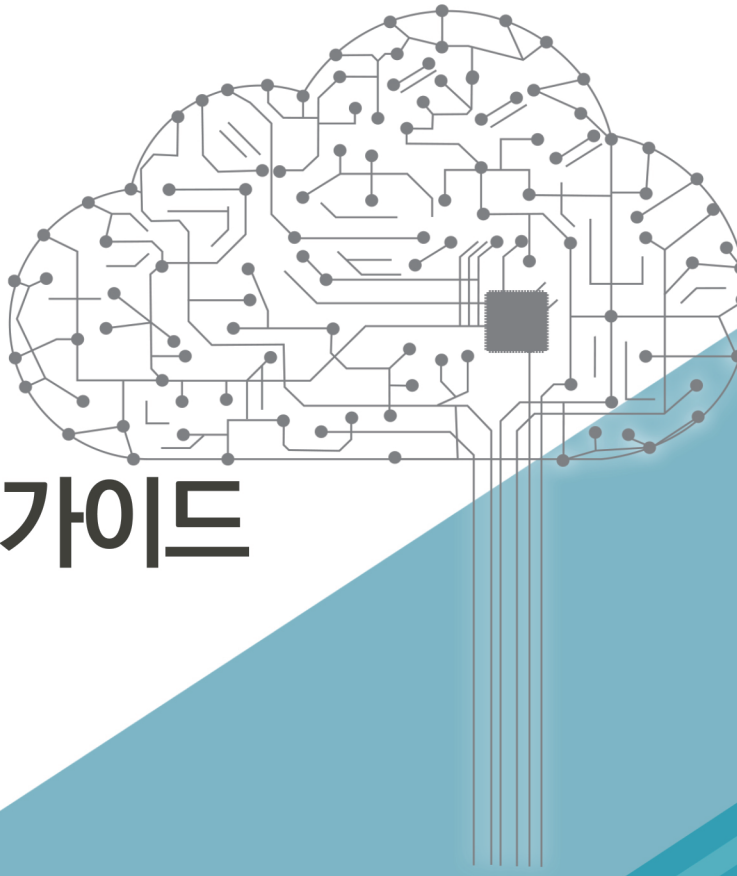
ADT캡스 | infosec



2021 클라우드 보안 가이드

-GCP

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 공식 기술 자료 문서(Google Cloud Platform docs: https://cloud.google.com/docs) 및 국내 발간 서적(구글 클라우드 플랫폼 입문 등) 자료를 바탕으로 작성하였으며, 각각 인증/인가(16개 항목), 데이터 보안(7개 항목), 가상 리소스 관리(10개 항목), 감사/추적(5개 항목)으로 총 4개 영역에서 38개 항목으로 구성되어 있습니다.

[표] 1. Google Cloud Platform 보안진단 체크리스트

영역	항목코드	항목명	중요도
인증/인가	1.1	Cloud ID 사용자 계정 최고권한 관리	상
	1.2	Cloud ID (Google Workspace) 사용자 역할 관리	중
	1.3	Cloud ID 사용자 계정 암호 관리	중
	1.4	Cloud ID 사용자 2-Factor-Authentication 로그인	중
	1.5	Google 사용자 계정 최고권한(소유자) 관리	중
	1.6	서비스 계정 관리	중
	1.7	Identity Platform 사용자 관리	중
	1.8	IAM 역할 관리	상
	1.9	Cloud API 키 활성화 관리	중
	1.10	SSH 키 사용	상
	1.11	Cloud SQL Root 계정관리	상
	1.12	Storage 리소스 권한 관리	중
	1.13	Storage 제어 관리 (서명된 URL 설정)	중
	1.14	Storage 버킷 퍼블릭 Access 관리	상
	1.15	Firebase Storage 규칙 설정	중
	1.16	IAP (Identity-Aware-Proxy)	하
데이터 보안	2.1	Compute Engine 디스크 암호화	중
	2.2	Compute Engine 이미지 암호화	중
	2.3	Cloud SQL 암호화	중
	2.4	Cloud SQL 네트워크 통신 암호화 설정	중
	2.5	Storage 데이터 보안 관리	중
	2.6	Compute Engine SSL 정책 관리	상
	2.7	App Engine SSL 정책 관리	상
가상 리소스 관리	3.1	ID 및 API 액세스	상
	3.2	VM 인스턴스 관리 및 보안	하
	3.3	애플리케이션 방화벽 (App Engine)	중
	3.4	네트워크 방화벽 규칙 관리	중
	3.5	네트워크 방화벽 IP Address 및 Port 관리	중
	3.6	VPC 네트워크 서브넷 관리	상

	3.7	VPC 네트워크 서브넷 비공개 구글 액세스 설정	중
	3.8	공유 VPC 관리	중
	3.9	VPN 연결 관리	중
	3.10	VPN 공용 IP 설정	하
감사/추적	4.1	감사 로그 기록 및 관리	중
	4.2	감사 로그 면제 사용자 존재 여부	중
	4.3	Google 계정 사용자 이상징후 알림 설정	중
	4.4	Cloud ID 계정 사용자 이상징후 알림 설정	하
	4.5	가상 리소스 이상징후 알림 설정	중

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 주요 정보 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. 인증/인가

1.1 Cloud ID 사용자 계정 최고권한 관리

분류	인증/인가	중요도	상
항목명	Cloud ID 사용자 계정 최고권한 관리		
항목 설명	Cloud ID는 Google에서 제공하는 IDaaS(Identity as a Service) 및 엔터프라이즈 모바일 관리(EMM) 제품입니다. Google Workspace에서 사용할 수 있는 독립형 제품으로 ID 서비스 및 엔드포인트 관리 기능을 제공합니다. 관리자는 Cloud ID를 사용하여 Google 관리 콘솔에서 사용자, 앱, 기기를 관리할 수 있으며, Google Cloud Platform(GCP) 관리자는 Cloud ID 서비스에 가입하고 Cloud ID 계정 및 첫 번째 관리자를 만들고 Cloud ID의 도메인을 확인하여 Cloud ID 서비스를 시작할 수 있습니다. 또한, Cloud ID 사용자 계정 중 최고 권한(최고관리자)은 Google Workspace 내 모든 리소스 작업이 가능하므로 인가되지 않은 사용자에게 부여되지 않도록 해야합니다.		
설정 방법	**G Suite 를 통한 Cloud ID 설정 방법 (https://support.google.com/cloudidentity/topic/7555414?hl=ko&ref_topic=7516500)** **가. GCP 관리자용 설정 방법** 1) GCP 콘솔에서 클라우드 ID 에 가입하기 - GCP 콘솔에 로그인합니다. - [제품 및 서비스] 메뉴에서 [IAM 및 관리자] > [ID]로 이동합니다. - ID 창에서 [가입]을 클릭합니다. 2) 클라우드 ID 계정 및 첫 번째 관리자 만들기 - 내 정보 섹션에서 이름 입력란에 성과 이름을 입력합니다. - 업무에 사용하는 현재 이메일 주소 입력란에 프로토타입 프로젝트를 만들 때 사용한 이메일을 입력합니다. - 업체 정보 섹션에서 회사 또는 조직명 입력란에 회사 이름을 입력합니다. - 국가/지역 입력란에서 해당되는 국가 또는 지역을 풀다운 목록에서 선택합니다. - 다음을 클릭하여 도메인을 설정합니다. - 클라우드 ID 도메인 창에 이미 구입한 회사 도메인을 추가합니다. - 클라우드 ID 계정 만들기 창에서 사용자 이름 및 비밀번호를 입력합니다. **※ 업무에 사용하는 현재 이메일 주소는 복구 주소로 사용됩니다. 복구 이메일 주소는 아래에서 Cloud ID 의 관리자 계정으로 사용하기 위해 만들 주소와 달라야 합니다. 또한, Cloud ID 를 통해 생성된 Gsuite 계정은 Cloud ID 관리자 계정이며 위의 2 단계에서 입력한**		

이메일 주소와 달라야 하며, 일반적으로 admin@yourdomain.com 과 같은 형식으로 사용자 이름을 입력하는 것이 좋습니다.

※ 클라우드 ID 의 도메인 확인에 필요한 관련 URL 정보

제목	URL
클라우드 ID 의 도메인 확인	https://support.google.com /cloudidentity/answer/7331243?hl=ko&ref_topic=7390701
도메인 등록기관	https://support.google.com /cloudidentity/topic/7558382?hl=ko&ref_topic=7390701
TXT 레코드를 사용하여 도메인 확인	https://support.google.com /cloudidentity/answer/183895?hl=ko&ref_topic=7390701
HTML 파일 또는 메타 태그를 통해 클라우드 ID 도메인 확인	https://support.google.com /cloudidentity/answer/7334392?hl=ko&ref_topic=7390701
현재 소유하고 있는 도메인으로 클라우드 ID 설정	https://support.google.com /cloudidentity/answer/7331013?hl=ko&ref_topic=7390701
클라우드 ID 에 CNAME 레코드 추가	https://support.google.com /cloudidentity/answer/7334202?hl=ko&ref_topic=7390701

3) 클라우드 ID 사용자 계정 만들기

- Google 관리 콘솔을 이용하여 사용자를 개별적으로 추가합니다
- CSV 파일로 사용자 이름을 업로드하여 여러 사용자를 한꺼번에 추가합니다.

조직에 LDAP 디렉터리가 있는 경우
- Google 계정으로 기존 LDAP 디렉터리에 있는 사용자 데이터(동기화 그룹, 연락처, 조직 포함)를 동기화하려면 Google 클라우드 디렉터리 동기화를 사용합니다. - Microsoft® Active Directory®와 같은 기존 LDAP 디렉터리의 데이터를 사용해 많은 수의 사용자를 프로비저닝하려면 Admin SDK Directory API 를 사용합니다. 이 API 는 Google 클라우드 디렉터리 동기화보다 유연하지만 프로그래밍이 필요합니다.
기타 지침
- 각 계정의 사용자 이름은 해당 사용자의 로그인 이름과 이메일 주소의 첫 번째 부분이 됩니다. 도메인이 solarmora.com 인 경우 이메일이 jsmith@solarmora.com 인 사용자의 사용자 이름은 jsmith 입니다. 조직의 클라우드 ID 계정과 연결된 도메인 이름이 여러 개인 경우 클라우드 ID 사용자 계정을 만들 때 사용할 도메인 이름을 지정합니다. - 검색 가능한 G Suite 디렉터리에 새 사용자 계정이 표시되는 데 최대 24 시간이 소요될 수 있습니다. - 사용자가 조직의 도메인 이름을 사용하여 개인 Google 계정을 만든 경우 중복 계정이 발생할 수 있습니다. 기존 개인 Google 계정과 동일한 사용자 이름으로 사용자 계정을 만든 다음 조직에 추가하면 개인 계정과 동일한 이메일 주소의 클라우드 ID 계정을 가지게 됩니다. 2 개의 계정이 동일한 사용자 이름을 가질 수 없습니다.

	4) GCP 콘솔을 사용하여 설정 단계 완료 - 클라우드 ID 서비스 가입 및 설정 단계를 완료하면 클라우드 ID 조직이 생성됩니다. 그러면 관리 콘솔의 클라우드 ID 계정을 Google Cloud Platform 에 매핑하고, 결제 및 관리 목적으로 모든 프로젝트를 그룹화하는 데 사용됩니다. 예를 들어 클라우드 ID 조직을 사용하면 프로젝트 액세스 권한을 클라우드 ID 사용자로만 제한할 수 있습니다. Google Cloud Platform 콘솔에 액세스하는 첫 번째 최고 관리자에게 조직 계정 소유자의 역할이 지정됩니다. 최고 관리자는 조직 설정을 관리하고 최상위 수준에서 정책을 지정할 수 있습니다. **※ 관리자가 아닌 Google Cloud Platform 계정에서 아래 1~3 단계를 완료합니다. 이 계정은 일반적으로 개인 Gmail 계정입니다.** 클라우드 ID 관리자 계정에서 4~6 단계를 완료합니다. 1. 결제 계정에 액세스 권한을 부여합니다. 2. 프로젝트에 액세스 권한을 부여합니다. 3. 클라우드 ID 계정에 로그인하고 프로젝트 초대를 수락합니다. 4. GCP 로 이동하여 클라우드 ID 계정으로 로그인하고 액세스 권한을 삭제합니다. 5. 프로젝트를 이전합니다. 6. 권한을 설정합니다.
진단 기준	**양호기준** : 최고관리자 계정이 단일 계정으로 관리되고 있을 경우 **취약기준** : 최고관리자 계정이 단일 계정으로 관리되고 있지 않을 경우
비고	-

1.2 Cloud ID (Google Workspace) 사용자 역할 관리

<table>
<tr><td>분류</td><td>인증/인가</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">Cloud ID (Google Workspace) 사용자 역할 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">
Google Workspace를 통해 Cloud ID 사용자에게 관리(Admin) 콘솔에 대해 완전한 최고 사용자 액세스 권한을 부여하는 대신 제한된 작업만 수행하는 관리자 역할을 할당할 수 있으며 사용자에 대한 직무 및 역할에 맞는 사용자 권한이 설정되어야 합니다. 또한, 권한 오남용이 발생하지 않도록 직무를 수행하는 임직원에 대한 목록을 최신으로 관리해야 합니다.

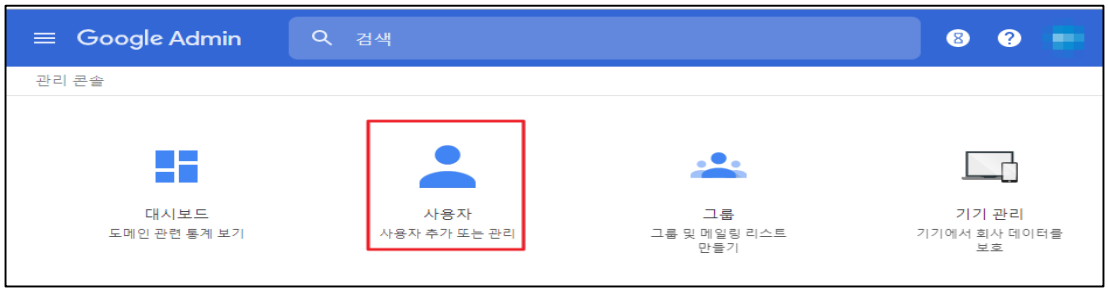
예를 들어 관리자가 A사용자에게 Gmail 설정 또는 헬프 데스크 작업(예: 사용자 비밀번호 재설정)만 관리하도록 허용하길 원할 경우 기본으로 제공되는 관리자 역할을 할당하거나 직접 맞춤 역할 등을 활용해 서비스를 이용해야합니다.

※ Google Workspace 사용자 기본 역할
<table>
<tr><th>역할명</th><th>상세내용</th></tr>
<tr><td>최고
관리자</td><td>관리 콘솔 및 Admin API 의 모든 기능에 액세스할 수 있고 조직 계정을 모든 측면에서 관리할 수 있습니다.
또한 최고 관리자는 모든 사용자의 캘린더 및 캘린더 일정 세부정보에 대한 전체 액세스 권한을 보유합니다. 최고 관리자 권한을 부여받은 사용자가 캘린더 권한을 사용할 수 있게 되려면 최대 24 시간이 걸릴 수 있습니다.

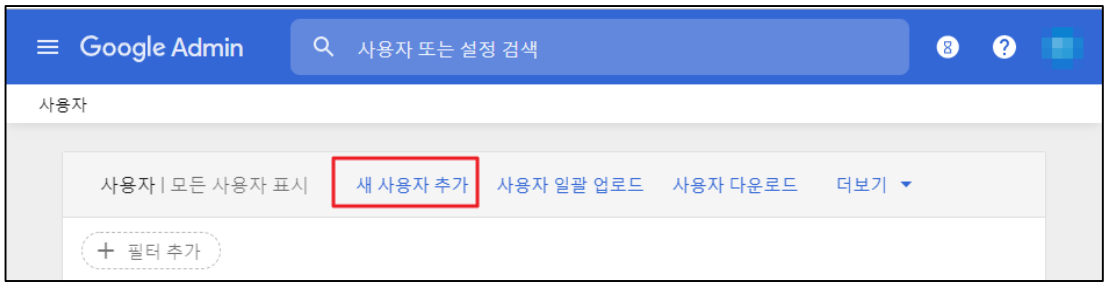
- 관리자 역할 생성 또는 지정
- 관리자 비밀번호 재설정
- 사용자를 삭제하는 중에 파일 소유권 이전
- 삭제된 사용자 복원
- 관리자 설정 관리
- 결제 설정 및 라이선스 관리 제어
- 사용자가 2 단계 인증을 사용하도록 허용
- Google Workspace Marketplace 앱 설치
- Google 캘린더 리소스 액세스 수준 제어 관리
- 전체 디렉터리 설정 관리
- 데이터 이전 서비스 사용
- 도메인 전체 위임/API 클라이언트 액세스 관리 권한 부여
- Google 을 SAML ID 공급업체로 설정 및 SAML 앱 추가/수정</td></tr>
</table>
</td></tr>
</table>

그룹스 관리자	관리 콘솔에서 생성한 Google 그룹스에 대해 모든 권한을 보유합니다. 이 관리자는 관리 콘솔 및 Admin API 를 통해 다음 작업을 수행할 수 있습니다. - 사용자 프로필 및 조직 구조 조회 - 관리 콘솔에서 새 그룹 생성 - 콘솔에서 만든 그룹의 회원 관리 - 그룹의 액세스 설정 관리 - 콘솔에서 그룹 삭제 - 조직 단위 조회(읽기만 가능)
사용자 관리 관리자	관리자가 아닌 사용자에 대해 모든 작업을 수행할 수 있습니다. 이 관리자는 관리 콘솔 및 Admin API 를 통해 다음 작업을 수행할 수 있습니다. - 사용자 프로필 및 조직 구조 조회 - 조직 단위 조회(읽기만 가능) - 사용자 계정 생성 및 삭제 - 사용자 이름 및 비밀번호 변경 - 사용자 개인의 보안 설정 관리 - 기타 사용자 관리 작업 수행 (*) 관리자가 아닌 사용자에게만 해당됩니다. 이 관리자는 관리자 권한을 할당하거나 관리자 비밀번호를 재설정할 수 없으며 관리자 계정의 기타 설정도 변경할 수 없습니다. 최고 관리자만 작업수행이 가능합니다.
헬프 데스크 관리자	관리 콘솔 및 Admin API 를 통해 관리자가 아닌 사용자의 비밀번호를 재설정할 수 있습니다. 이 관리자는 사용자의 프로필과 조직 구조를 볼 수 있습니다. 이 관리자는 조직 단위를 볼 수 있습니다. 사용자를 헬프 데스크 관리자 역할에 지정할 때 해당 사용자의 권한을 특정 조직 단위로 제한할 수 있습니다.
서비스 관리자	캘린더, 드라이브, 문서, 기타 서비스를 비롯하여 관리 콘솔에 추가된 특정 서비스 설정 및 기기를 관리할 수 있습니다. 이 관리자는 다음 작업을 수행할 수 있습니다. - 서비스 사용 또는 사용 중지 - 서비스 설정 및 권한 변경 - 캘린더 리소스 관리 (참고: 서비스 관리 역할을 가진 사용자는 리소스를 생성, 수정, 삭제할 수만 있고, 캘린더 리소스의 공유 설정은 수정할 수 없습니다.) - 콘솔에 표시된 Chrome 및 휴대기기 관리 - 조직 단위 조회(읽기만 가능) (*) 계정에 추가한 특정 제품(G Suite 서비스, 내 지도 프로 등), Marketplace 앱, 무료 Google 서비스(예: Google+ 및 Blogger)에만 적용됩니다. Google

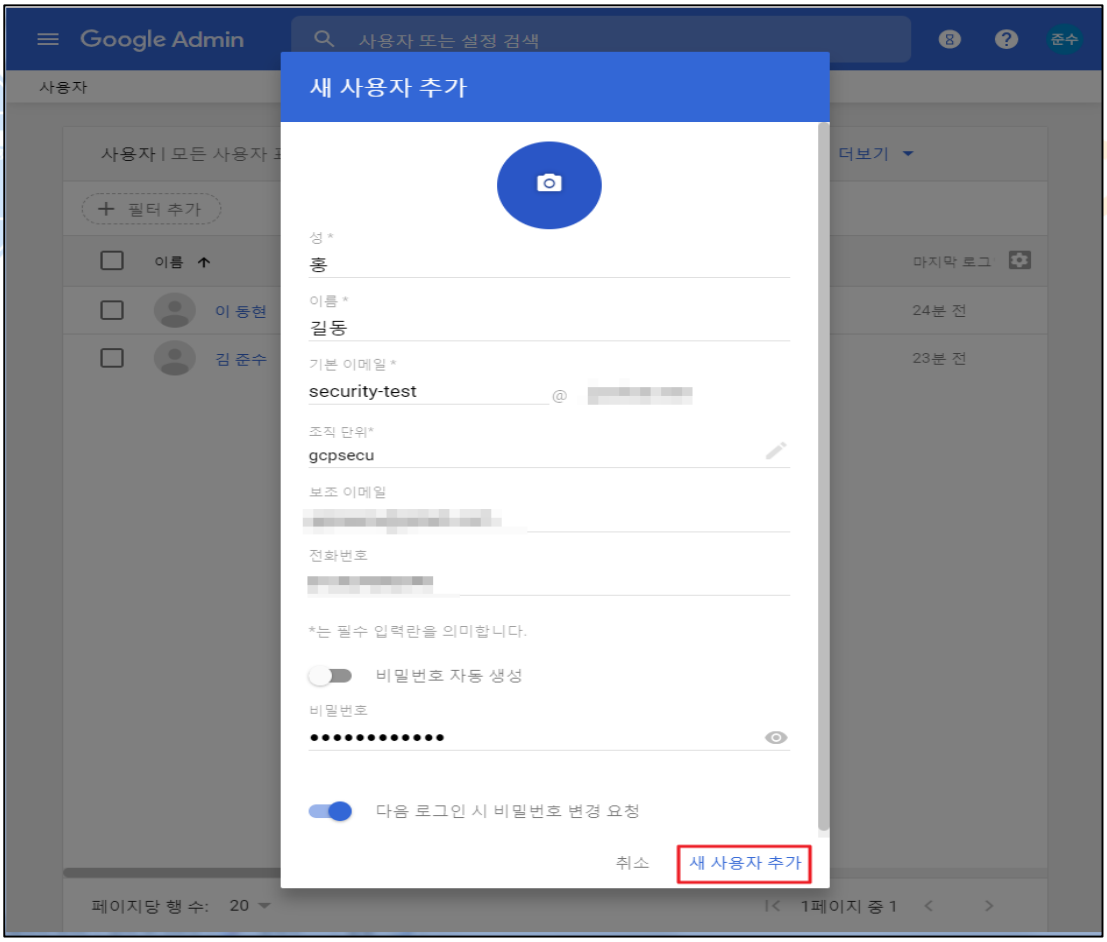
		Vault, 클라우드 프린트 등 일부 제품 및 서비스에서는 서비스 관리자 역할을 지원하지 않습니다.
	모바일 관리자	고급 휴대기기 관리를 통해 휴대기기를 관리할 수 있습니다. 이 관리자는 다음 작업을 수행할 수 있습니다. - 기기 프로비저닝 및 승인 - 앱 허용 - 기기 및 계정 차단 또는 초기화 - Android 기기 및 iOS 기기 정책 설정 - 도메인의 그룹 및 사용자 보기
	Google Voice 관리자	Voice 라이선스 할당을 제외한 모든 Google Voice 설정 및 프로비저닝을 관리할 수 있습니다. 이 관리자는 다음 작업을 수행할 수 있습니다. - 위치 추가 - 사용자에게 전화번호 할당 - 번호 이전 - 서비스 주소 변경 - 유선 전화 설정 - 자동 교환 설정
	리셀러 관리자	고객을 관리 및 프로비저닝할 수 있습니다. 이 관리자는 다음 항목에 액세스할 수 있습니다. - 채널 서비스 콘솔 - 고객 도메인의 관리 콘솔(선택사항) - 리셀러 관련 API 리셀러 관리자 역할만을 보유한 사용자가 로그인하면 이 사용자가 속한 조직의 관리 콘솔은 표시되지 않습니다.
설정 방법	**가. 관리자 및 사용자 역할 부여** 1) [Google Admin] > [관리콘솔] > [사용자]	



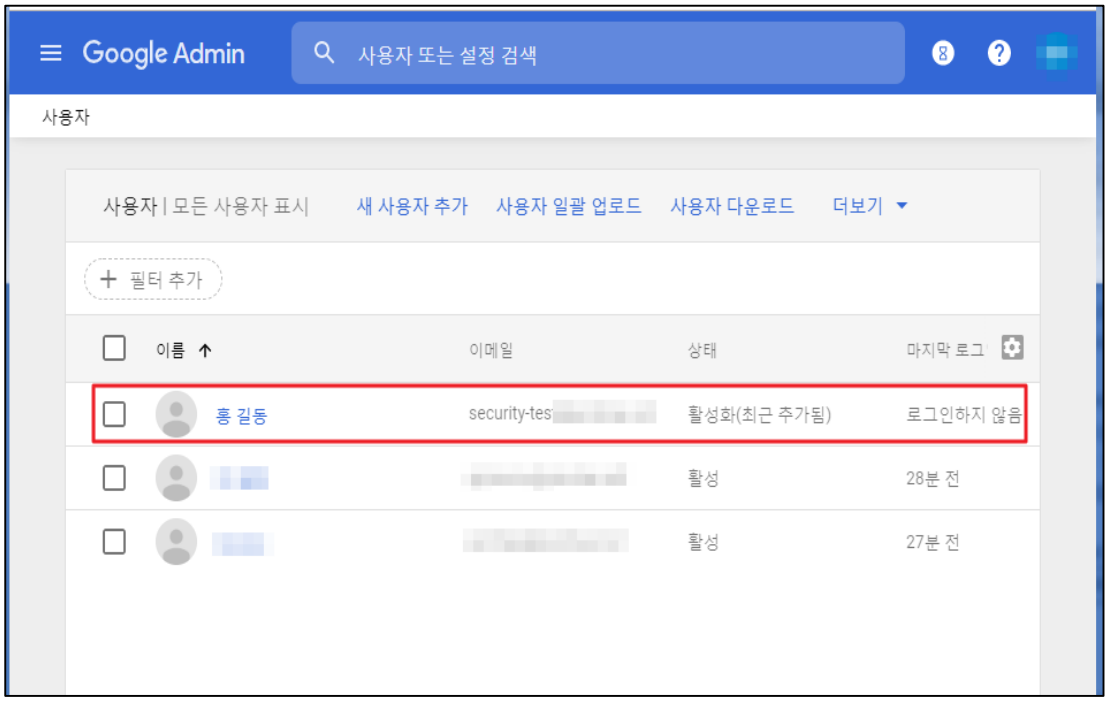
2) [사용자] > [새 사용자 추가]



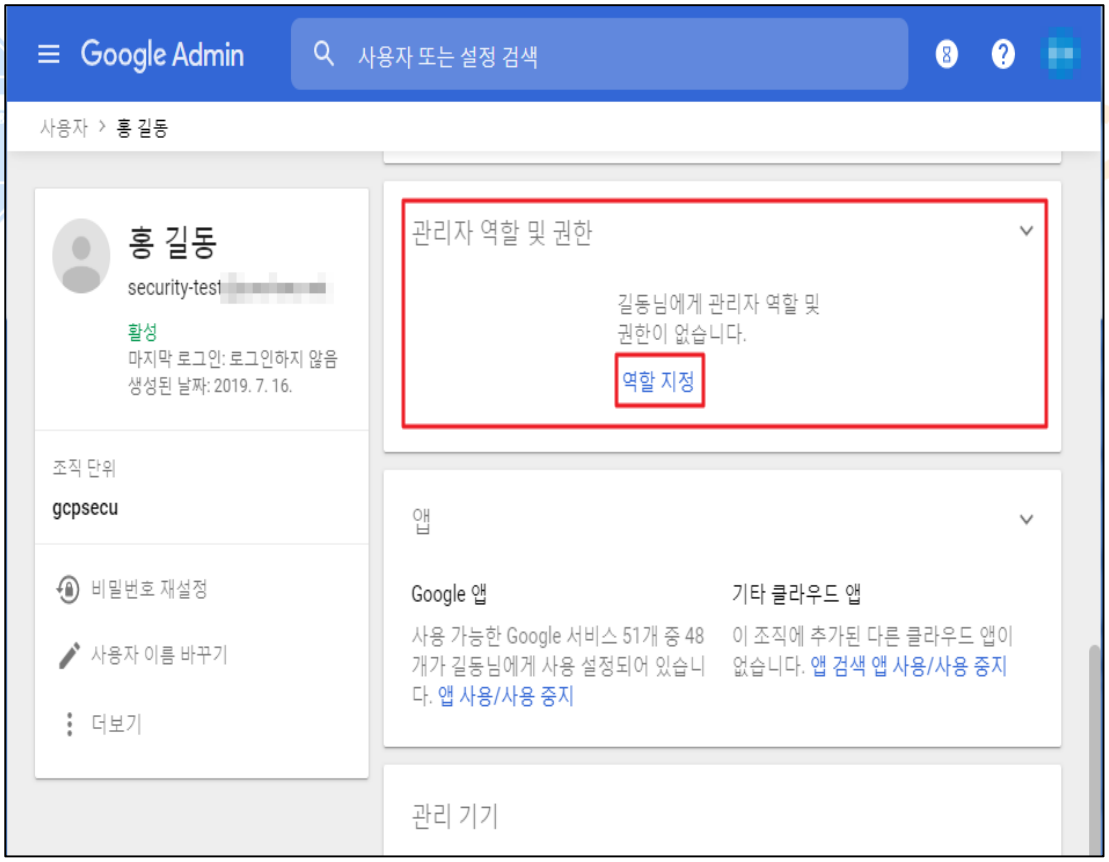
3) 사용자 관련 정보 입력



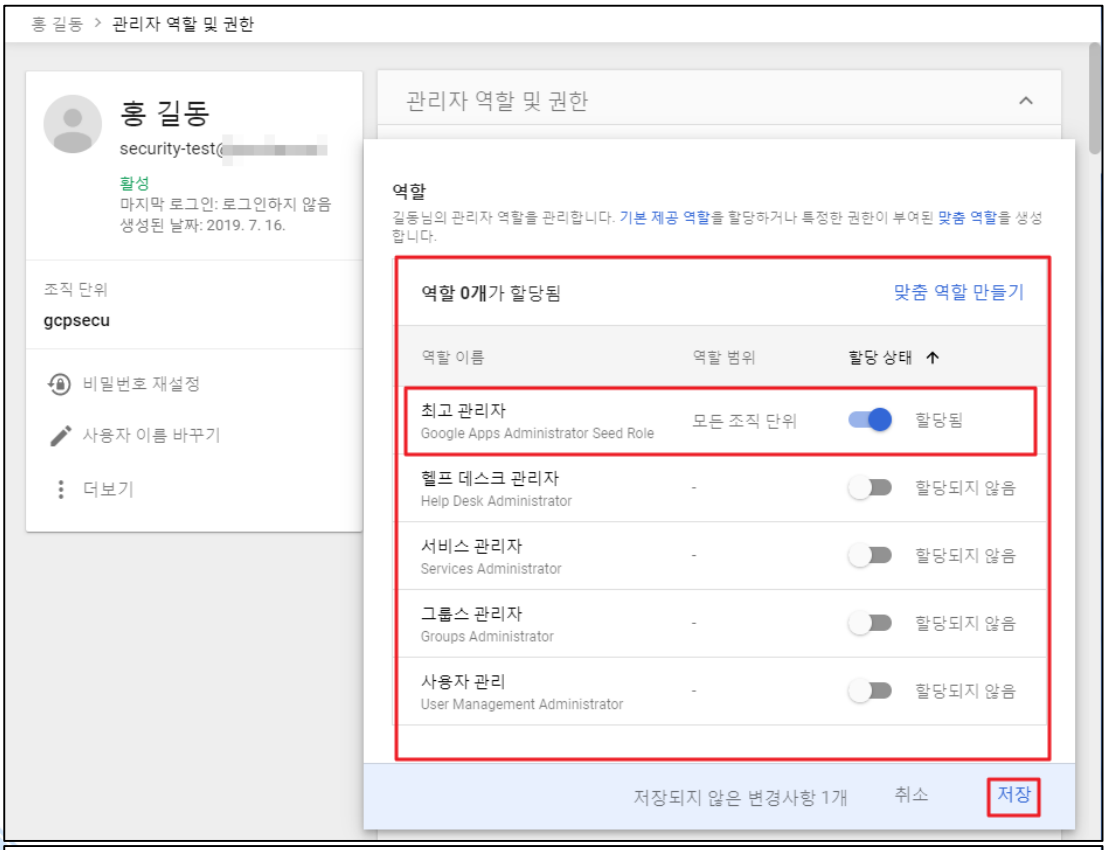
4) 사용자 생성 및 추가 확인

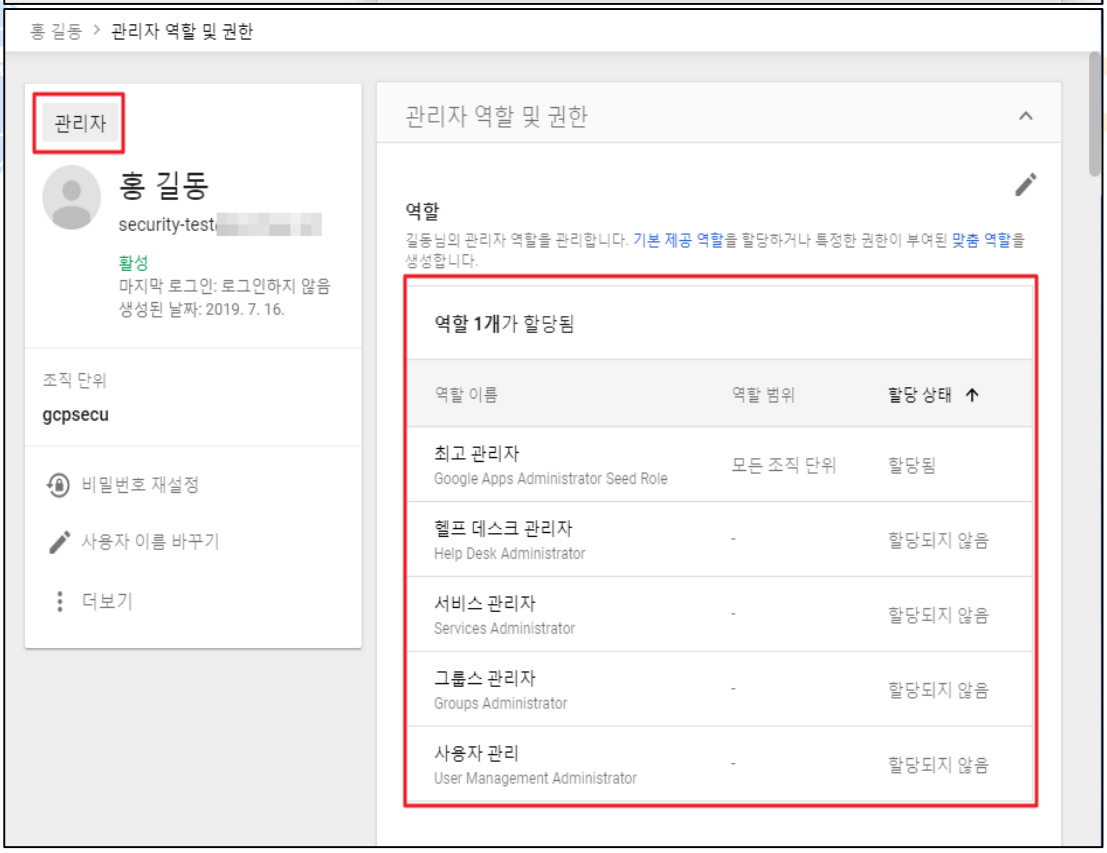


5) 관리자 역할 및 권한 지정



6) 역할 설정 후 저장





진단 기준	**양호기준** : 최고관리자 및 일반 계정에 대한 역할/권한 설명이 존재하는 경우

	취약기준 : 최고관리자 및 일반 계정에 대한 역할/권한 설명이 존재하지 않을 경우
비고	-

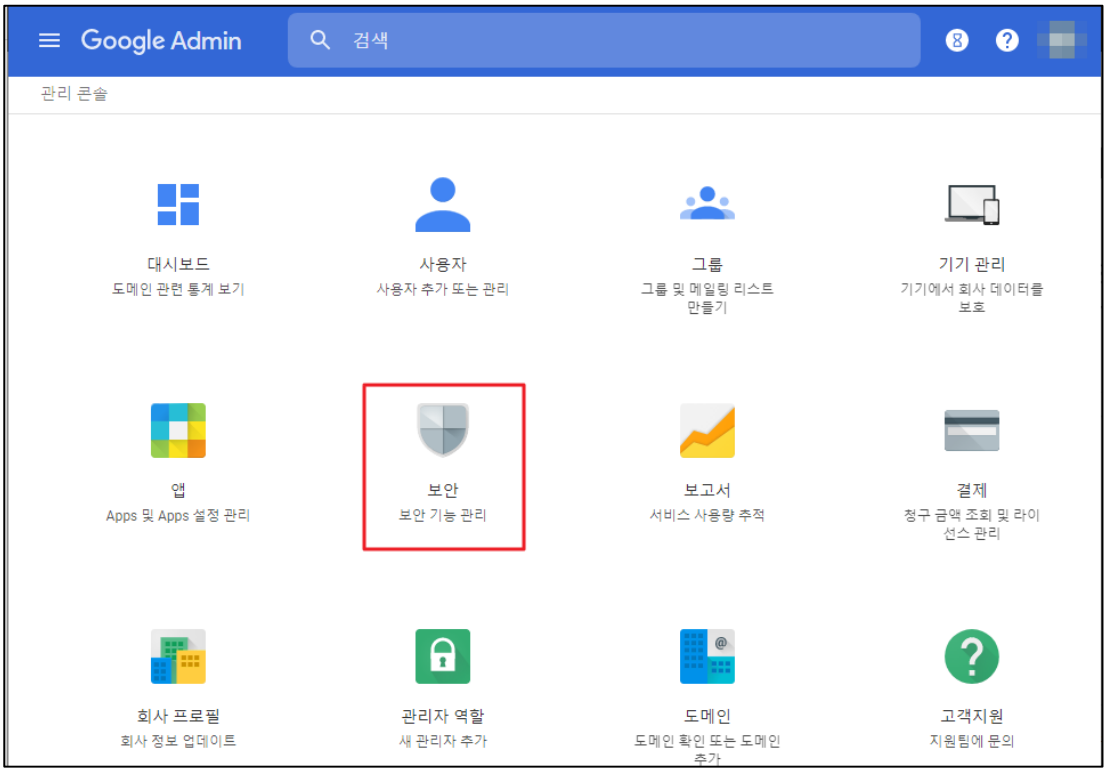
1.3 Cloud ID 사용자 계정 암호 관리

<table>
<tr><td>분류</td><td>인증/인가</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">Cloud ID 사용자 계정 암호 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">Cloud ID 사용자 계정을 통해 Google Workspace 등의 특정 서비스에 대한 권한을 보유할 경우 운영/관리/설정이 가능하기 때문에 암호 설정 시 유추하기 쉬운 암호로 설정하게 된다면 임의의 비인가 사용자들에게 계정 탈취의 빌미를 제공할 가능성이 있습니다. Cloud ID 계정의 암호 생성 및 변경 시 아래 패스워드 정책을 적용하여 악의적 계정 탈취를 방지해야 합니다.

