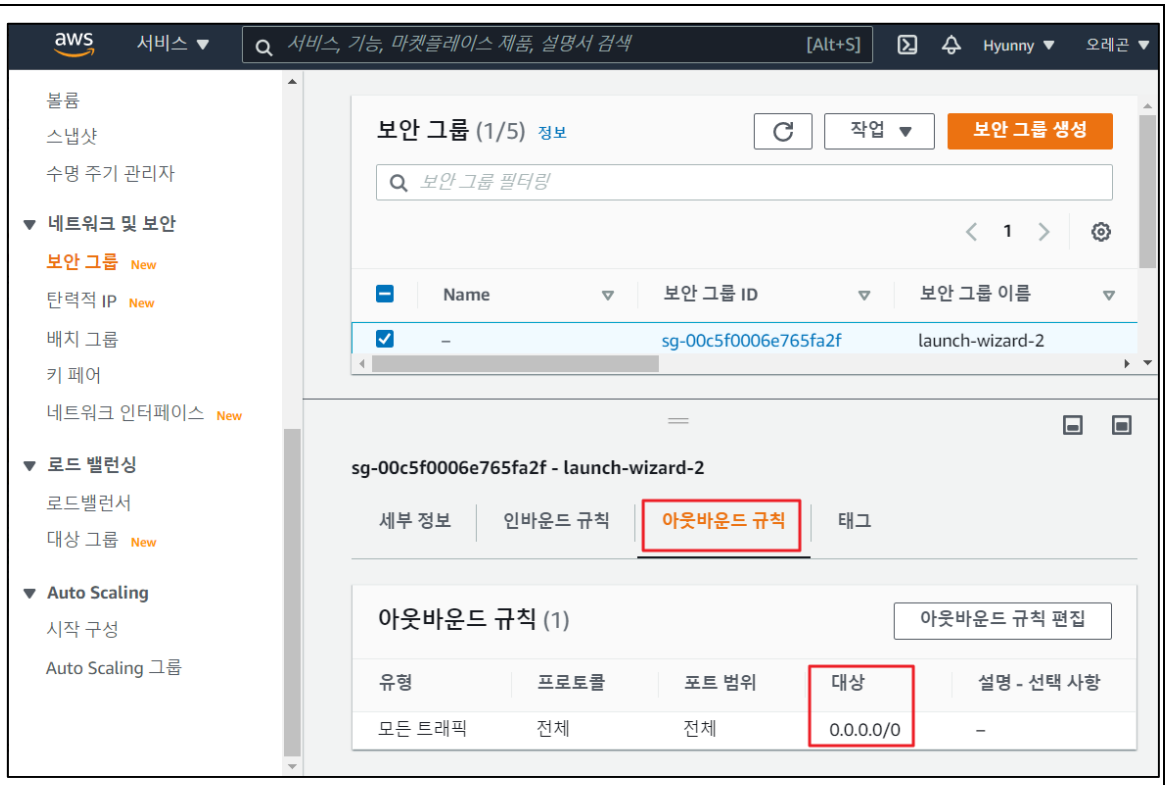
4.1 보안그룹 인/아웃바운드 ANY 설정 관리

분류	가상 리소스 관리	중요도	중
항목명	보안그룹 인/아웃바운드 ANY 설정 관리		
항목 설명	VPC에서의 Security Group은 EC2 인스턴스에 대한 인/아웃바운드 트래픽을 제어하는 가상 방화벽 역할을 합니다. VPC에서 EC2 인스턴스를 시작할 때 최대 5개의 Security Group에 인스턴스를 할당할 수 있습니다. Security Group은 서브넷 수준이 아니라 인스턴스 수준에서 작동하므로 VPC에 있는 서브넷의 각 인스턴스를 서로 다른 Security Group 세트에 할당할 수 있습니다. 보안그룹은 인/아웃바운드의 규칙 편집을 통해 특정 소스(출발지)에서의 통신이 가능하도록 유형(네트워크 프로토콜) 및 단일/범위 Port를 설정할 수 있습니다.		
설정 방법	**가. 보안그룹 인/아웃바운드 포트 정책 확인** 1) EC2 내 보안 그룹 탭 접근 -> 보안그룹 ID 선택  2) 선택된 보안 그룹 인바운드 규칙 내 포트 확인  3) 선택된 보안 그룹 아웃바운드 규칙 내 포트 확인		

	
진단 기준	**양호기준** : EC2 인스턴스에 대한 인/아웃바운드의 Port가 Any로 허용되어 있지 않을 경우 **취약기준** : EC2 인스턴스에 대한 인/아웃바운드의 Port가 Any로 허용되어 있을 경우
비고	

4.2 보안그룹 인/아웃바운드 불필요 정책 관리

분류	가상 리소스 관리	중요도	중
항목명	보안그룹 인/아웃바운드 불필요 정책 관리		
항목 설명	VPC에서의 Security Group은 EC2 인스턴스에 대한 인/아웃바운드 트래픽을 제어하는 가상 방화벽 역할을 합니다. VPC에서 EC2 인스턴스를 시작할 때 최대 5개의 Security Group에 인스턴스를 할당할 수 있습니다. Security Group은 서브넷 수준이 아니라 인스턴스 수준에서 작동하므로 VPC에 있는 서브넷의 각 인스턴스를 서로 다른 Security Group 세트에 할당할 수 있습니다. 보안그룹은 인/아웃바운드의 규칙 편집을 통해 특정 소스(출발지)에서의 통신이 가능하도록 유형(네트워크 프로토콜) 및 단일/범위 정책을 설정할 수 있습니다.		
설정 방법	**가. 보안그룹 인/아웃바운드 소스 정책 확인** 1) EC2 내 보안 그룹 탭 접근 -> 보안그룹 ID 선택  2) 선택된 보안 그룹 인바운드 규칙 내 소스 확인  3) 선택된 보안 그룹 아웃바운드 규칙 내 소스 확인		

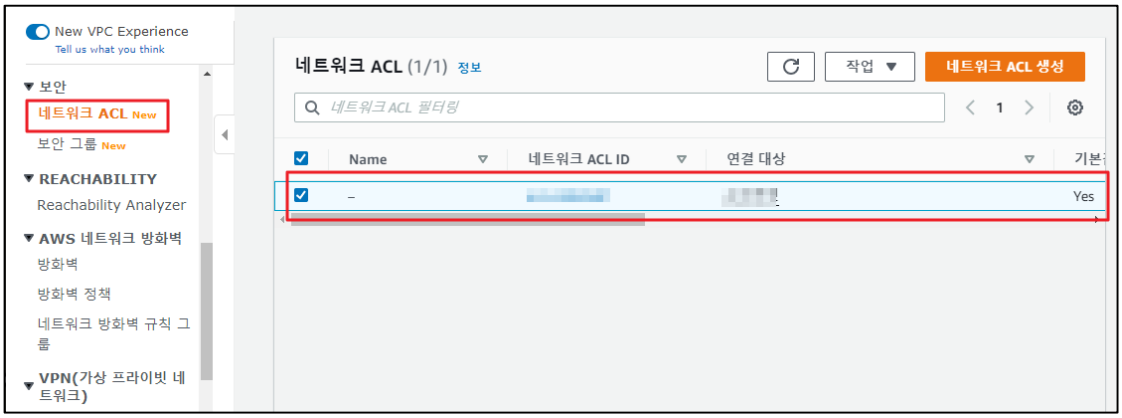
	
진단 기준	**양호기준** : EC2 인스턴스에 대한 인/아웃바운드 소스와 목적지의 불필요한 정책이 허용되어 있지 않을 경우 **취약기준** : EC2 인스턴스에 대한 인/아웃바운드 소스와 목적지의 불필요한 정책이 허용되어 있을 경우
비고	

4.3 ACL 네트워크 인/아웃바운드 트래픽 정책 관리

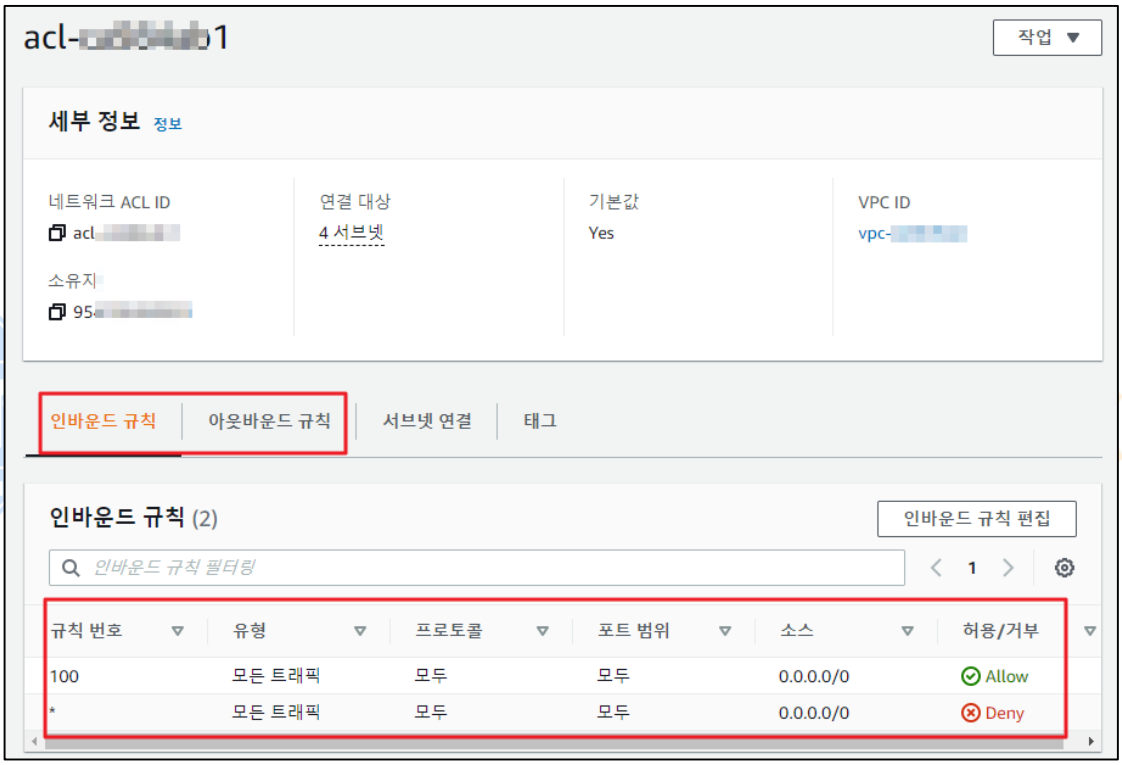
<table>
<tr><td>분류</td><td>가상 리소스 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">ACL 네트워크 인/아웃바운드 트래픽 정책 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">
ACL(Access Control List)은 1개 이상의 서브넷 내부와 외부의 트래픽을 제어하기 위한 방화벽 역할을 하는 VPC의 선택적 보안 계층입니다. 보안 그룹과 비슷한 규칙으로 네트워크 ACL을 설정하여 VPC에 보안 계층을 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 사용이됩니다.

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 서브넷을 드나드는 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">Inbound</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">Outbound</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>

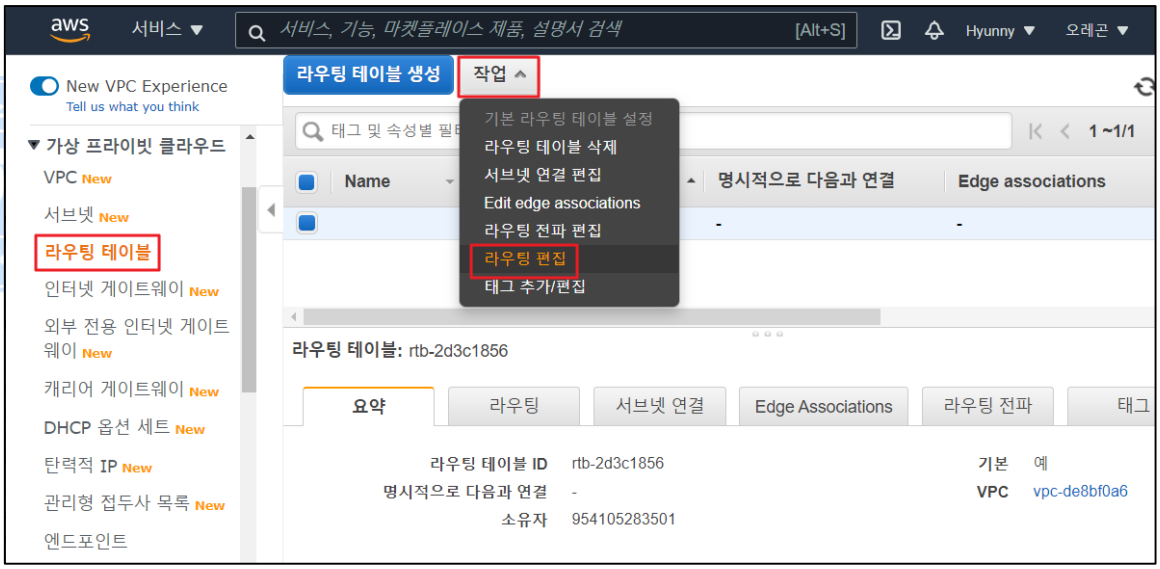


2) 인바운드/아웃바운드 규칙 확인

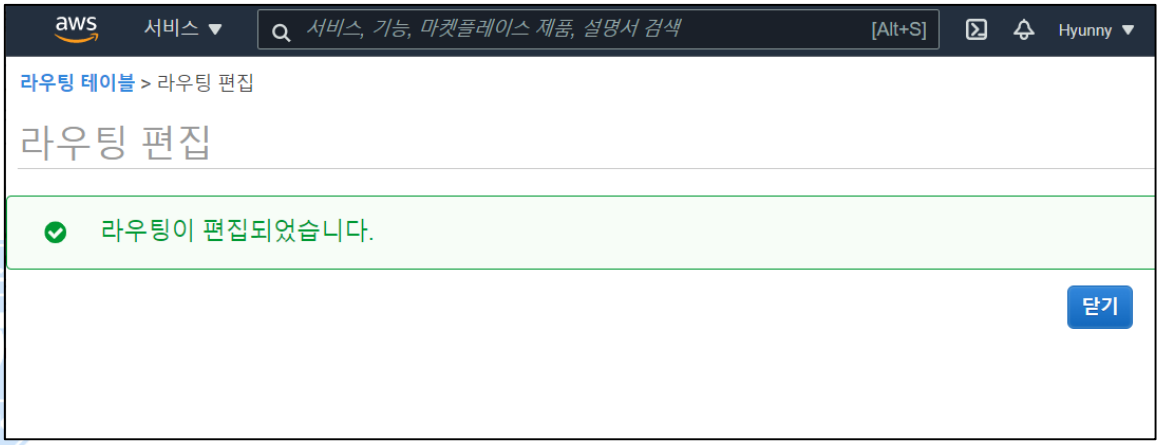


진단 기준	**양호기준** : 인/아웃바운드에 대한 모든 트래픽이 허용되어 있지 않을 경우 **취약기준** : 인/아웃바운드에 대한 모든 트래픽이 허용되어 있을 경우
비고	

4.4 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 라우트을 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 라우트을 제어합니다. 기본 라우팅 테이블에서 라우트를 추가 및 제거하고 수정할 수 있습니다.		
설정 방법	**가. 라우팅 테이블 설정 방법** 1) VPC → 라우팅 테이블 → 라우팅 테이블 선택 → 작업 → 라우팅 편집 → 라우팅 추가 		

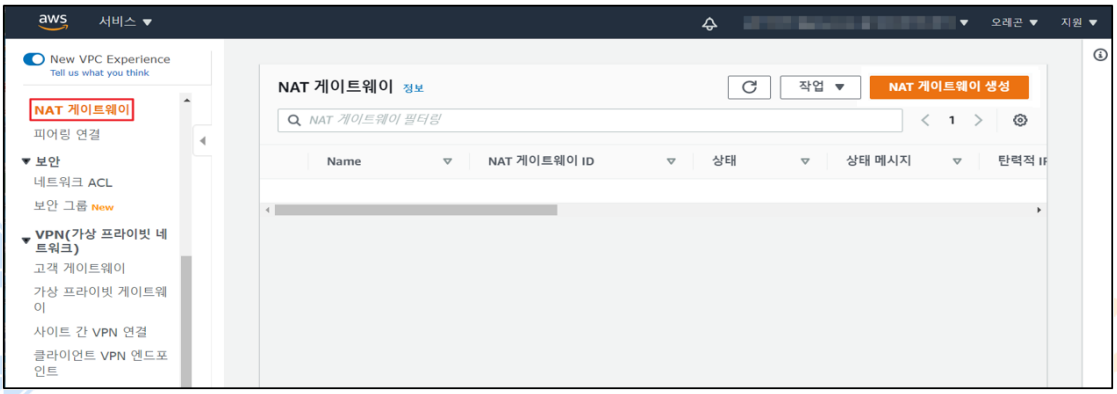
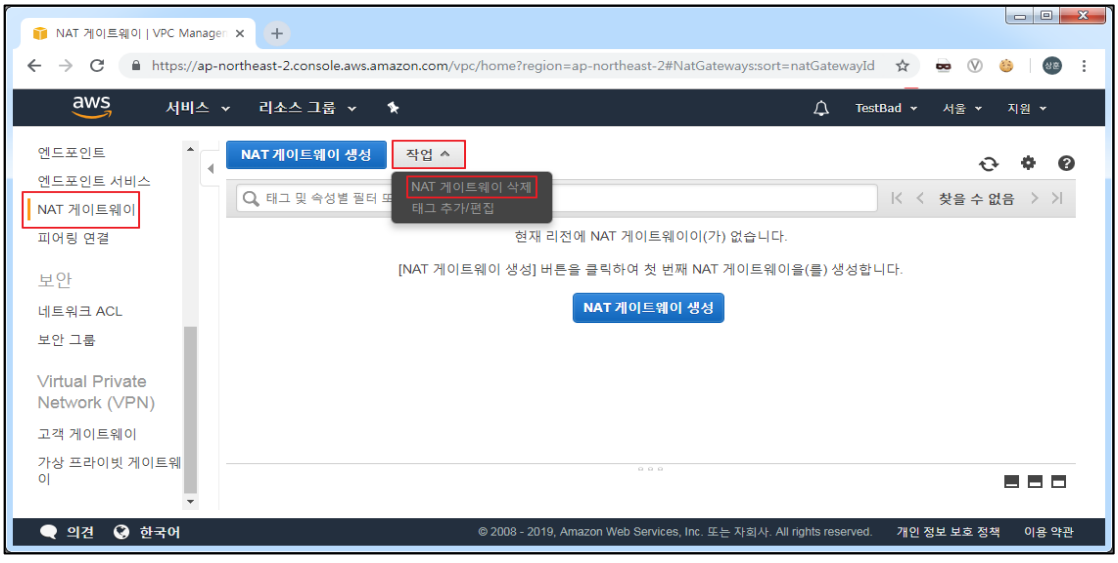
<table>
<tr>
<td></td>
<td>

</td>
</tr>
<tr>
<td>진단 기준</td>
<td>
양호기준
: 목적지가 ANY 미설정 및 서비스 타켓별로 설정 또는 활성화 되어 있을 경우

취약기준
: 목적지가 ANY로 설정되어 있을 경우
</td>
</tr>
<tr>
<td>비고</td>
<td></td>
</tr>
</table>

4.5 NAT 게이트웨이 연결 관리

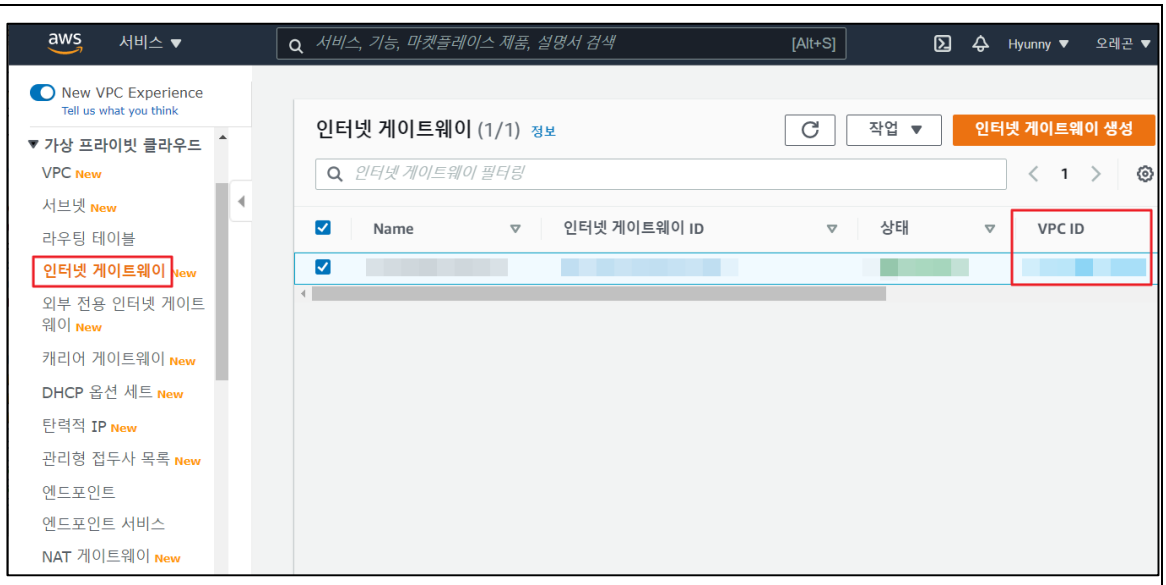
분류	가상 리소스 관리	중요도	중
항목명	NAT 게이트웨이 연결 관리		
항목 설명	NAT 게이트웨이는 NAT 디바이스를 사용하여 프라이빗 서브넷의 인스턴스를 인터넷(예: 소프트웨어 업데이트용) 또는 기타 AWS 서비스에 연결하는 한편, 인터넷에서 해당 인스턴스와의 연결을 시작하지 못하도록 할 수 있습니다. NAT 디바이스는 프라이빗 서브넷의 인스턴스에서 인터넷 또는 기타 AWS 서비스로 트래픽을 전달한 다음 인스턴스에 응답을 다시 보냅니다. 트래픽이 인터넷으로 이동하면 소스 IPv4 주소가 NAT 디바이스의 주소로 대체되고, 이와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

기준	: NAT 게이트웨이가 설정되어 있지 않거나 실 사용중인 Private 서브넷 인스턴스가 연결되어 있을 경우 **취약기준** : NAT 게이트웨이를 사용할 경우 사용하지 않는 Private 서브넷 인스턴스가 연결되어 있을 경우
비고	

4.6 인터넷 게이트웨이 연결 관리

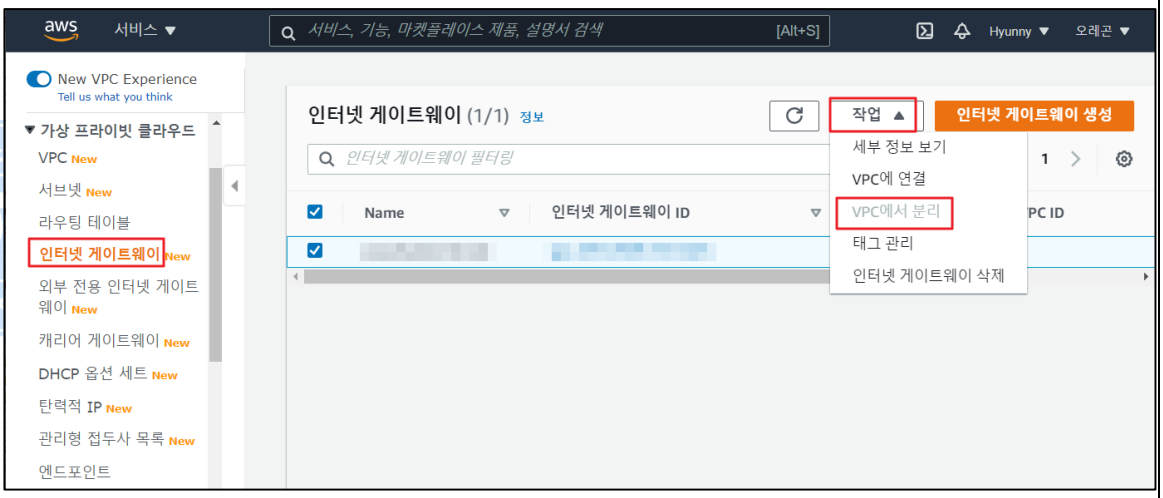
<table>
<tr><td>분류</td><td>가상 리소스 관리</td><td>중요도</td><td>하</td></tr>
<tr><td>항목명</td><td colspan="3">인터넷 게이트웨이 연결 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">인터넷 게이트웨이는 수평 확장되고 가용성이 높은 중복 VPC 구성요소로, VPC의 인스턴스와 인터넷간에 통신이 가능할 수 있게 해주는 기능이며 네트워크 트래픽 가용성 위험이나 대역폭 제약조건이 별도로 발생하진 않습니다.
인터넷 게이트웨이에는 인터넷 Route 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>



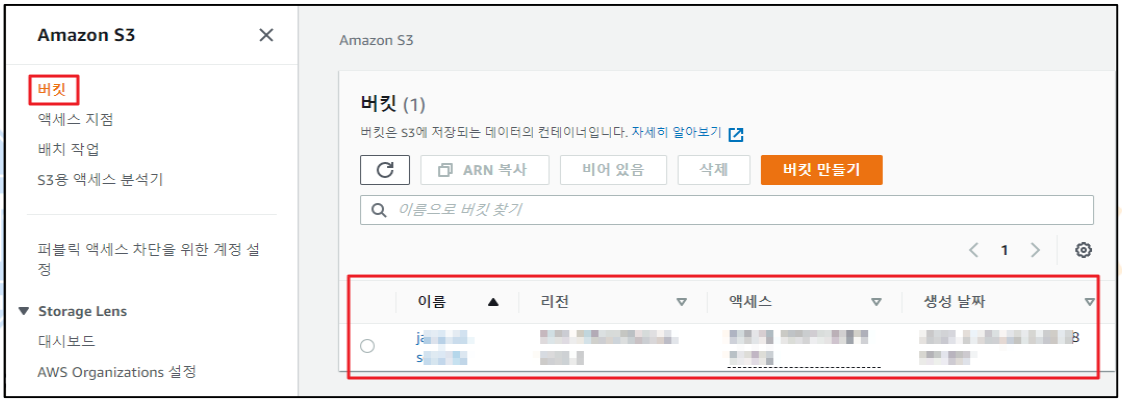
나. 인터넷 게이트웨이 삭제 방법

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



진단 기준	**양호기준** : 다수의 인터넷 게이트웨이 관리 시 연결된 VPC내 인스턴스가 존재할 경우 **취약기준** : 다수의 인터넷 게이트웨이 관리 시 연결된 VPC내 인스턴스가 존재하지 않을 경우
비고	

4.7 S3 버킷 접근 관리

분류	가상 리소스 관리	중요도	중
항목명	S3 버킷 접근 관리		
항목 설명	S3는 AWS 인터넷 클라우드 스토리지 서비스로 언제 어디서나 원하는 양의 데이터를 저장하고 검색할 수 있는 서비스이며, 데이터 저장/관리를 하기 위해 S3 서비스 내 버킷 사용이 필요하며 버킷 설정 시 접근 보안에 대해 다음과 같은 설정 / 관리 / 정책 등을 고려해야 합니다. **1) 버킷 권한 부여** -Public S3: 외부 사용의 관한 연결 통로를 제공하는 것이기 때문에 설정을 제한해야 합니다. -Private S3: 접근가능한 IAM 계정에 대한 권한이 설정되어 있어야 합니다. **※ AWS Root Account로의 접근은 지양하며 가급적 IAM 계정을 통한 S3 접근을 권장함**		
설정 방법	**가. S3 버킷 그룹 권한 확인** 1) S3 버킷 선택  2) S3 버킷 권한 확인  		
진단	양호기준		