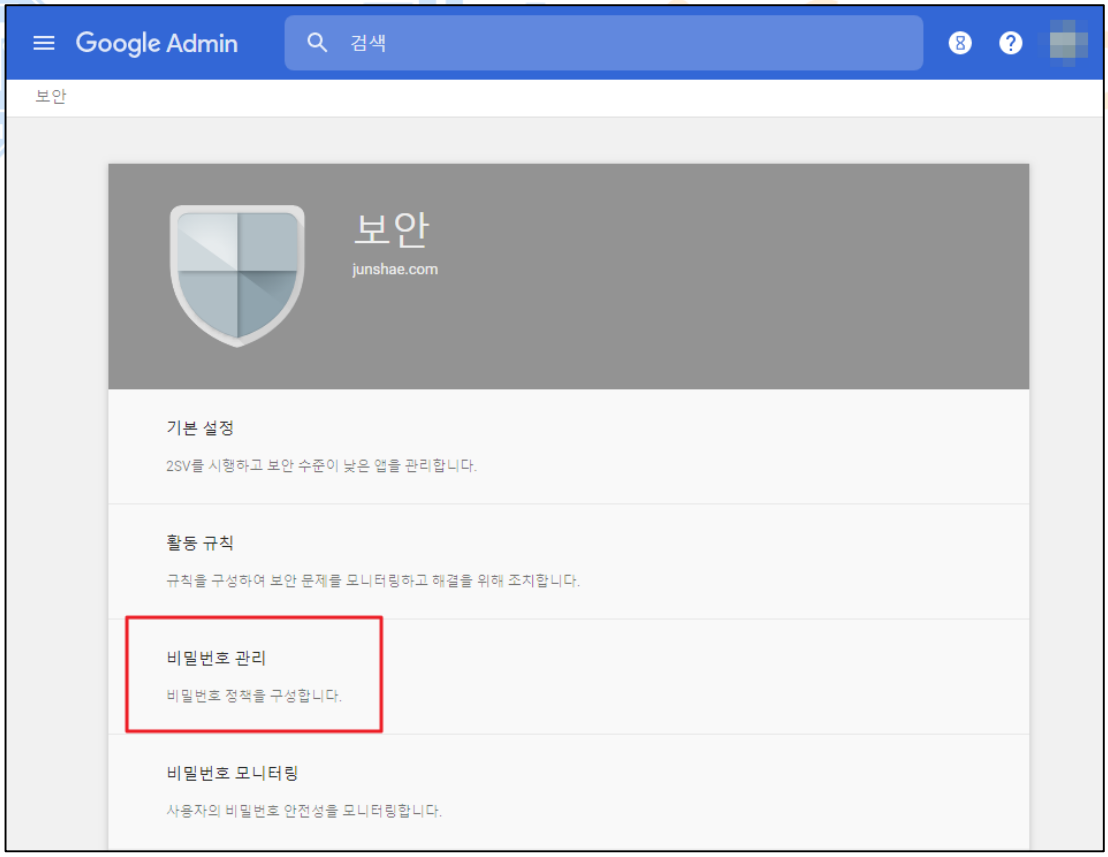
<패스워드 설정기준>
패스워드는 영문 대문자(26개), 영문 소문자(26개), 숫자(10개), 특수문자(32개)의 4종류
- 2종류 이상의 문자구성과 8자리 이상의 길이로 구성된 문자열
- 10자리 이상의 길이로 구성된 문자열 (숫자로만 구성할 경우 취약할 수 있음)

<추측이 어렵도록 패스워드 반영 설계>
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

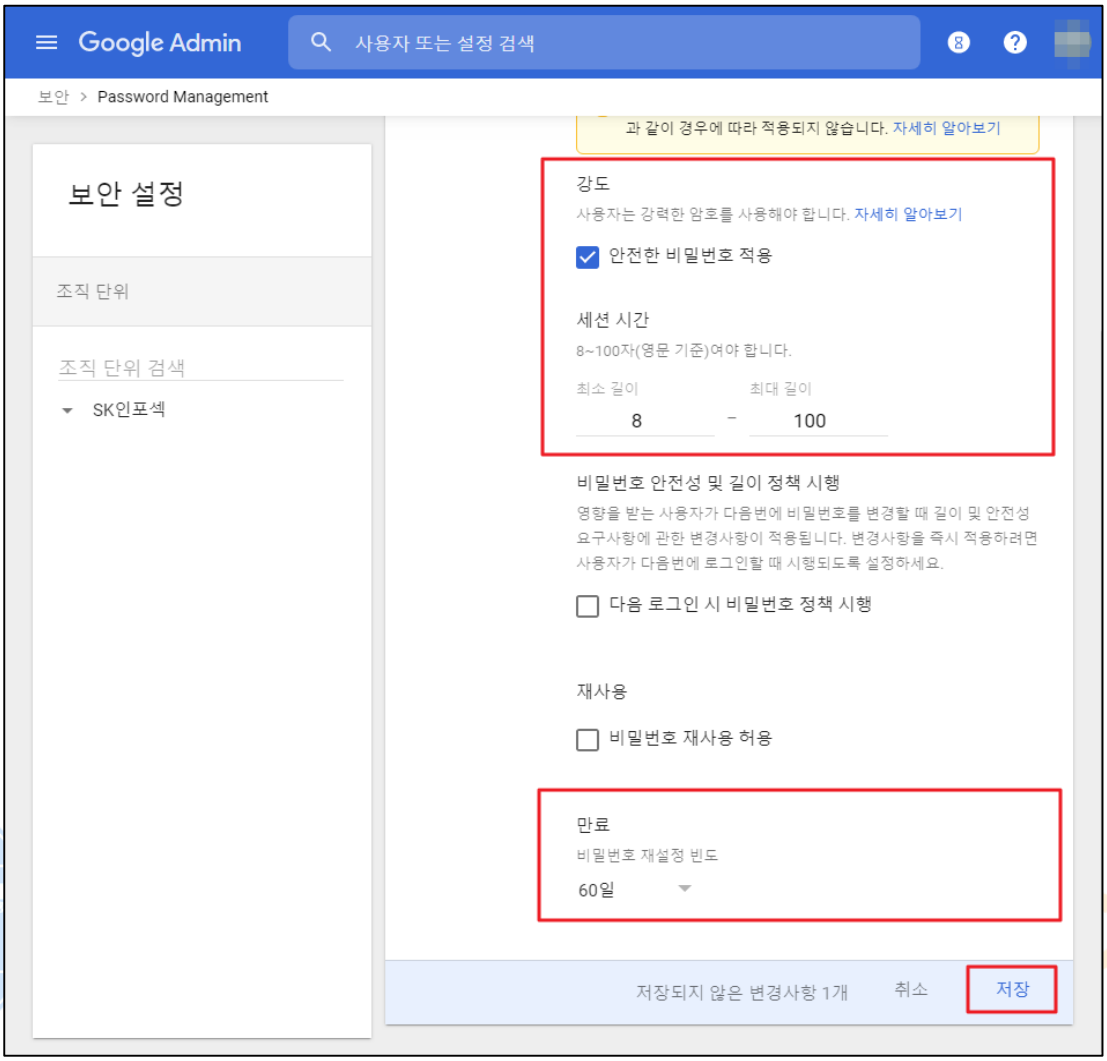
(*) 패스워드 설정기준은 KISA '패스워드 선택 및 이용 안내서'를 참고 (2019.06)
https://seed.kisa.or.kr/kisa/Board/53/detailView.do</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. G Suite 계정의 패스워드 복잡도 및 만료 기간 설정
1) [관리콘솔] > [보안]
- G Suite 계정 패스워드 정책 설정 시도</td></tr>
</table>



2) [비밀번호 관리]



3) 패스워드 강도 및 만료기간 설정

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단
기준</td><td>양호기준
: Cloud ID 사용자 패스워드의 복잡도 및 만료기간 설정이 되어 있을 경우

취약기준
: Cloud ID 사용자 패스워드의 복잡도 및 만료기간 설정이 되어 있지 않을 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

1.4 Cloud ID 사용자 2-Factor-Authentication 로그인

분류	인증/인가	중요도	중
항목명	Cloud ID 사용자 2-Factor-Authentication 로그인		

항목 설명

GCP는 Cloud ID 계정 사용자의 보안 강화를 위해 사용자에게 2-Factor-Authentication(MFA) 인증을 추가할 수 있습니다. 2-Factor-Authentication(MFA)를 사용할 경우 계정 암호나 액세스 키뿐 아니라 GCP가 지원하는 추가 인증을 요청 함으로써 보안을 강화하며 2-Factor-Authentication(MFA)는 다음의 형태로 사용자 인증을 할 수 있습니다.

(*) 사용 가능한 2단계 인증(2-Factor-Authentication, MFA) 방식

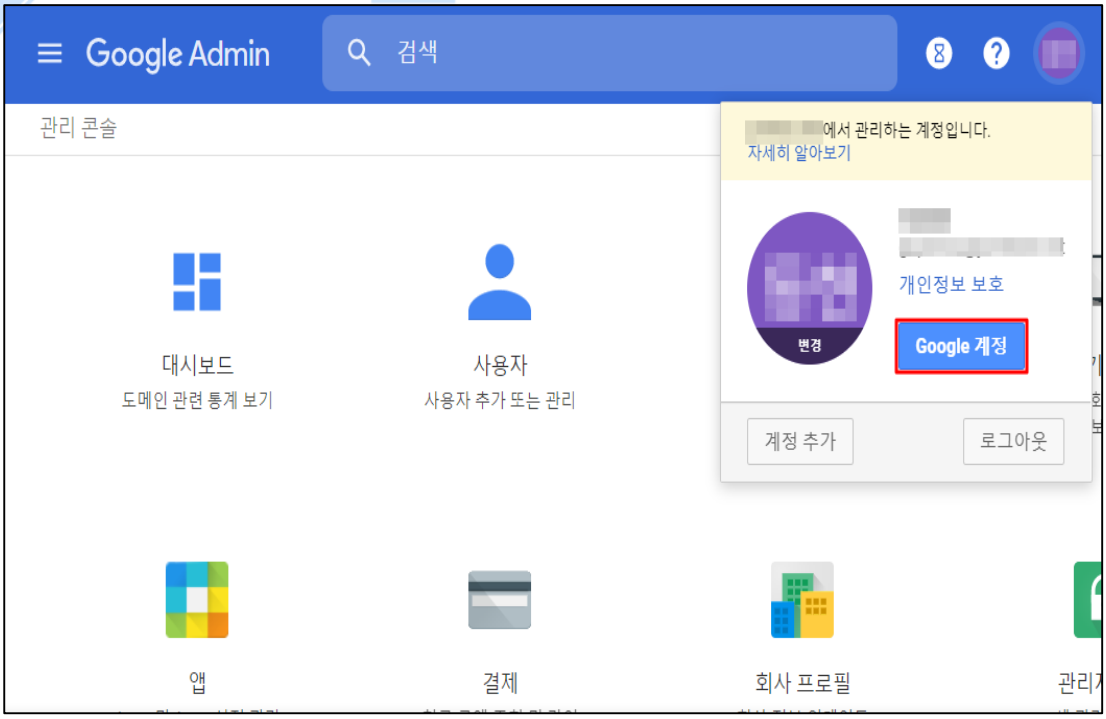
No	인증 수단
1	Google 메시지
2	보안 키
3	Google OTP 또는 기타 인증 코드 생성기
4	SMS 또는 전화로 인증 코드 받기
5	백업 코드

(*) 2단계 인증(2-Factor-Authentication, MFA) 설정은 각 사용자별 각자 맞는 방식으로 추가 설정해야 합니다.

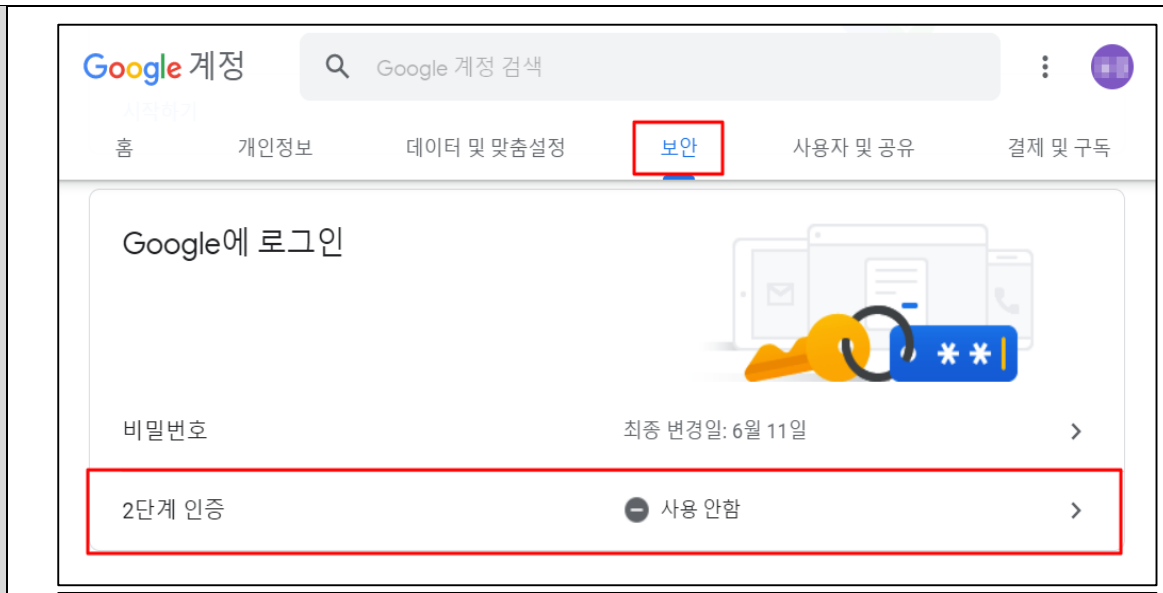
설정 방법

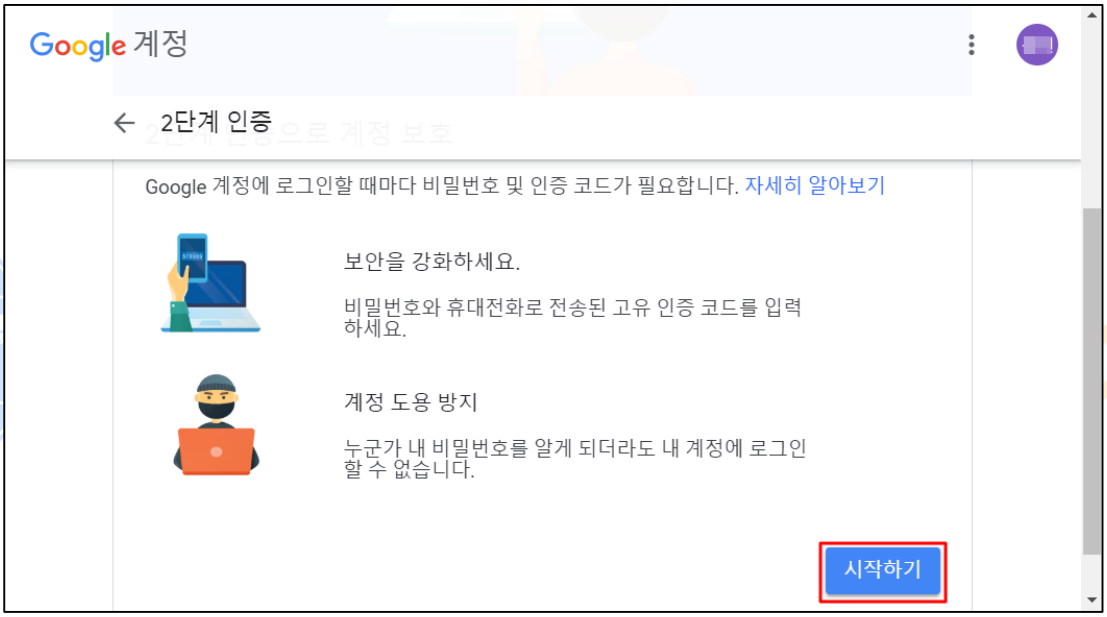
가. 관리자 2-factor 설정

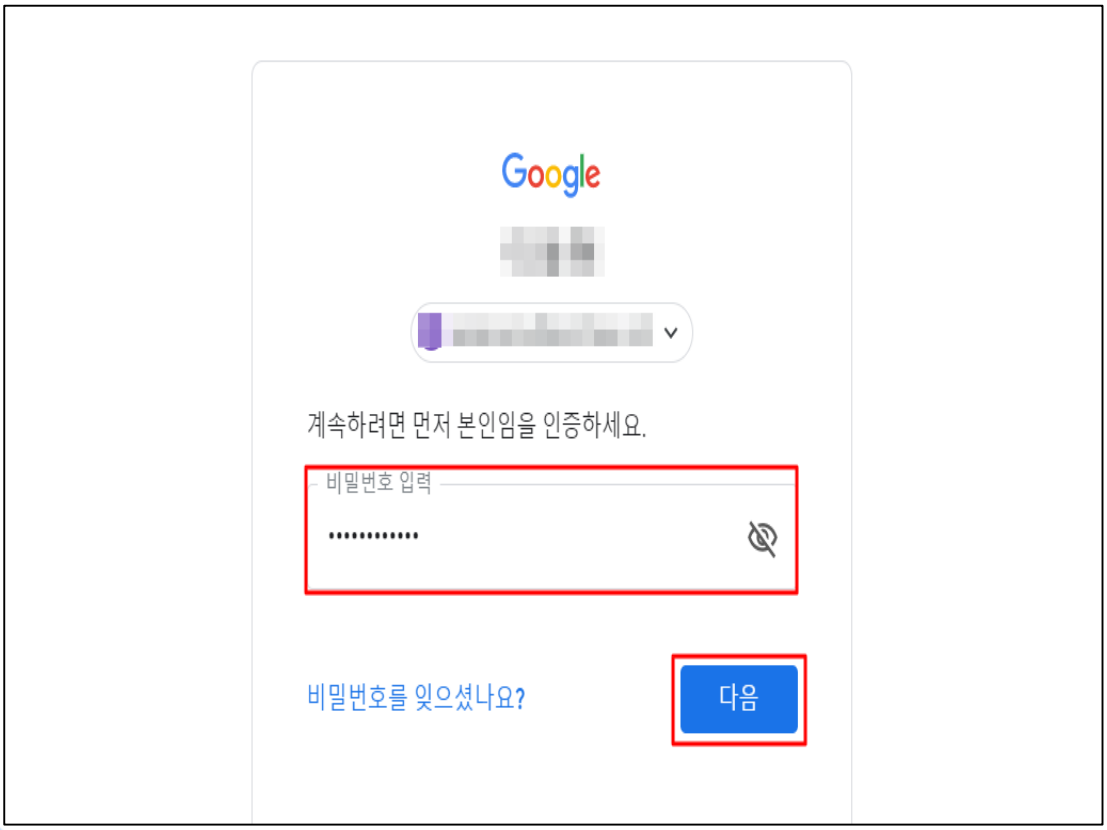
1) [메인] > [Google 계정]



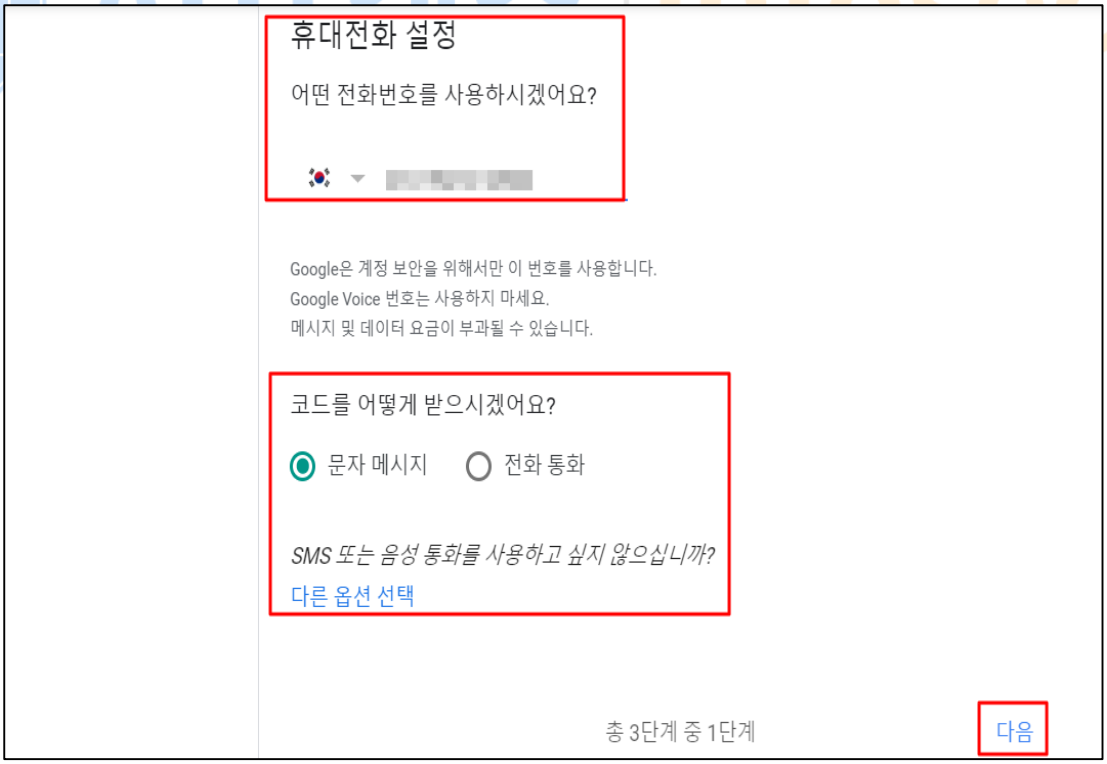
2) [보안] > [2단계 인증]



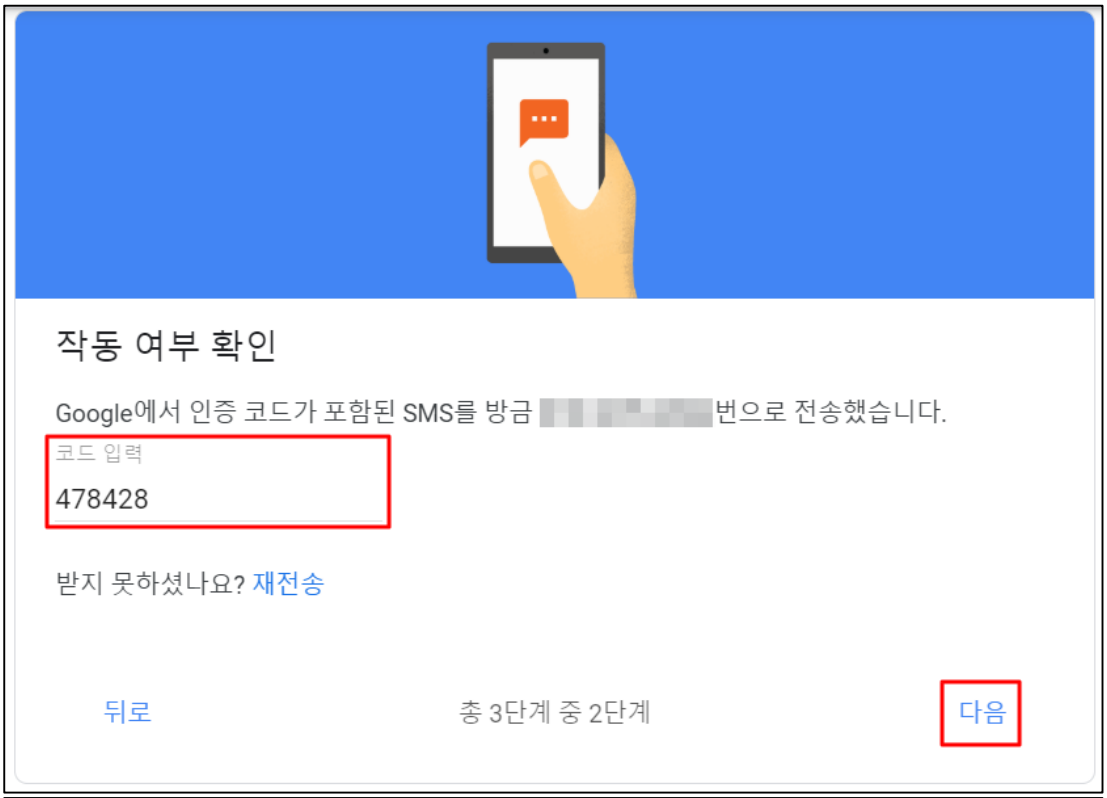


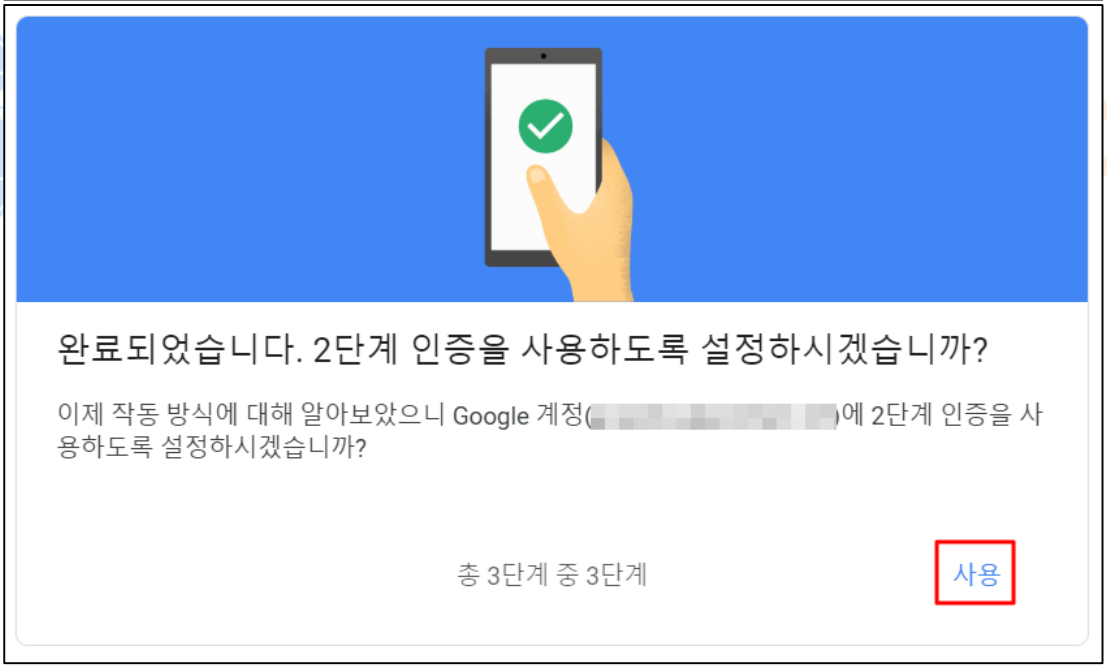


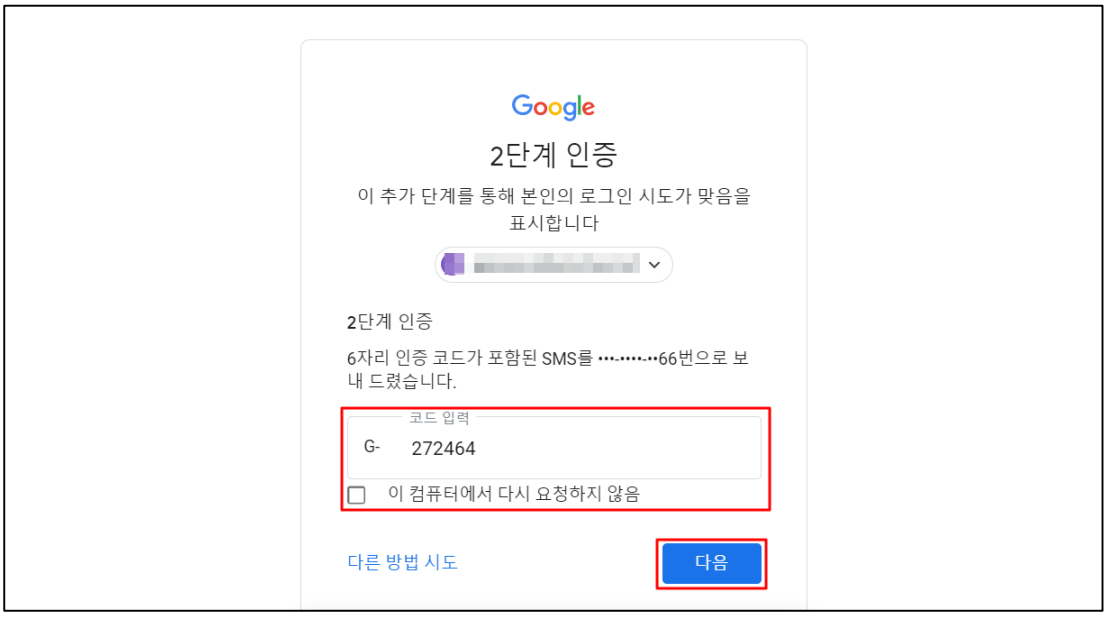
3) [휴대전화 설정]



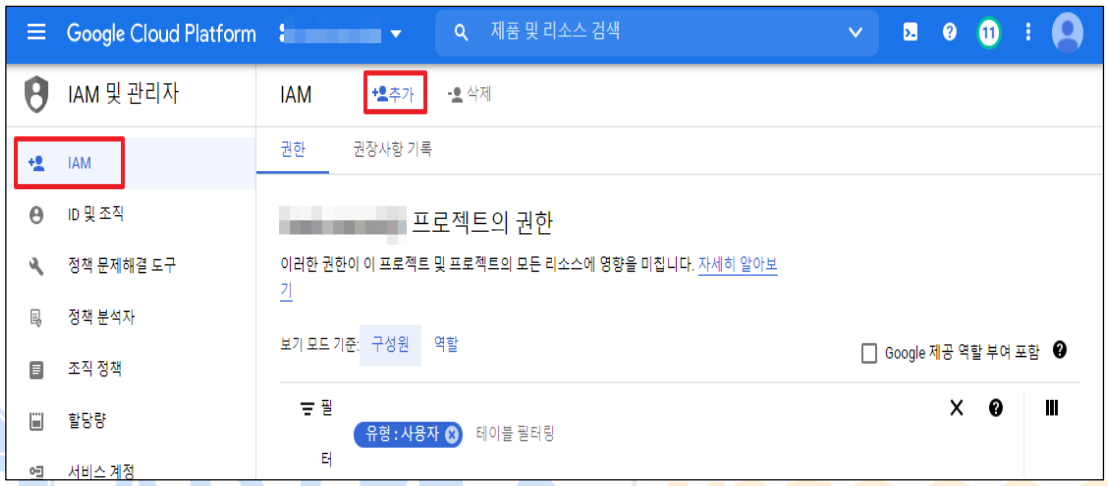
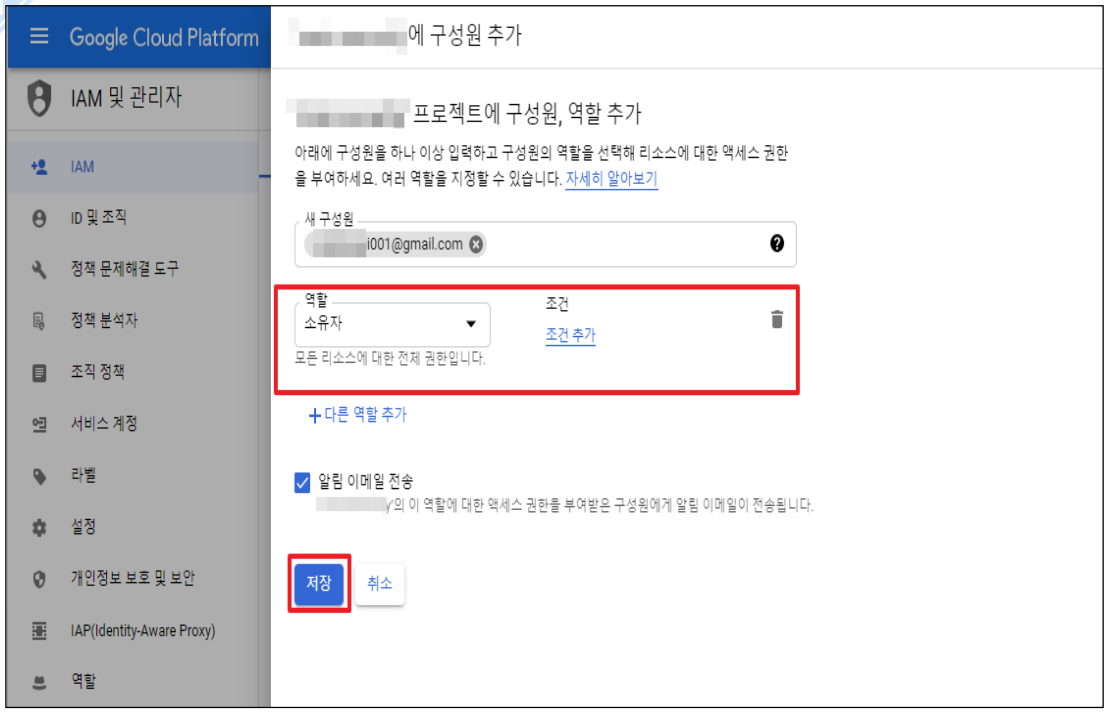
4) [인증번호 확인]