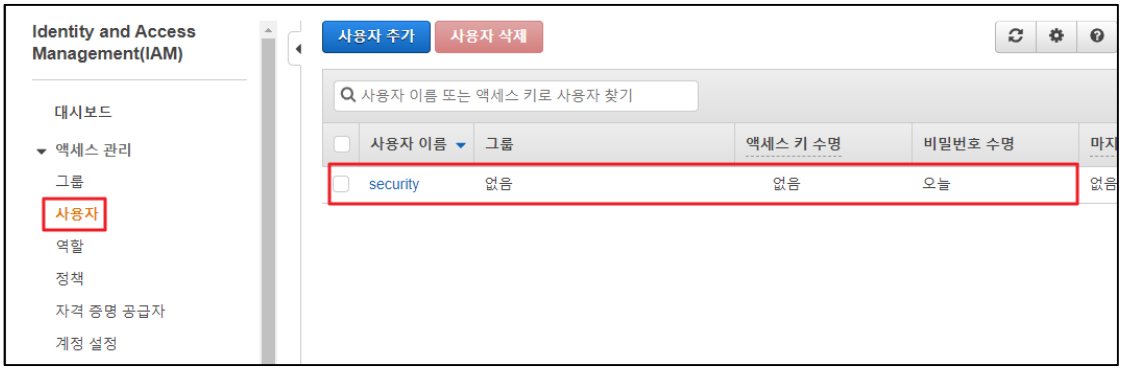
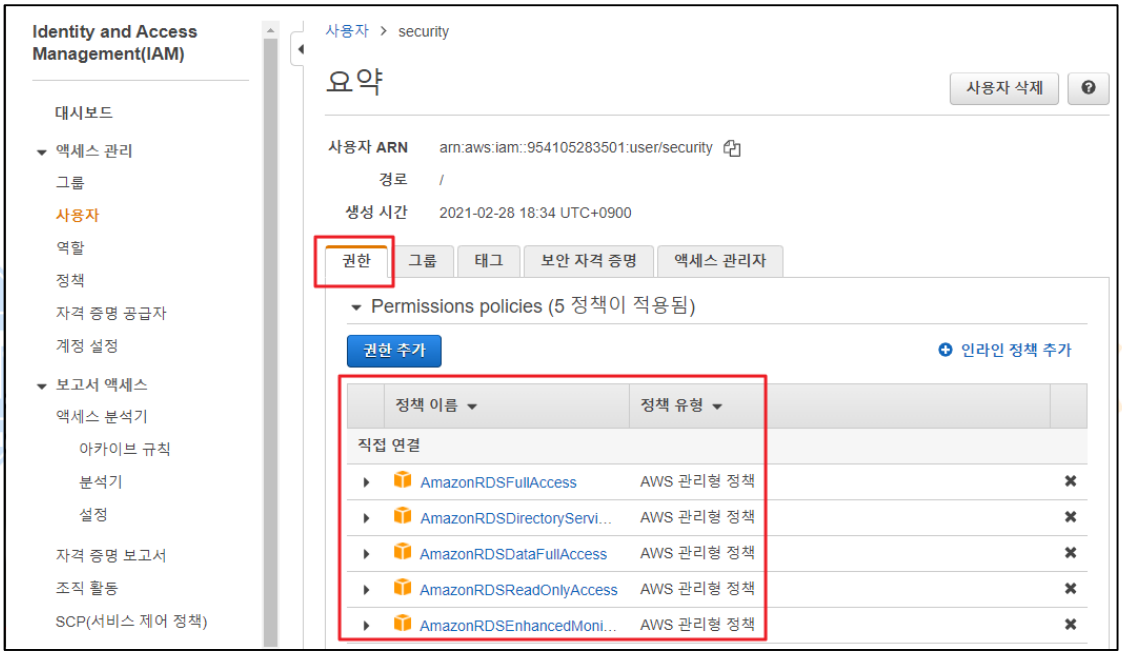
기준	: "Everyone" 그룹에 권한이 모두 미설정일 경우 **취약기준** : "Everyone" 그룹에 " 객체 목록 생성", "객체 쓰기", "버킷 읽기 권한", "버킷 쓰기 권한"이 부여되어 있을 경우
비고	

4.8 RDS 리소스 액세스 권한 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">RDS 리소스 액세스 권한 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">
Amazon RDS에서의 기본 리소스는 DB 인스턴스입니다. Amazon RDS 기본 리소스와 함께 사용할 수 있는 다른 리소스 (예:DB 스냅샷, 파라미터 그룹, 이벤트 구독 등)를 지원하며 이러한 리소스를 가리켜 하위 리소스라고 합니다.
하기 표에 나와 있는 것처럼 이러한 리소스와 하위 리소스에는 고유한 Amazon 리소스 이름(ARN)이 연결되어 있습니다.

※ RDS 리소스 유형 및 ARN 형식 표
<table>
<tr><th>리소스 유형</th><th>ARN 형식</th></tr>
<tr><td>DB 클러스터</td><td>arn:aws:rds:region:account-id:cluster:db-cluster-name</td></tr>
<tr><td>DB 클러스터 파라미터 그룹</td><td>arn:aws:rds:region:account-id:cluster-pg:cluster-parameter-group-name</td></tr>
<tr><td>DB 클러스터 스냅샷</td><td>arn:aws:rds:region:account-id:cluster-snapshot:cluster-snapshot-name</td></tr>
<tr><td>DB 인스턴스</td><td>arn:aws:rds:region:account-id:db:db-instance-name</td></tr>
<tr><td>DB 옵션 그룹</td><td>arn:aws:rds:region:account-id:og:option-group-name</td></tr>
<tr><td>DB 파라미터 그룹</td><td>arn:aws:rds:region:account-id:pg:parameter-group-name</td></tr>
<tr><td>DB 스냅샷</td><td>arn:aws:rds:region:account-id:snapshot:snapshot-name</td></tr>
<tr><td>DB 보안 그룹</td><td>arn:aws:rds:region:account-id:secgrp:security-group-name</td></tr>
<tr><td>DB 서브넷 그룹</td><td>arn:aws:rds:region:account-id:subgrp:서브넷-group-name</td></tr>
<tr><td>이벤트 구독</td><td>arn:aws:rds:region:account-id:es:subscription-name</td></tr>
<tr><td>읽기 전용 복제본</td><td>arn:aws:rds:region:account-id:db:db-instance-name</td></tr>
<tr><td>예약 DB 인스턴스</td><td>arn:aws:rds:region:account-id:ri:reserved-db-instance-name</td></tr>
</table>

RDS 정책을 "계정 내 사용자 또는 그룹에 권한 정책 연결" 및 "역할에 권한 정책 연결(교차 계정 권한 부여)" 같이 IAM 자격 증명에 연결할 수 있습니다.
- 계정 내 사용자 또는 그룹에 권한 정책 연결: 계정 관리자는 특정 사용자에 연결된 권한 정책을 사용하여 해당 사용자에게 Amazon RDS 리소스 생성 권한을 부여 할 수 있습니다.
- 역할에 권한 정책 연결(교차 계정 권한 부여): 자격 증명 기반 권한 정책을 IAM 역할에 연결하여 교차 계정 권한을 부여할 수 있습니다. 예를 들어, 계정 A의 관리자는 다음과 같이 다른 AWS 계정(예: 계정 B) 또는 AWS 서비스에 교차 계정 권한을 부여할 역할을 생성할 수 있습니다.
: 계정 A 관리자는 IAM 역할을 생성하고 계정 A의 리소스에 대한 권한을 부여하는 역할에 권한 정책을 연결
: 계정 A 관리자는 계정 B 역할을 대신할 보안 주체로 신뢰정책을 연결
: 계정 B 관리자는 계정 B의 사용자에게 역할을 수임할 권한을 위임할 수 있습니다.
이럴 경우 계정 B의 사용자가 계정 A에서 리소스를 생성하거나 액세스 할 수 있게 됩니다.
</td></tr>
</table>

설정 방법	**가. 계정별 권한 확인** 1) 사용자 계정 선택  2) 부여된 권한 확인 
진단 기준	**양호기준** : root 계정 관리자가 다수 사용자에게 RDS 리소스 생성 권한을 설정하지 않았을 경우 **취약기준** : root 계정 관리자가 다수 사용자에게 RDS 리소스 생성 권한을 설정했을 경우
비고	

4.9 RDS API 작업 권한 관리

분류	가상 리소스 관리	중요도	중
항목명	RDS API 작업 권한 관리		

항목 설명

Amazon RDS는 관리자 콘솔 외 API를 통해 리소스 접근 및 사용이 가능하기에 역할에 맞게 권한을 부여하여 비인가된 사용자가 API를 통해 RDS 관련 작업을 할 수 없도록 해야 합니다.

※ 예) 역할에 따른 권한 부여
AWS Root Account, 관리자(Infra, DBMS): AmazonRDSFullAccess
DBMS 개발 및 운영자: AmazonRDSDataFullAccess
DBMS 감사 및 비용담당자: AmazonRDSReadOnlyAccess

또한, CLI/API를 통해 RDS 리소스 접근 및 작업 시 사용되는 Access Key에 대해 주기적(3개월)으로 관리하여 보안상 문제가 발생되지 않도록 해야 합니다.
※ Access Key 수명(60일 이내), 비밀번호 수명(60일 이내), 마지막 활동(30일 이내)

※ RDS IAM Default 정책표

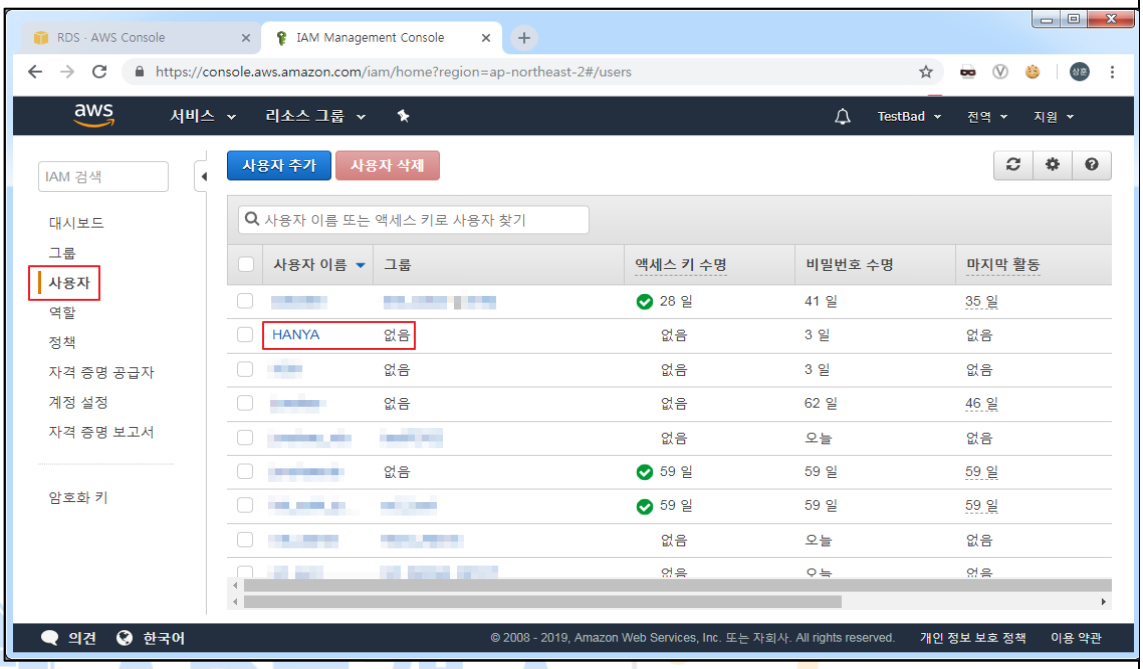
구분	AWS 관리형 정책	정책 설명
RDS	**AmazonRDSDataFullAccess**	**RDS 데이터 API, 자격 증명을 위한 비밀 저장소 API, DB 콘솔 쿼리 관리 API를 통한 AWS 계정의 Aurora Serverless 클러스터에서 SQL 문 실행 권한**
	AmazonRDSFullAccess	**Management Console을 통해 Amazon RDS에 대한 전체 액세스 권한 제공**
	AmazonRDSReadOnlyAccess	**Management Console을 통해 Amazon RDS에 대한 읽기 전용 액세스 권한 제공**
	AWSApplicationAutoscaling RDSClusterPolicy	Application Auto Scaling에 대한 권한을 부여하여 RDS 및 CloudWatch에 액세스하는 정책
	AmazonRDSBetaServiceRolePolicy	RDS가 사용자를 대신하여 AWS 리소스를 관리함
	AmazonRDSDirectoryServiceAccess	RDS가 도메인에 가입 한 SQL Server DB 인스턴스에 대해 고객 대신 Directory Service Managed AD에 액세스하도록 허용함
	AmazonRDSEnhancedMonitoringRole	Cloudwatch for RDS Enhanced Monitoring에 대한 액세스 제공
	AmazonRDSPreviewServiceRolePolicy	RDS 미리보기 서비스 역할 정책
	AmazonRDSServiceRolePolicy	RDS가 사용자를 대신하여 AWS 리소스를 관리함
	AWSQuickSightDescribeRDS	QuickSight에서 RDS 리소스를 설명하도록

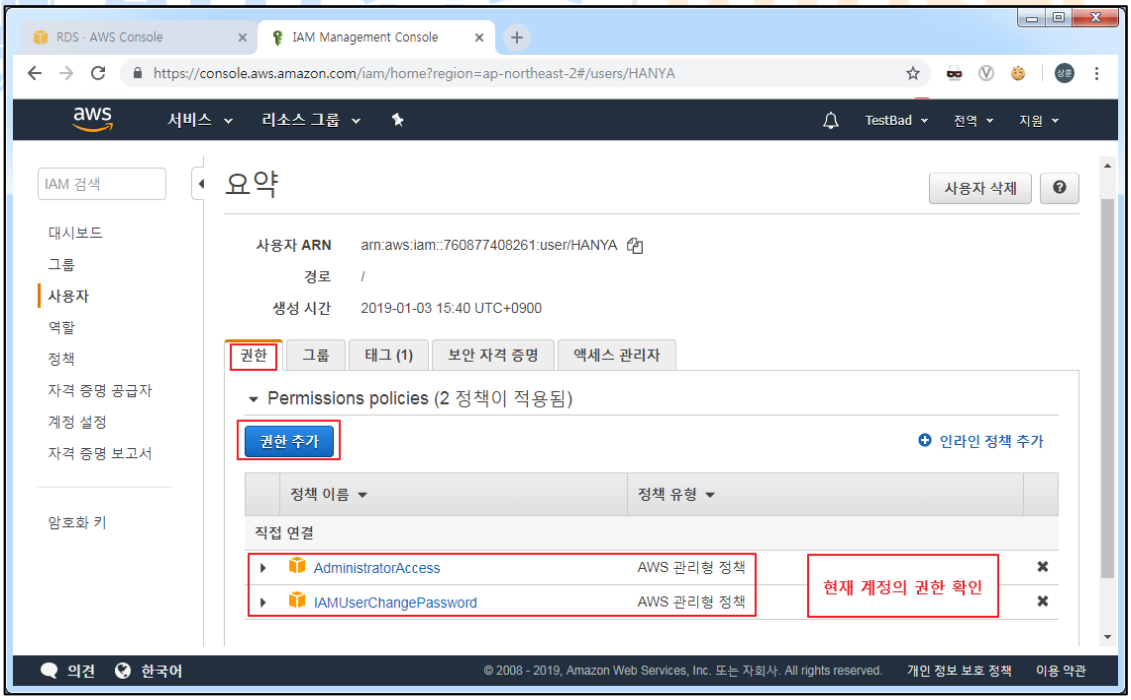
		허용
	RDSCloudHsmAuthorizationRole	RDS 서비스 역할의 기본 정책