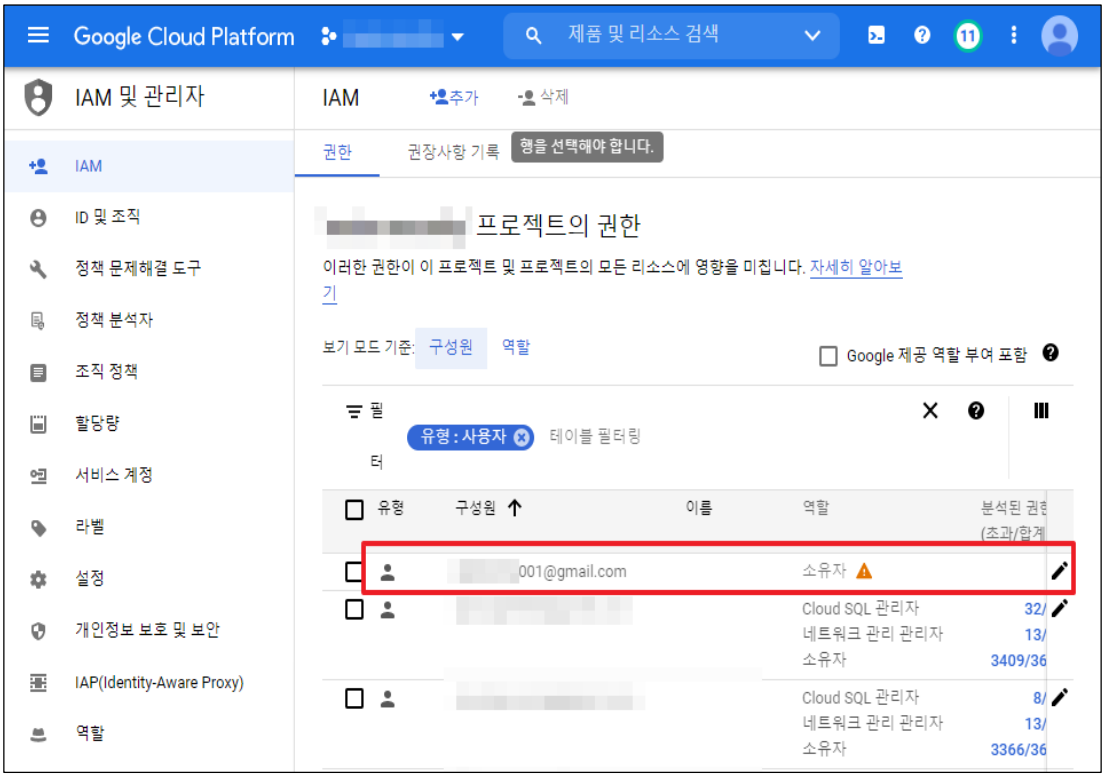




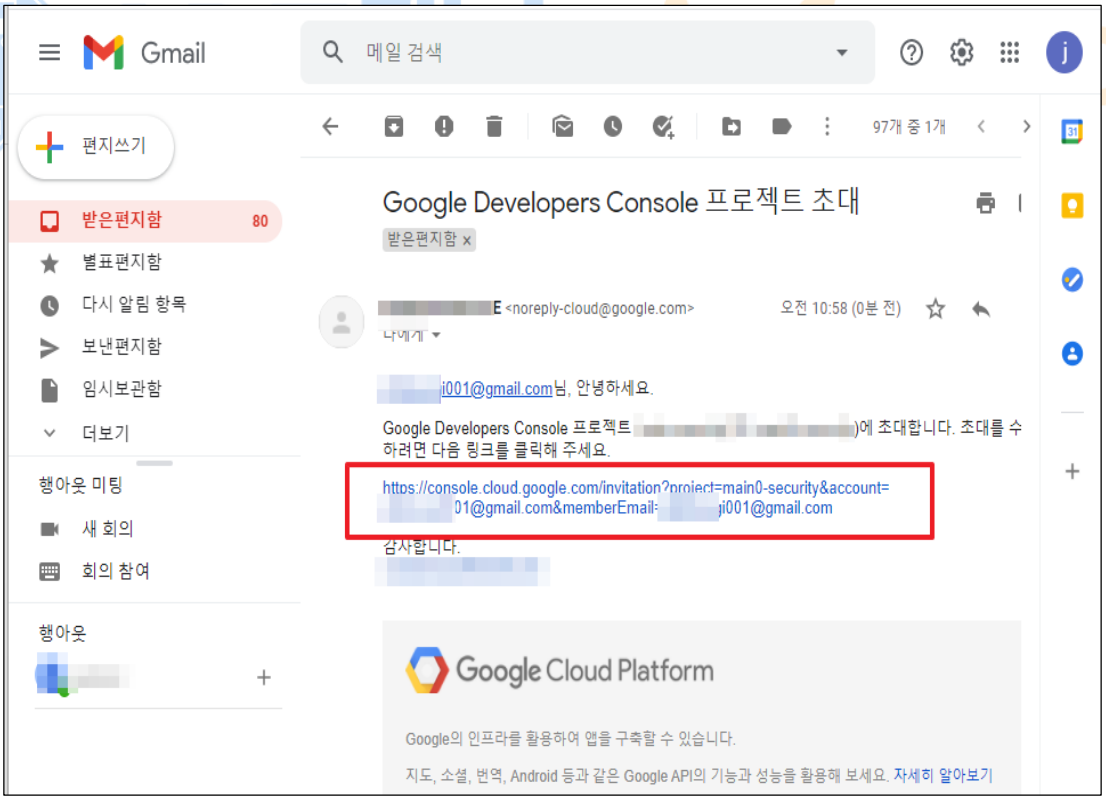
	
진단 기준	**양호기준** : Cloud ID 모든 사용자 계정이 2-Factor 인증으로 적용되어 있을 경우 **취약기준** : Cloud ID 모든 사용자 계정이 2-Factor 인증으로 적용되어 있지 않을 경우
비고	

1.5 Google 사용자 계정 최고권한(소유자) 관리

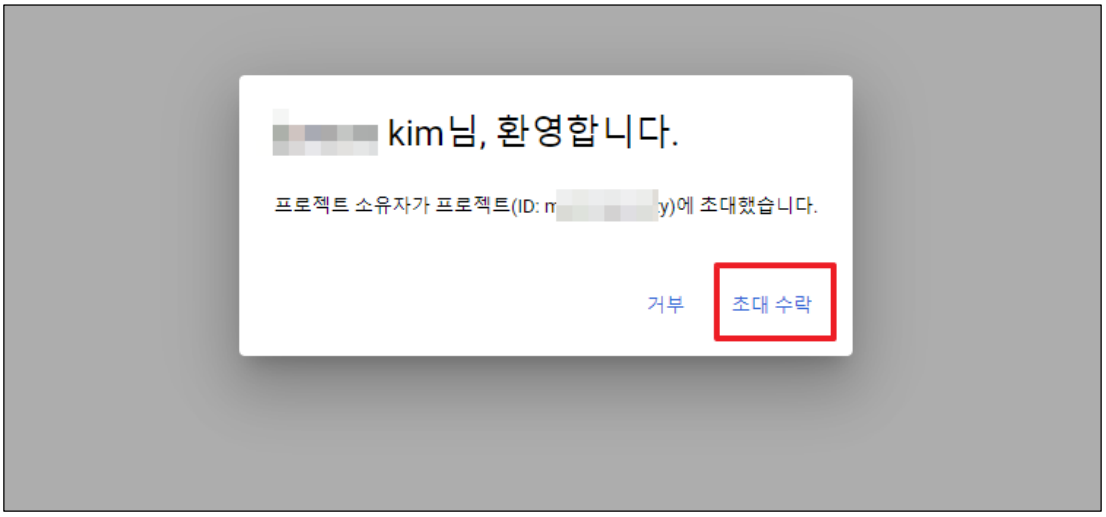
분류	인증/인가	중요도	중
항목명	Google 사용자 계정 최고권한(소유자) 관리		
항목 설명	"소유자(roles/owner)" 권한은 GCP 서비스 내 가장 높은 권한으로 모든 GCP 서비스와 계정 내 모든 리소스에 대한 작업을 가능하게 합니다. 이처럼 가장 높은 권한(소유자(roles/owner))은 인가되지 않은 Google 계정 사용자에게 부여되지 않아야 합니다.		
설정 방법	**가. IAM 내 Cloud ID/Google Google 계정 사용자 추가** 1) IAM 사용자 추가 버튼 클릭  2) Google 계정 사용자 추가 (역할 부여: 소유자)  3) 신규 사용자 추가 및 Google 계정에 최고권한(소유자) 부여 확인		



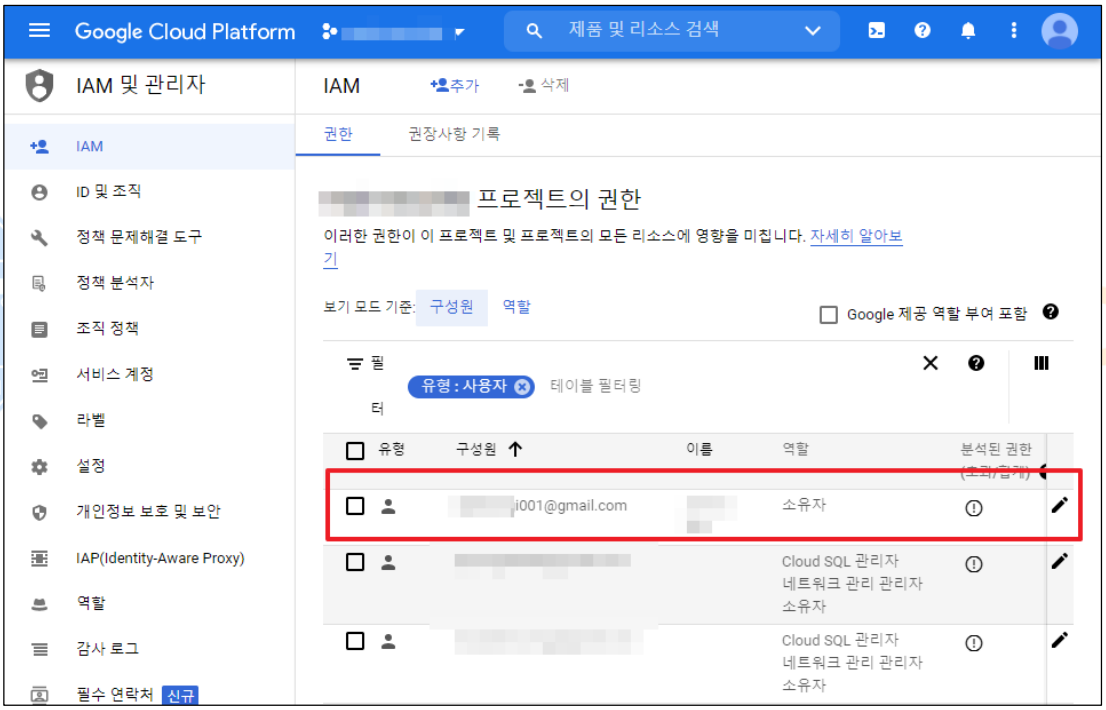
4) Google 계정 사용자 최고권한(소유자) 획득을 위한 이메일 인증



5) 프로젝트 내 최고권한(소유자) 인증을 위한 초대 수락 버튼 클릭



6) 추가된 신규 Google 계정 사용자 최종 권한 여부 확인



진단 기준	**양호기준** : '소유자(Owner)' IAM 역할이 최고 관리자에게만 부여되어 있을 경우 **취약기준** : '소유자(Owner)' IAM 역할이 최고 관리자 외 일반 사용자에게 부여되어 있을 경우
비고	

1.6 서비스 계정 관리

분류	인증/인가	**중요도**	중

<table>
<tr><td>항목명</td><td>서비스 계정 관리</td></tr>
<tr><td>항목
설명</td><td>
서비스 계정은 개별 최종 사용자가 아닌 애플리케이션 또는 가상 머신에 속한 특별한 Google 계정입니다. 애플리케이션은 서비스 계정을 사용하여 서비스의 Google API를 호출하므로 사용자가 직접 관여하지 않습니다.

예를들어 Compute Engine 가상 머신을 서비스 계정으로 실행할 수 있으며 해당 계정에 필요한 리소스에 대한 액세스 권한을 부여할 수 있습니다. 이렇게 하면 서비스 계정은 서비스의 ID가 되며 서비스 계정의 권한은 서비스가 액세스할 수 있는 리소스를 제어합니다.

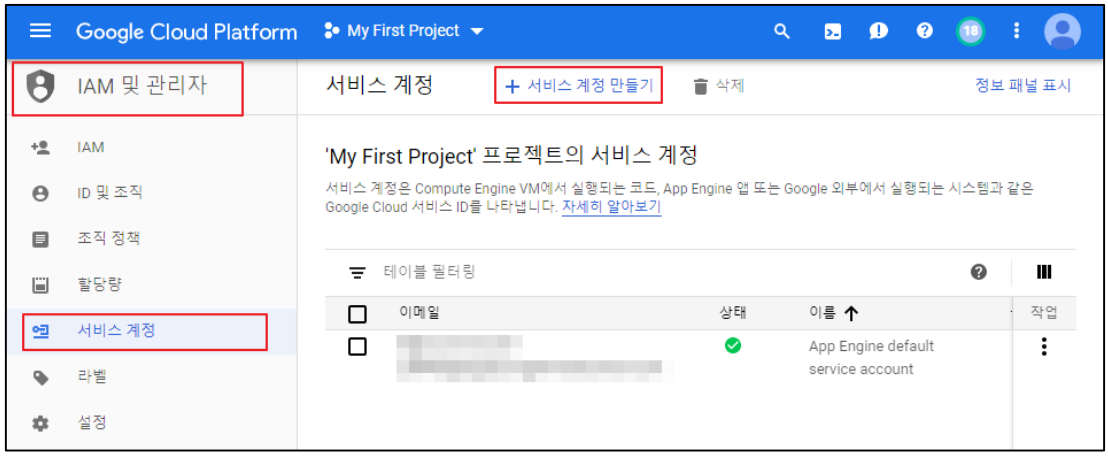
서비스 계정은 계정 고유의 이메일 주소로 식별되며 기본 서비스 계정은 Compute Engine 및 App Engine에서 사용하도록 설계되었기 때문에 해당 계정의 생성 시점 및 프로젝트에 표시되는 방식은 추후 변경될 수 있습니다. 따라서 서비스 계정을 사용할 때는 이러한 기본 계정에 의존하지 않는 것이 좋습니다. 계정을 장기간 사용하려면 IAM API, GCP 콘솔, gcloud 명령줄 도구를 사용하여 명시적으로 추가 서비스 계정을 만드는 것이 좋습니다.

※ 서비스 계정 유형
<table>
<tr><th>계정 유형</th><th>상세내용</th><th>예시</th></tr>
<tr><td rowspan="3">사용자 관리 서비스 계정</td><td>GCP 콘솔을 사용하여 새로운 Cloud 프로젝트를 만들 때 프로젝트에 Compute Engine API 가 사용 설정된 경우 Compute Engine 서비스 계정이 기본적으로 생성됩니다.</td><td>PROJECT_NUMBER-compute@developer.gserviceaccount.com</td></tr>
<tr><td>프로젝트에 App Engine 애플리케이션이 포함되어 있으면 프로젝트에 기본 App Engine 서비스 계정이 기본적으로 생성됩니다. 이는 다음 이메일을 사용하여 식별할 수 있습니다.</td><td>PROJECT_ID@appspot.gserviceaccount.com</td></tr>
<tr><td>프로젝트에서 서비스 계정을 만드는 경우 서비스 계정의 이름을 지정하면 다음과 같은 형식의 이메일이 할당됩니다.</td><td>SERVICE_ACCOUNT_NAME@PROJECT_ID.iam.gserviceaccount.com</td></tr>
<tr><td>Google 관리 서비스 계정</td><td>사용자 관리 서비스 계정 외에도 프로젝트의 IAM 정책 또는 GCP 콘솔에 몇 가지 추가 서비스 계정이 나타날 수 있습니다. 이러한 서비스 계정은 Google 에서 만들고 소유합니다. 해당 계정은 다른 Google 서비스를 나타내며 각 계정에는 GCP 프로젝트에 액세스할 수 있는 IAM 역할이 자동으로 부여됩니다.</td><td>Google API 서비스 계정
PROJECT_NUMBER@cloudservices.gserviceaccount.com
(*) 해당 계정은 GCP 콘솔의 서비스 계정 섹션에서는 나타나지 않음</td></tr>
</table>
</td></tr>
</table>

설정 방법

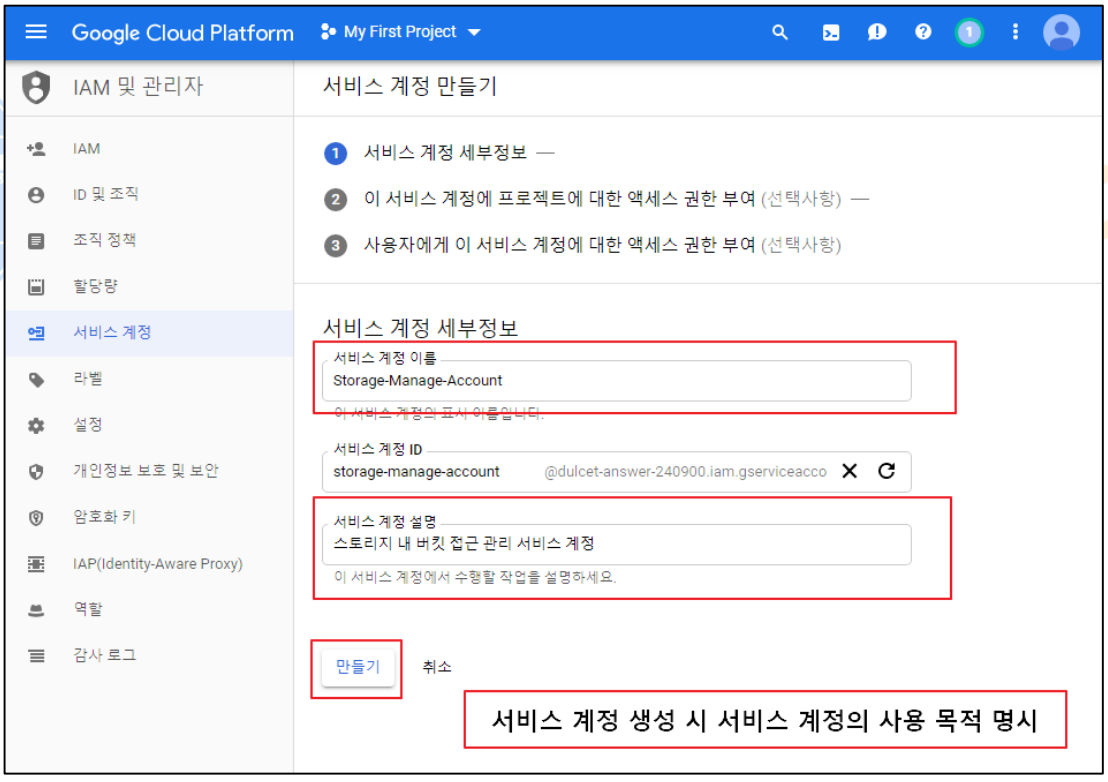
가. 서비스 계정 생성 시 생성 계정에 대한 서비스 역할 작성

1) [IAM 및 관리자] > [서비스 계정] > [서비스 계정 만들기]

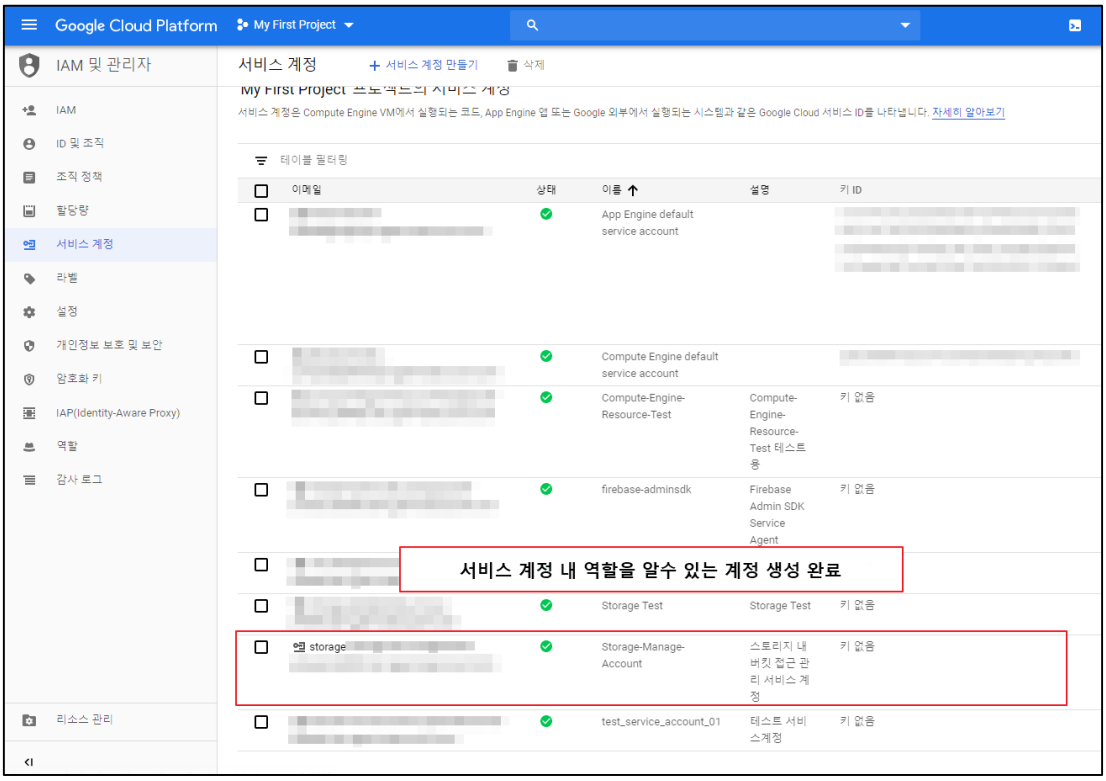


2) 서비스 계정 이름 및 설명 작성 후 계정 생성

- 서비스 계정에 대한 사용자 IAM 권한 할당은 선택 사항이며 계정 생성 이후에도 설정이 가능합니다.



3) 서비스 계정 내 역할을 알 수 있는 계정 생성 완료

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단 기준</td><td>양호기준
: 서비스 역할을 알 수 없는 서비스 계정이 존재하지 않을 경우

취약기준
: 서비스 역할을 알 수 없는 서비스 계정이 존재하는 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

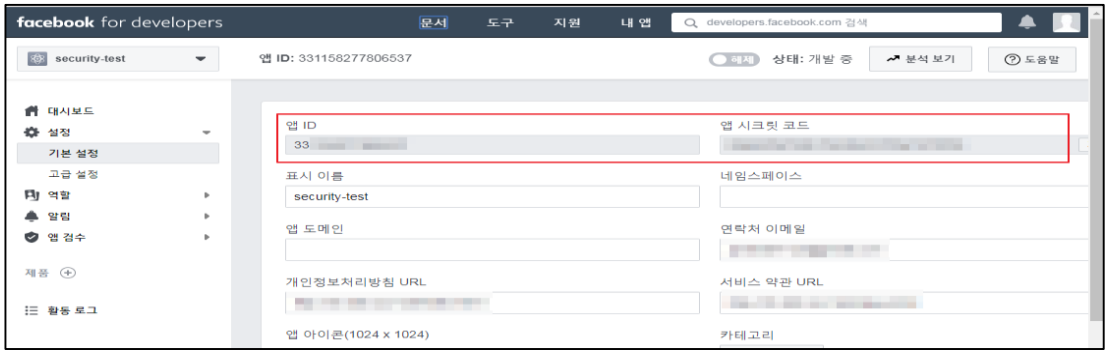
1.7 Identity Platform 사용자 관리

<table>
<tr><td>분류</td><td>인증/인가</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">Identity Platform 사용자 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">Identity Platform을 통해 사용자는 멀티 테넌트 SaaS 애플리케이션, 모바일 / 웹 애플리케이션, 게임, API 등과 같은 애플리케이션 및 서비스에 대해 인증 할 수 있습니다. Identity Platform은 Google Cloud Platform (GCP), 자체 백엔드 또는 다른 플랫폼에서 서비스를 작성하는 경우 안전하고 사용하기 쉬운 인증을 제공합니다.

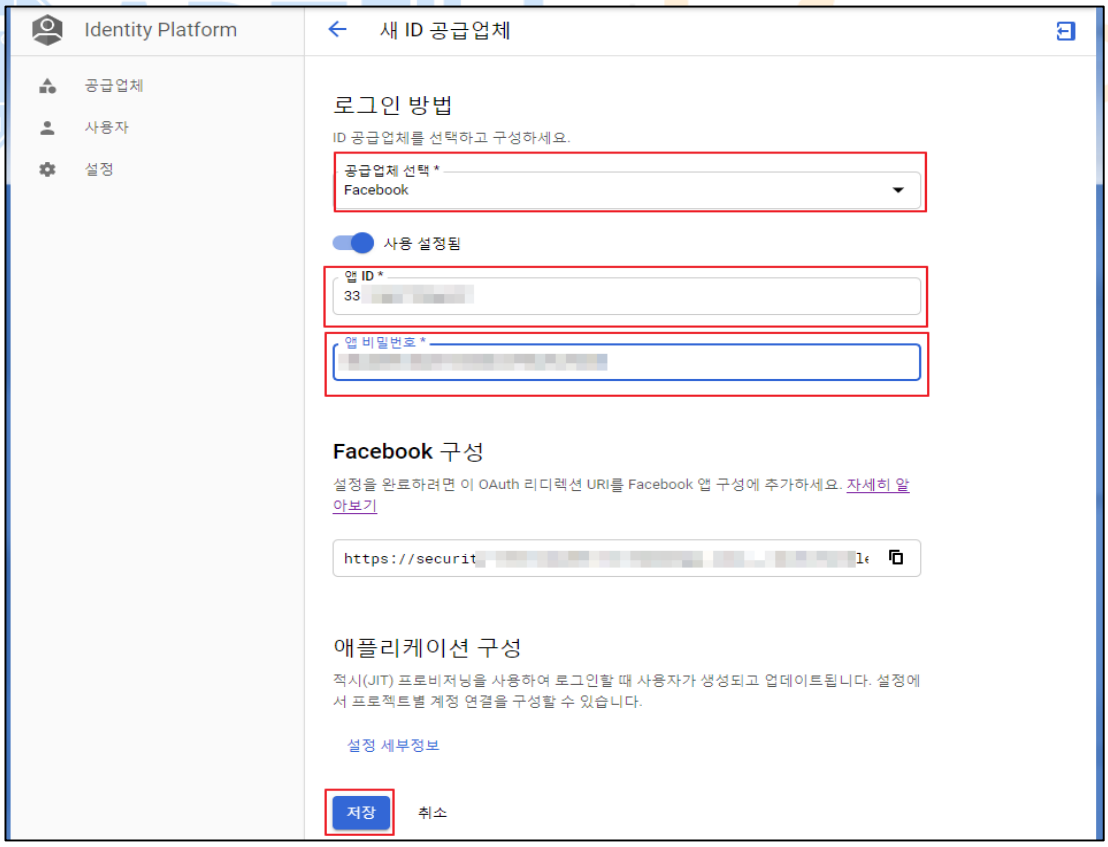
Identity Platform은 백엔드 서비스를 제공하며 사용하기 쉬운 SDK 및 기성 UI 라이브러리와 함께 작동하여 사용자를 앱에 인증합니다. 암호, 전화 번호, Google, Facebook, Twitter 및 SAML 또는 OpenID Connect 프로토콜을 지원하는 모든 제공 업체와 같은 인기있는 통합 ID 공급자를 사용하여 인증을 지원합니다.

※ SDK를 사용한 인증
<table>
<tr><th>인증 구분</th><th>상세 내용</th></tr>
<tr><td>전자 메일 및 암호 기반 인증</td><td>전자 메일 주소와 암호로 사용자를 인증하는 방법입니다. SDK 는 전자 메일 주소와 암호를 사용하여 로그인하는 사용자를 만들고 관리하는 방법을 제공합니다.</td></tr>
<tr><td>페더레이션 ID 공급자 통합</td><td>타 플랫폼 ID 공급자와 통합하여 사용자를 인증하는 방법입니다. SDK 는 사용자가 Google, FaceBook, Twitter 및 GitHub 계정으로 로그인 할 수 있는 방법을 제공합니다.</td></tr>
<tr><td>전화 번호 인증</td><td>휴대 전화로 SMS 메시지를 보내 사용자를 인증합니다.</td></tr>
<tr><td>사용자 정의 인증 시스템 통합</td><td>앱의 기존 로그인 시스템을 Identity Platform 에 연결하고 서버에서 생성 된 토큰을 GCP, firebase 또는 기타 서비스로 실행중인 앱에 사용할 수 있는 Identity Platform 토큰과 교환합니다.</td></tr>
<tr><td>익명 인증</td><td>임시 익명 계정을 만들어 사용자가 먼저 로그인 할 필요 없이 인증이 필요한 기능을 사용할 수 있습니다. 사용자가 나중에 가입하도록 선택하면 익명 계정을 일반 계정으로 업그레이드 할 수 있으므로 사용자는 중단 한 위치에서 계속할 수 있습니다.</td></tr>
</table>
※ 공급업체 (Email/Password) 적용 시 ‘안전한 패스워드 정책’ 적용 및 ‘비밀번호 없는 로그인 허용’을 설정하여 사용하지 마시기 권고 드립니다. 또한, 사용자가 인증된 수만큼 금액이 부가될 수 있는 옵션 기능으로 필수적으로 적용해야 하는 기능은 아닙니다.</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. Identity Platform 설정 방법 (페더레이션 ID 공급자 통합)
1) [Tool] > [Identity Platform] > [공급업체] > [공급업체 추가]</td></tr>
</table>

2) 공급업체 인증을 사용하기 위한 공급업체(ex_ Facebook) 내 앱 ID /앱 시크릿 코드 확인



3) 공급 업체에서 확인한 앱 ID / 앱 시크릿 코드 등 작성 후 저장



4) 공급 업체 추가 완료

	
진단 기준	**양호기준** : ID 공급업체 설정 중 '익명(Anonymous)' 인증이 존재하지 않을 경우 **취약기준** : ID 공급업체 설정 중 '익명(Anonymous)' 인증이 존재할 경우
비고	

1.8 IAM 역할 관리

<table>
<tr><td>분류</td><td>인증/인가</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">IAM 역할 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">Google Cloud Platform(GCP)에서 제공하는 Cloud IAM을 사용하면 누가(ID) 어떤 리소스에 대한 어떤 액세스 권한(역할)을 갖는지 정의해 액세스 제어를 관리할 수 있습니다. 또한, Cloud IAM을 사용하면 특정 GCP 리소스에 대해 세밀한 액세스를 부여하고 다른 리소스에 대한 무단 액세스를 방지할 수 있습니다. Cloud IAM으로 최소 권한의 보안 원칙을 적용하여 필요한 리소스에 대한 액세스 권한만 부여할 수 있습니다.

※ IAM 역할
<table>
<tr><th>IAM
역할 구분</th><th>역할
이름</th><th>상세설명</th></tr>
<tr><td rowspan="3">기본 역할</td><td>뷰어</td><td>상태에 영향을 주지 않는 읽기 전용 작업에 대한 권한이 부여됩니다.
예) 기존 리소스 또는 데이터의 조회(수정 제외)가 해당됨</td></tr>
<tr><td>편집자</td><td>모든 뷰어 권한에 더해 기존 리소스 변경과 같이 상태를 변경하는 작업에 대한 권한까지 포함됩니다.</td></tr>
<tr><td>소유자</td><td>모든 편집자 권한 및 다음 작업에 대한 권한이 포함됩니다.
- 프로젝트 및 프로젝트 내의 모든 리소스에 대한 역할 및 관리
- 프로젝트에 대한 결제 설정</td></tr>
<tr><td rowspan="2">프로젝트 역할</td><td>서비스 계정 행위자</td><td>해당 역할은 지원이 중단되었기 때문에 서비스 계정으로서 작업을 실행하려면 서비스 계정 사용자 역할을 사용해야 합니다.
서비스 계정 행위자로서 동일한 권한을 효과적으로 제공하려면 서비스 계정 토큰 생성자 권한도 부여해야 합니다.</td></tr>
<tr><td>브라우저</td><td>폴더, 조직, Cloud IAM 을 포함한 프로젝트의 계층구조를 탐색할 수 있는 읽기 액세스입니다.
해당 역할에는 프로젝트의 리소스를 볼 수 있는 권한이 제공되지 않습니다.</td></tr>
<tr><td rowspan="3">App Engine 역할</td><td>App Engine 관리자</td><td>모든 애플리케이션 구성 및 설정에 대한 읽기/쓰기/수정 액세스입니다.</td></tr>
<tr><td>App Engine 서비스 관리자</td><td>모든 애플리케이션 구성과 설정에 대한 읽기 전용 액세스입니다.
모듈 수준 및 버전 수준 설정에 대한 쓰기 액세스를 가지고 있으며 새로운 버전은 배포할 수 없습니다.</td></tr>
<tr><td>App Engine 배포자</td><td>모든 애플리케이션 구성과 설정에 대한 읽기 전용 액세스입니다.
새로운 버전 생성만 가능한 쓰기 액세스로 트래픽을 수신하지</td></tr>
</table></td></tr>
</table>

		않는 버전을 삭제하는 경우를 제외하면 기존 버전을 수정할 수 없습니다.
	App Engine 뷰어	모든 애플리케이션 구성과 설정에 대한 읽기 전용 액세스입니다.
	App Engine 코드 뷰어	모든 애플리케이션 구성, 설정 및 배포된 소스 코드에 대한 읽기 전용 액세스입니다.
Cloud Bigtable 역할	Cloud Bigtable 관리자	테이블 내에 저장된 데이터를 비롯하여 프로젝트 내의 모든 인스턴스를 관리합니다. 새 인스턴스를 만들 수 있습니다. 프로젝트 관리자용입니다.
	Cloud Bigtable 사용자	테이블 내에 저장된 데이터에 대한 읽기/쓰기 액세스를 제공합니다. 애플리케이션 개발자 또는 서비스 계정용입니다.
	Cloud Bigtable 리더	테이블 내에 저장된 데이터에 대한 읽기 전용 액세스를 제공합니다. 데이터 과학자, 대시보드 생성기, 기타 데이터 분석 시나리오용입니다.
	Cloud Bigtable 뷰어	데이터 액세스를 제공하지 않습니다. Cloud Bigtable 용 GCP 콘솔에 액세스하기 위한 최소 권한 집합으로 사용됩니다.
Cloud Billing 역할	결제 계정 관리자	결제 계정의 모든 요소를 보고 관리하기 위한 액세스 권한을 제공합니다.
	프로젝트 결제 관리자	프로젝트의 결제 계정을 할당하거나 프로젝트 결제를 사용 중지하는 액세스 권한을 제공합니다.
	결제 계정 사용자	프로젝트를 결제 계정과 연결하기 위한 액세스 권한을 제공합니다.
	결제 계정 생성자	결제 계정 생성을 위한 액세스를 제공합니다.
	결제 계정 뷰어	결제 계정 비용 정보 및 거래를 봅니다.
Cloud Dataflow 역할	Cloud Dataflow 뷰어	모든 Cloud Dataflow 관련 리소스에 대한 읽기 전용 액세스를 제공합니다.
	Cloud Dataflow 개발자	Cloud Dataflow 작업을 실행 및 조작하는 데 필요한 모든 권한을 제공합니다.
	Cloud Dataflow 작업자	Cloud Dataflow 파이프라인에 대한 작업 단위를 실행하기 위한 Compute Engine 서비스 계정에 필요한 권한을 제공합니다.
Cloud	Cloud	머신 유형, 네트워크, 프로젝트 및 영역 등 Cloud Dataproc

Dataproc 역할	Dataproc 편집기	관리에 필수적인 리소스를 보는 데 필요한 권한을 제공합니다.
	Cloud Dataproc 뷰어	Cloud Dataproc 리소스에 대한 읽기 전용 액세스를 제공합니다.
Cloud Datastore 역할	Cloud Datastore 가져오기 내보내기 관리자	가져오기 및 내보내기를 관리할 수 있는 전체 액세스 권한을 제공합니다.
	Cloud Datastore 색인 관리자	색인 정의를 관리할 수 있는 전체 액세스 권한을 제공합니다.
	Cloud Datastore 소유자	Cloud Datastore 리소스에 대한 전체 액세스 권한을 제공합니다.
	Cloud Datastore 사용자	Cloud Datastore 데이터베이스의 데이터에 대한 읽기/쓰기 액세스를 제공합니다.
	Cloud Datastore 뷰어	리소스에 대한 읽기 액세스 권한을 제공합니다.
Dialogflow 역할	Dialogflow API 관리자	모든 Dialogflow(API 전용) 및 GCP 리소스에 대한 전체 액세스입니다. API 및 Dialogflow 콘솔(일반적으로 Dialogflow 콘솔에서 에이전트를 생성하기 위해 필요)에도 유사한 액세스를 확보하려면 roles/owner 기본 역할을 사용하세요.
	Dialogflow API 클라이언트	모든 Dialogflow(API 전용) 및 GCP 리소스에 대한 액세스를 수정합니다. API 및 Dialogflow 콘솔(일반적으로 Dialogflow 콘솔에서 에이전트를 생성하기 위해 필요)에도 유사한 액세스를 확보하려면 roles/editor 기본 역할을 사용하세요.
	Dialogflow API 리더	모든 Dialogflow(API 전용) 및 GCP 리소스에 대한 읽기 액세스입니다. 의도는 감지하지 못합니다. API 및 Dialogflow 콘솔에도 유사한 액세스 권한을 부여하려면 roles/viewer 기본 역할을 사용하세요.
Cloud DNS 역할	DNS 관리자	모든 Cloud DNS 에 대한 읽기 및 쓰기 액세스 권한을 제공합니다.
	DNS 리더	모든 Cloud DNS 리소스에 대한 읽기 전용 액세스 권한을 제공합니다.