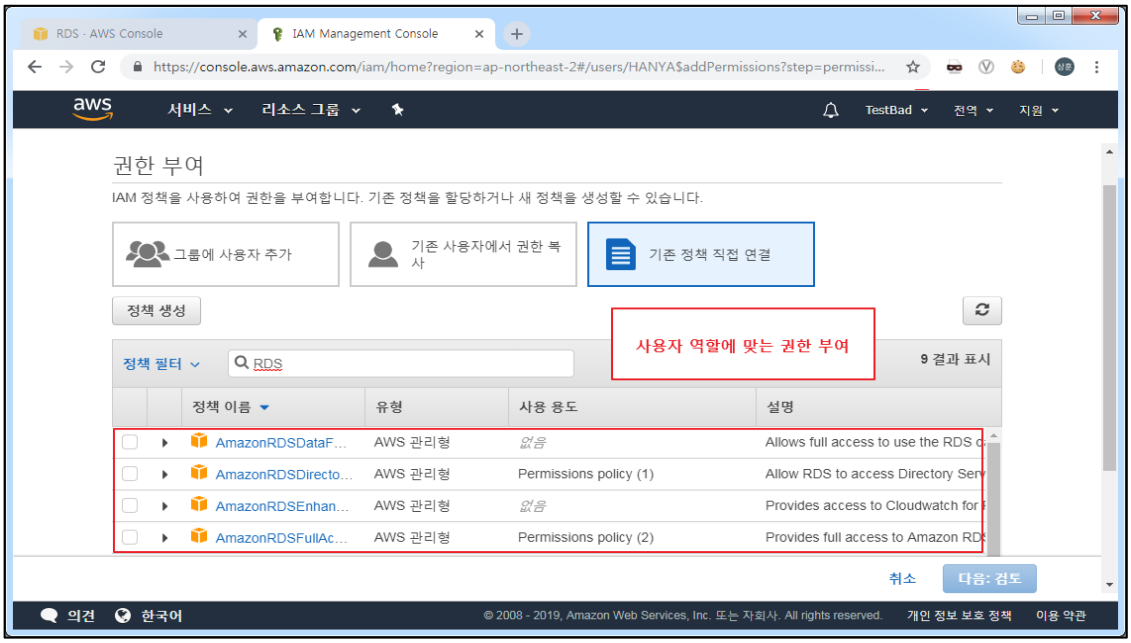
설정 방법

가. IAM User Account 별 권한 확인 및 설정

1) IAM → 사용자 → 계정 선택 → 권한 → 부여된 권한 확인 → 권한 추가 → 추가/삭제

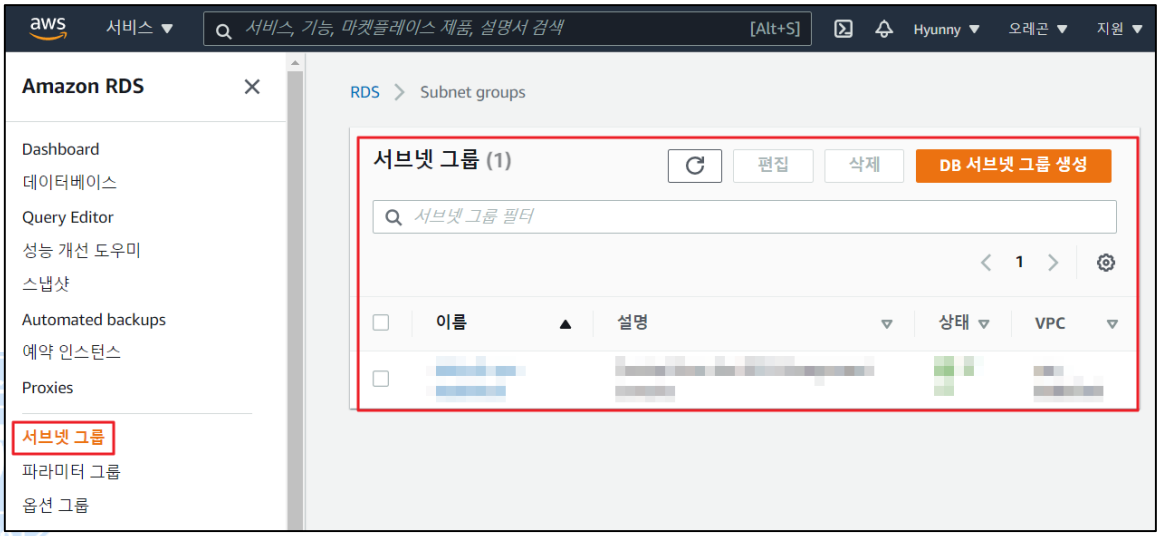
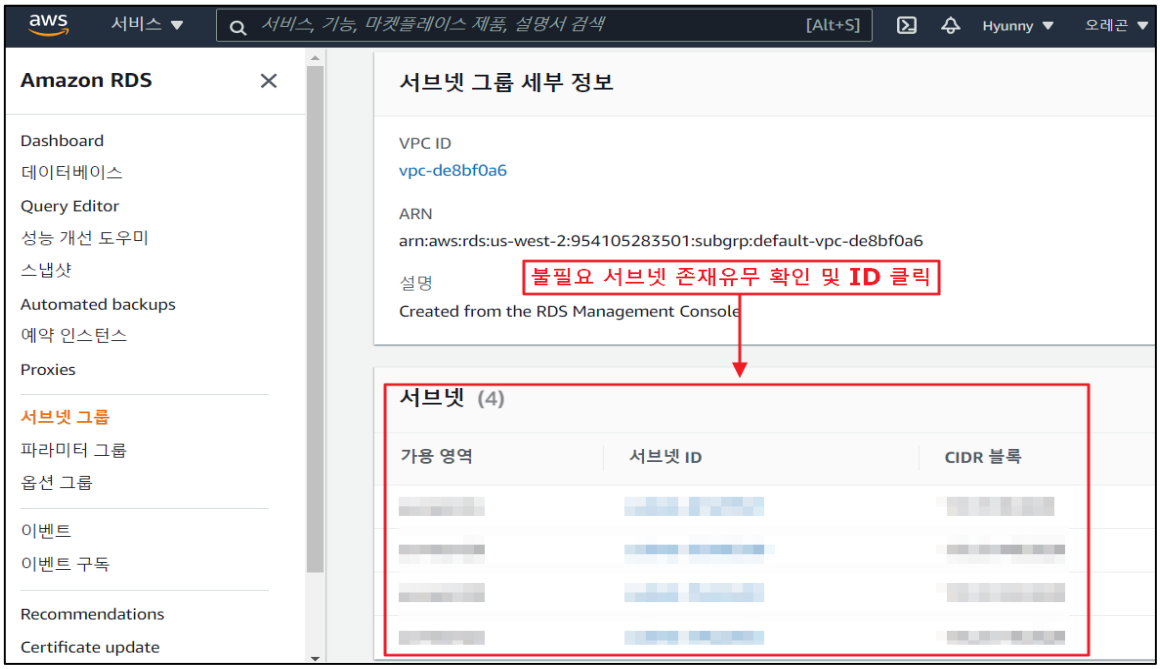




<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단 기준</td><td>양호기준
: IAM 일반 사용자 권한에 RDS API 기능을 사용할 수 있는 권한이 부여되어 있지 않은 경우

취약기준
: IAM 일반 사용자 권한에 RDS API 기능을 사용할 수 있는 권한이 부여되어 있을 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

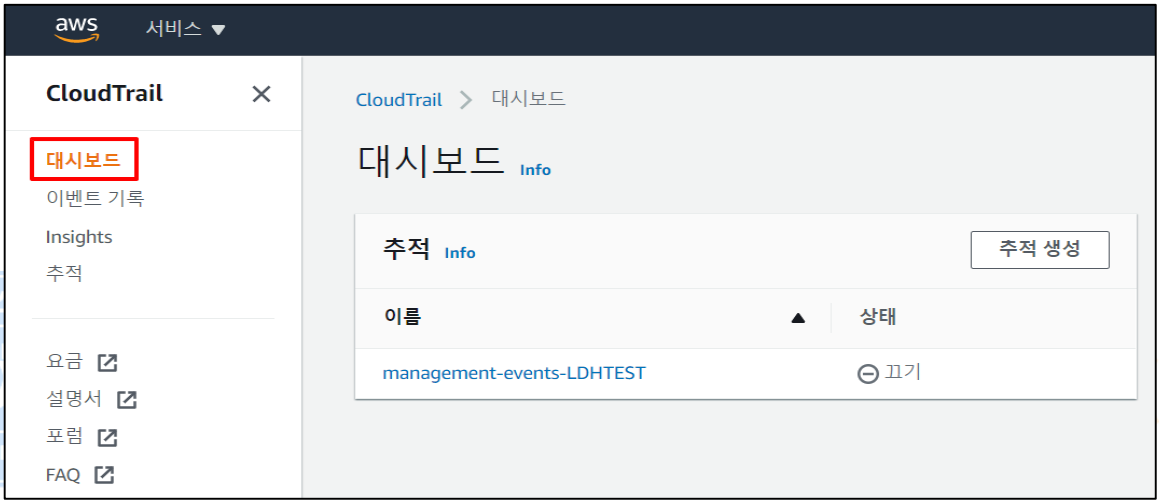
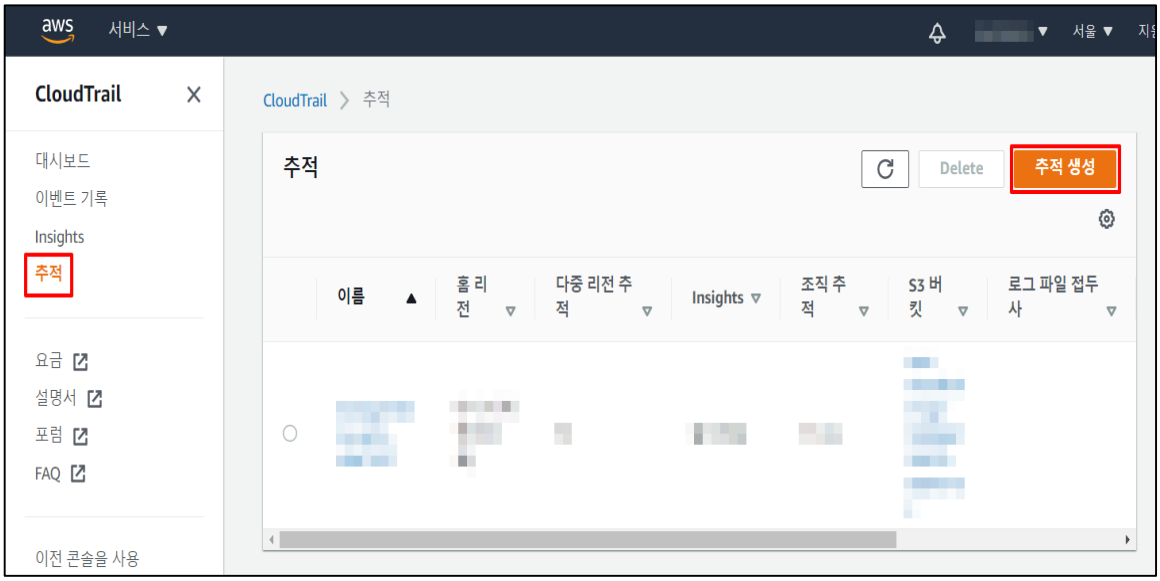
4.10 RDS 서브넷 가용 영역 관리

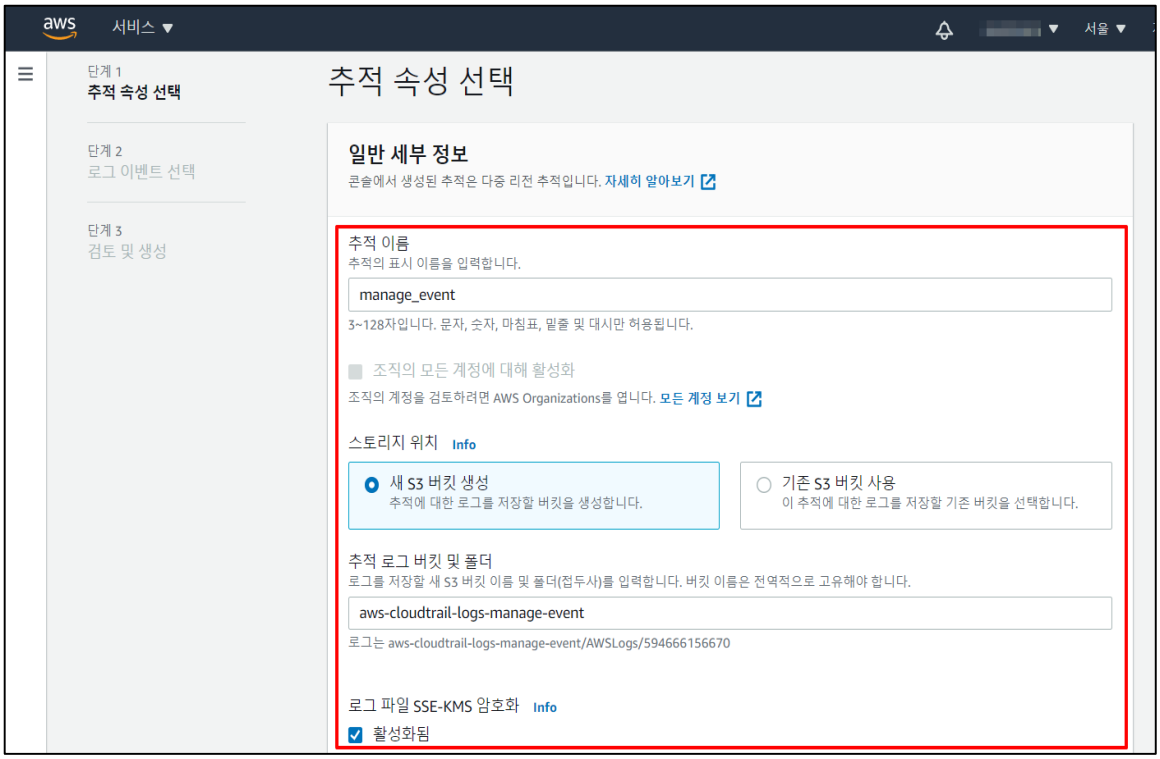
분류	가상 리소스 관리	중요도	중
항목명	RDS 서브넷 가용 영역 관리		
항목 설명	서브넷이란 하나의 IP 네트워크 주소를 지역적으로 나누어 이 하나의 네트워크 IP 주소가 실제로 여러개의 서로 연결된 지역 네트워크로 사용할 수 있도록 하는 방법으로 EC2 인스턴스와 RDS 상호 통신 시 필요하나 불필요한 서브넷이 포함되어 있을 경우 보안성 위험을 발생시킬 수 있으므로 불필요한 서브넷의 유무를 관리해야 합니다.		
설정 방법	**가. 서브넷 그룹 설정 확인** 1) 서브넷 그룹 확인  2) 연결된 서브넷 확인 		
진단	양호기준		

기준	: 가상 인스턴스와 RDS 연결 간의 서브넷이 설정되어 있을 경우 **취약기준** : 가상 인스턴스와 RDS 연결 간의 불필요한 서브넷이 설정되어 있을 경우
비고	

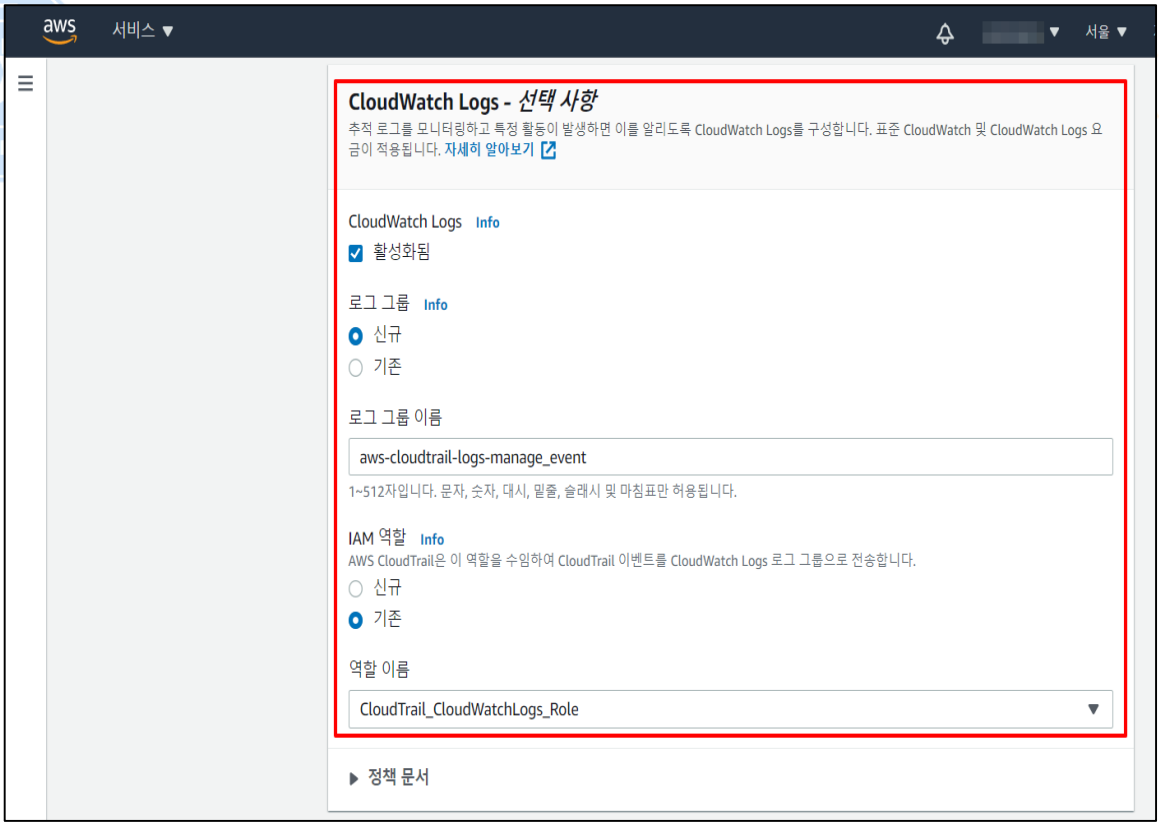
5. 감사/추적 관리

5.1 AWS 사용자 계정 로깅 설정

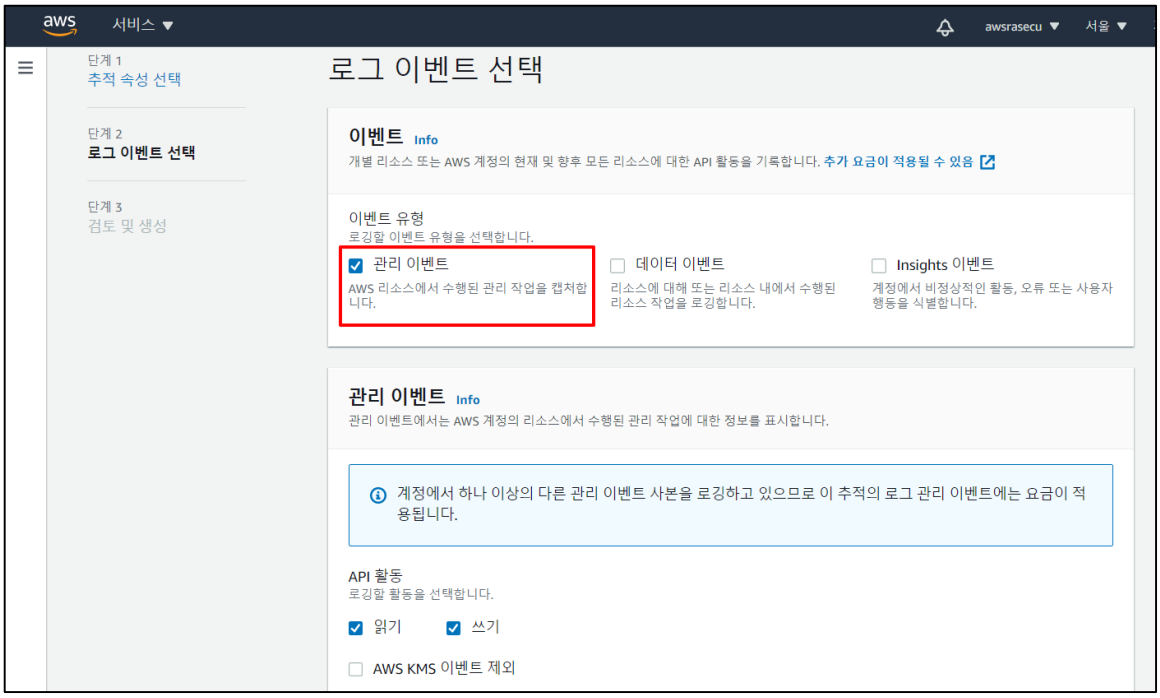
분류	감사/추적 관리	중요도	하
항목명	AWS 사용자 계정 로깅 설정		
항목 설명	AWS CloudTrail 은 계정의 거버넌스, 규정 준수, 운영 및 위험 감사를 활성화하도록 도와주는 서비스로서 사용자, 역할 또는 AWS 서비스가 수행하는 작업들의 이벤트가 기록됩니다. 또한 CloudTrail 은 생성 시 AWS 계정에서 활성화됩니다. 활동이 AWS 계정에서 이루어지면 해당 활동이 CloudTrail 이벤트에 기록됩니다.		
설정 방법	**가. CloudTrail 및 CloudWatch 관리 이벤트 설정 방법** 1) CloudTrail 대시보드 진입 및 관리 이벤트 추적 확인  2) CloudTrail 추적 생성 버튼 클릭  3) CloudTrail 추적 속성 설정		



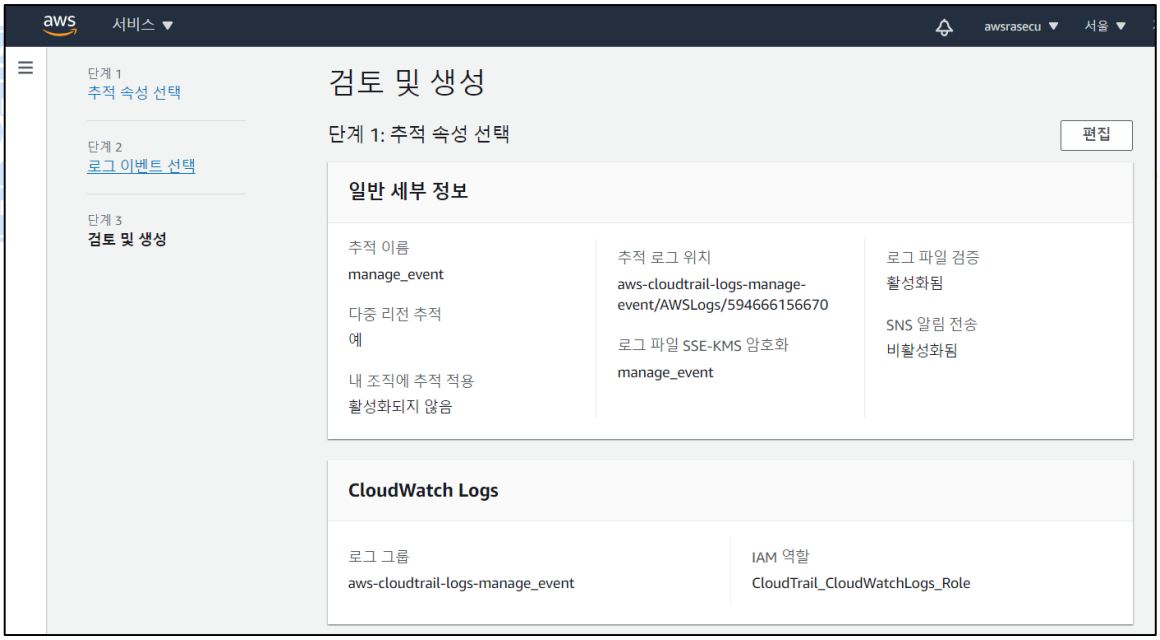
4) CloudTrail CloudWatch Logs 설정



5) 로그 이벤트 선택 – 관리 이벤트

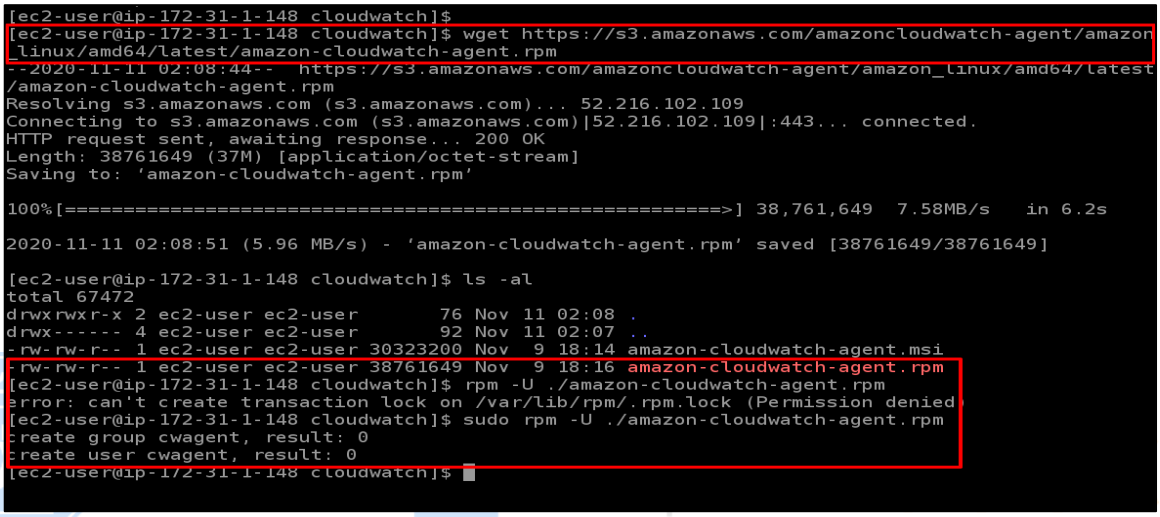
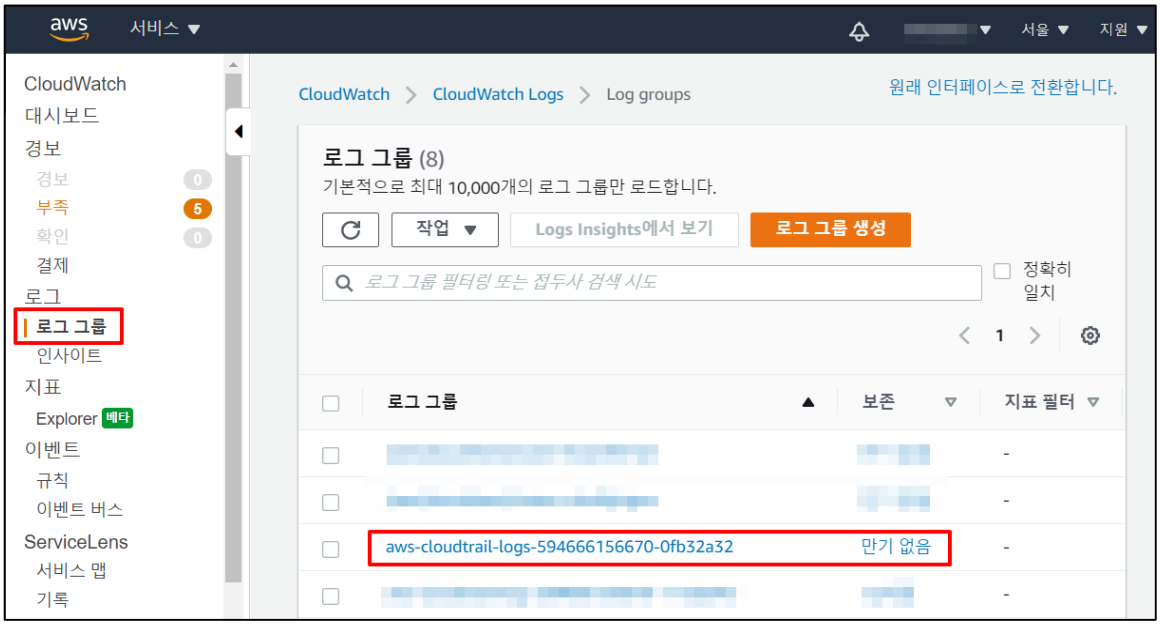