Cloud KMS 역할	클라우드 KMS 관리자	Cloud KMS 리소스에 대한 전체 액세스를 제공합니다(암호화/복호화 작업 제외).
	클라우드 KMS 암호화/복호화	암호화/복호화 작업 전용으로 Cloud KMS 리소스를 사용할 수 있는 기능을 제공합니다.
	Cloud KMS 암호화	암호화 작업 전용으로 Cloud KMS 리소스를 사용할 수 있는 기능을 제공합니다.
	Cloud KMS 복호화	복호화 작업 전용으로 Cloud KMS 리소스를 사용할 수 있는 기능을 제공합니다.
Cloud Pub/Sub 역할	게시/구독 게시자	주제에 메시지를 게시하기 위한 액세스 권한을 제공합니다.
	게시/구독 구독자	구독에서 메시지를 사용하고 주제에 구독을 연결하기 위한 액세스 권한을 제공합니다.
	게시/구독 뷰어	주제와 구독을 보기 위한 액세스 권한을 제공합니다.
	게시/구독 편집자	주제 및 구독 항목을 수정하고, 메시지를 게시하고 사용하기 위한 액세스 권한을 제공합니다.
	게시/구독 관리자	주제 및 구독 항목에 대한 전체 액세스 권한을 제공합니다.
Cloud SQL 역할	Cloud SQL 관리자	Cloud SQL 리소스를 관리할 수 있는 전체 권한을 제공합니다.
	Cloud SQL 편집자	기존 Cloud SQL 인스턴스를 관리할 수 있는 전체 권한을 제공하지만 사용자 수정, SSL 인증서 수정, 리소스 삭제 권한은 제외됩니다.
	Cloud SQL 뷰어	Cloud SQL 리소스에 대한 읽기 전용 액세스 권한을 제공합니다.
	Cloud SQL 클라이언트	Cloud SQL 인스턴스에 대한 연결 액세스 권한을 제공합니다.
Cloud Storage 역할	저장소 객체 생성자	사용자에게 객체를 생성할 권한을 부여합니다. 객체를 삭제하거나 덮어쓰기할 권한은 부여하지 않습니다.
	저장소 객체 뷰어	객체 및 ACL 을 제외한 객체의 메타데이터를 보기 위한 액세스 권한을 부여합니다.
	저장소 객체 관리자	객체 전체 제어 권한을 부여합니다.
	저장소	객체와 버킷에 대한 전체 제어 권한을 부여합니다.

Compute Engine 역할	관리자	
	기존 객체 리더	ACL 을 제외한 객체 및 객체의 메타데이터를 볼 수 있습니다.
	기존 객체 소유자	storage.legacyObjectReader 역할이 있습니다. 또한 버킷의 메타데이터를 보고 편집할 수 있습니다. ACL 역시 포함되며, ACL 은 Cloud IAM 정책으로 반환됩니다.
	기존 버킷 리더	Cloud IAM 정책을 제외한 버킷의 콘텐츠를 나열하고 버킷 메타데이터를 읽을 수 있습니다. 또한 객체 메타데이터를 읽을 수 있으며, Cloud IAM 정책은 객체 나열 시 제외됩니다. 이 역할의 사용은 버킷의 ACL 에도 반영됩니다. 자세한 정보는 Cloud IAM 과 ACL 의 관련성에서 확인하세요
	기존 버킷 작성자	storage.legacyBucketReader 역할이 있습니다. 버킷에서 객체를 생성, 덮어쓰기, 삭제할 수 있습니다. 이 역할의 사용은 버킷의 ACL 에도 반영됩니다. 자세한 정보는 Cloud IAM 과 ACL 의 관련성에서 확인하세요.
	기존 버킷 소유자	storage.legacyBucketWriter 역할이 있습니다. 또한 버킷 Cloud IAM 정책을 읽고 Cloud IAM 정책을 포함한 버킷 메타데이터를 편집할 수 있습니다. 이 역할의 사용은 버킷의 ACL 에도 반영됩니다. 자세한 정보는 Cloud IAM 과 ACL 의 관련성에서 확인하세요.
	Compute 인스턴스 관리자	가상 머신 인스턴스를 생성, 수정, 삭제할 권한이 부여됩니다. 여기에는 디스크를 생성, 수정, 삭제할 권한이 포함됩니다. 사용자가 서비스 계정으로서 실행하도록 구성된 가상 머신 인스턴스를 관리하는 경우에는 roles/iam.serviceAccountUser 역할도 부여해야 합니다. 예를 들어, 가상 머신 인스턴스 그룹을 관리하지만 네트워크 또는 보안 설정은 관리하지 않으며 서비스 계정으로서 실행되는 인스턴스를 관리하지 않는 사람이 회사에 있는 경우 이 역할을 부여하면 됩니다.
	Compute 네트워크 사용자	공유 VPC 네트워크에 대한 액세스 권한을 제공합니다. 허용되면 서비스 소유자는 호스트 프로젝트에 속한 VPC 네트워크와 서브넷을 사용할 수 있습니다. 예를 들어, 네트워크 사용자는 호스트 프로젝트 네트워크에 속하는 VM 인스턴스를 생성할 수 있지만 호스트 프로젝트에서 새로운 네트워크를 삭제 또는 생성할 수 없습니다.
	Compute 네트워크 뷰어	모든 네트워킹 리소스에 대한 읽기 전용 액세스 권한입니다. 예를 들어, 네트워크 구성을 검사하는 소프트웨어가 있는 경우, 해당 소프트웨어의 서비스 계정에 networkViewer 역할을 부여할 수 있습니다.

Compute 네트워크 관리자	방화벽 규칙과 SSL 인증서를 제외한 네트워킹 리소스를 생성, 수정, 삭제할 권한이 부여됩니다. 네트워크 관리자 역할에는 방화벽 규칙, SSL 인증서, 인스턴스에 대한 읽기 전용 액세스가 허용됩니다 (임시 IP 주소를 보기 위한 목적). 네트워크 관리자 역할에는 인스턴스를 생성, 시작, 중지 또는 삭제할 권한이 없습니다. 예를 들어, 방화벽과 SSL 인증서를 관리하는 보안 팀과 나머지 네트워킹 리소스를 관리하는 네트워킹팀이 회사에 있는 경우, 네트워킹팀의 그룹에 networkAdmin 역할을 부여하면 됩니다.
Compute 보안 관리자	방화벽 규칙과 SSL 인증서를 생성, 수정, 삭제할 권한이 있습니다. 예를 들어, 방화벽과 SSL 인증서를 관리하는 보안 팀과 나머지 네트워킹 리소스를 관리하는 네트워킹팀이 회사에 있는 경우, 보안 팀의 그룹에 securityAdmin 역할을 부여하면 됩니다.
컴퓨팅 이미지 사용자	프로젝트의 리소스에 대한 다른 권한 없이 이미지를 나열하고 읽을 수 있는 권한입니다. compute.imageUser 역할을 부여하면 사용자는 프로젝트의 모든 이미지를 나열할 수 있게 되고 프로젝트의 이미지를 기반으로 인스턴스 및 영구 디스크 등의 리소스를 생성할 수 있게 됩니다.
Compute Storage 관리자	디스크, 이미지, 스냅샷을 생성, 수정, 삭제할 권한이 있습니다. 예를 들어, 회사에 이미지 관리 담당자가 있지만 이들에게 프로젝트에 대한 편집자 역할은 주고 싶지 않은 경우, 이들의 계정에 storageAdmin 역할을 부여하면 됩니다.
공유 VPC 관리자	공유 VPC 호스트 프로젝트를 관리할 권한이 있습니다. 구체적으로 프로젝트를 호스팅하고 공유 VPC 서비스 프로젝트를 호스트 프로젝트 네트워크에 연결할 수 있는 권한입니다. 조직 관리자만이 이 역할을 조직에 부여할 수 있습니다.
Compute 관리자	모든 Compute Engine 리소스를 관리할 수 있는 전체 권한입니다. 사용자가 서비스 계정으로서 실행하도록 구성된 가상 머신 인스턴스를 관리하는 경우에는 roles/iam.serviceAccountUser 역할도 부여해야 합니다.
Compute 뷰어	Compute Engine 리소스를 가져와 나열할 수 있지만 리소스에 저장된 데이터를 읽을 수는 없는 읽기 전용 액세스 권한입니다. 예를 들어, 이 역할을 부여 받은 계정은 모든 디스크를 프로젝트에 목록화할 수 있지만 해당 디스크의 데이터는 전혀

		읽을 수 없습니다.
Deployment Manager 역할	배포 관리자 뷰어	배포 관리자 관련 리소스에 대한 읽기 전용 액세스 권한을 제공합니다.
	배포 관리자 편집자	배포를 생성 및 관리하는 데 필수적인 권한을 제공합니다.
	배포 관리자 유형 뷰어	모든 유형 레지스트리 리소스에 대한 읽기 전용 액세스 권한을 제공합니다.
	배포 관리자 유형 편집자	모든 유형 레지스트리 리소스에 대한 읽기 및 쓰기 액세스 권한을 제공합니다.
Cloud IAM 역할	조직 역할 관리자	조직 및 조직에 속한 프로젝트의 모든 커스텀 역할을 관리할 수 있는 액세스 권한을 제공합니다.
	역할 관리자	프로젝트의 모든 커스텀 역할에 대한 읽기 액세스 권한을 제공합니다.
	조직 역할 뷰어	조직 및 조직에 속한 프로젝트의 모든 커스텀 역할에 대한 읽기 액세스 권한을 제공합니다.
	역할 뷰어	프로젝트의 모든 커스텀 역할에 대한 읽기 액세스 권한을 제공합니다.
	보안 검토자	모든 리소스와 해당 리소스에 대한 Cloud IAM 정책을 나열할 수 있는 권한을 제공합니다.
Cloud IAP 역할	IAP 보안 웹 앱 사용자	IAP(Identity-Aware Proxy)를 사용하는 HTTPS 리소스에 대한 액세스 권한을 제공합니다.
Resource Manager 역할	조직 정책 관리자	조직 정책을 설정함으로써 조직에서 클라우드 리소스의 구성에 적용하려는 제한사항을 정의할 수 있는 액세스 권한을 제공합니다.
	폴더 관리자	폴더와 관련된 작업을 위해 사용 가능한 모든 권한을 제공합니다.
	폴더 생성자	계층구조를 찾아보고 폴더를 생성하는 데 필요한 권한을 제공합니다.
	폴더 편집자	폴더 수정 권한과 폴더의 Cloud IAM 정책을 볼 수 있는 권한을 제공합니다.
	폴더 IAM	폴더에 대한 Cloud IAM 정책을 관리할 수 있는 권한을

	관리자	제공합니다.
	폴더 이동자	프로젝트와 폴더를 상위 조직 또는 폴더 안팎으로 이동시킬 수 있는 권한을 제공합니다.
	폴더 뷰어	리소스에 속한 폴더와 프로젝트를 가져와 나열할 수 있는 권한을 제공합니다.
	조직 뷰어	조직을 볼 수 있는 액세스 권한을 제공합니다.
	프로젝트 생성자	새로운 프로젝트를 생성할 수 있는 액세스 권한을 제공합니다. 사용자가 프로젝트를 생성하면 해당 사용자에게 해당 프로젝트의 소유자 역할이 자동으로 부여됩니다.
	프로젝트 삭제자	GCP 프로젝트를 삭제할 수 있는 액세스 권한을 제공합니다.
	프로젝트 IAM 관리자	프로젝트에 대한 Cloud IAM 정책을 관리할 수 있는 권한을 제공합니다.
	프로젝트 선취권 수정자	프로젝트의 선취권을 수정할 수 있는 액세스 권한을 제공합니다.
	프로젝트 이동자	프로젝트를 업데이트하고 이동시킬 수 있는 액세스 권한을 제공합니다.
서비스 계정 역할	서비스 계정 관리자	서비스 계정을 만들고 관리합니다.
	서비스 계정 키 관리자	서비스 계정 키를 만들고, 관리하고, 순환할 수 있습니다.
	서비스 계정 토큰 생성자	OAuth2 액세스 토큰, 서명 blob, JWT 생성 등과 같이 서비스 계정을 가장하는 작업을 합니다.
	서비스 계정 사용자	서비스 계정으로서 작업을 실행합니다.
서비스 관리 역할	서비스 컨트롤러	서비스 사용량을 확인 및 보고하는 런타임의 관리 권한입니다.
	할당량 관리자	서비스 할당량을 관리할 수 있는 액세스 권한을 제공합니다.
	할당량 뷰어	서비스 할당량을 볼 수 있는 액세스 권한을 제공합니다.
소스 저장소 역할	소스 저장소 관리자	저장소를 생성, 업데이트, 삭제, 나열, 수정, 복제, 가져오기, 찾아 보기할 권한을 제공합니다. 또한 IAM 정책을 읽고 변경할 권한도 제공합니다.

	소스 저장소 리더	저장소를 나열, 복제, 가져오기, 찾아 보기할 권한을 제공합니다.
	소스 저장소 작성자	저장소를 나열, 복제, 가져오기, 찾아보기, 업데이트할 권한을 제공합니다.
Stackdriver Debugger 역할	Debugger 에이전트	디버그 대상을 등록하고 활성 중단점을 읽고 중단점 결과를 보고할 수 있는 권한을 제공합니다.
	Debugger 사용자	중단점(스냅샷 및 로그 지점)을 생성, 조회, 나열, 삭제할 권한과 디버그 대상(debuggees)을 나열할 권한을 제공합니다.
Stackdriver Error Reporting 역할	오류 보고 뷰어	오류 보고 데이터에 대한 읽기 전용 액세스를 제공합니다.
	오류 보고 사용자	오류 보고 데이터 읽기/쓰기 권한(새로운 오류 이벤트 전송하는 경우 제외)을 제공합니다.
	Error Reporting 작성자	오류 보고에 오류 이벤트를 전송할 권한을 제공합니다.
	Error Reporting 관리자	오류 보고 데이터에 전체 액세스를 제공합니다.
Stackdriver Logging 역할	로그 뷰어	로그를 볼 수 있는 액세스 권한을 제공합니다.
	로그 작성자	로그 항목을 쓸 수 있는 권한을 제공합니다.
	비공개 로그 뷰어	로그 뷰어 역할에 대한 권한을 제공하고 추가로 비공개 로그에서 로그 항목에 대한 읽기 전용 액세스 권한을 제공합니다.
	로그 구성 작성자	로그 기반 측정항목 구성과 로그 내보내기에 대한 싱크를 읽기/쓰기 할 권한을 제공합니다.
	로깅 관리자	Stackdriver Logging 의 모든 기능을 사용하는 데 필수적인 모든 권한을 제공합니다.
Stackdriver Monitoring 역할	모니터링 뷰어	모든 모니터링 데이터 및 구성에 관한 정보를 가져와 나열할 수 있는 읽기 전용 액세스 권한을 제공합니다.
	모니터링 측정항목 작성자	측정항목에 대한 쓰기 전용 액세스 권한을 제공합니다. 측정항목을 전송하는 Stackdriver 에이전트와 기타 시스템에 필요한 권한을 정확히 제공합니다.
	모니터링 편집자	데이터 모니터링과 구성에 관한 모든 정보에 대한 전체 액세스 권한을 제공합니다.
	모니터링 관리자	roles/monitoring.editor 와 동일한 액세스 권한을 제공합니다.

Stackdriver Trace 역할	Cloud 추적 에이전트	서비스 계정용입니다. Stackdriver Trace 에 데이터를 전송함으로써 추적을 쓸 수 있는 기능을 제공합니다.
	Cloud 추적 사용자	Trace 콘솔에 대한 전체 액세스 권한과 추적에 대한 읽기 액세스 권한을 제공합니다.
	Cloud Trace 관리자	Trace 콘솔에 대한 전체 액세스 권한과 추적에 대한 쓰기 액세스 권한을 제공합니다.
Cloud Source Repositories 역할	소스 저장소 리더	저장소 (Repo) 내 나열, 클론, 가져오기, 찾아오기 기능을 제공합니다.
	소스 저장소 작성자	소스 저장소 리더 권한에서 저장소 업데이트 기능을 추가 제공합니다.
	소스 저장소 관리자	저장소 (Repo) 내 모든 기능 사용이 가능합니다.
FileStore 역할	Filestore 뷰어	Filestore 인스턴스 조회 및 작업 상태, 나열이 가능합니다.
	Filestore 편집자	Filestore 인스턴스 생성/삭제/조회를 포함한 Filestore 내 모든 리소스를 사용 가능합니다.
MemoryStore 역할	Redis 뷰어	모든 Memorystore for Redis 리소스에 대한 읽기 전용 액세스 권한
	Redis 편집자	Memorystore for Redis 인스턴스 관리 인스턴스를 만들거나 삭제할 수 없습니다.
	Redis 관리자	모든 Memorystore for Redis 리소스에 대한 전체 제어 권한

※ IAM 역할별 권한 관리 (예시)

역할	IAM 관리형 정책명
Console 관리자	Owner(소유자)
Infra 관리자	editor(편집자), dns.admin(DNS 관리자), cloudkms.admin(클라우드 KMS 관리자), compute.instanceAdmin(beta)(Compute 인스턴스 관리자), compute.networkAdmin(Compute 네트워크 관리자), compute.storageAdmin(beta)(Compute Storage 관리자)
Infra 운영 및 담당자	viewer(뷰어), dns.reader(DNS 리더), compute.networkUser(Compute 네트워크 사용자), compute.networkViewer(Compute 네트워크 뷰어), compute.imageUser(컴퓨팅 이미지 사용자)
Application 관리자	appengine.appAdmin(App Engine 관리자),

	dialogflow.admin(Dialogflow API 관리자)
Application 운영 및 담당자	appengine.serviceAdmin(App Engine 서비스 관리자), appengine.deployer(App Engine 배포자), appengine.appViewer(App Engine 뷰어), appengine.codeViewer(App Engine 코드 뷰어), dialogflow.client(Dialogflow API 클라이언트), dialogflow.reader(Dialogflow API 리더)
개발 관리자	bigquery.admin(BigQuery 관리자), bigquery.dataOwner(BigQuery 데이터 소유자), bigtable.admin(Cloud Bigtable 관리자), bigtable.admin(Cloud Bigtable 관리자), dataflow.developer(Cloud Dataflow 개발자), cloudsql.admin(Cloud SQL 관리자)
개발 운영 및 담당자	bigquery.dataEditor(BigQuery 데이터 편집자), bigquery.dataViewer(BigQuery 데이터 뷰어), bigquery.jobUser(BigQuery 작업 사용자), bigquery.user(BigQuery 사용자), bigtable.user(Cloud Bigtable 사용자), bigtable.reader(Cloud Bigtable 리더), dataflow.worker(Cloud Dataflow 작업자), cloudsql.editor(Cloud SQL 편집자), cloudsql.viewer(Cloud SQL 뷰어)
데이터 관리자	datastore.owner(Cloud Datastore 소유자), datastore.indexAdmin(Cloud Datastore 색인 관리자), datastore.importExportAdmin(Cloud Datastore 가져오기 내보내기 관리자), storage.admin(저장소 관리자), storage.objectAdmin(저장소 객체 관리자), storage.legacyObjectOwner(기존 객체 소유자), storage.legacyBucketOwner(기존 버킷 소유자), compute.storageAdmin(beta)(Compute Storage 관리자), source.admin(소스 저장소 관리자)
데이터 운영 및 담당자	datastore.user(Cloud Datastore 사용자), datastore.viewer(Cloud Datastore 뷰어), storage.objectViewer(저장소 객체 뷰어), storage.objectCreator(저장소 객체 생성자), storage.legacyBucketWriter(기존 버킷 작성자), storage.legacyBucketReader(기존 버킷 리더), source.writer(소스 저장소 작성자)
보안 관리자	pubsub.admin(게시/구독 관리자), pubsub.editor(게시/구독 편집자), compute.securityAdmin(Compute 보안 관리자), iam.organizationRoleAdmin(조직 역할 관리자), iam.roleAdmin(역할 관리자), iam.securityReviewer(보안 검토자), orgpolicy.policyAdmin(조직 정책 관리자), resourcemanager.folderAdmin(폴더 관리자),

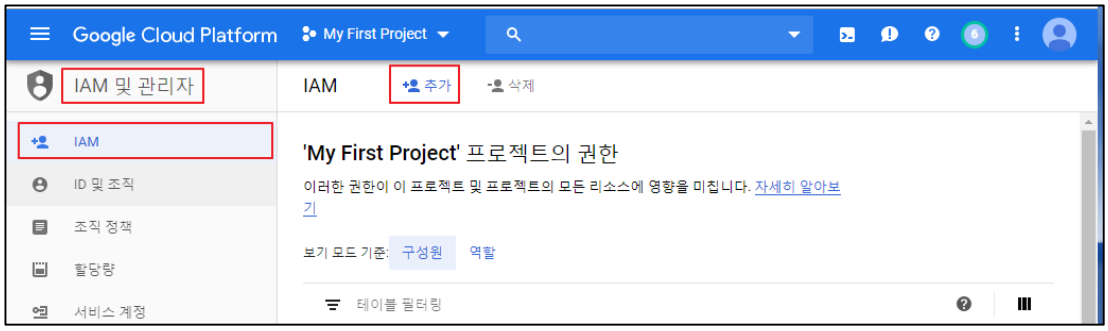
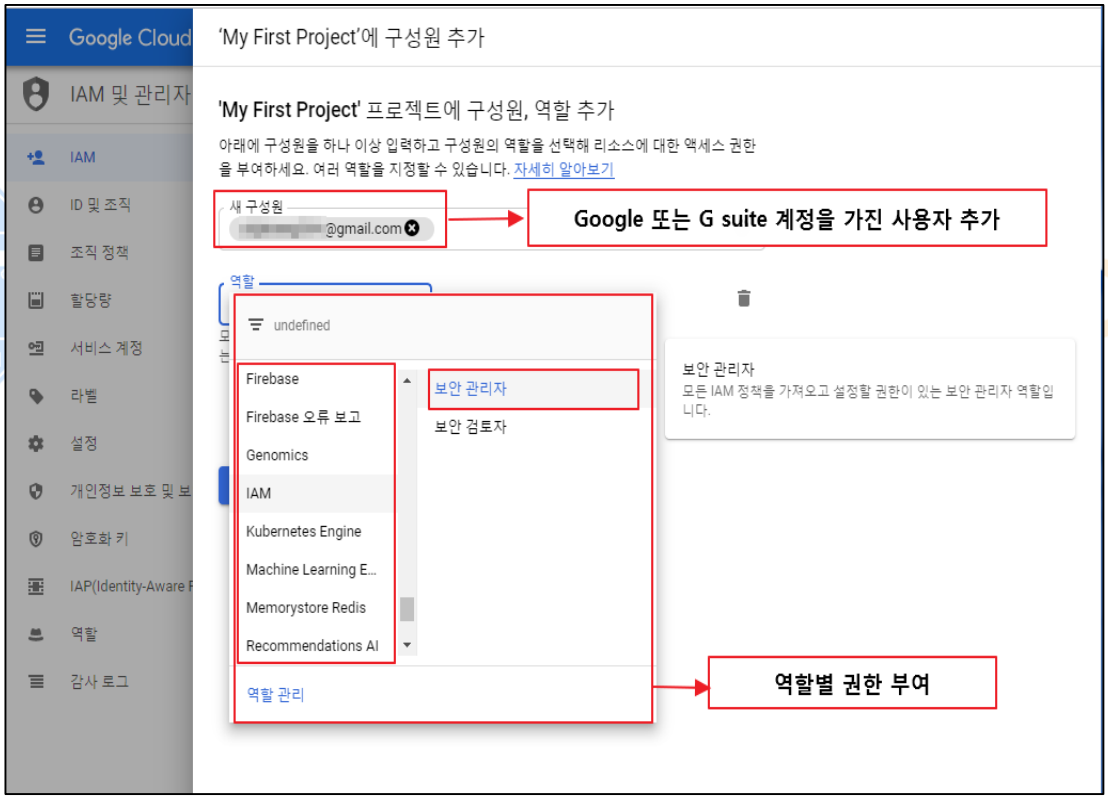
	resourcemanager.folderIamAdmin(폴더 IAM 관리자), resourcemanager.projectIamAdmin(프로젝트 IAM 관리자), iam.serviceAccountAdmin(서비스 계정 관리자), iam.serviceAccountKeyAdmin(서비스 계정 키 관리자), servicemanagement.serviceController(서비스 컨트롤러), servicemanagement.quotaAdmin(할당량 관리자)
보안 운영 및 담당자	pubsub.publisher(게시/구독 게시자), pubsub.viewer(게시/구독 뷰어), iam.organizationRoleViewer(조직 역할 뷰어), iam.roleViewer(역할 뷰어), resourcemanager.folderEditor(폴더 편집자), resourcemanager.folderCreator(폴더 생성자), resourcemanager.projectCreator(프로젝트 생성자), iam.serviceAccountTokenCreator(서비스 계정 토큰 생성자), servicemanagement.quotaViewer(할당량 뷰어)
로깅 관리자	logging.admin(로깅 관리자), monitoring.admin(모니터링 관리자)
로깅 운영 및 담당자	logging.configWriter(로그 구성 작성자), logging.logWriter(로그 작성자), monitoring.metricWriter(모니터링 측정항목 작성자), monitoring.editor(모니터링 편집자)
재무/비용 관리자	billing.admin(결제 계정 관리자), billing.projectManager(프로젝트 결제 관리자)

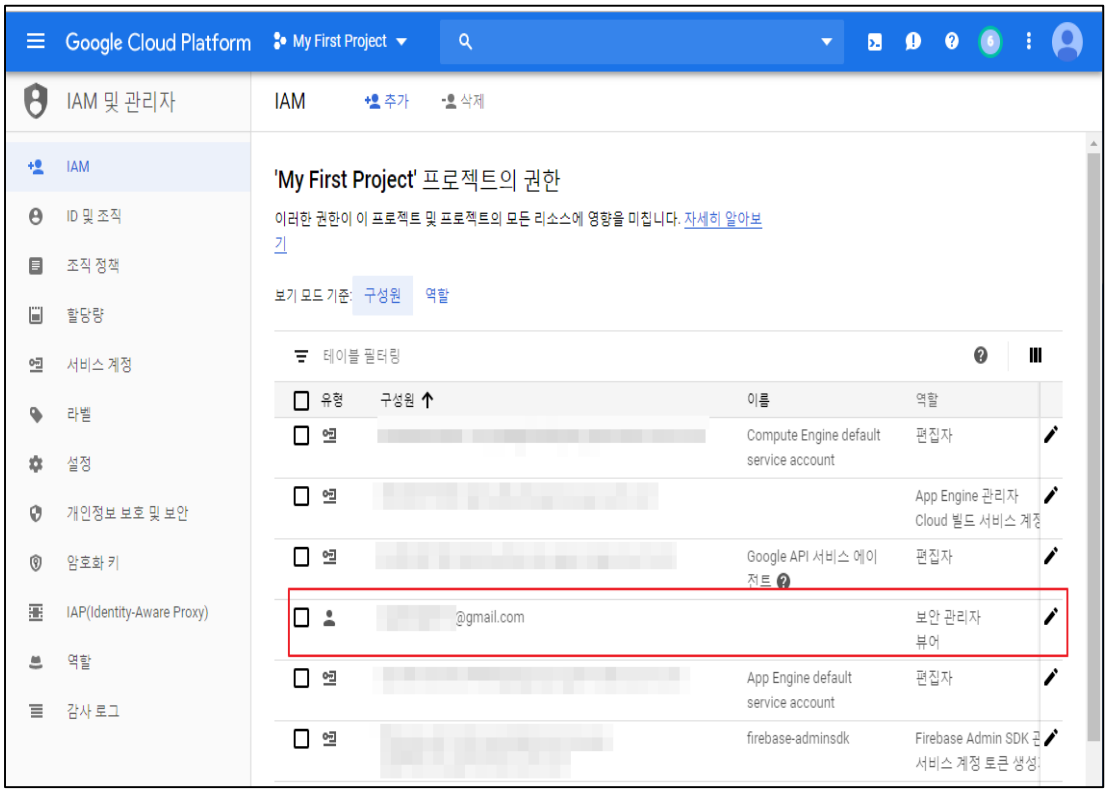
※ IAM 관리형 정책 권한 관리 List (예시)

역할	계정 관리 (그룹 및 계정명)	관리형 정책	취약 유/무
Console 관리자	Ex) Owner(소유자)	Ex) Owner(소유자)	N/A
Infra 관리자/운영 및 담당자			N/A
Application 관리자/ 운영 및 담당자			N/A
개발 관리자/ 운영 및 담당자			N/A
재무 / 비용 관리자 및 담당자			N/A

※ Google Cloud IAM 역할 설정 및 부여 시 소유자 등의 권한과 같이 중요도가 높은 권한은 관련 담당자에게만 할당이 되도록 해야하며 최소한의 계정 수가 유지되어야 합니다.

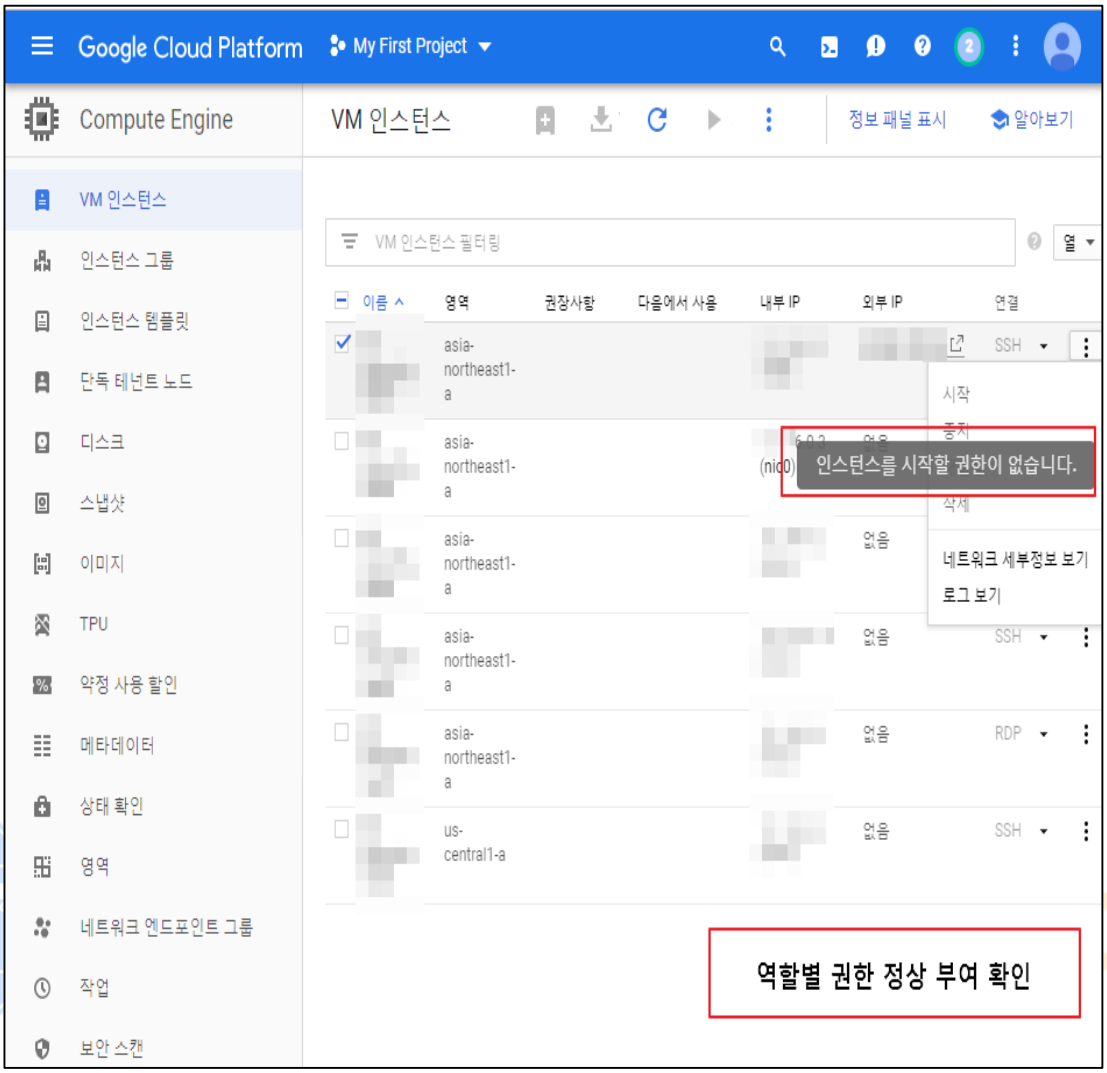
※ 서비스 담당자에 대한 Google Cloud IAM 권한 부여 시 최소한의 권한을 부여하시기 바라며, 주기적인 계정 관리를 통해 미사용 및 만료 계정에 대한 삭제 조치가 필요합니다.