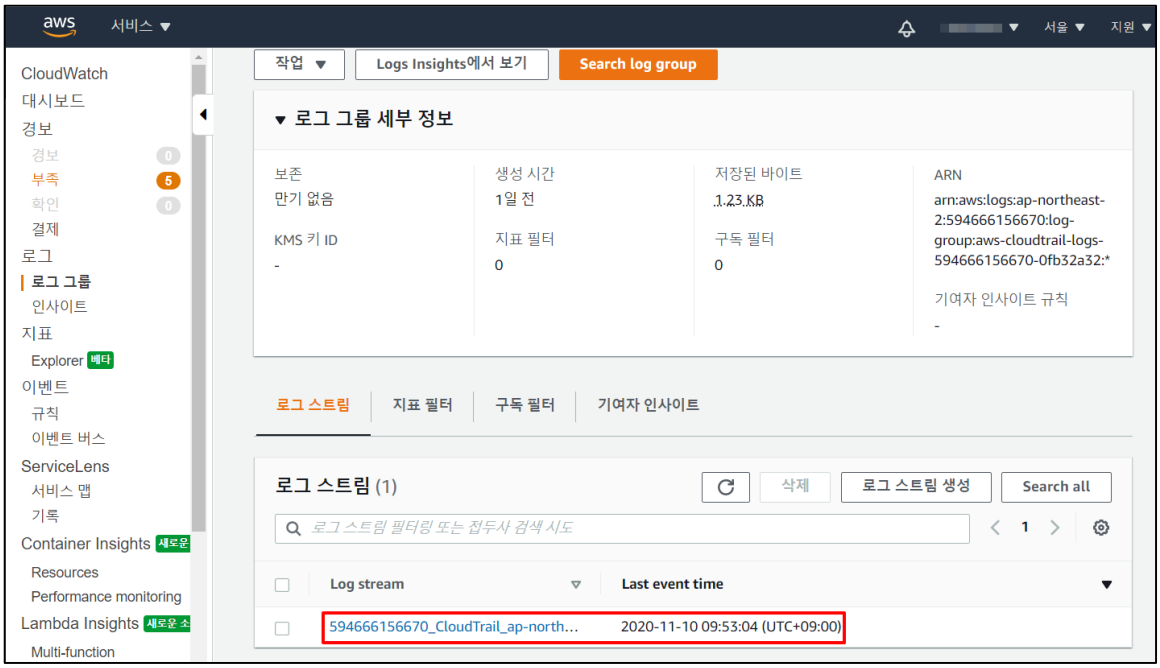
6) CloudTrail 검토 및 생성 내용 확인



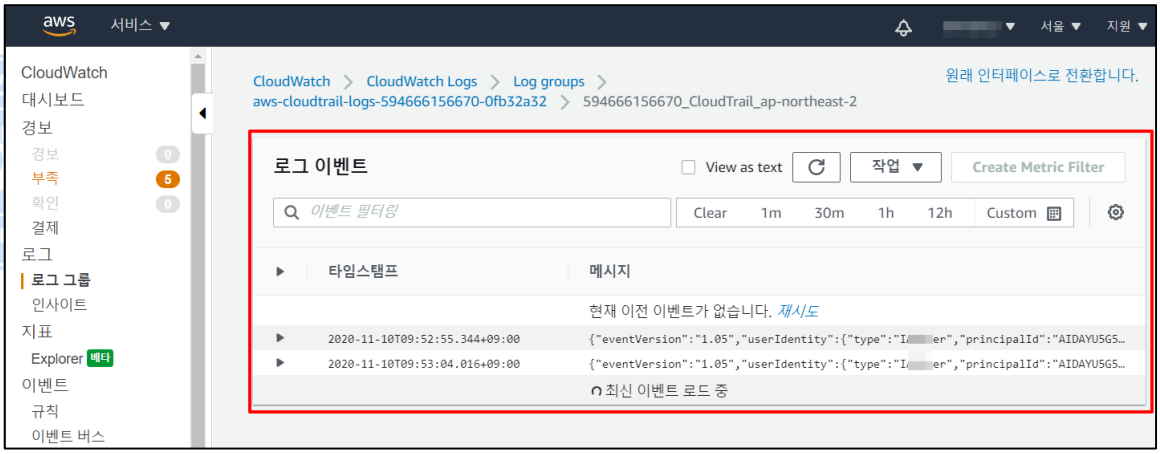
진단 기준	**양호기준** : AD 감사 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있을 경우 **취약기준** : AD 감사 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있지 않을 경우
비고	

5.2 가상 인스턴스 로깅 설정

분류	감사/추적 관리	중요도	하
항목명	가상 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 agent 를 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

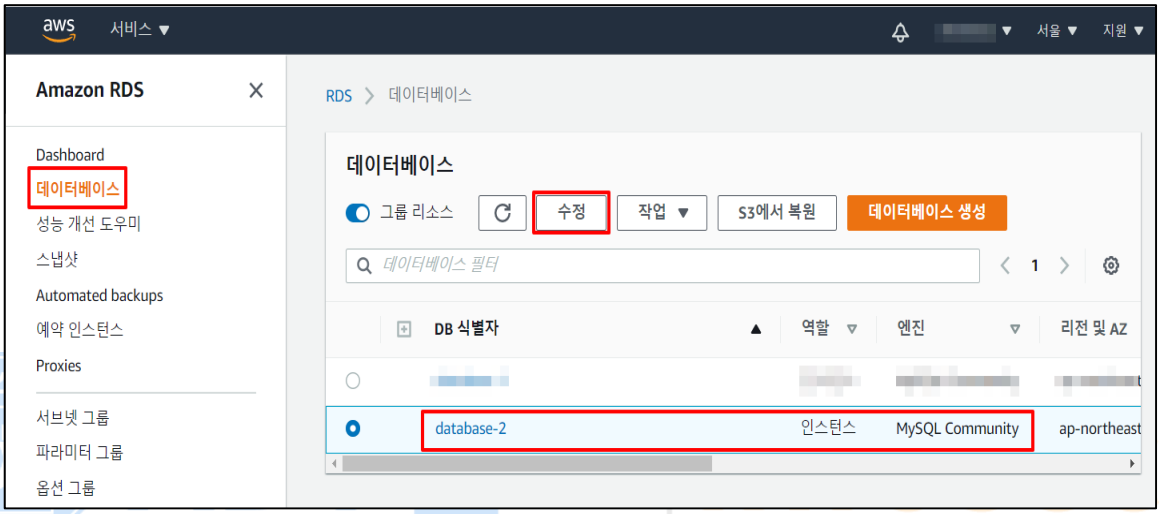
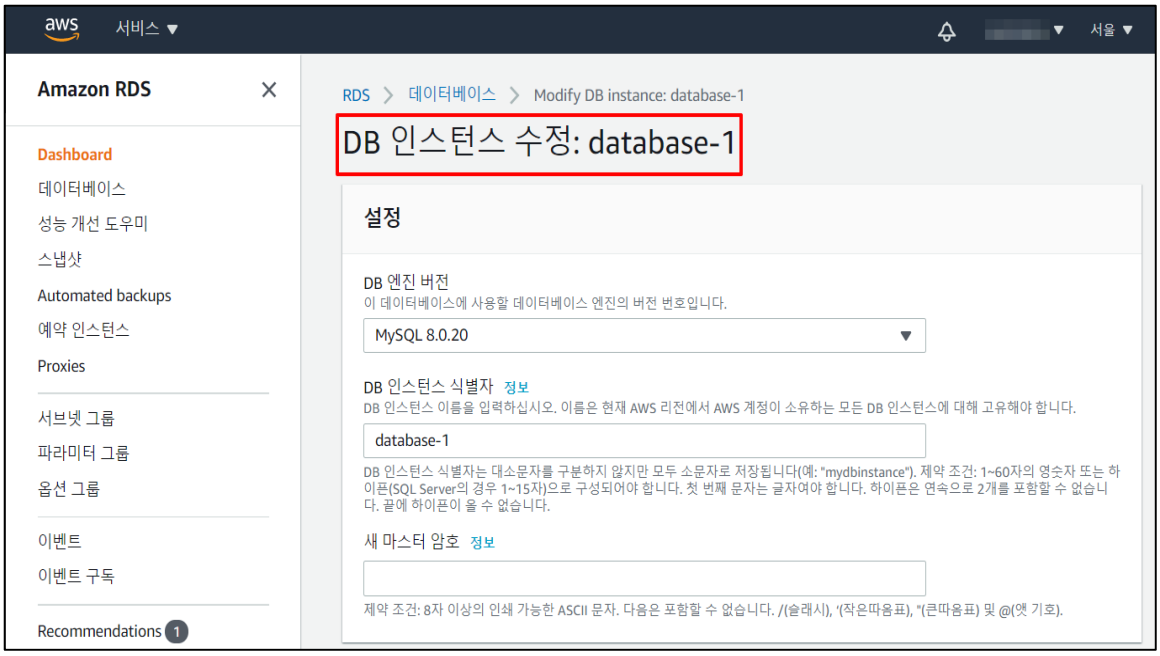
: 가상 인스턴스 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있을 경우

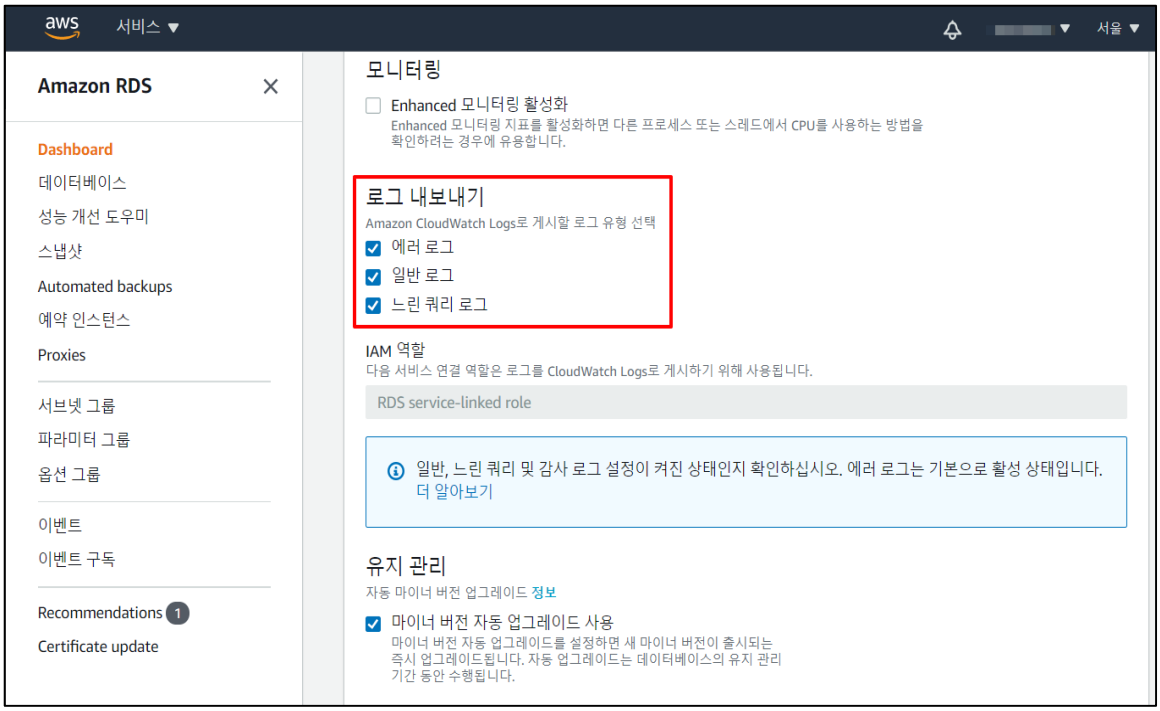
취약기준

: 가상 인스턴스 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있지 않을 경우

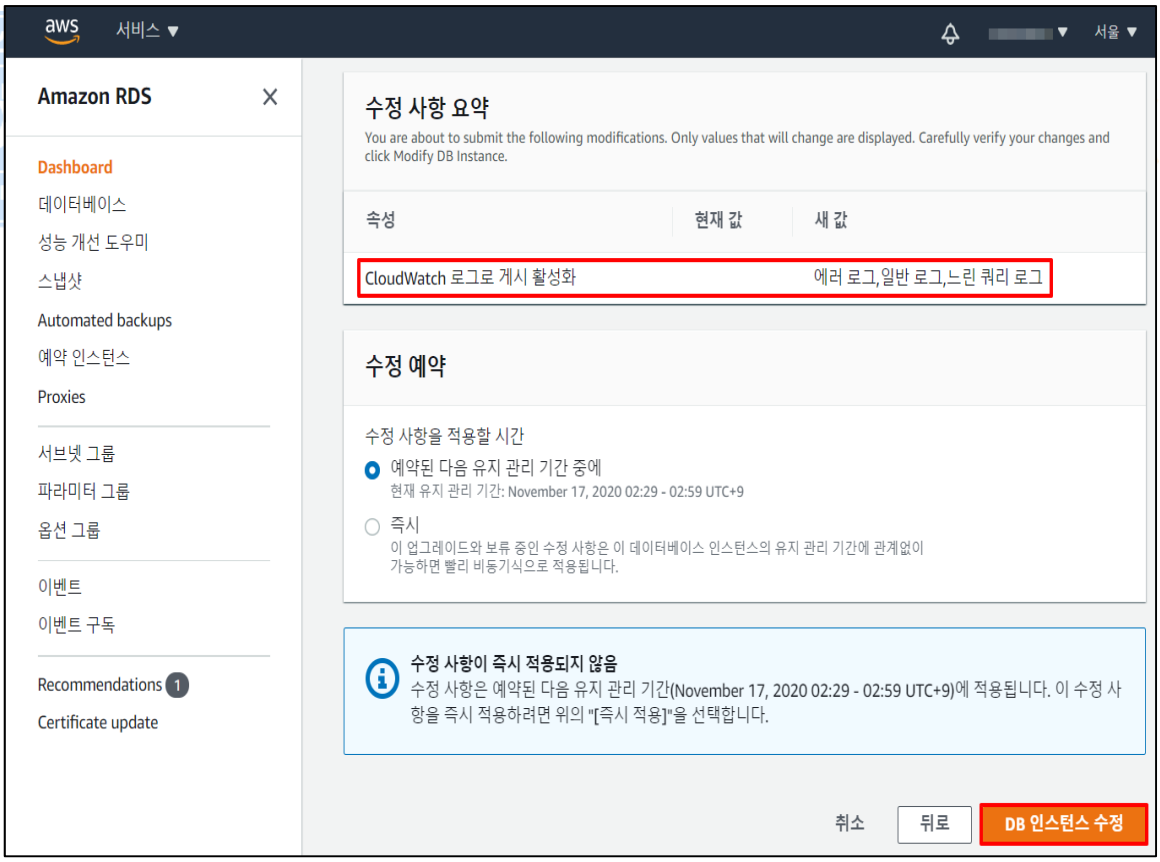
비고

5.3 RDS 로깅 설정

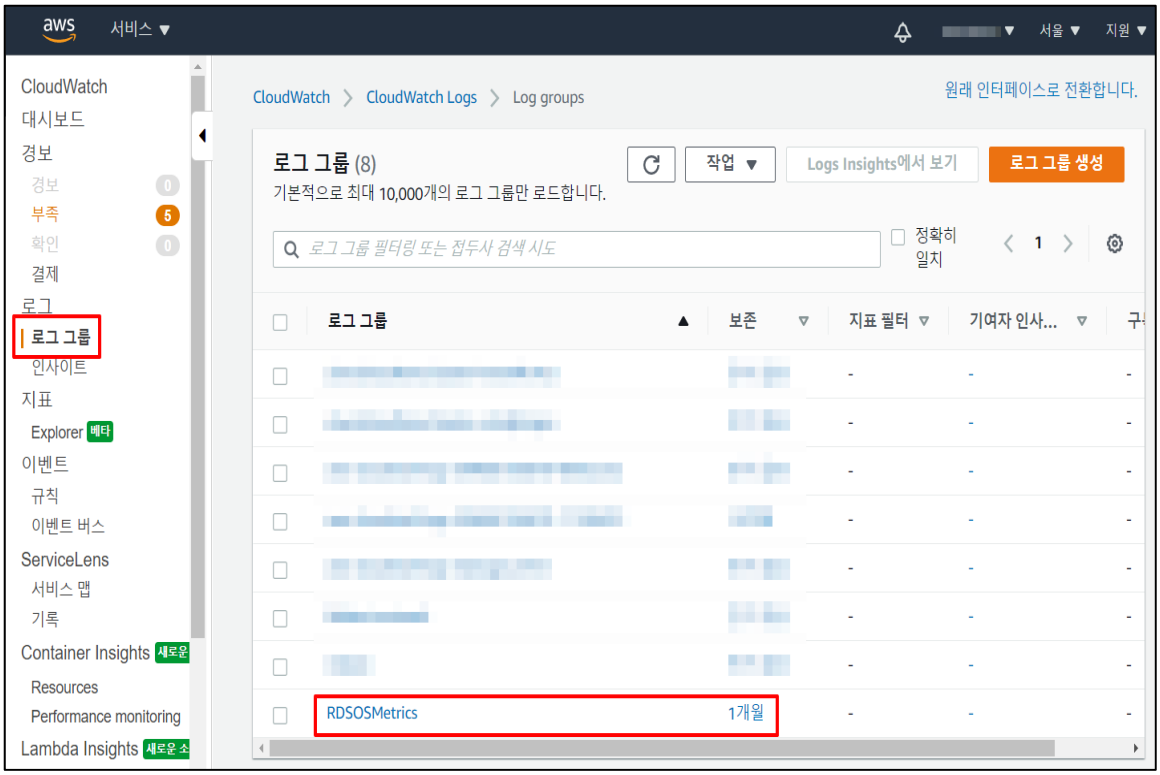
분류	감사/추적 관리	중요도	하
항목명	RDS 로깅 설정		
항목 설명	Amazon CloudWatch Logs 는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스, AWS CloudTrail, Route 53 및 기타 소스에서 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다. 또한, 데이터베이스 옵션(로그 내보내기)을 수정하여 로그 그룹에 등록된 로그 스트림을 통해 RDS 로그를 확인할 수 있습니다.		
설정 방법	**가. 로그 그룹 및 로그 스트림 내 RDS 로깅 확인 방법** 1) RDS 내 데이터베이스 수정  2) 데이터베이스 수정 페이지 접근  3) 로그 내보내기 옵션 선택		



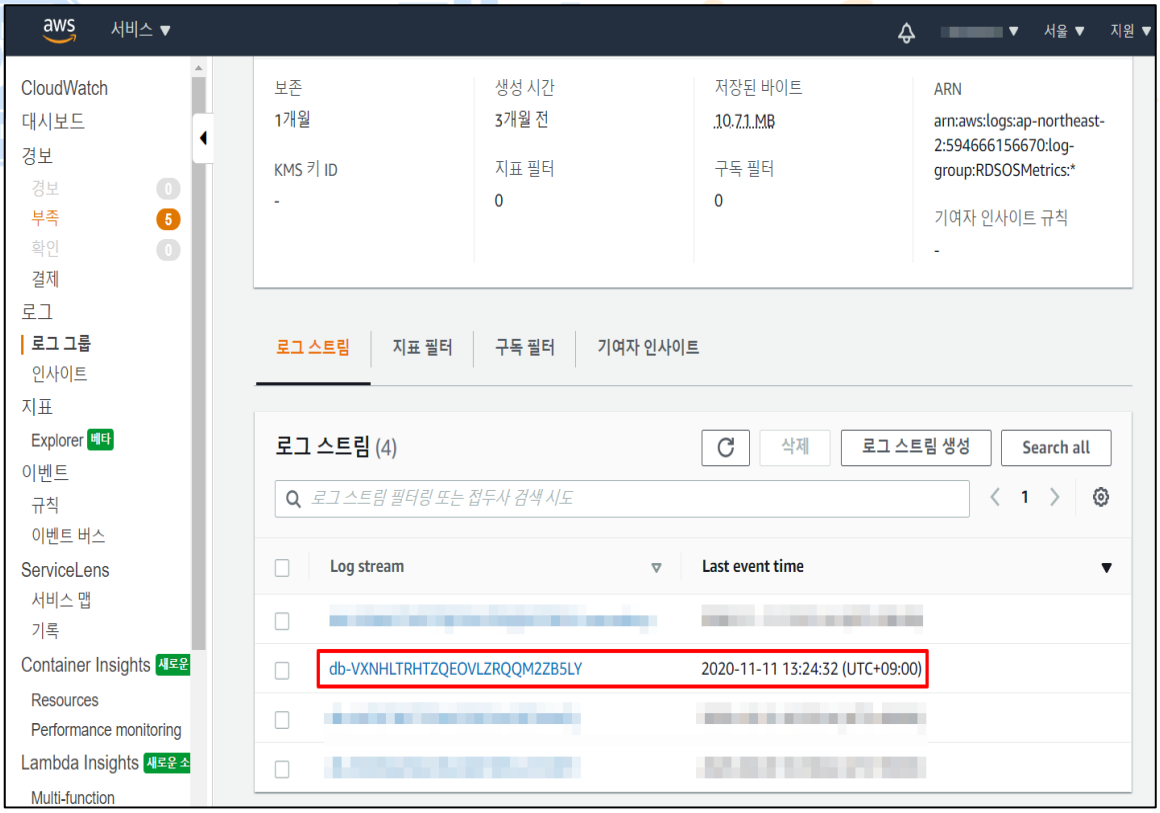
4) DB 인스턴스 수정 클릭



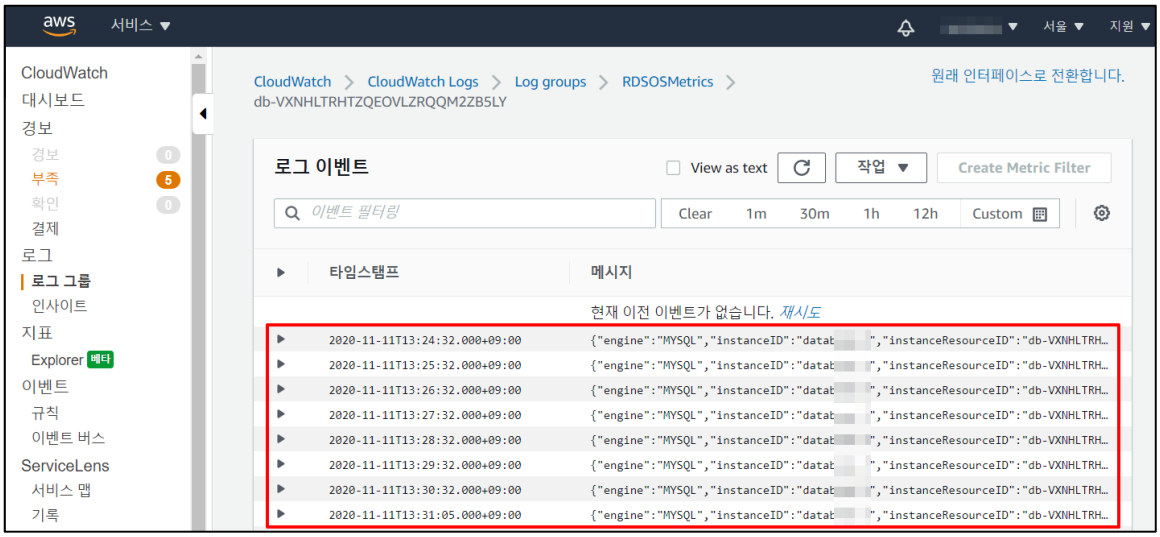
5) 로그 그룹 확인 및 클릭



6) 로그 스트림 확인 및 클릭

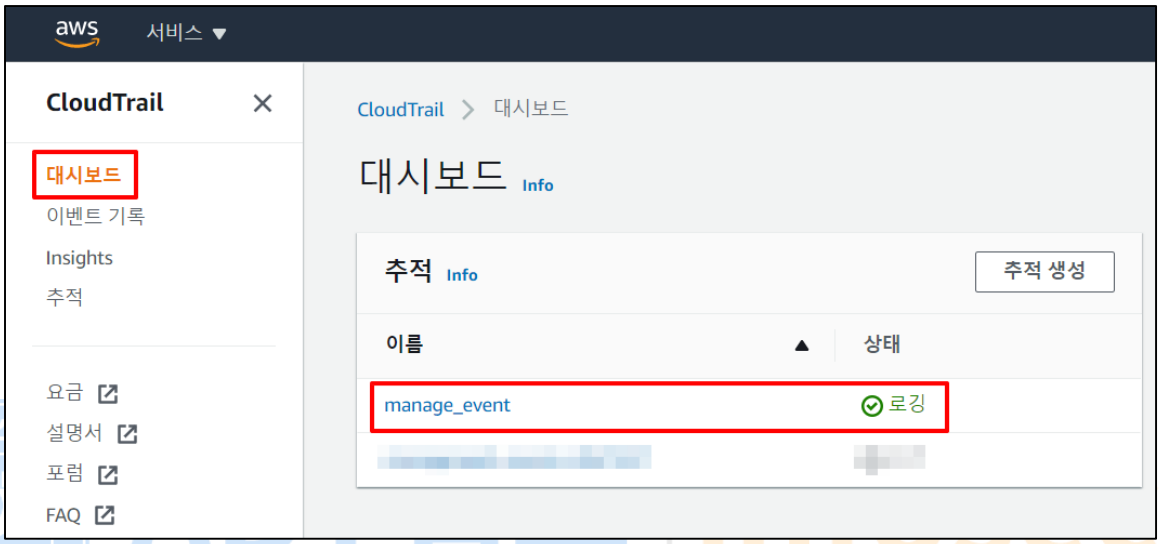
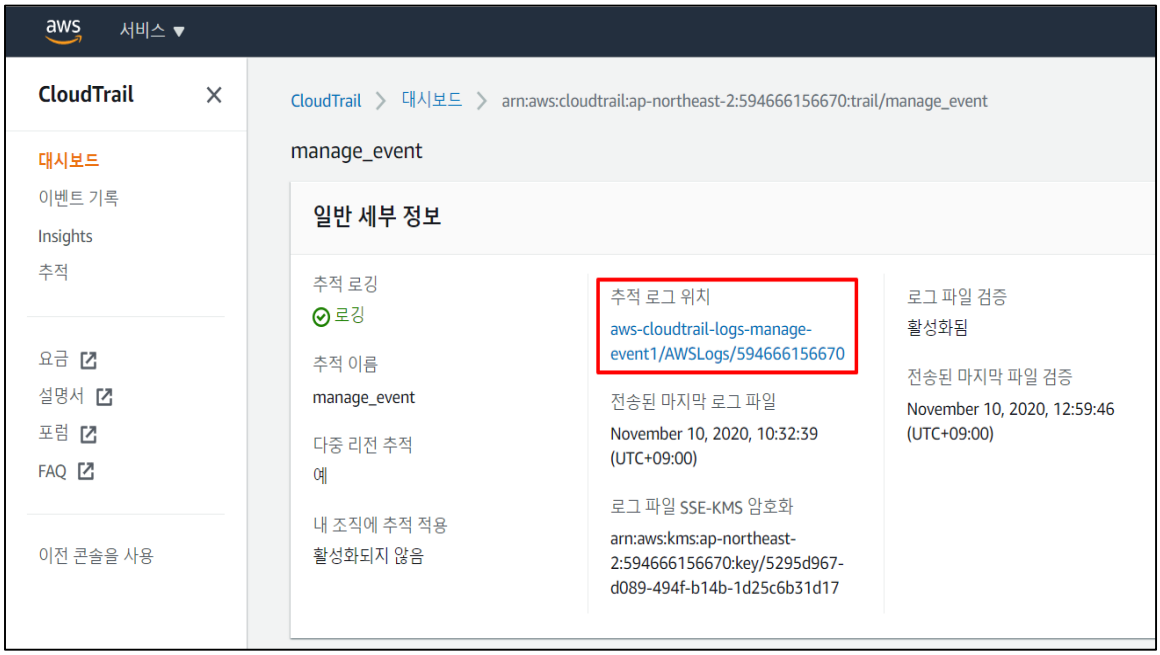