	※ Google Cloud에서 제공되는 역할별 정책이 아닌 고객 커스텀 정책을 통한 IAM 권한 관리가 이루어질 경우 고객 커스텀 정책 내 권한에 대해서는 별도 담당자 확인이 필요합니다.
설정 방법	**가. Google Cloud 에서 사전 정의된 역할로의 IAM 사용자 계정 생성** 1) [IAM 및 관리자] > [IAM] > [추가]  2) 권한을 부여하고자 하는 사용자 추가 (Google 또는 G Suite 계정) 및 역할별 권한 부여  3) 사용자 추가 확인



4) 권한을 부여한 사용자로 Google Cloud Console 로그인 시도

5) 권한 정상 부여 확인

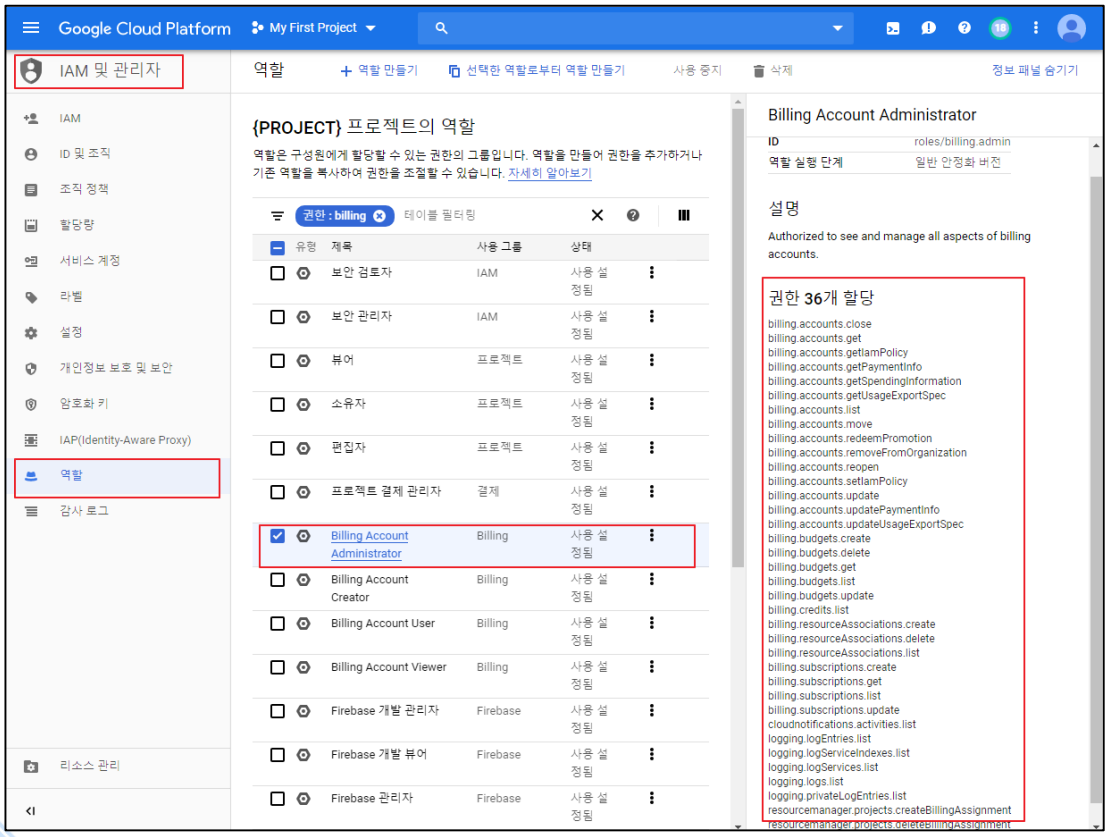


예제 1. 계정 사용 권한이 서비스 역할에 맞게 정의되어 있을 경우

- 사내 Google Cloud 이용 요금에 대한 원할한 비용 처리를 위해 최고 관리자(소유자) 외의 별도 '비용 및 재무 관리자' 역할의 담당자를 두고 있을 경우

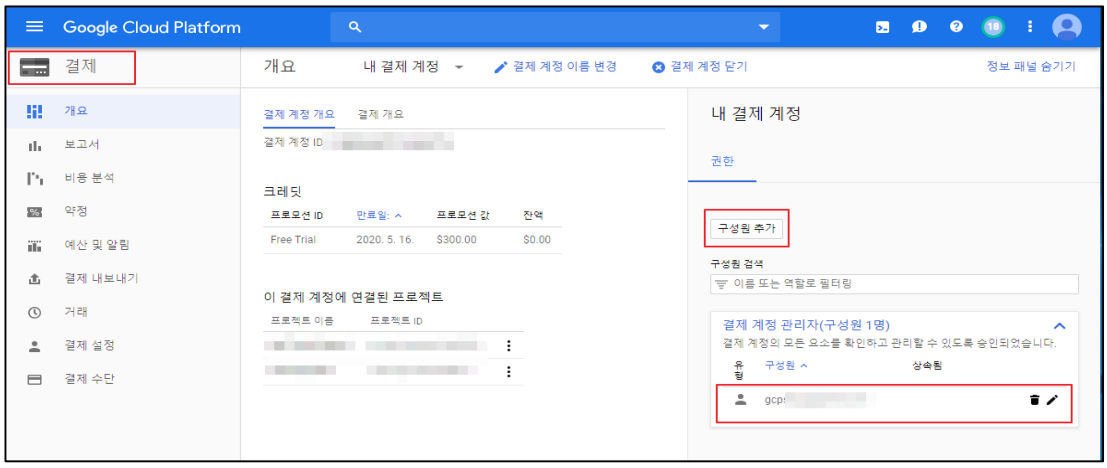
1) [IAM 및 관리자] > [역할]

- '비용 및 재무 관리자' 에게 필요한 역할 및 권한 확인

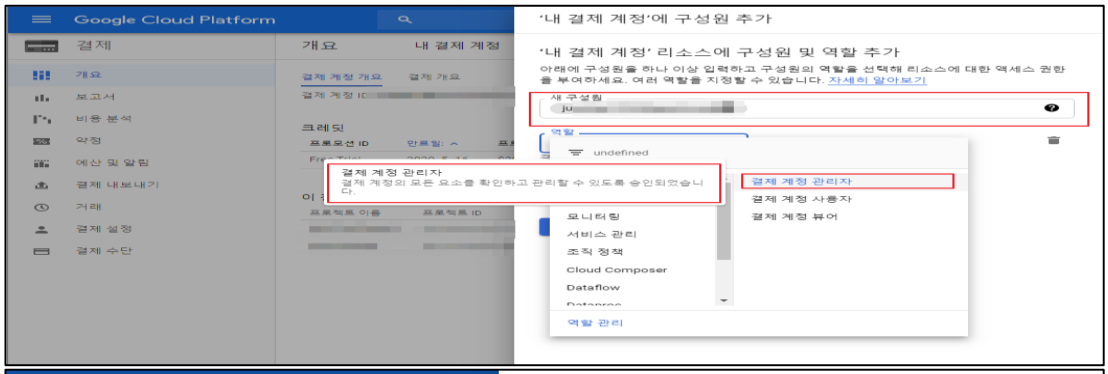


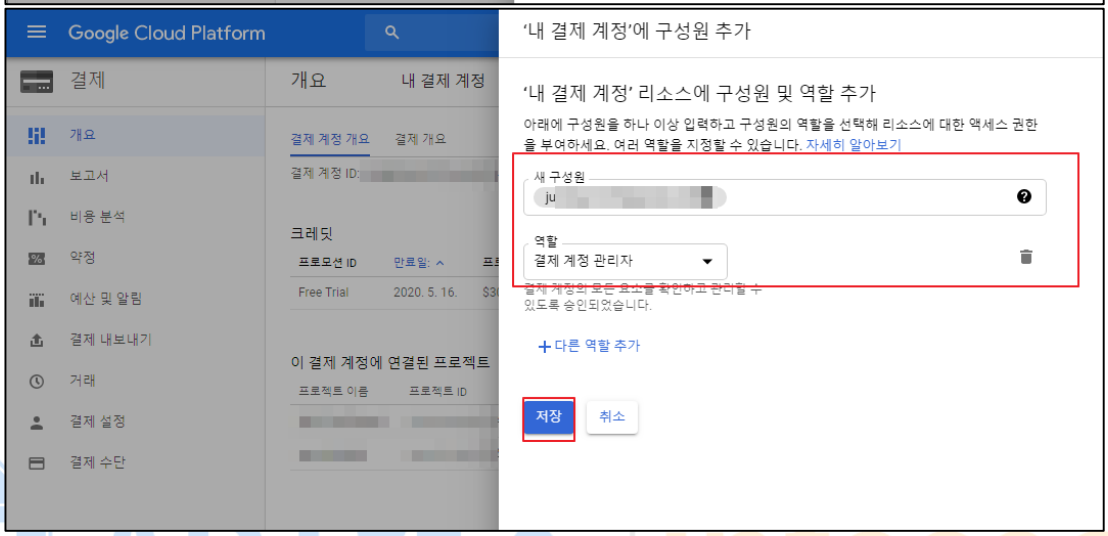
2) [결제] > [구성원 추가]

- '비용 및 재무 관리자' 역할 부여를 위한 사용자 추가
- 그림 내 '결제 계정 관리자'의 경우 최고 관리자에 한해서만 권한이 부여되어 있음

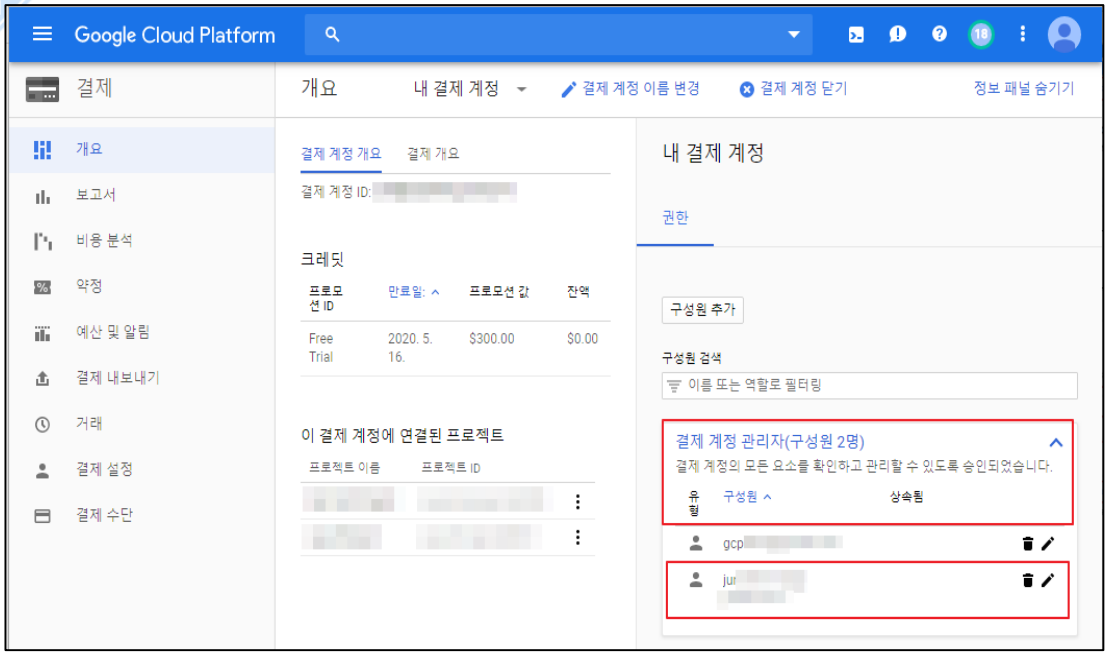


3) '비용 및 재무 관리자' 지정을 위한 역할(결제 계정 관리자) 설정



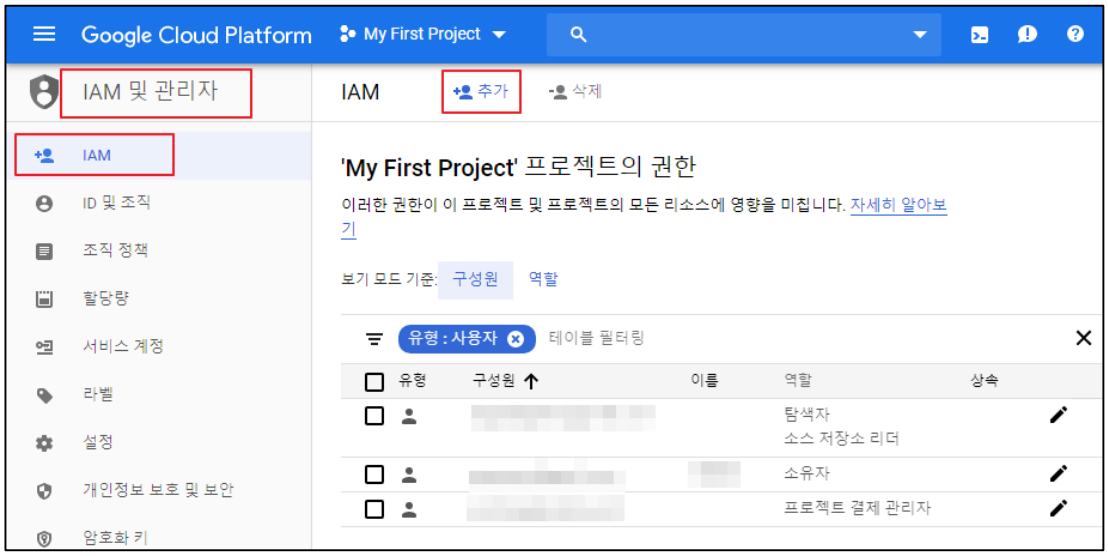


4) '비용 및 재무 관리자' 지정을 위한 역할(결제 계정 관리자) 설정 완료

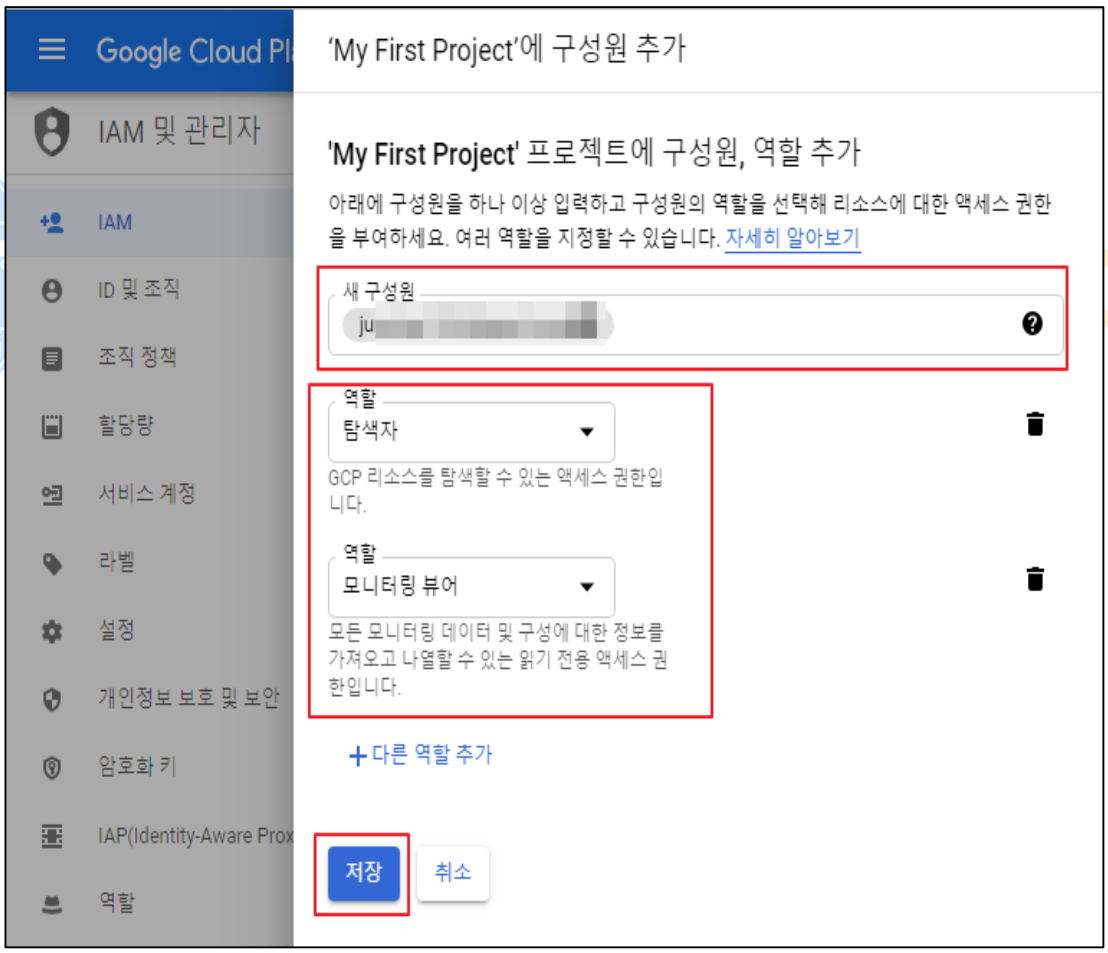


5) [IAM 및 관리자] > [IAM] > [추가]

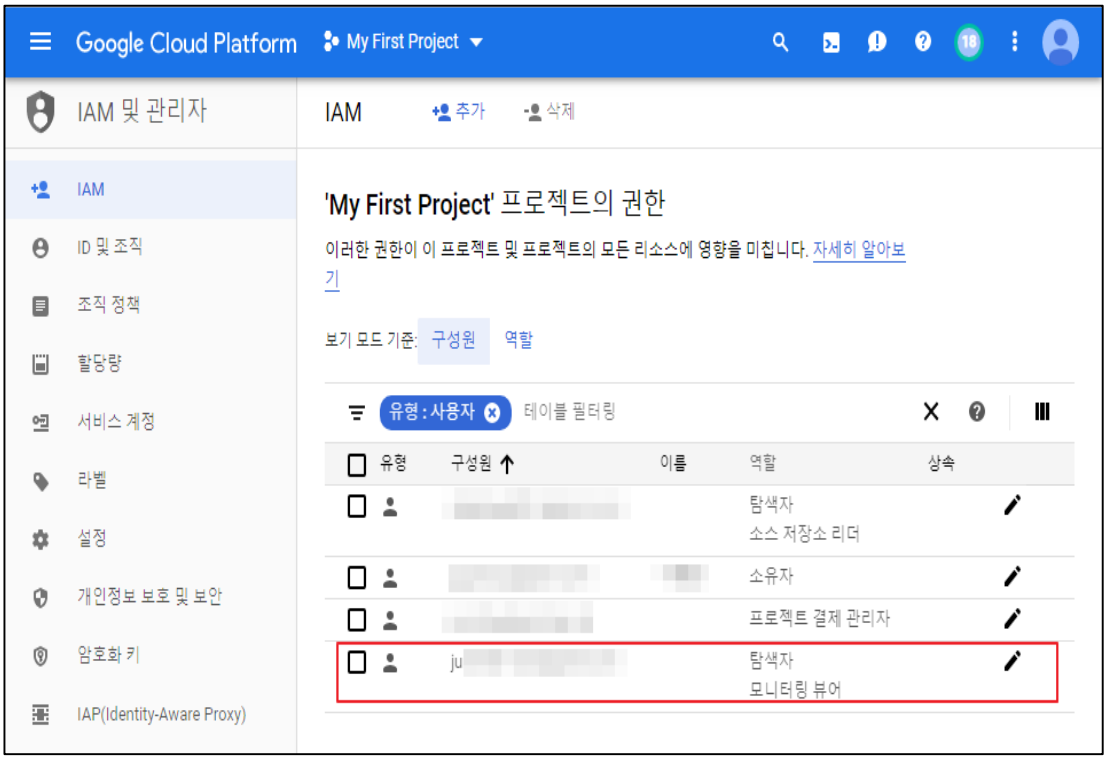
- '결제 계정 관리자' 권한 외 '비용 및 재무 관리자'에게 필요한 추가 역할 부여



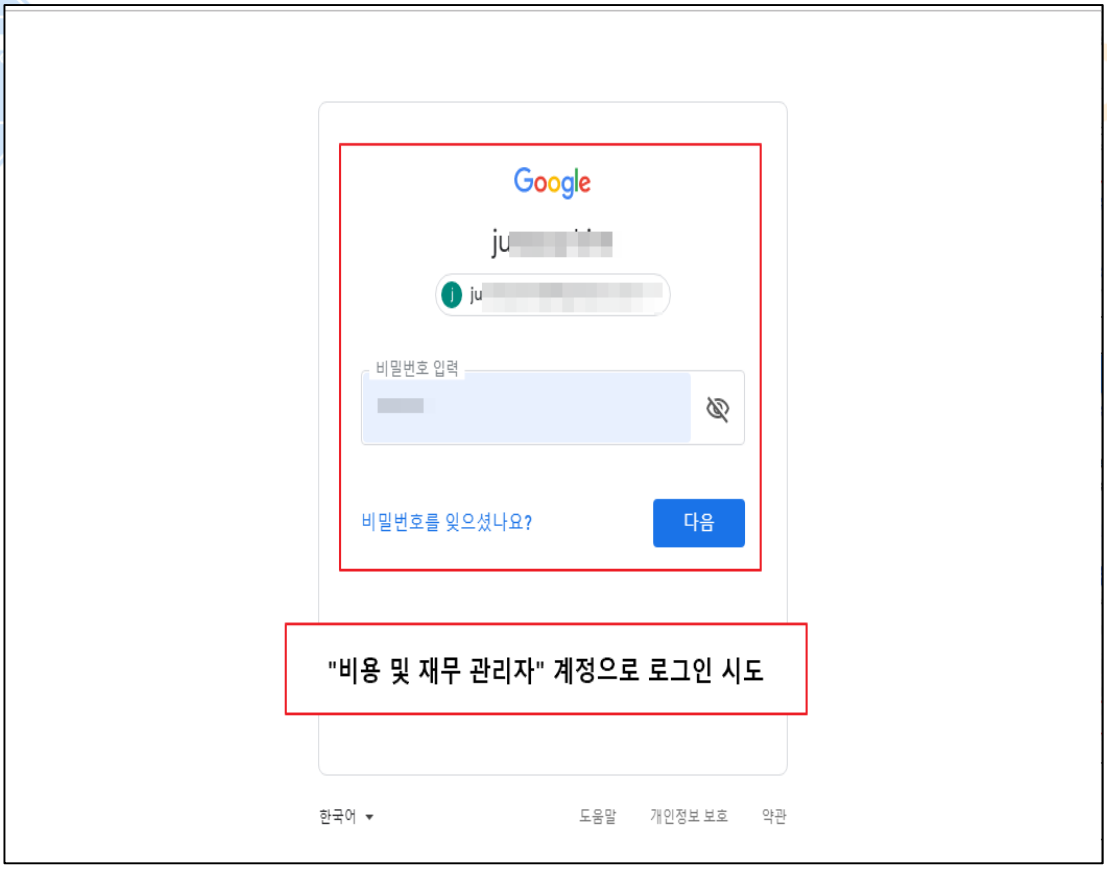
6) '비용 및 재무 관리자'에게 '프로젝트 탐색자' 및 '모니터링 뷰어' 역할 권한 할당



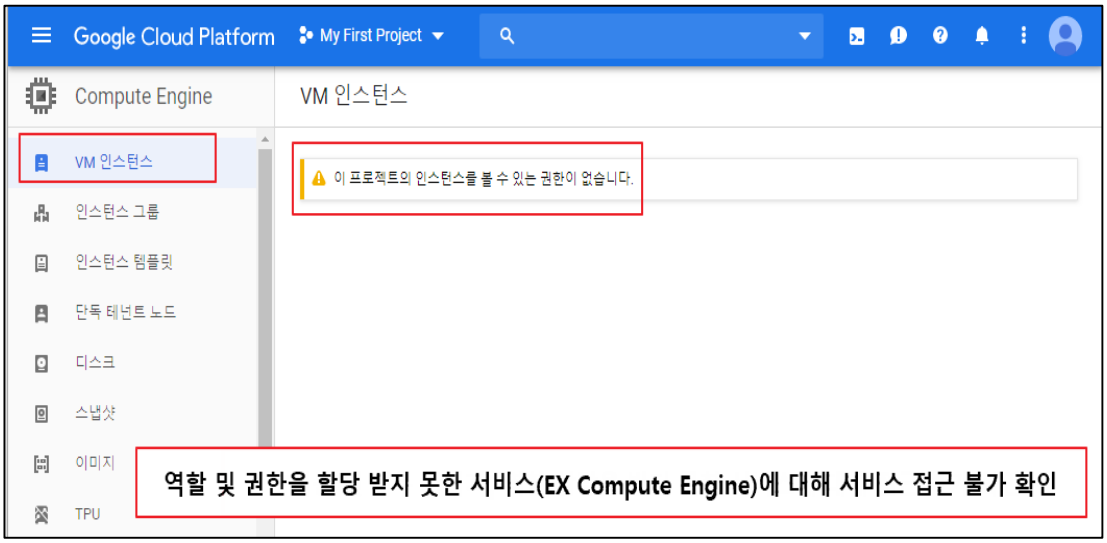
7) 추가로 설정한 '비용 및 재무 관리자'의 역할 확인



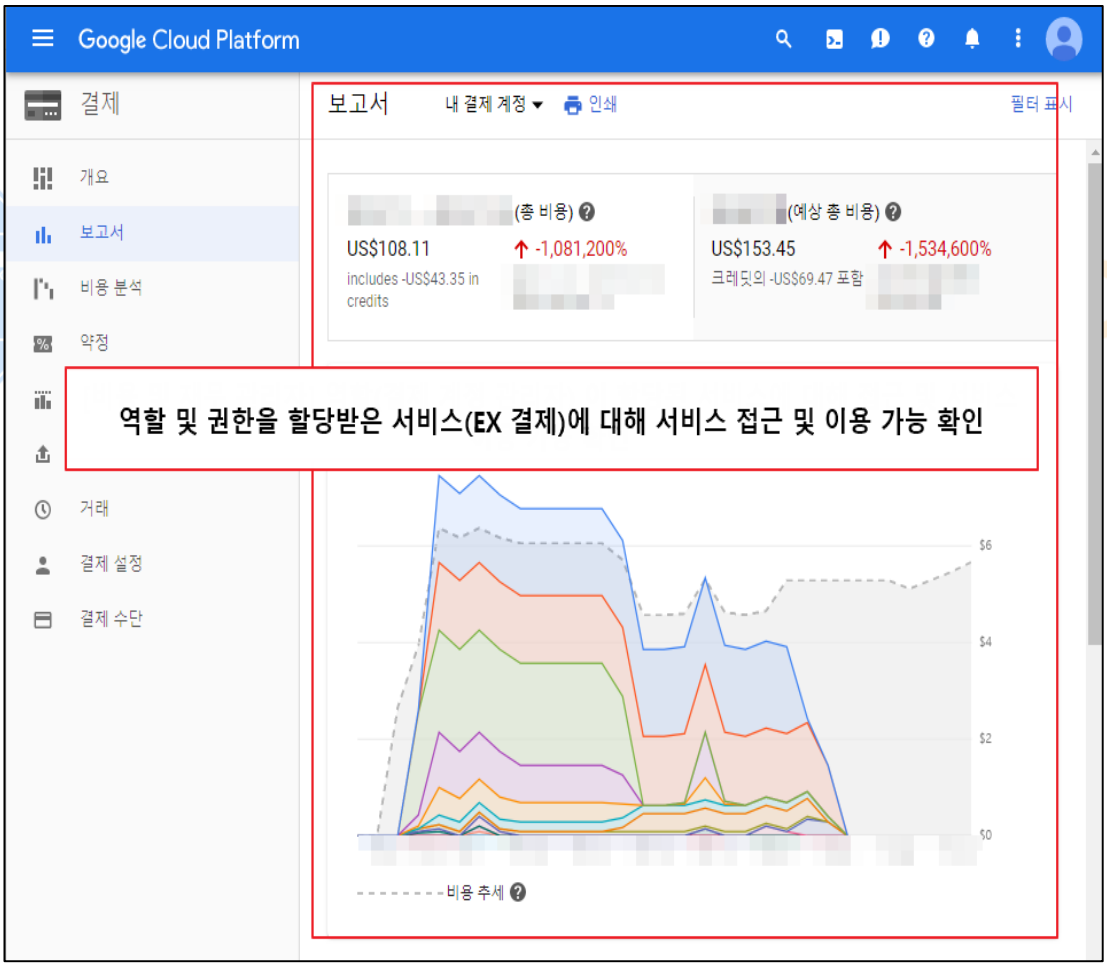
8) 역할 할당 후 '비용 및 재무 관리자' 계정으로 로그인 시도



9) 역할 및 권한을 할당 받지 못한 서비스(Compute Engine)에 대해 접근 불가 확인



10) 역할 및 권한을 할당 받은 서비스에 대해 서비스 접근 및 이용 가능 확인

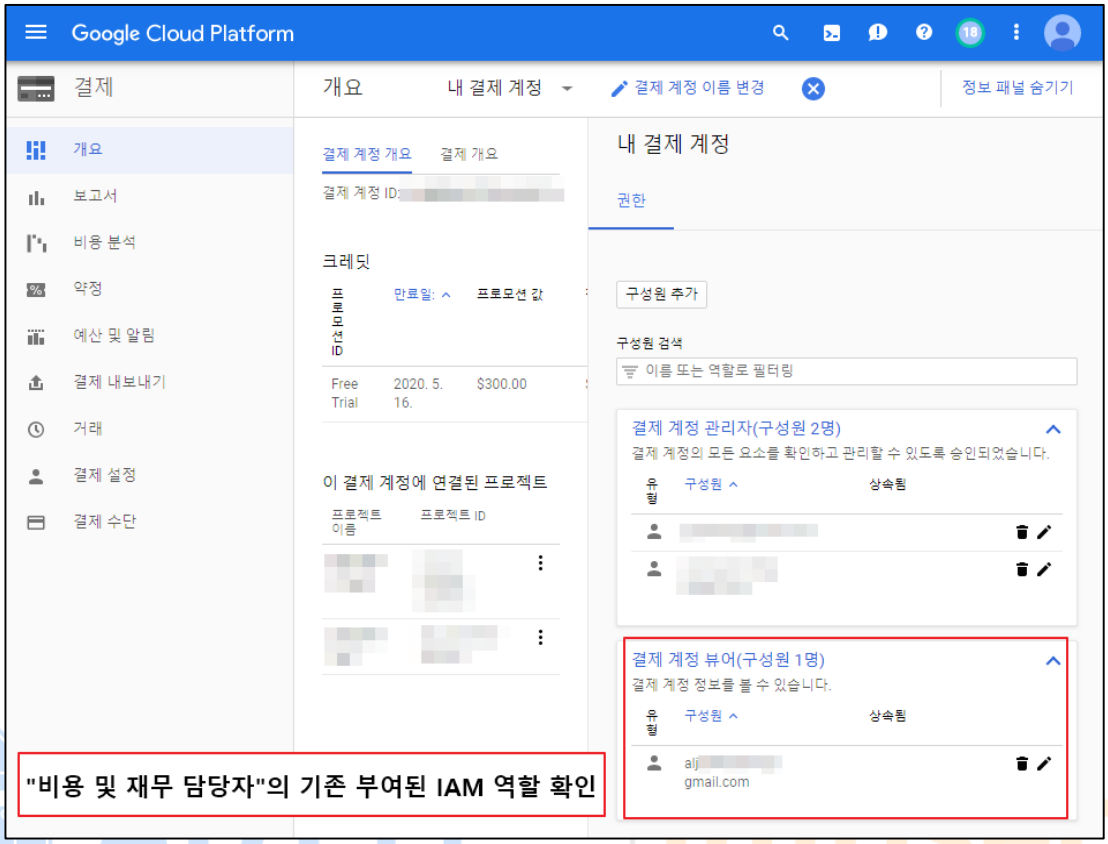


예제 2. 계정 사용 권한이 서비스 역할에 맞게 정의되어 있지 않을 경우

- '재무 및 비용 담당자'가 프로젝트 내 역할에 맞지 않는 서비스 (Compute Engine Resource)를 이용하는 경우

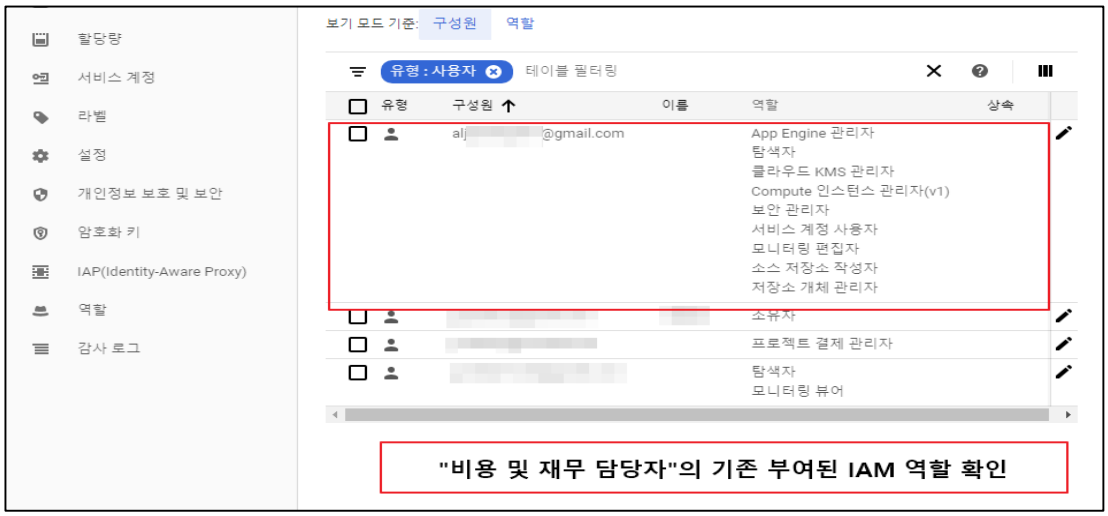
1) [결제] > [결제 계정 선택]

- '비용 및 재무 담당자' 계정 및 사용자 역할 권한 확인



2) [IAM 및 관리자] > [IAM]

- '비용 및 재무 담당자'의 기존에 부여된 IAM 역할 확인

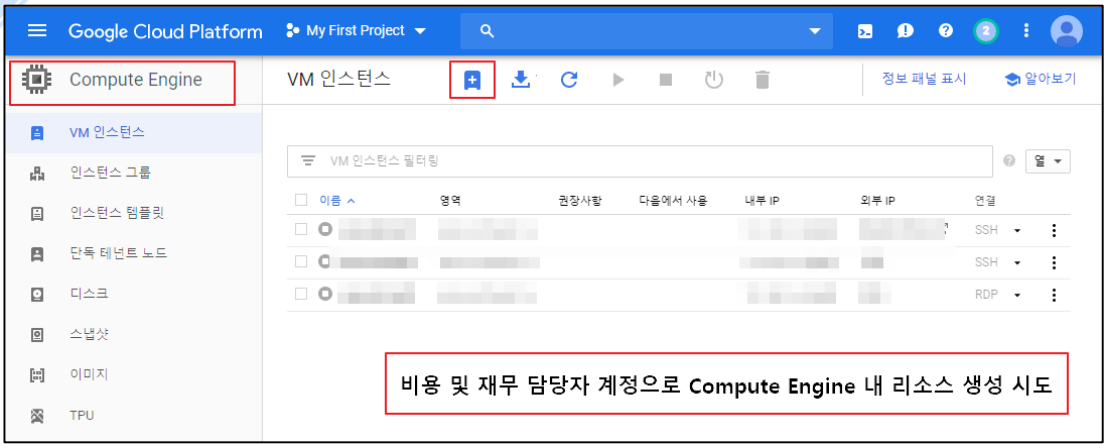


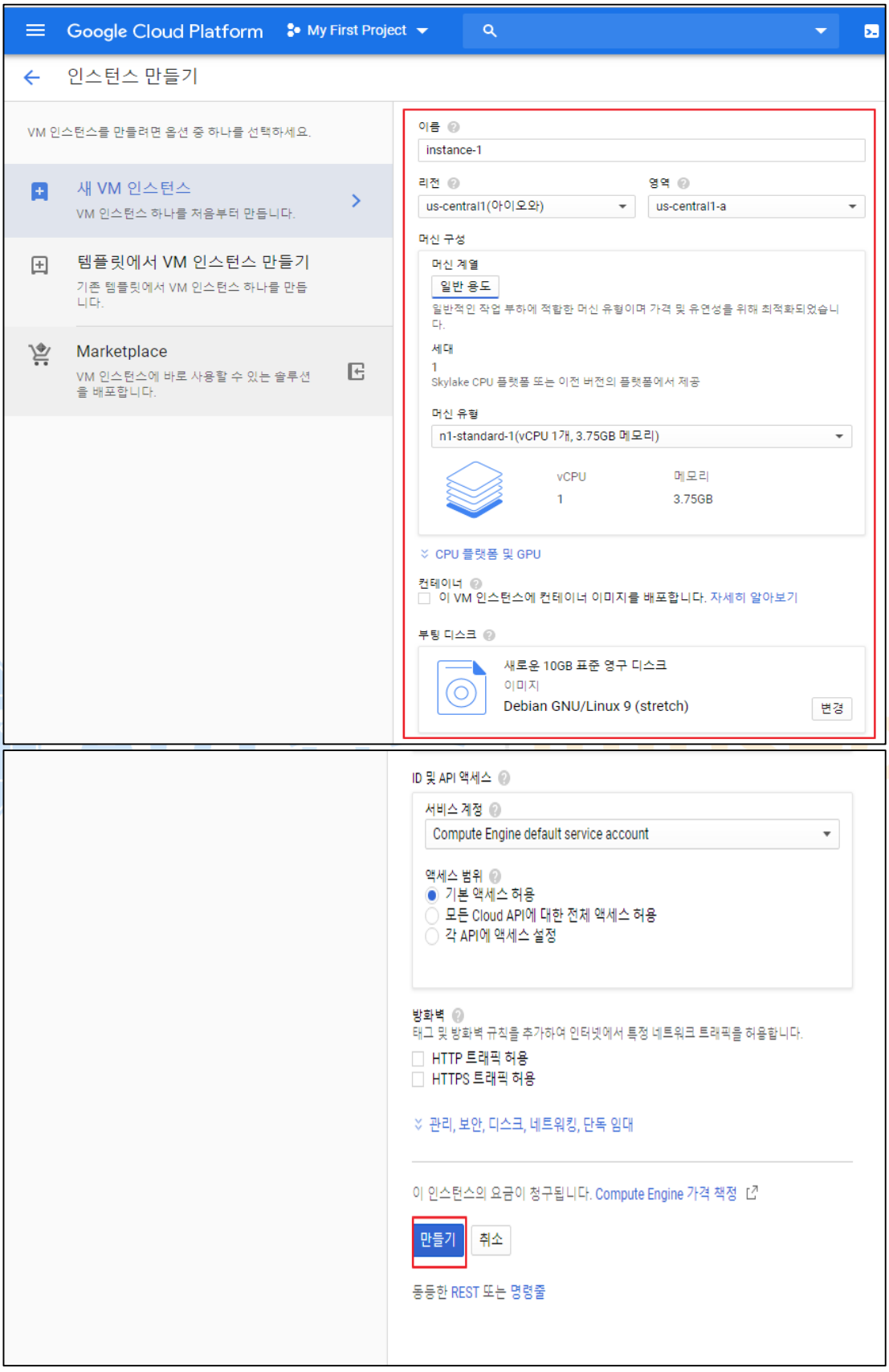
3) '비용 및 재무 담당자' 계정으로 로그인 시도

4) 담당 역할(비용 및 재무 담당자) 외 Google Cloud 내 서비스 이용 시도 ①

- [Compute Engine] > [VM 인스턴스] > [인스턴스 만들기]

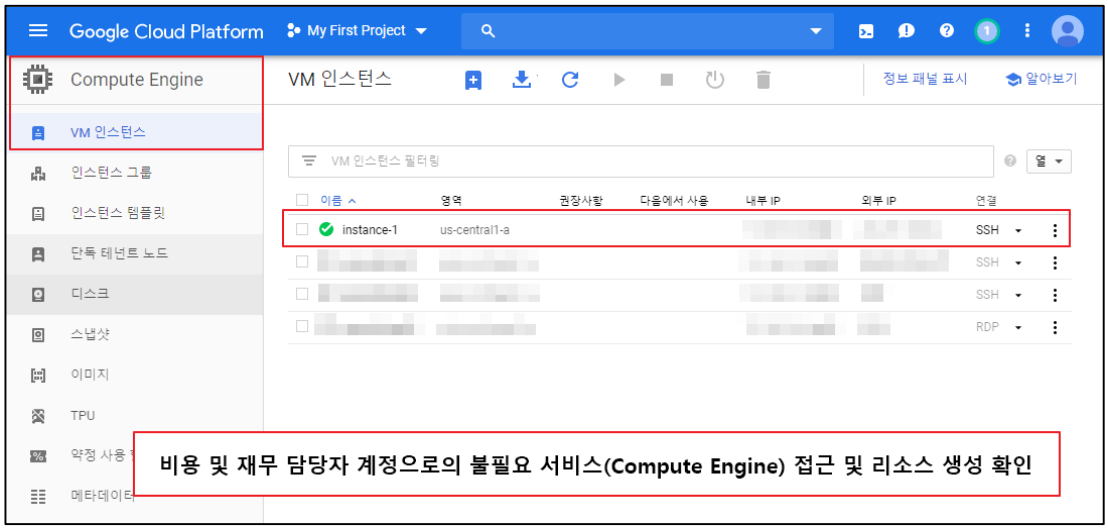
-'비용 및 재무 담당자' 계정으로 Compute Engine 내 리소스 생성 (임의의 VM 인스턴스 생성)





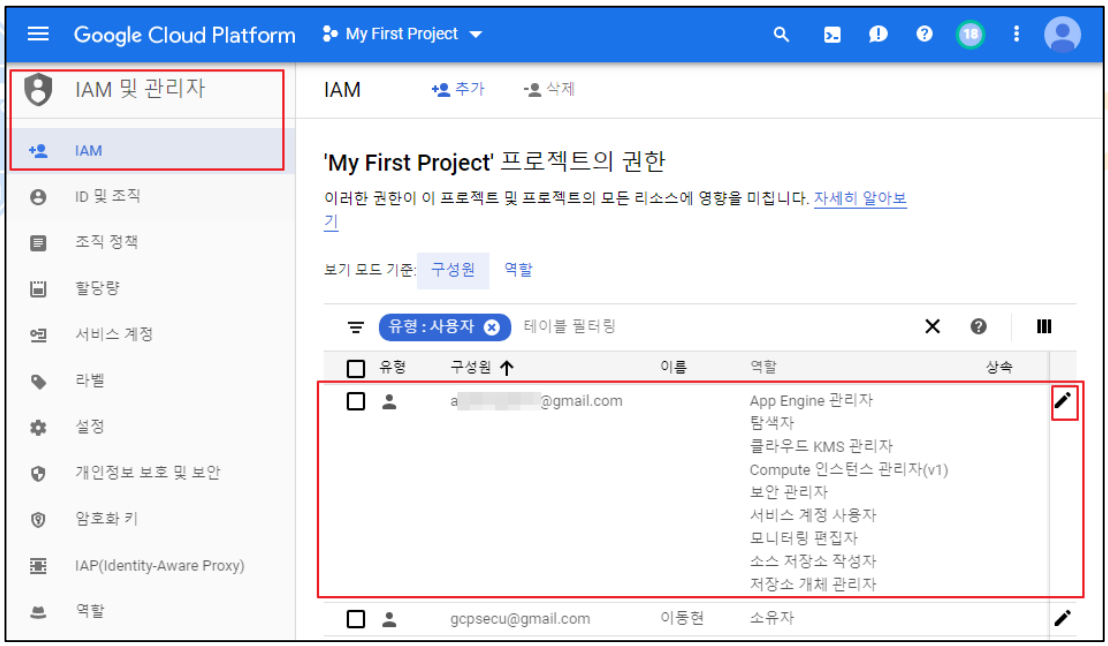
5) 담당 역할(비용 및 재무 담당자) 외 Google Cloud 내 서비스 이용 시도 ②

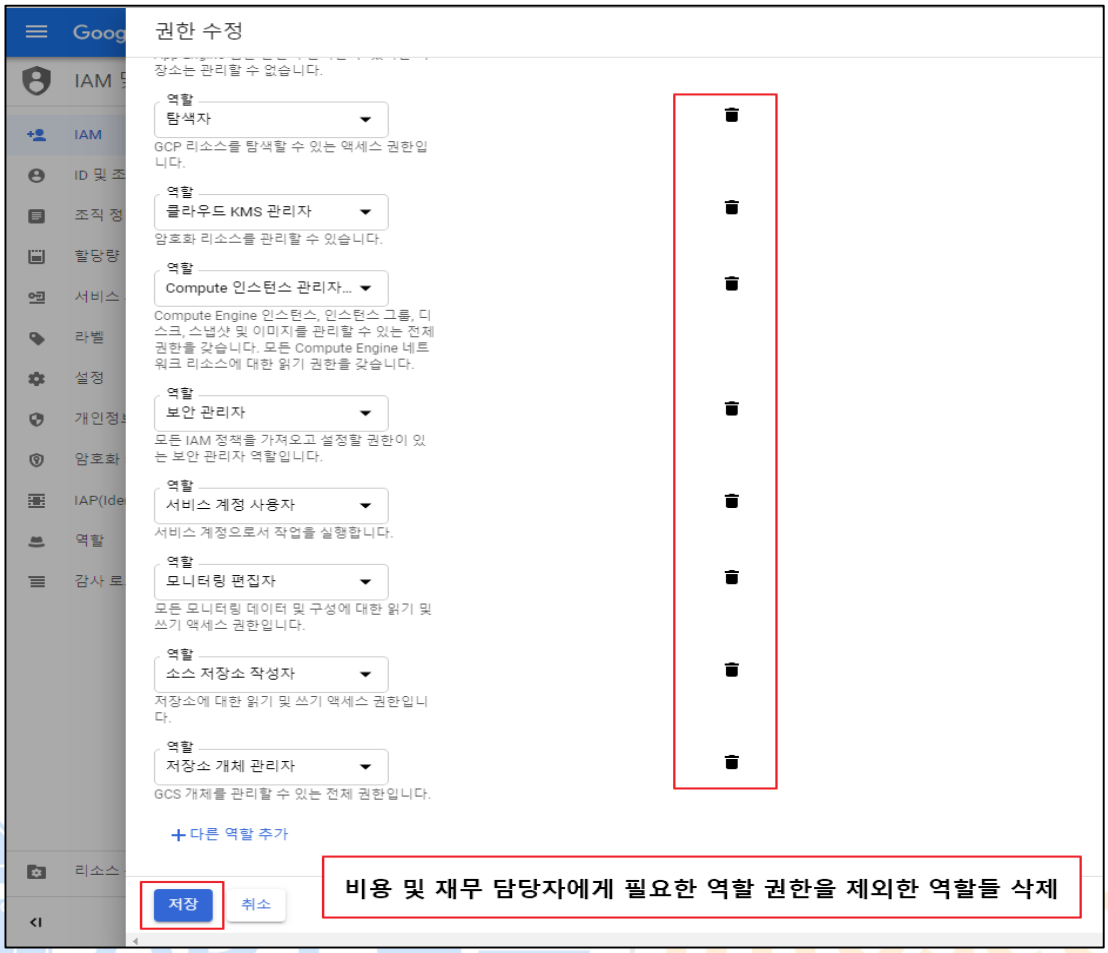
- 임의의 VM 인스턴스(instance-1) 생성 완료



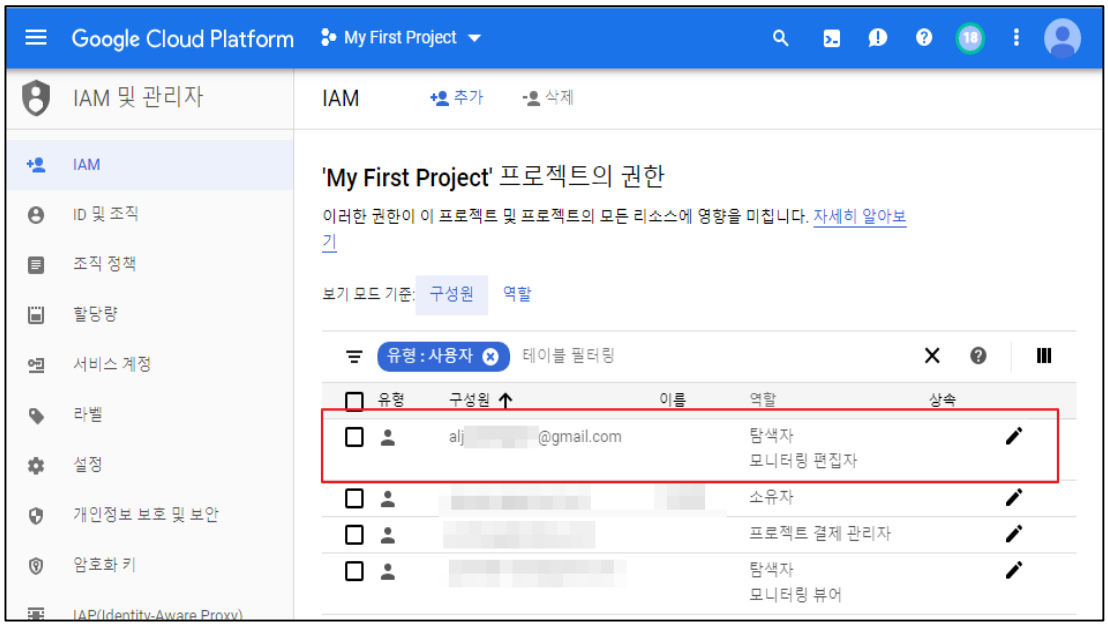
6) [IAM 및 관리자] > [IAM] > [사용자 계정 역할 권한 수정]

- '비용 및 재무 담당자' 테스트 계정 내 필요 이상의 역할 권한 할당되어 있어 담당 서비스(비용 및 재무 관리) 이용에 필요한 역할 권한 외 나머지 역할 권한 삭제(최소한의 권한 유지)

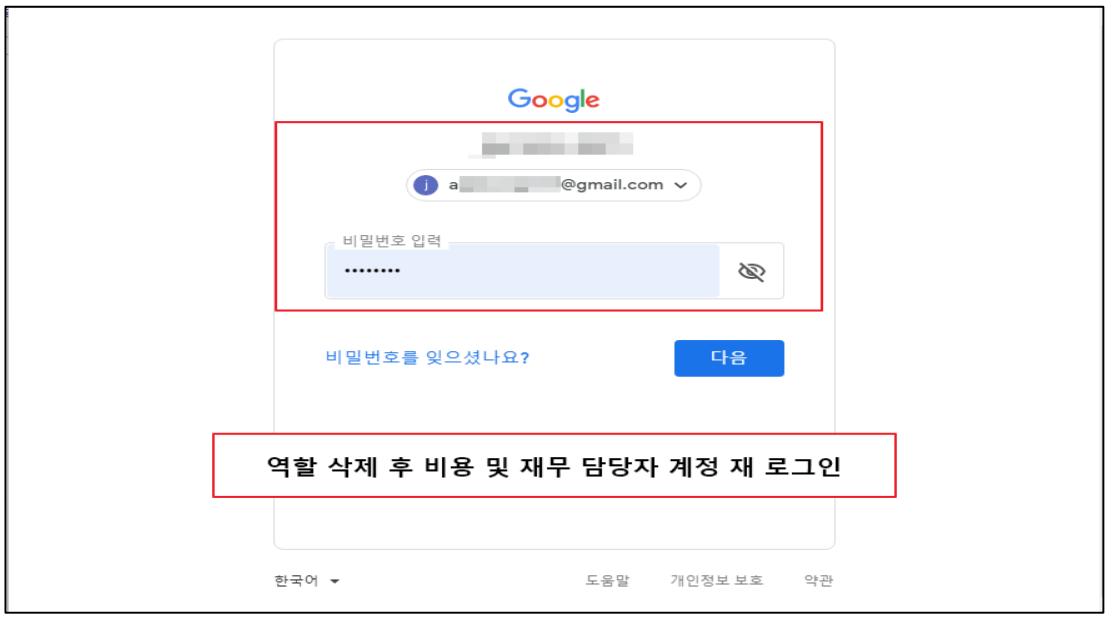


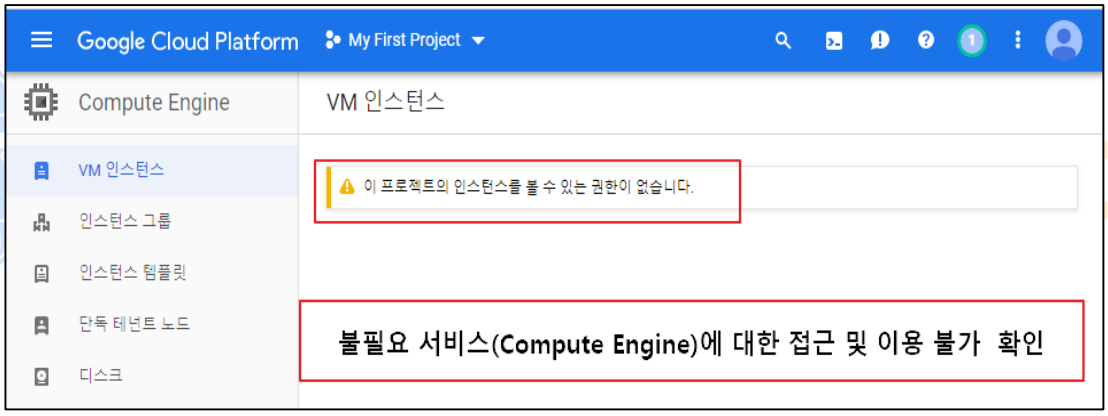


7) '비용 및 재무 담당자' 테스트 계정 내 담당 서비스(비용 및 재무 관리)에 필요한 최소 권한만 할당됨을 확인



8) 역할 권한 수정 후 '비용 및 재무 담당자' 테스트 계정으로 재 로그인 시도

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


9) ‘비용 및 재무 담당자’ 테스트 계정으로 재 로그인 후 불필요 서비스(Compute Engine)에 대한 접근 및 이용 불가 확인


※ 상기 설정 방법은 진단 기준을 설명하기 위한 예제임을 알려드리며 IAM 내 계정 역할 설정 시 참고용으로 사용하시기 바랍니다.
</td>
</tr>
<tr>
<td>진단 기준</td>
<td>
양호기준
: 서비스 별 IAM 계정 사용 권한이 각각 서비스 역할에 맞게 설정되어 있을 경우

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

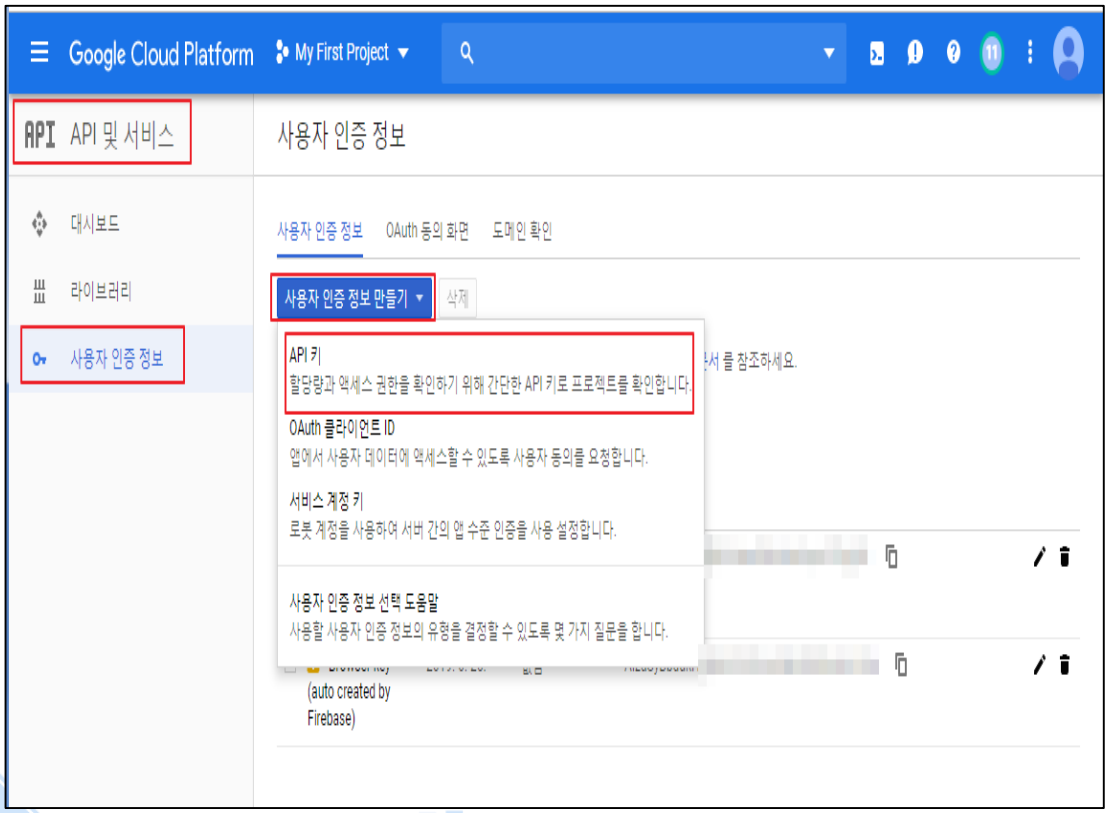
1.9 Cloud API 키 활성화 관리

<table>
<tr><td>분류</td><td>인증/인가</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">Cloud API 키 활성화 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">
Google Cloud API는 Google Cloud Platform의 핵심으로서 저장소 액세스부터 머신러닝 기반 이미지 분석 및 Cloud Platform 애플리케이션에 이르기까지 모든 기능을 손쉽게 추가할 수 있도록 지원합니다. 이처럼 Google Cloud API 키 인증은 서비스 제공자가 발급해준 키를 통해 인증을 하는 방식으로 API 키가 노출되면 전체 보안이 뚫리게 되므로 API 키는 잘 관리되어야 합니다.

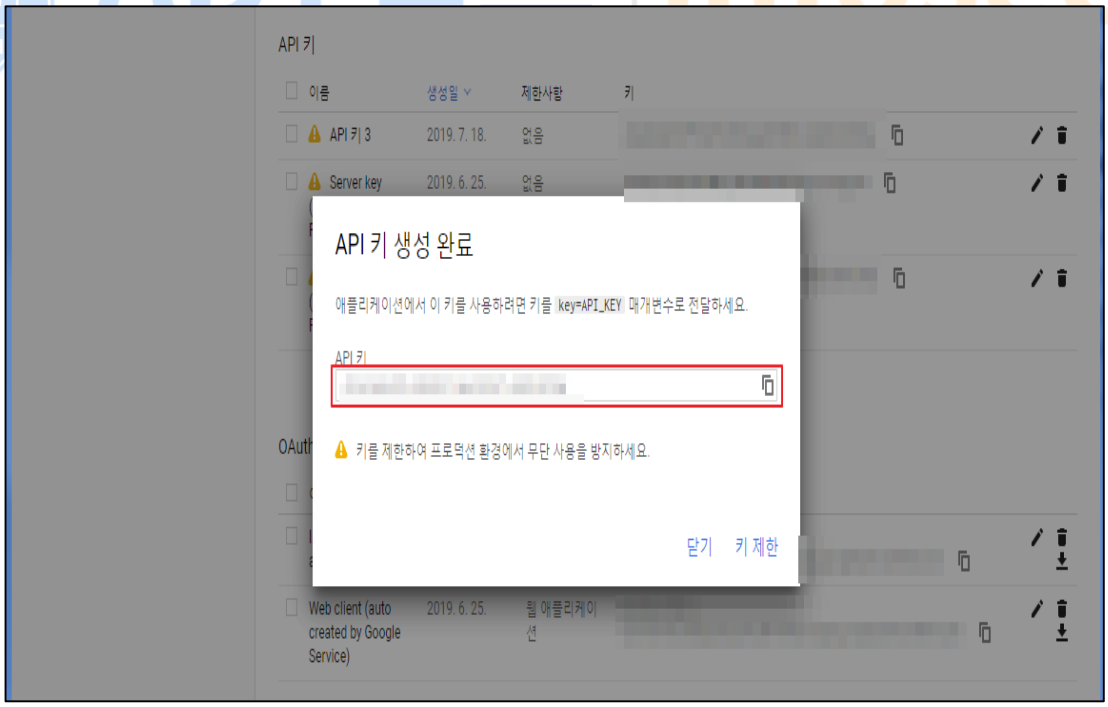
일반적으로 클라이언트가 API 키에 액세스할 수 있으므로 API 키를 쉽게 도난당할 수 있습니다. API 키를 도난 당하면 만료 기간이 없으므로 프로젝트 소유자가 키를 취소하거나 다시 생성하지 않는 한 무기한으로 사용할 수 있습니다. 이에 안전한 API 키 사용을 위해 API 키에 제한을 설정하여 이를 보완하거나 Google ID 토큰 인증과 같은 사용자 인증을 통해 보완해 사용해야 합니다.

※ Cloud API 키 속성
<table>
<tr><th>구분</th><th>속성</th><th>내용</th></tr>
<tr><td rowspan="4">키</td><td>HTTP 리퍼러</td><td>지정된 페이지만 API 를 호출할 수 있도록 웹브라우저에서 실행되는 API 클라이언트에는 HTTP 리퍼러를 사용해 API 를 호출 하며, 이러한 유형의 애플리케이션은 API 키를 공개적으로 노출하므로, 대신 서비스 계정을 사용하는 것이 좋습니다.</td></tr>
<tr><td>IP 주소</td><td>API 키 액세스를 특정 IP 주소로 제한을 가능하게 해줍니다.</td></tr>
<tr><td>Android 앱</td><td>Android 애플리케이션의 경우에는 Android 앱을 사용합니다. 이 옵션을 사용하려면 패키지 이름과 SHA-1 서명 인증서 디지털 지문을 추가해야 합니다.</td></tr>
<tr><td>IOS 앱</td><td>iOS 애플리케이션의 경우, iOS 앱을 사용합니다. 이 옵션을 사용하려면 API 호출을 특정 iOS 번들로 제한하도록 iOS 번들 식별자를 최소한 하나 이상 추가해야 합니다.</td></tr>
<tr><td>웹사이트</td><td>URL 경로 지정</td><td>URL 경로 설정을 통해 API 키의 적용 범위 지정이 가능합니다.</td></tr>
<tr><td>API 키</td><td>API 키 지정</td><td>API 제한사항은 API 키를 사용해서 호출할 수 있는 API 를 지정합니다. 프로덕션 애플리케이션에서 사용되는 모든 API 키는 API 제한사항을 사용해야 합니다.</td></tr>
</table>
※ 모든 제한사항에 대해 ‘없음 또는 제한 안 함’ 설정은 ‘테스트 목적’ 등과 같은 서비스 특성을 고려해 사용하시기 바랍니다.
</td></tr>
<tr><td>설정</td><td colspan="3">가. API 키 생성</td></tr>
</table>

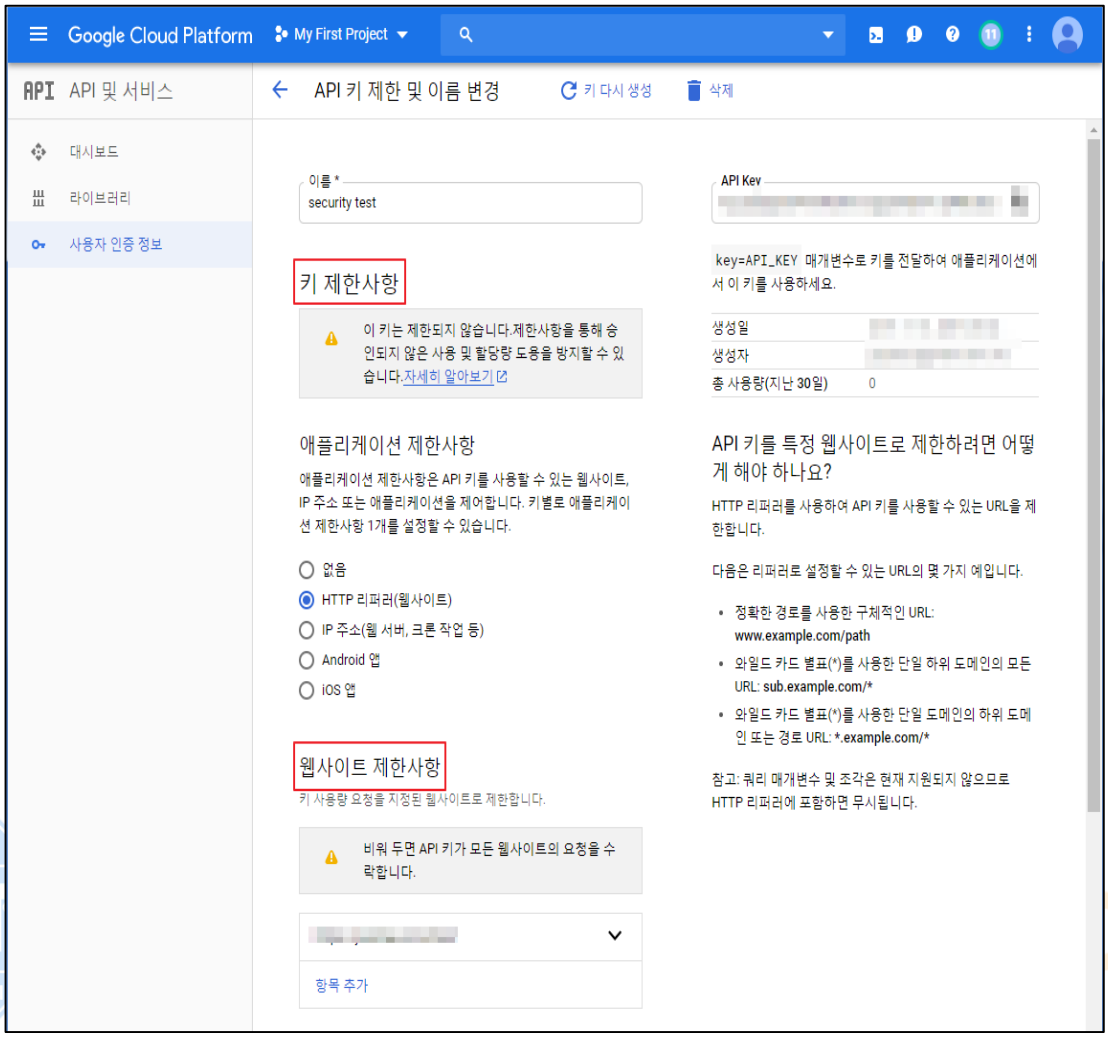
방법	1) [API 및 서비스] > [사용자 인증 정보] > [사용자 인증 정보 만들기] > [API 키]



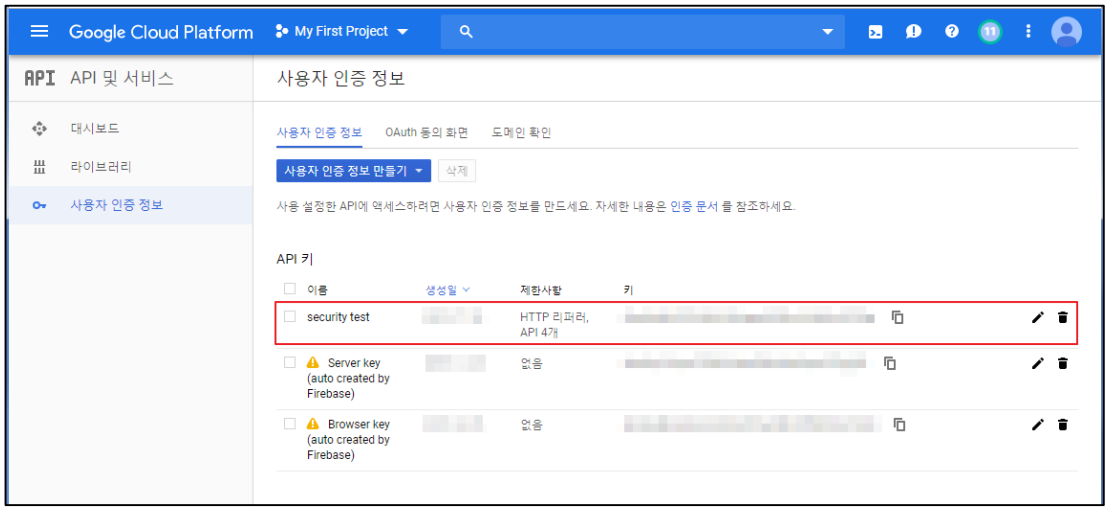
2) API 키 생성완료



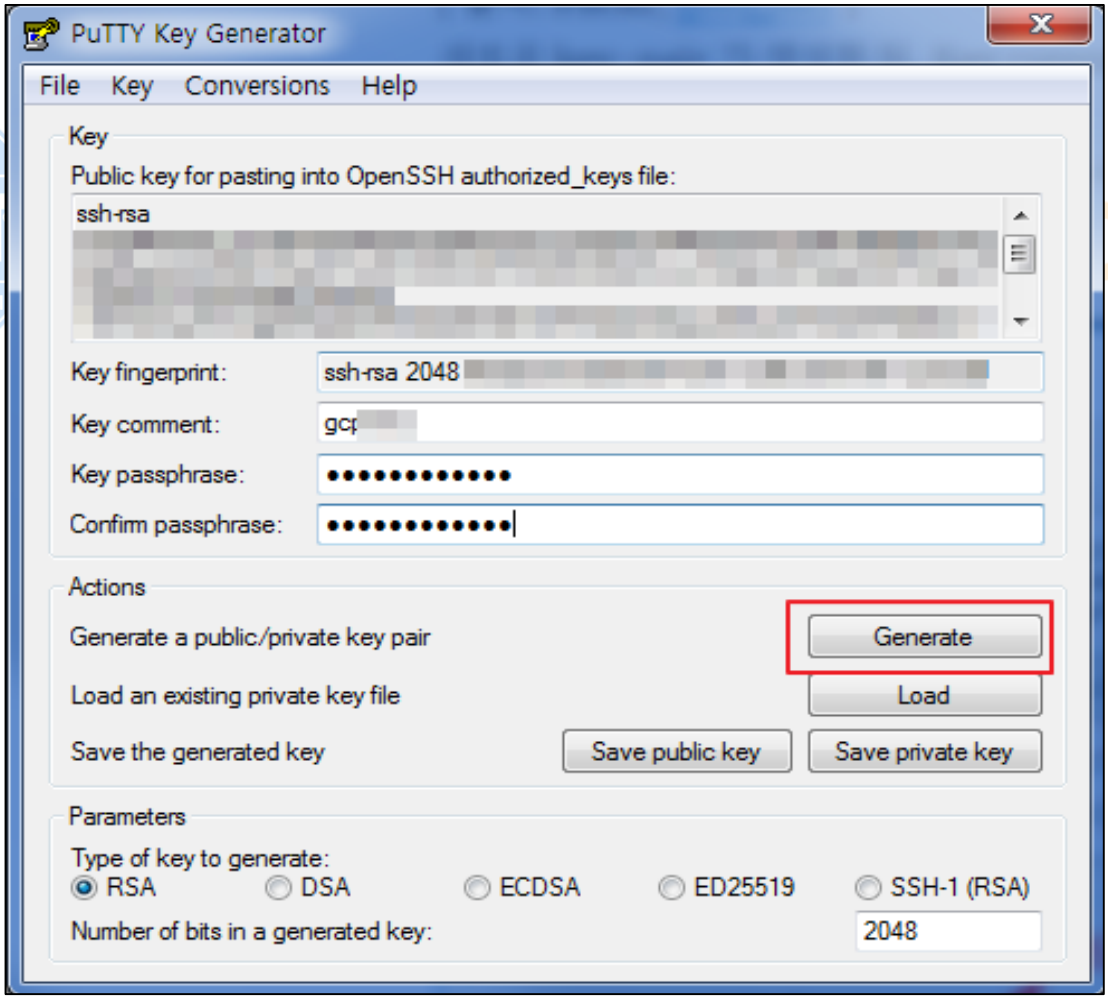
3) API 키 생성 완료 후 '키 / 웹사이트 / API 제한사항' 설정

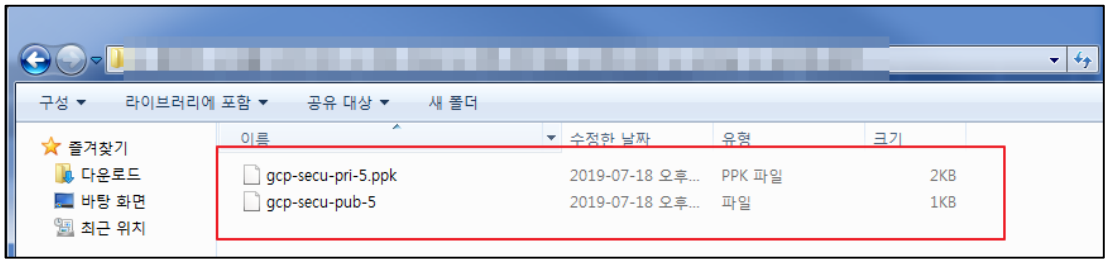


4) API 키 제한 설정 완료

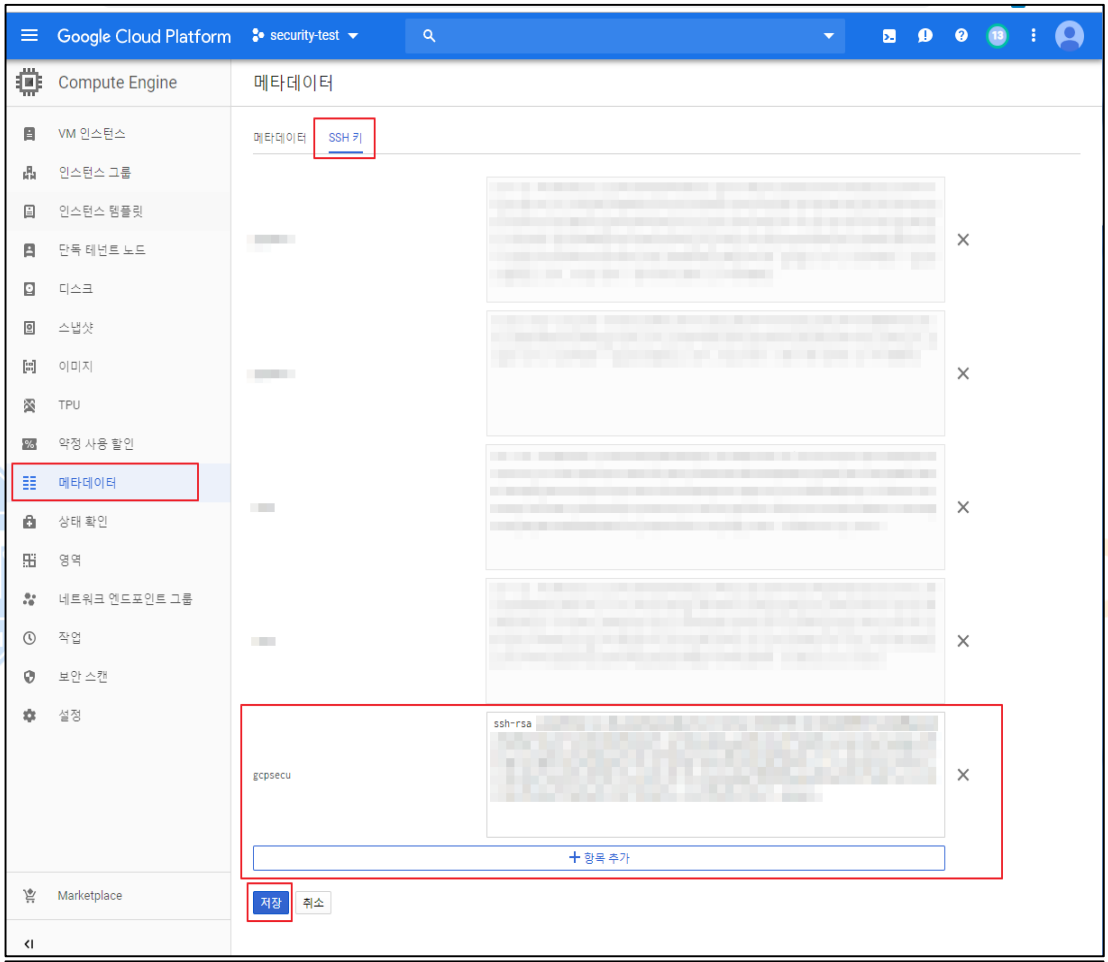
	
진단 기준	**양호기준** : API 키에 접근 제한(키, 웹사이트, API) 사항이 존재하는 경우 **취약기준** : API 키에 접근 제한(키, 웹사이트, API) 사항이 존재하지 않는 경우
비고	