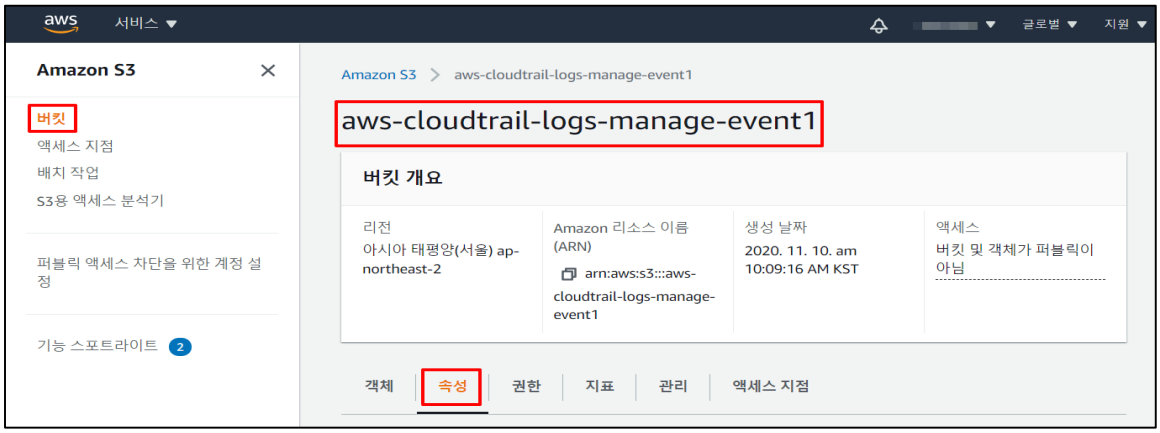
7) 로그 스트림 내 RDS 로깅 확인

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단 기준</td><td>양호기준
: RDS 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있을 경우

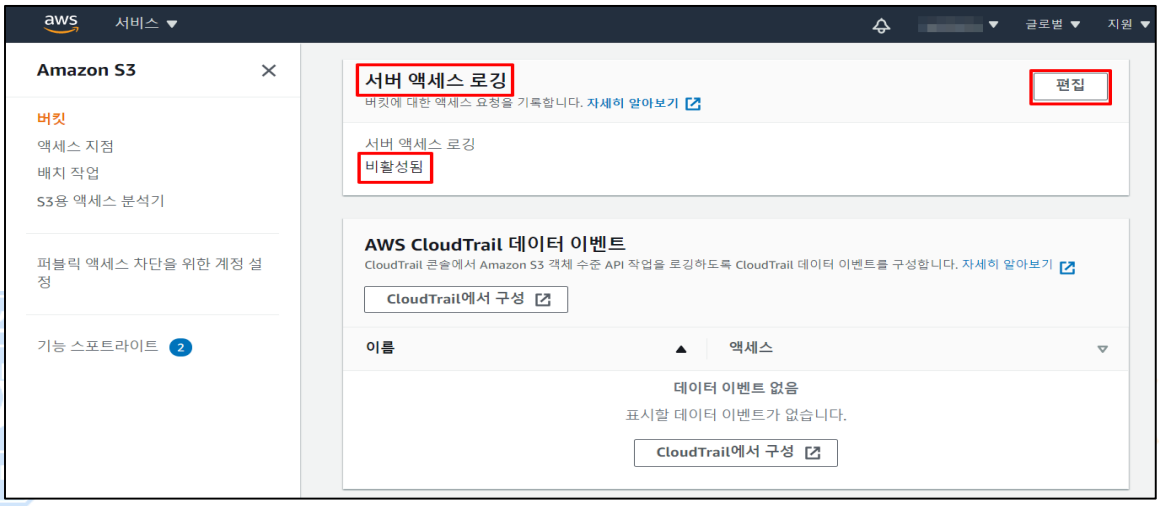
취약기준
: RDS 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있지 않을 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

5.4 S3 버킷 로깅 설정

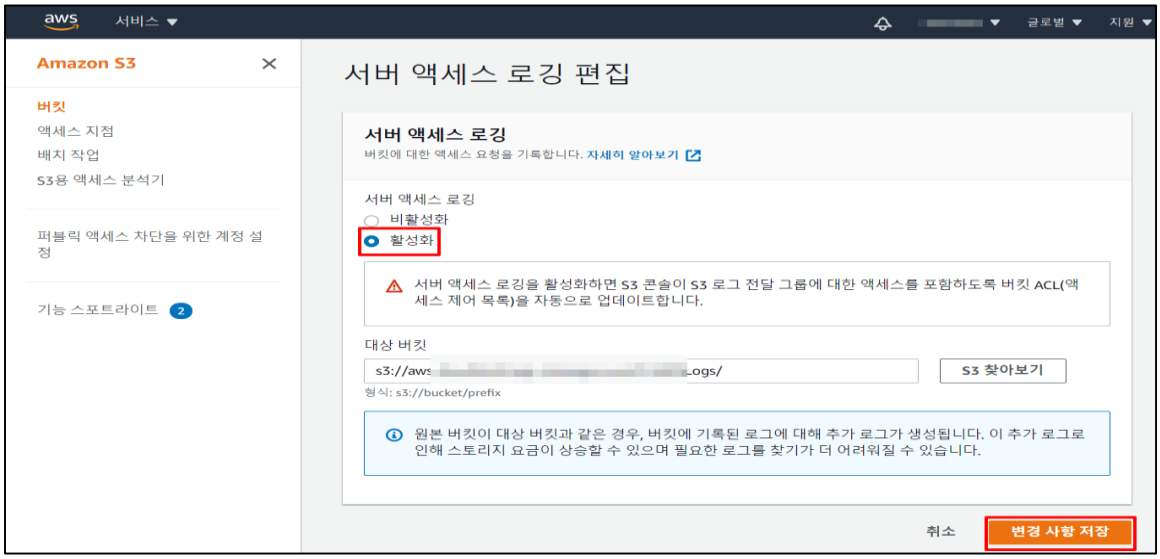
분류	감사/추적 관리	중요도	하
항목명	S3 버킷 로깅 설정		
항목 설명	AWS CloudTrail 은 계정의 거버넌스, 규정 준수, 운영 및 위험 감사를 활성화하도록 도와주는 서비스로서 사용자, 역할 또는 AWS 서비스가 수행하는 작업들의 이벤트가 기록됩니다. 또한 버킷의 옵션(서버 액세스 로깅) 활성화를 통해 API 호출 및 관련 이벤트를 추적할 수 있습니다.		
설정 방법	**가. CloudTrail 서버 액세스 로그 설정 방법** 1) CloudTrail 대시보드 진입 및 로깅 내용 확인  2) CloudTrail 추적 로그 위치 확인  3) CloudTrail 추적 로그 S3 버킷 위치 접근		



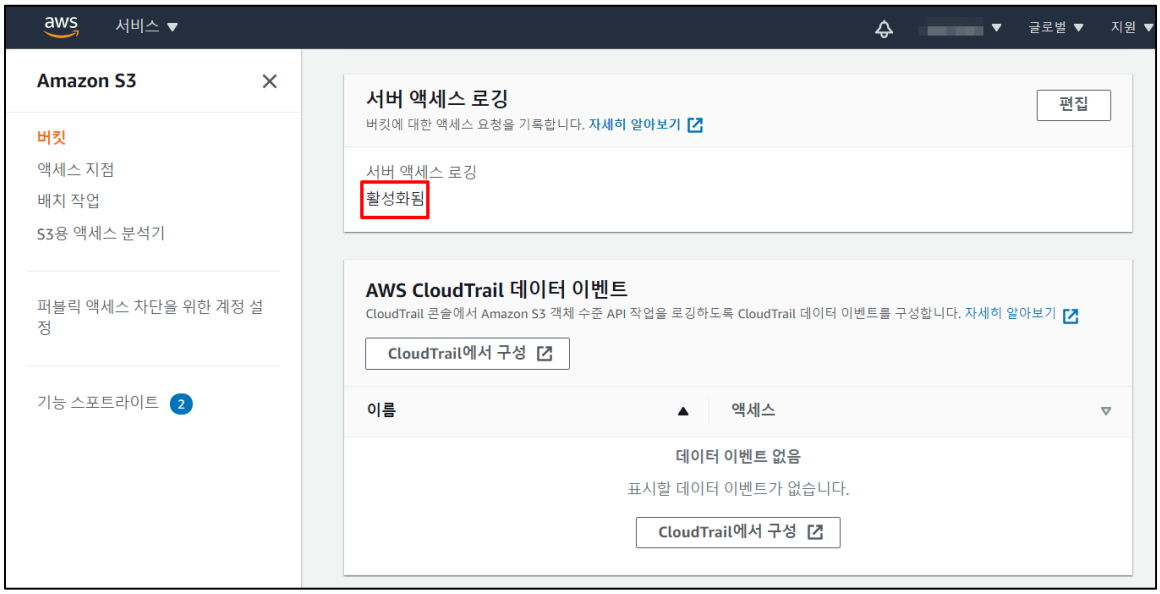
4) S3 버킷 서버 액세스 로깅 비활성화 확인 및 편집 버튼 클릭



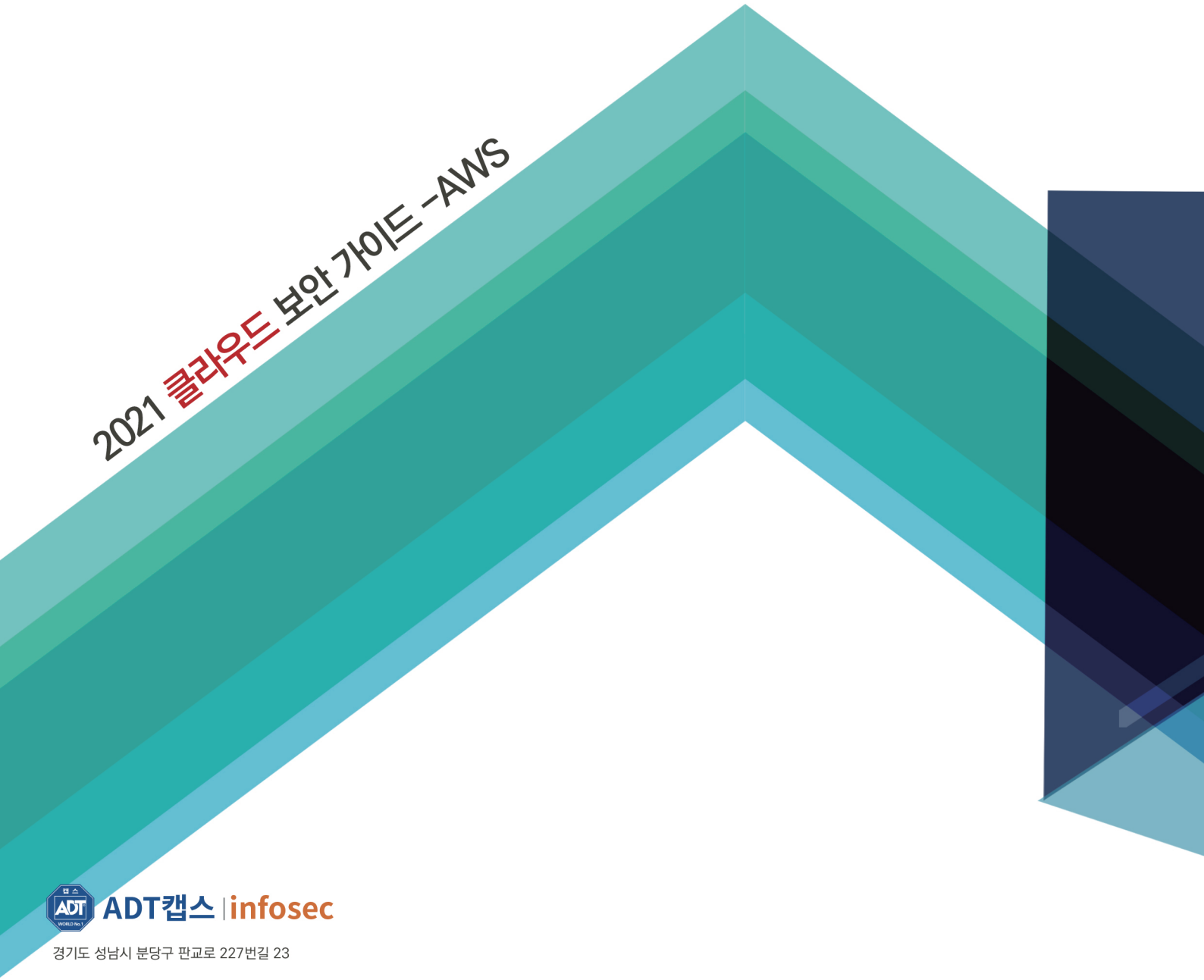
5) S3 버킷 서버 액세스 로깅 활성화



6) S3 버킷 서버 액세스 로깅 활성화 확인

	
진단 기준	**양호기준** : S3 버킷 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있을 경우 **취약기준** : S3 버킷 로그를 별도로 보관(물리적/논리적)하는 정책이 존재하고 있지 않을 경우
비고	

2021 클라우드 보안 가이드 -AWS



ADT캡스 | infosec

경기도 성남시 분당구 판교로 227번길 23

발행인 : ADT캡스 취약점진단팀