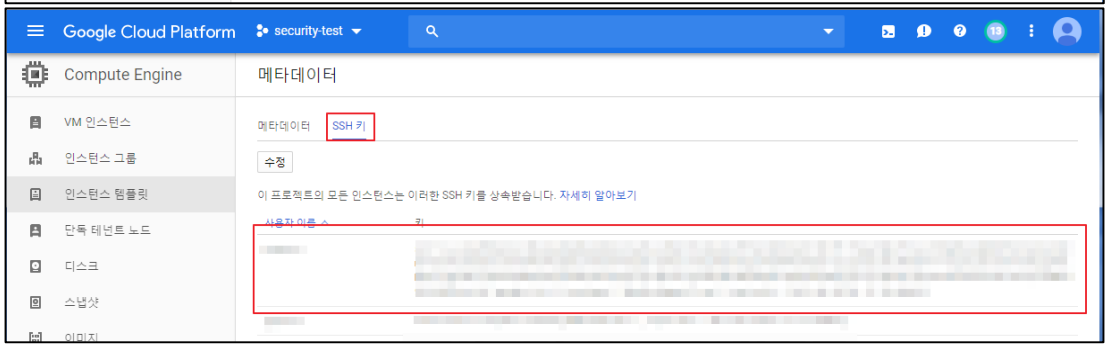
1.10 SSH 키 사용

분류	인증/인가	중요도	상
항목명	SSH 키 사용		
항목 설명	Linux VM 인스턴스를 연결하려면 고유 한 개인 SSH 키 파일과 일치하는 공용 SSH 키 파일로 구성된 고유 한 SSH 키가 필요합니다. SSH 키는 Compute Engine 도구를 사용하여 연결할 때마다 생성되고 관리됩니다. 그러나 타사 도구와 연결하려면 다음 옵션 중 하나를 사용하여 공개 SSH 키를 인스턴스에 제공해야 합니다. Public/Private Cloud Compute 에 안전한 보안접속을 하기 위해서는 필수로 설정 적용이 필요한 기능으로 Linux 의 경우 ssh-keygen 명령어를 통해 RSA 키페어를 생성하고, Windows 는 puttygen 을 이용하여 RSA 키페어를 생성합니다. 생성이 완료된 RSA 키페어를 메타데이터 내 SSH 키 기능에 추가하게 되면 Virtual Compute 에 보안 접속이 가능해지게 됩니다.		
설정 방법	**가. SSH 키 생성 및 VM Instance 적용** 1) Putty-Key Generator를 통해 RSA 키페어 생성  2) 생성된 키 페어 파일을 타사용자 접근이 불가능한 저장공간에 보관		

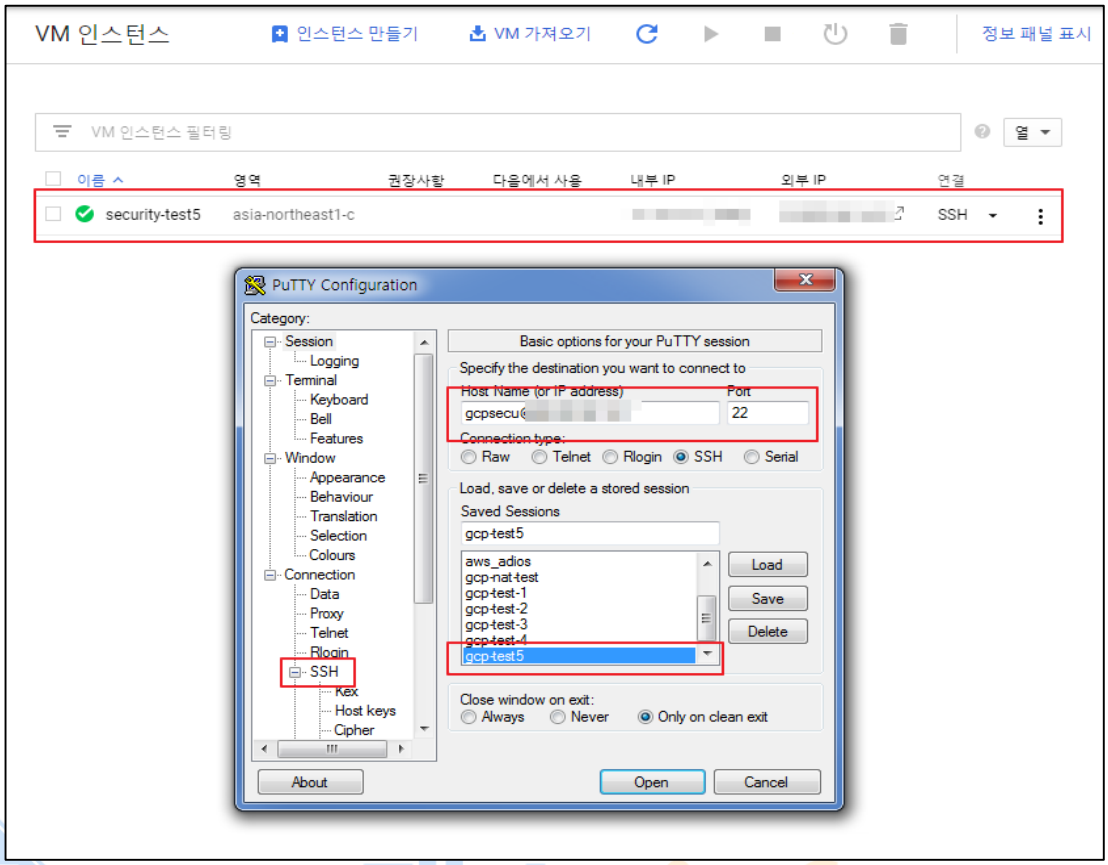


3) [메타데이터] > [SSH키] 내 Putty-Generator 로 생성한 Public Key 등록

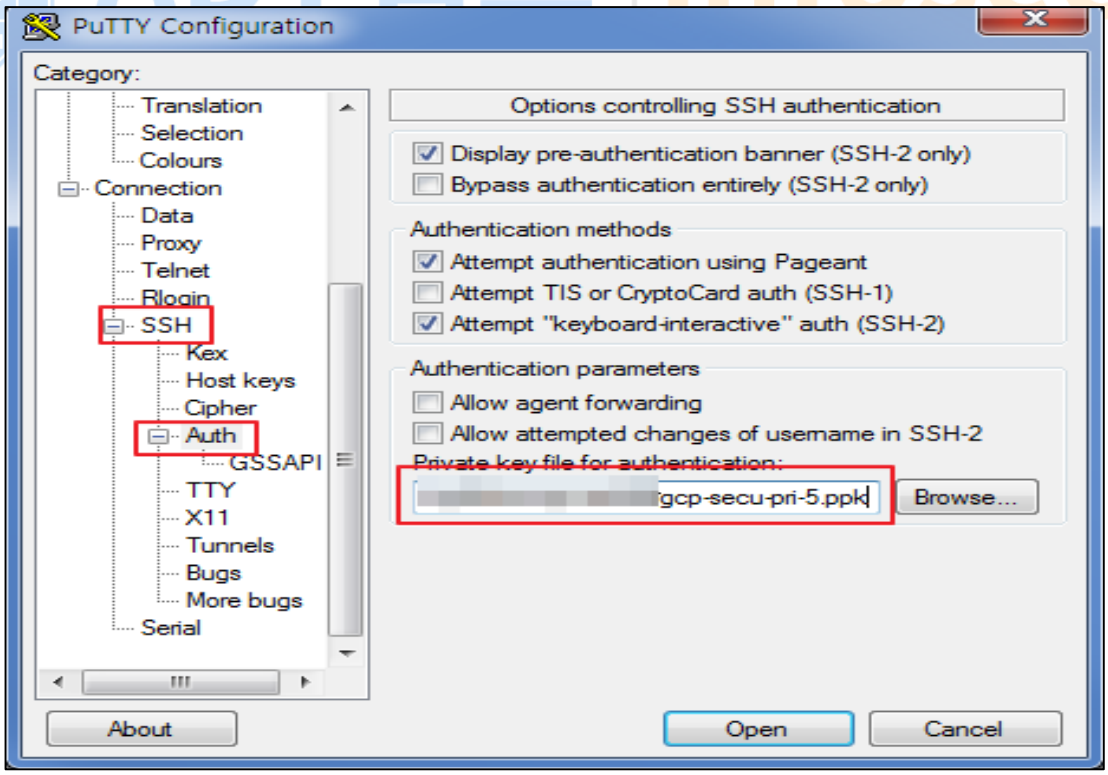




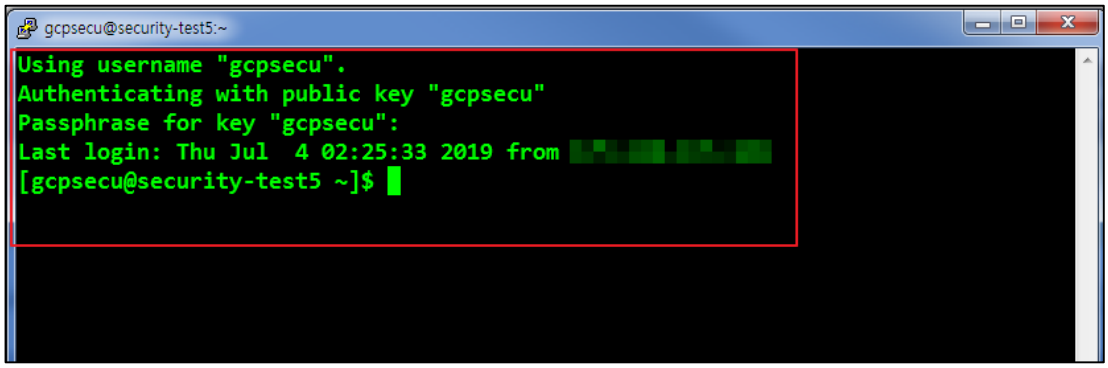
4) putty 내 SSH 접근을 위한 '계정명@hostname(IP)' 및 SSH 키 등록



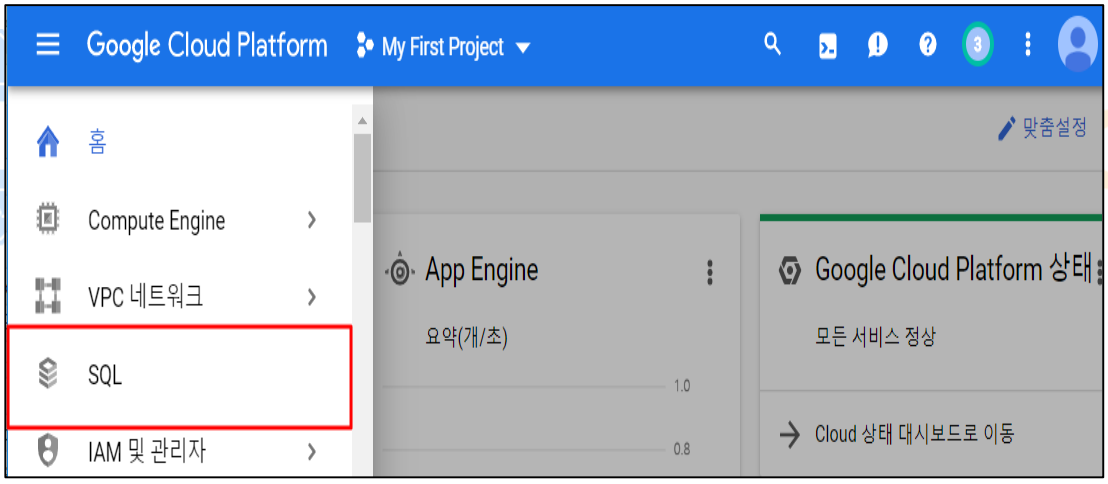
5) ppk(개인키)가 저장되어 있는 위치로 경로 지정 후 SSH 접근 시도

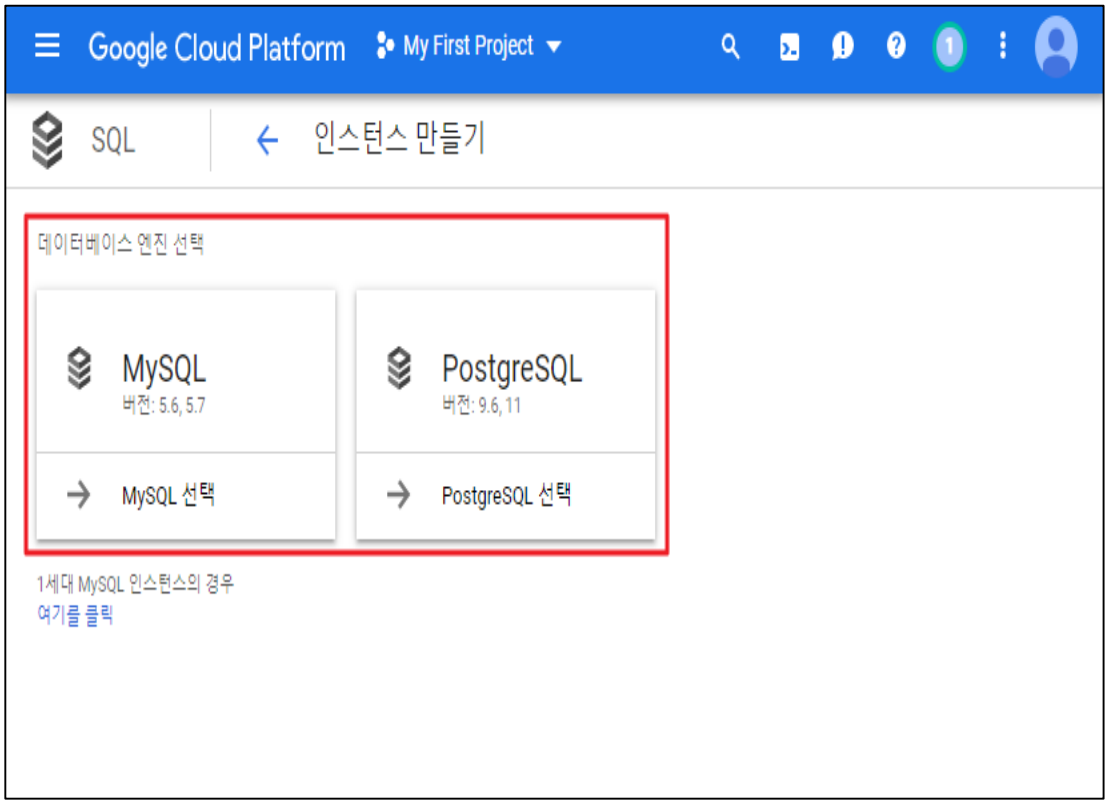


6) SSH 키를 통한 Linux VM Instance 접근 성공 확인

	
진단 기준	**양호기준** : SSH 키를 통해 VM 인스턴스에 접근이 가능할 경우 **취약기준** : SSH 키를 통하지 않고 일반 아이디/패스워드를 통해 VM 인스턴스에 접근이 가능할 경우
비고	

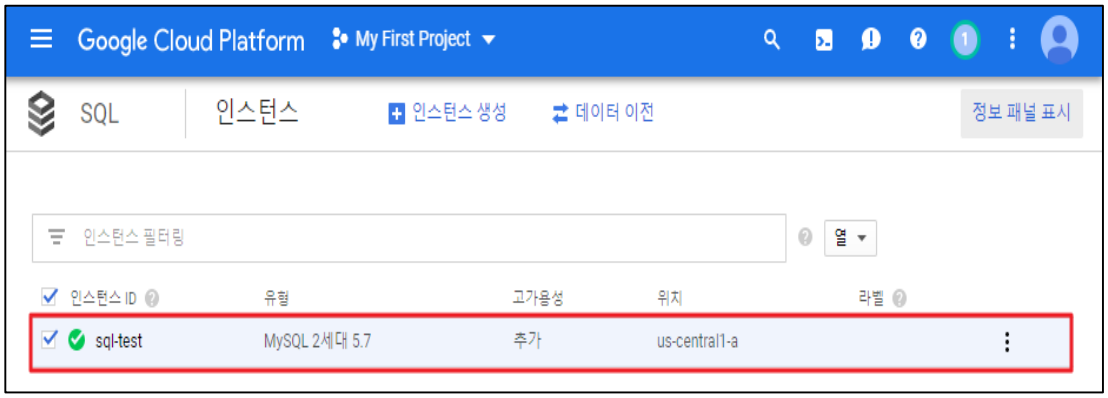
1.11 Cloud SQL Root 계정관리

분류	인증/인가	중요도	상
항목명	Cloud SQL Root 계정관리		
항목 설명	Cloud SQL은 Google Cloud Platform에서 관계형 데이터베이스를 손쉽게 설정하고 유지하고 관리할 수 있게 해주는 완전 관리형 데이터베이스 서비스이며, GCP에서는 MySQL 및 PostgreSQL에서 Cloud SQL을 사용할수 있습니다. SQL DB의 루트 비밀번호가 없으면 누구나 전체 관리 권한으로 이 인스턴스에 연결할 수 있습니다. 승인된 사용자에게만 권한이 부여되도록 루트 비밀번호를 설정해야 합니다. Cloud SQL 인스턴스에서 비공개 IP를 사용하도록 구성할 때는 비공개 서비스 액세스를 사용하면 됩니다. 비공개 서비스 액세스는 VPC 네트워크와 Cloud SQL 인스턴스가 상주하는 Google 서비스 VPC 네트워크 사이에서 VPC 피어링 연결로 구현됩니다. 비공개 서비스 액세스를 사용하는 IP 트래픽은 공개 인터넷에 노출되지 않습니다.		
설정 방법	**가. Cloud SQL 루트 패스워드 및 SSL 연결 설정 (TLS)** 1) [메인] > [SQL]  2) Cloud SQL 인스턴스 생성  3) 데이터베이스 엔전 선택		



4) 인스턴스의 루트 비밀번호 작성 후 생성

5) 생성된 인스턴스 생성 완료

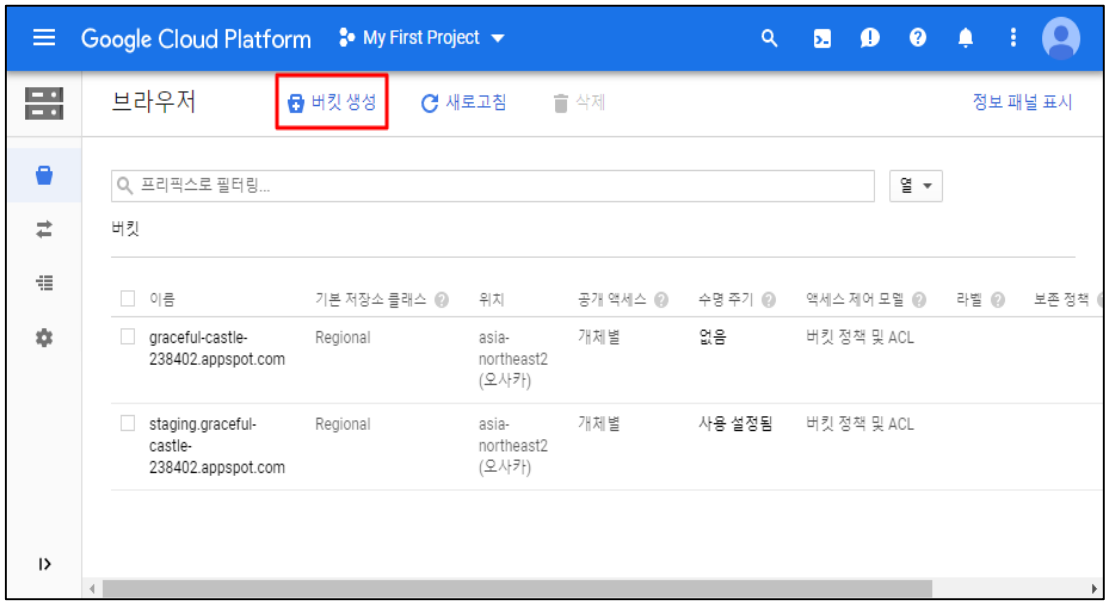
	
진단 기준	**양호기준** : SQL 루트 패스워드가 설정 되어 있고 루트 패스워드를 통해 접근이 가능할 경우 **취약기준** : SQL 루트 패스워드 설정 없이 루트 계정에 접근이 가능할 경우
비고	

1.12 Storage 리소스 권한 관리

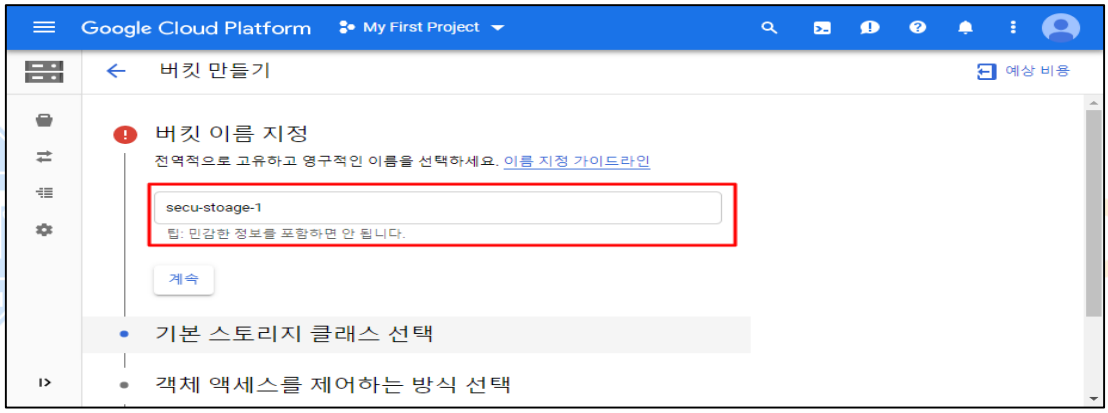
<table>
<tr><td>분류</td><td>인증/인가</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">Storage 리소스 권한 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">Cloud Storage는 버킷과 객체에 대한 액세스 권한을 사용자에게 부여하는데 사용되는 Cloud Identity and Access Management(Cloud IAM) 및 액세스제어 목록(ACL)이라는 두 시스템을 제공합니다. 이러한 시스템은 동시에 작동합니다. 사용자가 Cloud Storage 리소스에 액세스할 수 있게 하려면 시스템 중 하나만 사용자에게 권한을 부여해야 합니다. Cloud IAM은 GCP 전체에서 사용되며 버킷 및 프로젝트 수준에서 세부적인 권한을 부여할 수 있게 해줍니다. ACL은 Cloud Storage에서만 사용되며 권한 옵션이 더 적지만 객체 단위로 권한을 부여할 수 있습니다.

※ Cloud Storage 버킷 및 객체 액세스 제어 옵션
<table>
<tr><th>구분</th><th>상세내용</th></tr>
<tr><td>Cloud Identity and Access Management(Cloud IAM)</td><td>버킷에 대한 액세스 권한과 버킷 내 객체에 대한 일괄 액세스 권한을 부여합니다. Cloud IAM 권한으로 프로젝트와 객체의 광범위한 제어가 가능하지만 개별 객체의 세부적인 제어는 불가능합니다.</td></tr>
<tr><td>액세스제어 목록(ACL)</td><td>사용자에게 개별 버킷이나 객체에 대한 읽기 또는 쓰기 액세스 권한을 부여합니다. 대부분의 경우 ACL 대신 Cloud IAM 권한을 사용해야 합니다. 개별 개체의 세부적인 제어가 필요한 경우에만 ACL 을 사용하시기 바랍니다.</td></tr>
<tr><td>서명된 정책 문서</td><td>버킷에 업로드 할 수 있는 항목을 지정합니다. 정책 문서를 통해 크기, 콘텐츠 유형, 서명된 URL 이외의 기타 업로드 문자를 더 세부적으로 제어할 수 있으며, 웹사이트 소유자는 정책 문서를 사용하여 방문자가 Cloud Storage 에 파일을 업로드 하도록 허용할 수 있습니다.</td></tr>
</table></td></tr>
<tr><td>설정
방법</td><td colspan="3">가. Cloud IAM 및 액세스제어 목록(ACL) 설정
1) [관리 콘솔] > [Storage] > [브라우저]
 

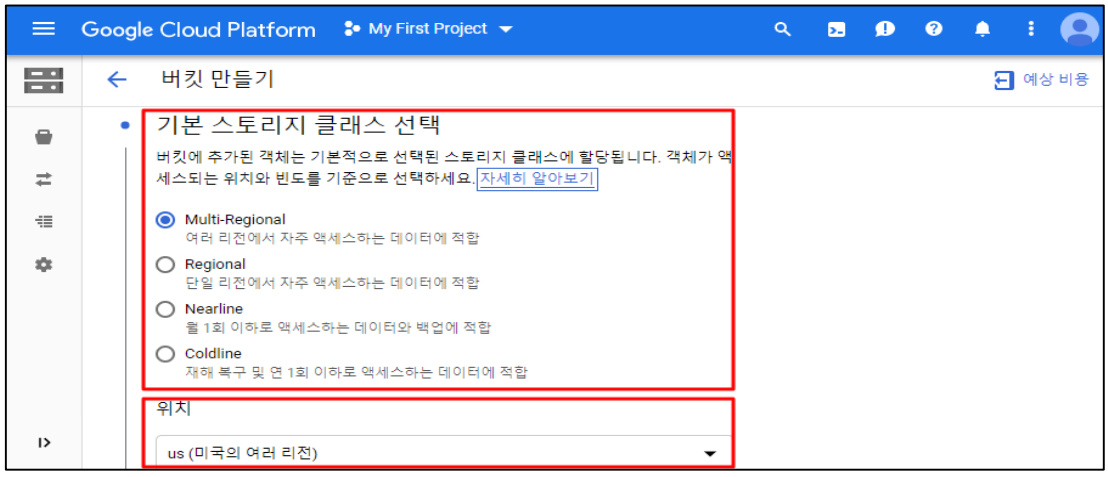
2) 버킷 생성</td></tr>
</table>



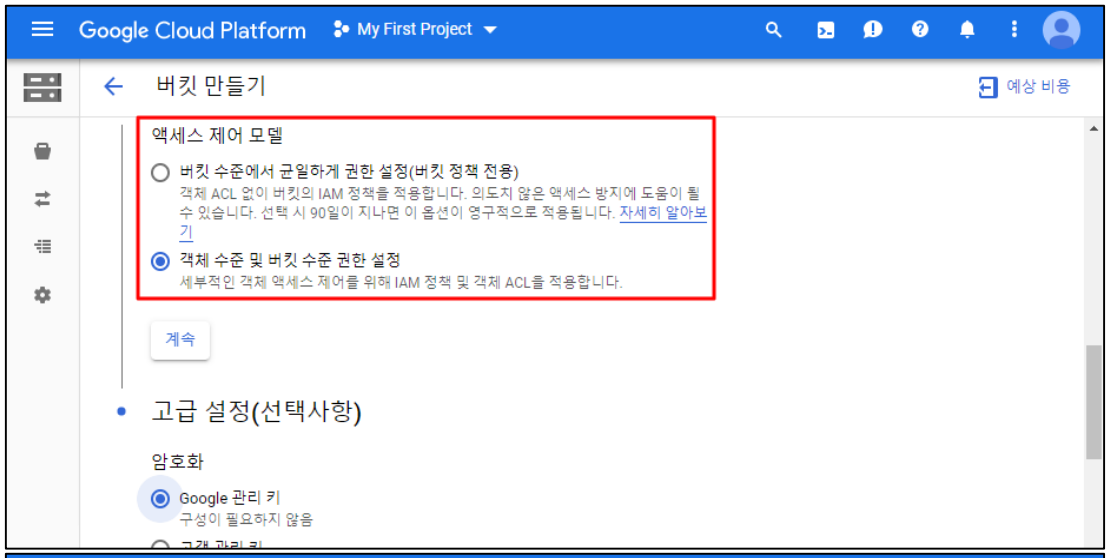
3) 버킷 정보 입력

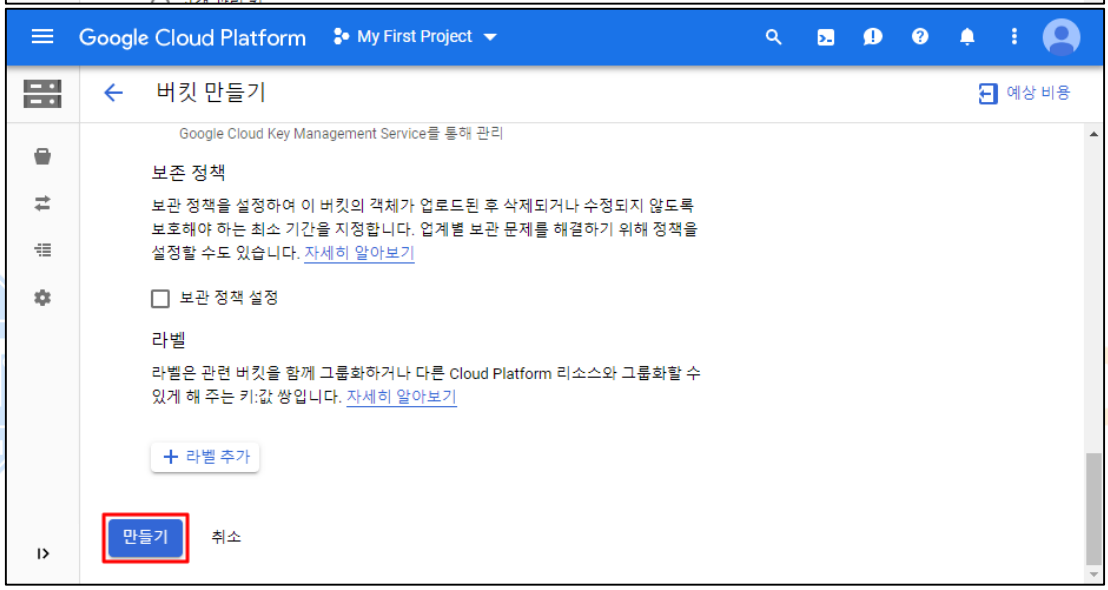


4) 기본 스토리지 클래스 선택

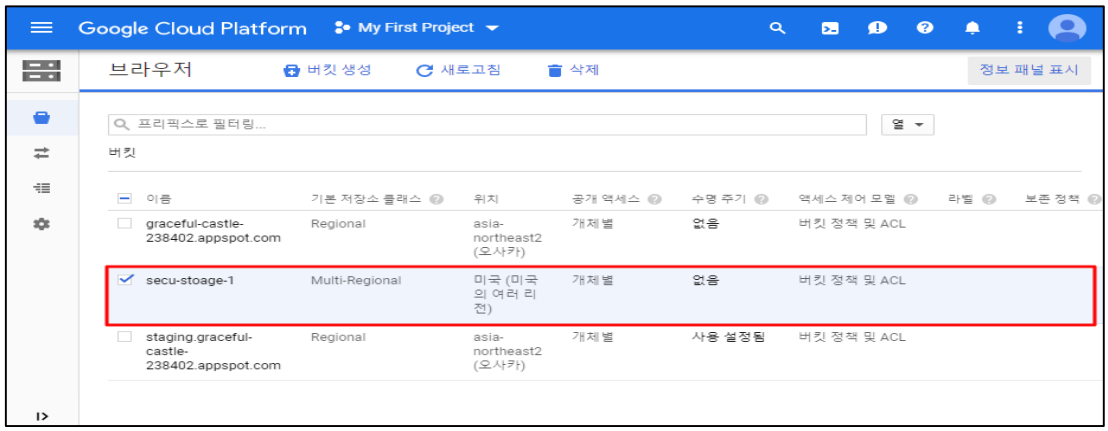


5) 액세스 제어 모델 설정 및 버킷 만들기

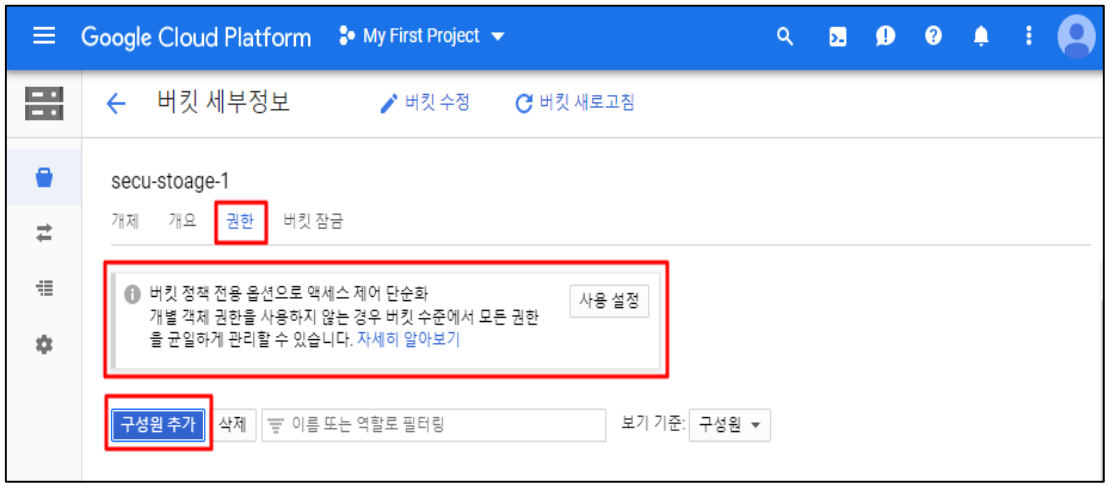




6) 생성된 버킷 접근

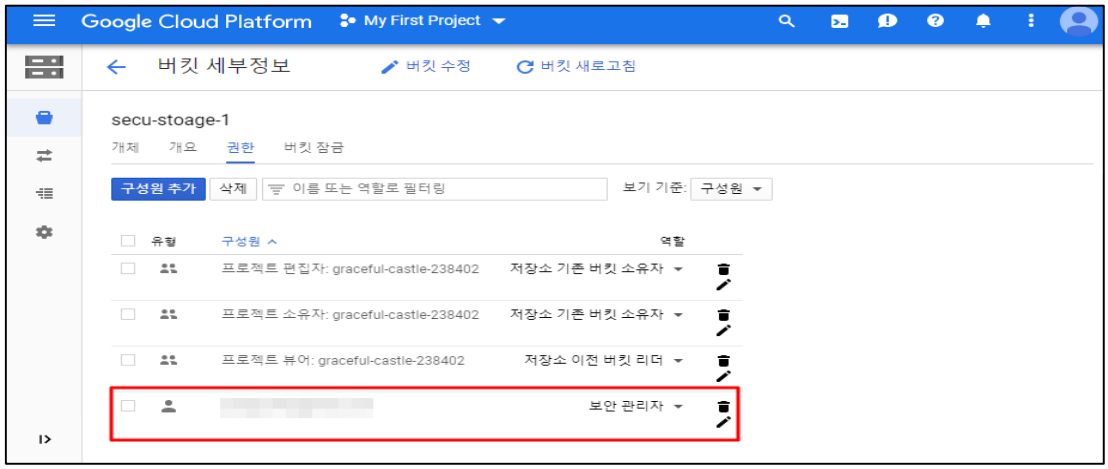


7) 버킷 권한 및 구성원 추가 설정



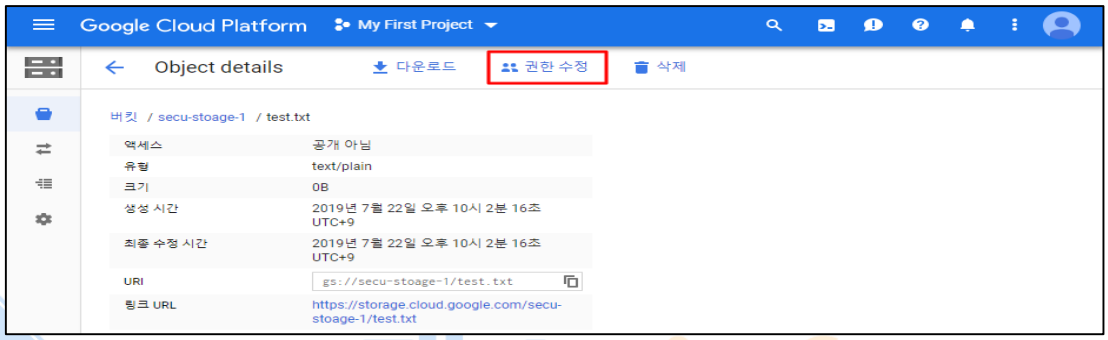
8) 새 구성원 및 IAM 역할 추가

9) 권한 추가 완료

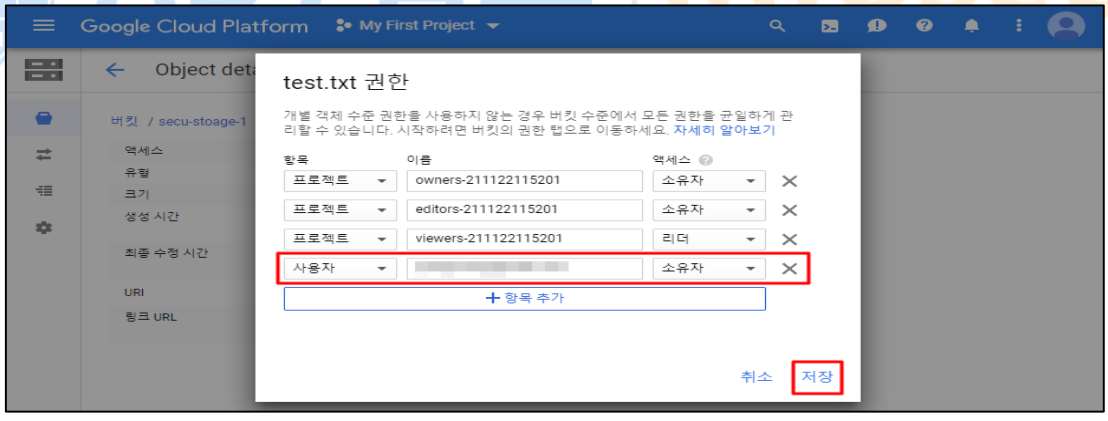


10) 생성된 버킷 내 객체 업로드

11) 객체 내 권한 수정



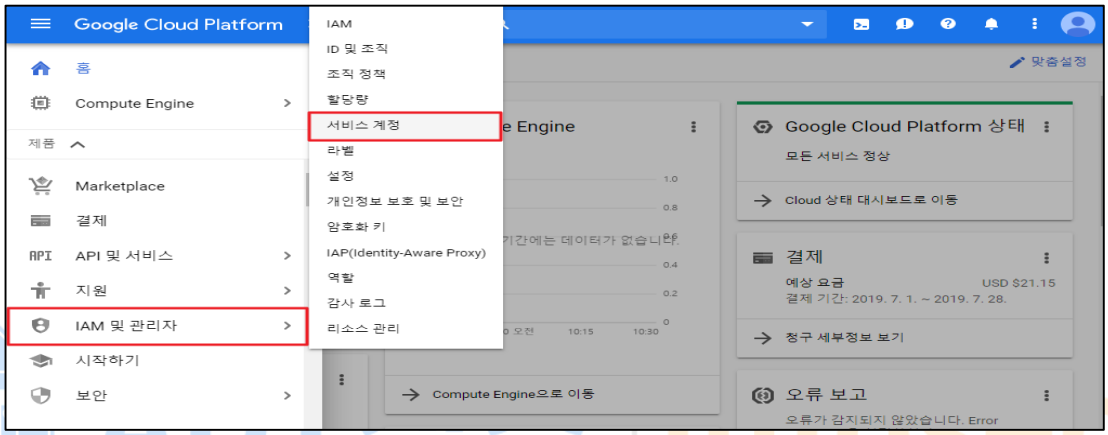
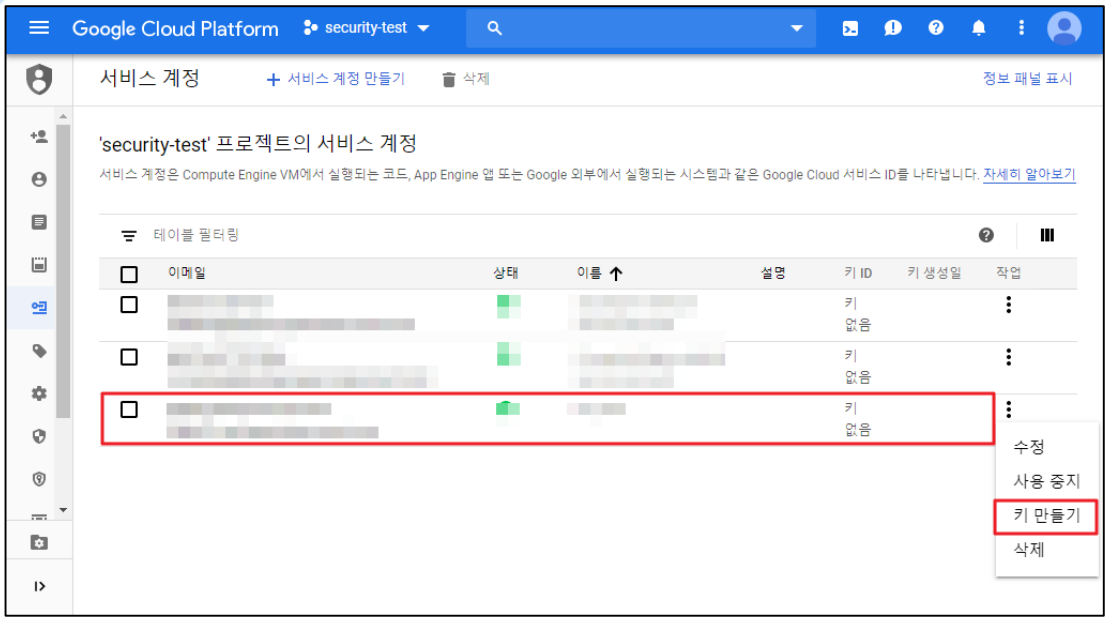
12) ACL 설정 추가

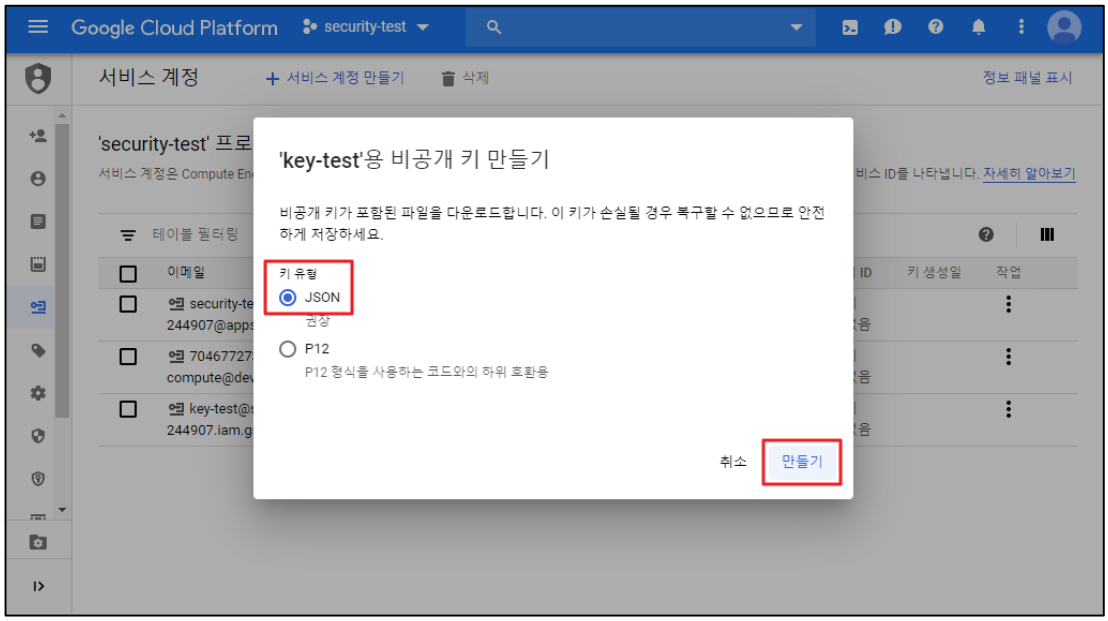


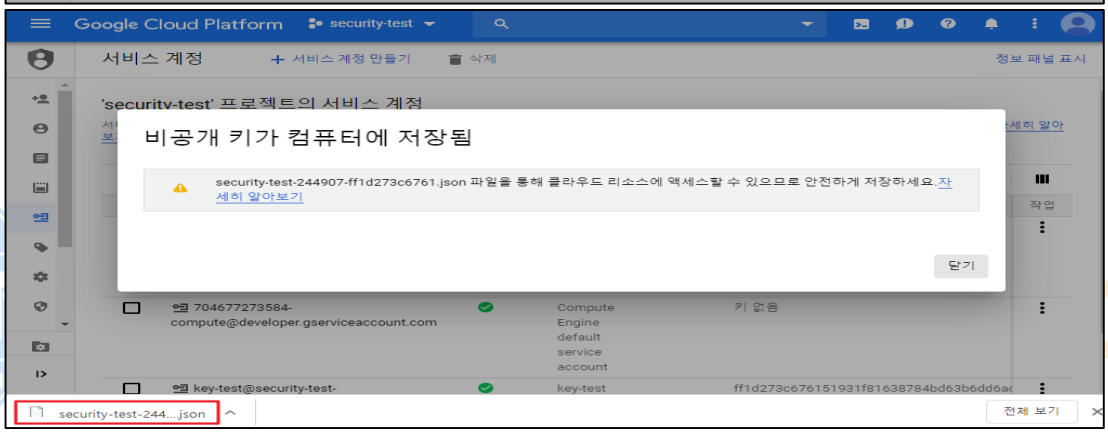
진단 기준	**양호기준** : Storage 버킷 서비스의 ACL 계정 사용 권한이 역할에 맞게 설정되어 있을 경우 **취약기준** : Storage 버킷 서비스의 ACL 계정 사용 권한이 역할에 맞지 않게 설정되어 있을 경우
비고	

1.13 Storage 제어 관리 (서명된 URL 설정)

분류	인증/인가	**중요도**	중

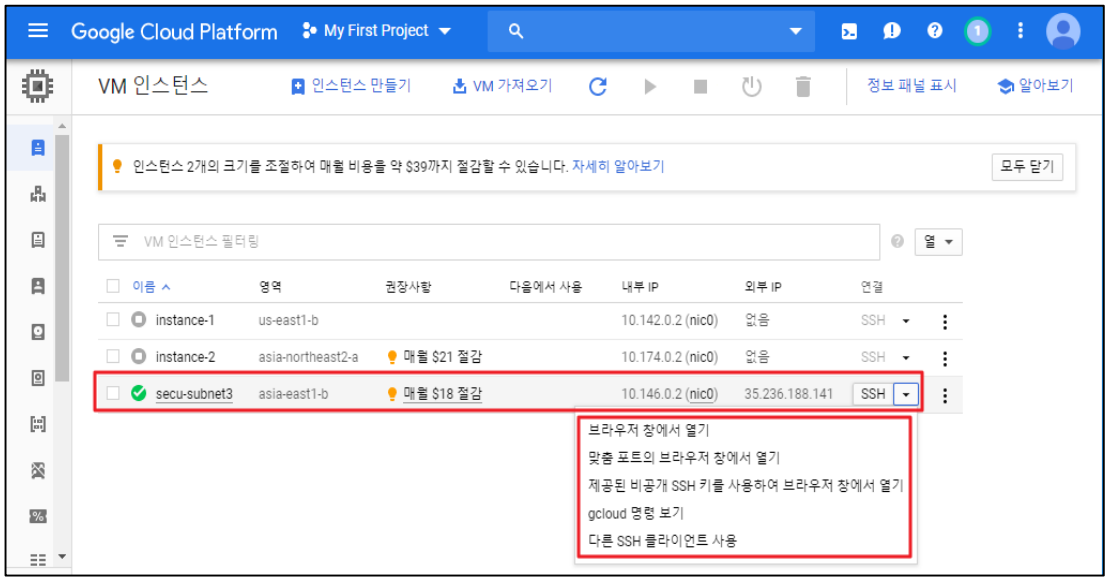
항목명	Storage 제어 관리 (서명된 URL 설정)
항목 설명	Cloud Storage 내 서명된 URL은 사용자에게 제공하여 제한된 시간 동안 해당 리소스에 대한 읽기, 쓰기, 삭제 액세스 권한을 부여하는 URL로서 서명된 URL은 쿼리 문자열에 인증 정보가 포함되어 있어 사용자 인증 정보가 없는 사용자도 리소스에 대한 특정 작업을 수행할 수 있습니다. 서명된 URL을 생성할 때는 서명된 URL이 수행할 요청에 필요한 권한이 있는 사용자 또는 서비스 계정을 지정합니다. 서명된 URL을 생성하면 서명된 URL을 소유한 모든 사람이 이를 사용하여 지정된 기간 내에 객체 읽기와 같은 지정된 작업을 수행할 수 있습니다.
설정 방법	**가. 서명된 URL 설정** 1) [메인] > [IAM 및 관리자] > [서비스 계정]  2) 서명된 URL 생성에 필요한 키 만들기 





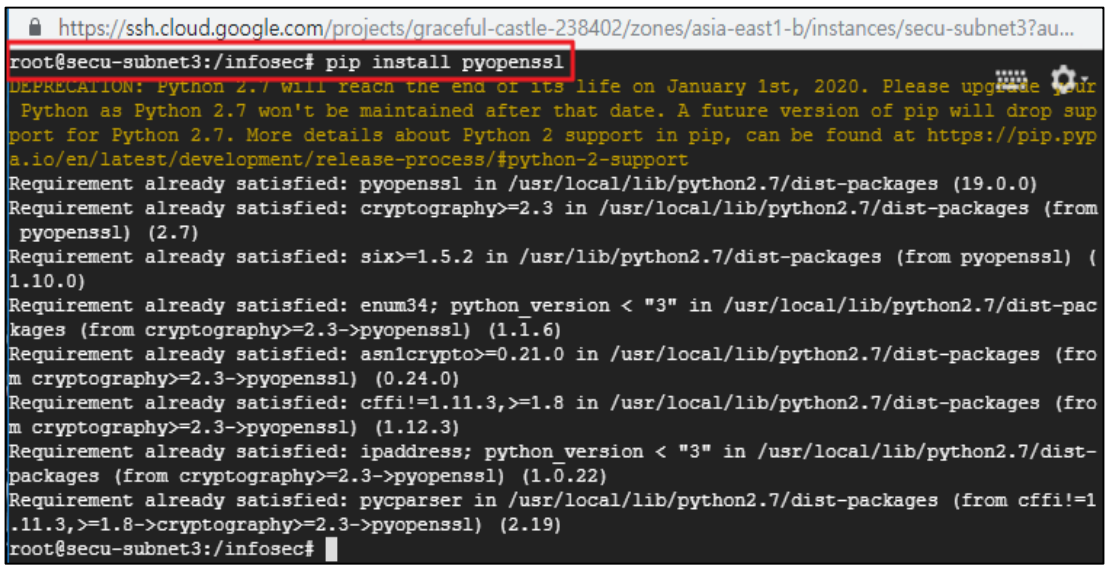
3) 생성된 키 정보 확인

4) 서명된 URL을 생성할 인스턴스 접근

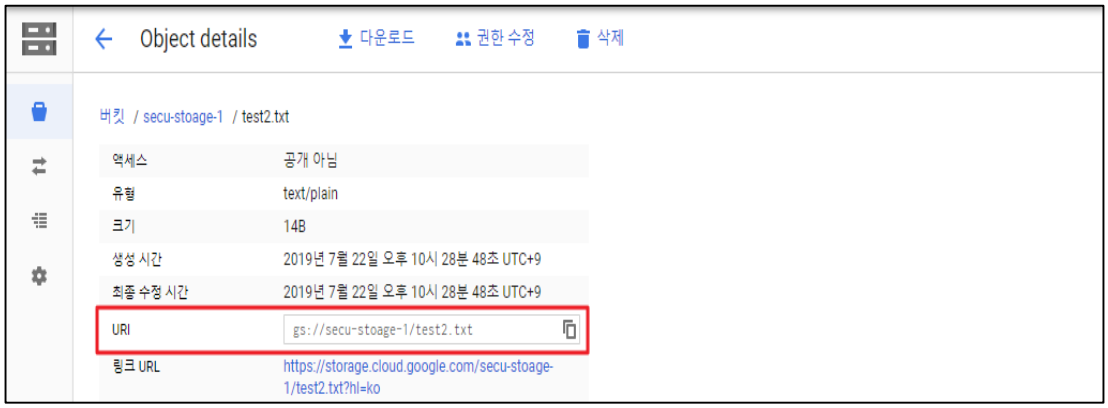


5) 인스턴스 내 생성한 키 저장

6) 서명된 URL 생성에 필요한 도구 설치



7) 공유할 객체 URI 정보 확인

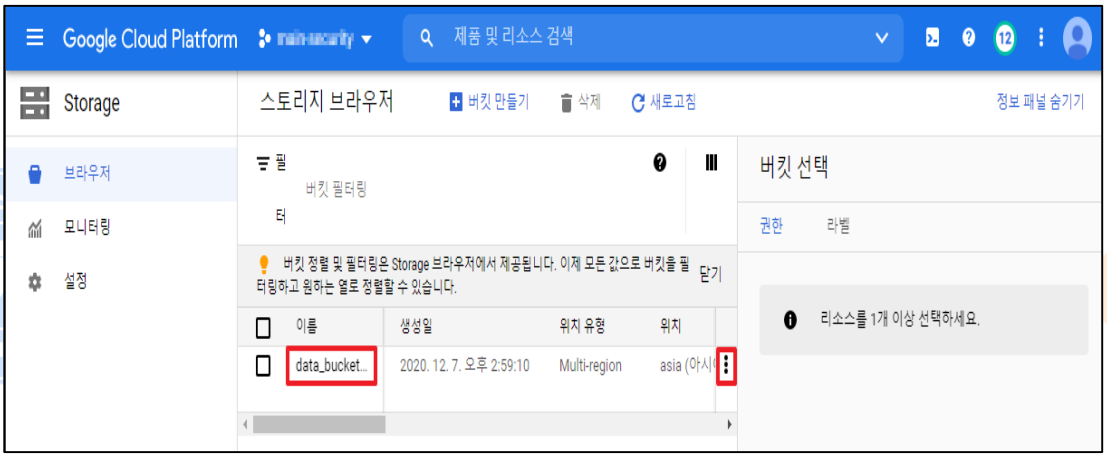
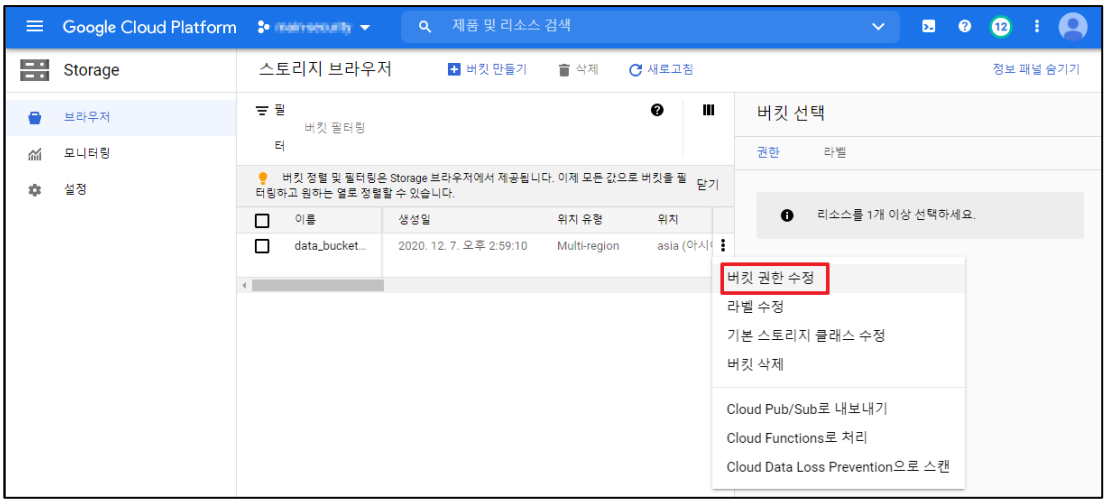
<table>
<tr>
<td></td>
<td>


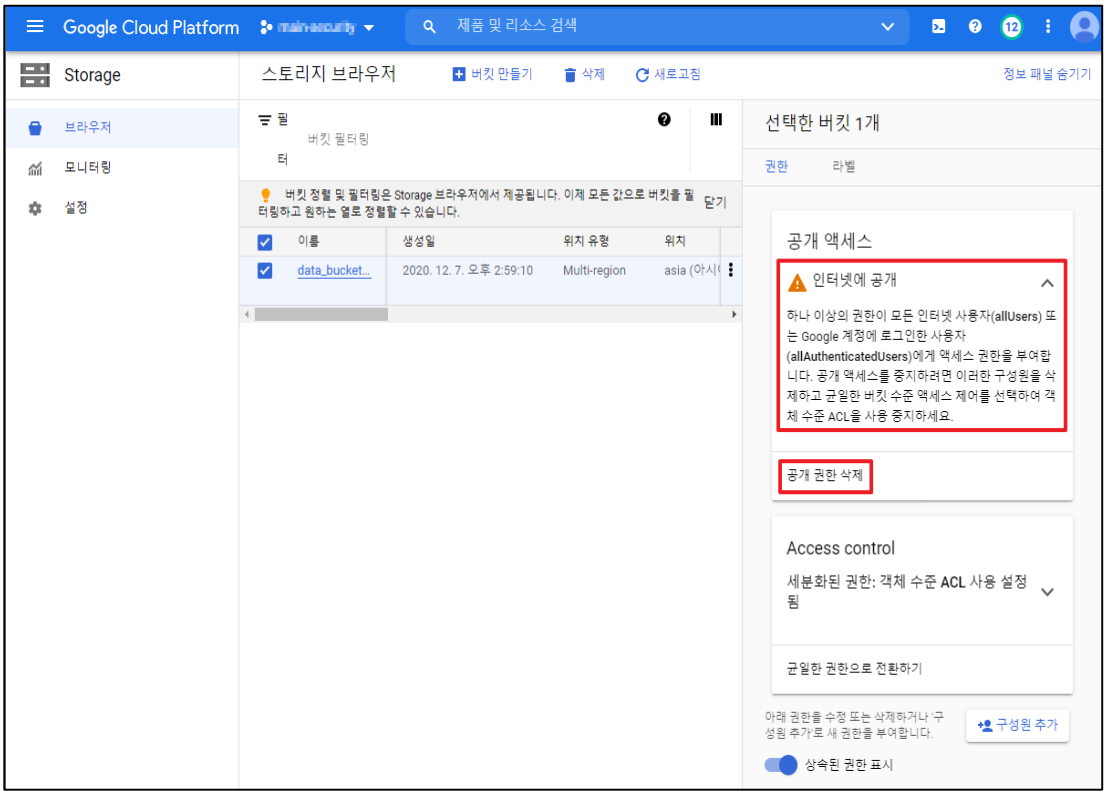
8) 서명된 URL 생성


</td>
</tr>
<tr>
<td>진단 기준</td>
<td>
양호기준
: 서명된 URL을 사용하지 않거나 사용시간을 최소한으로 설정되어 있을 경우

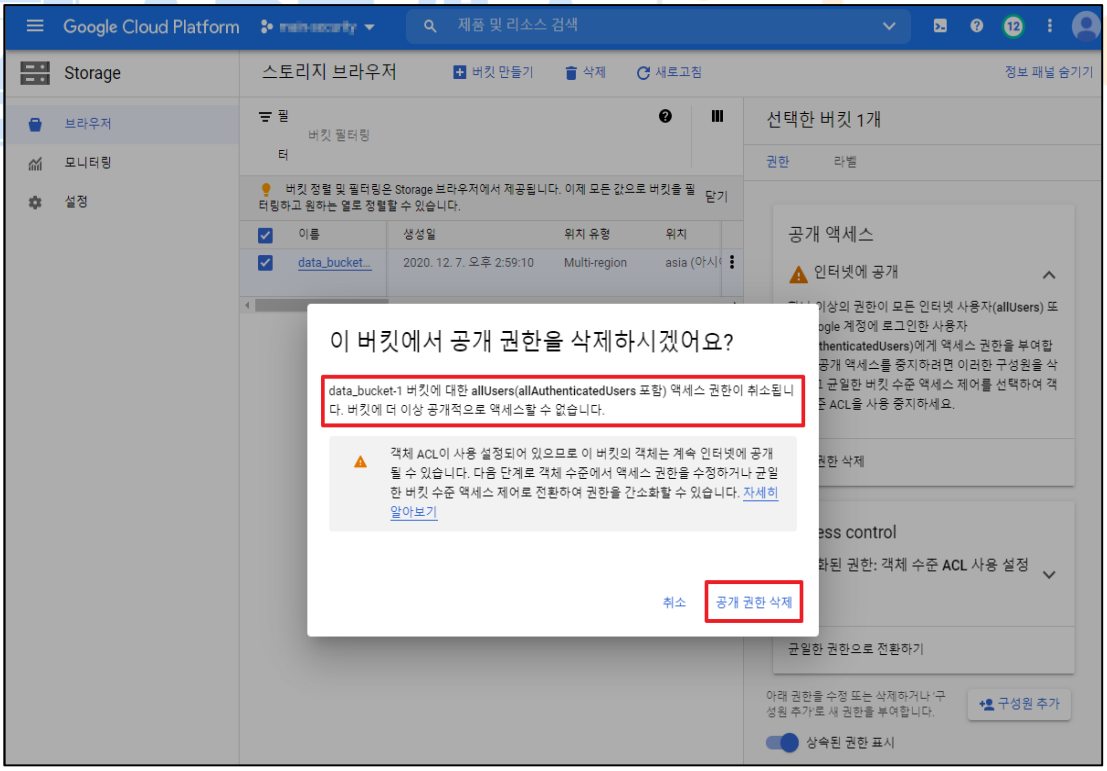
취약기준
: 서명된 URL 사용 시 사용시간을 최소한으로 설정하지 않은 경우
</td>
</tr>
<tr>
<td>비고</td>
<td></td>
</tr>
</table>

1.14 Storage 버킷 퍼블릭 Access 관리

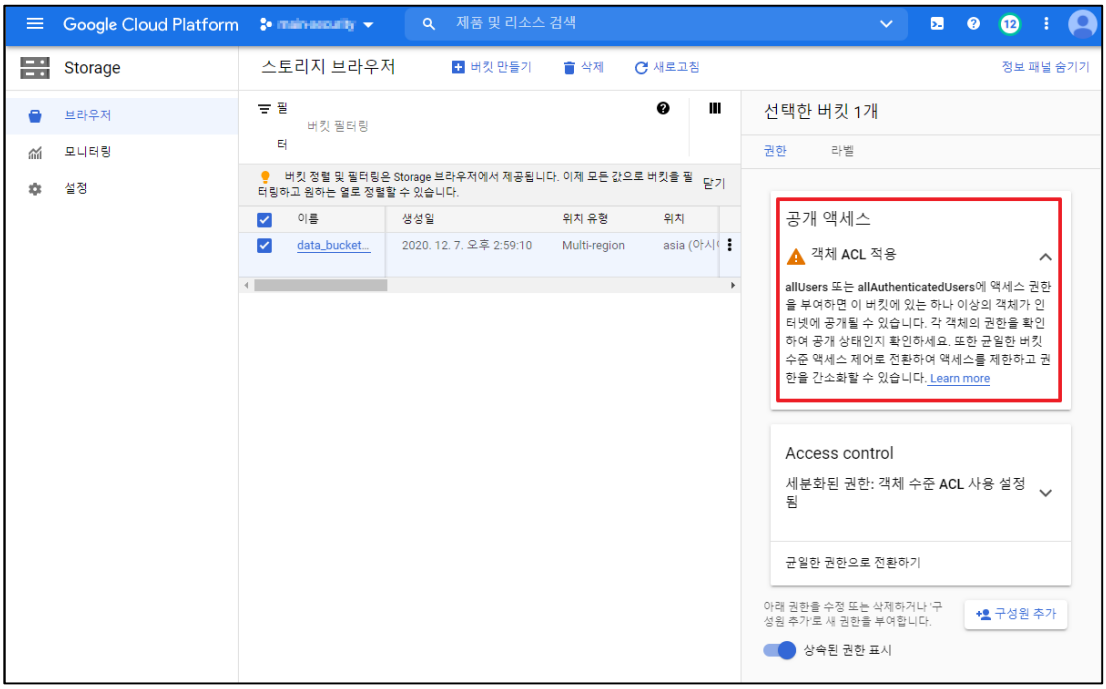
분류	인증/인가	중요도	상
항목명	Storage 버킷 퍼블릭 Access 관리		
항목 설명	공개 액세스는 모든 인터넷 사용자(allUsers) 또는 Google 계정에 로그인한 모든 사용자(allAuthenticatedUsers)가 버킷 또는 버킷 데이터에 액세스할 수 있는지를 나타냅니다. 인터넷에 공개는 1개 이상의 버킷 수준 권한에서 allUsers 또는 allAuthenticatedUsers에 액세스 권한을 부여한다는 의미를 가지며 Storage 버킷의 경우 IAM 또는 ACL을 통해 균일한 액세스 제어 또는 세분화된 액세스 제어 등이 가능하며, 퍼블릭 액세스를 허용하여 allUsers 또는 allAuthenticatedUsers에 액세스 권한을 부여하면 외부로부터 버킷 및 객체가 노출되므로 안전한 버킷/객체 접근을 위해 목적에 맞는 접근 설정을 해야 합니다.		
설정 방법	**가. 퍼블릭 Access 삭제 방법** 1) Storage 내 "작업 더 보기(:)" 클릭  2) 버킷 권한 수정 클릭  3) 퍼블릭 Access 권한 설정 확인 후 공개 권한 삭제 클릭		



4) 퍼블릭 Access 삭제 버튼 클릭

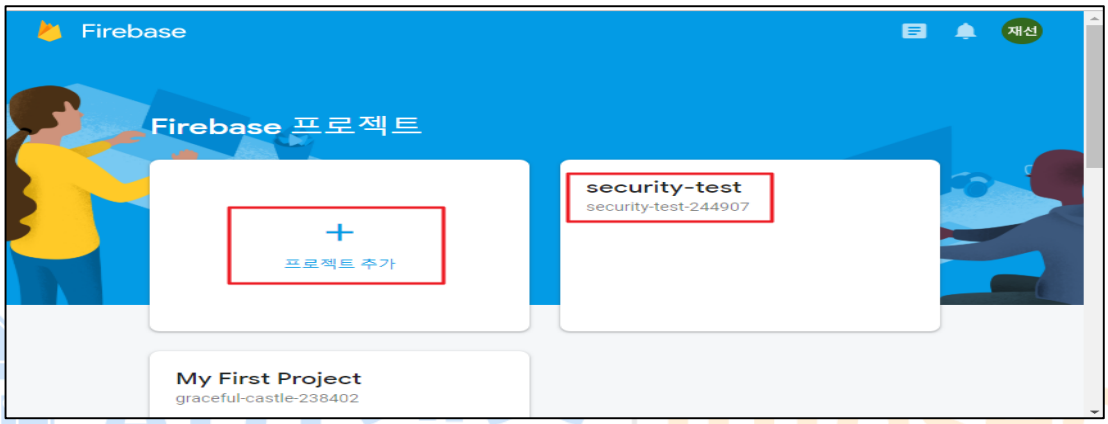
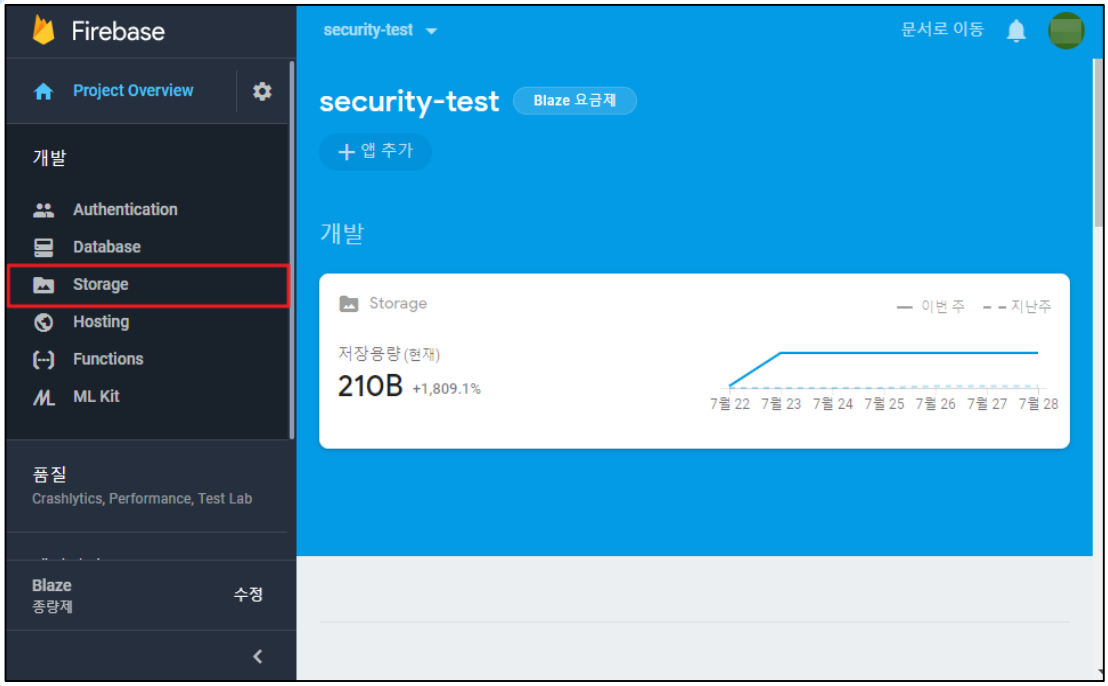


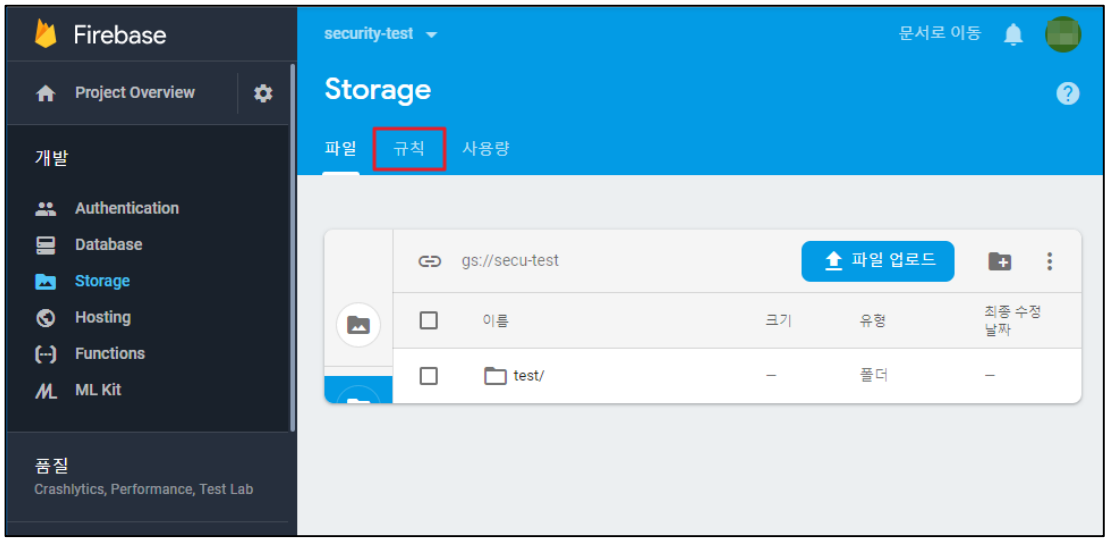
5) 퍼블릭 Access 권한 삭제 완료

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단 기준</td><td>양호기준
: Storage 버킷 내 불필요한 공개 액세스 설정이 되어 있지 않은 경우

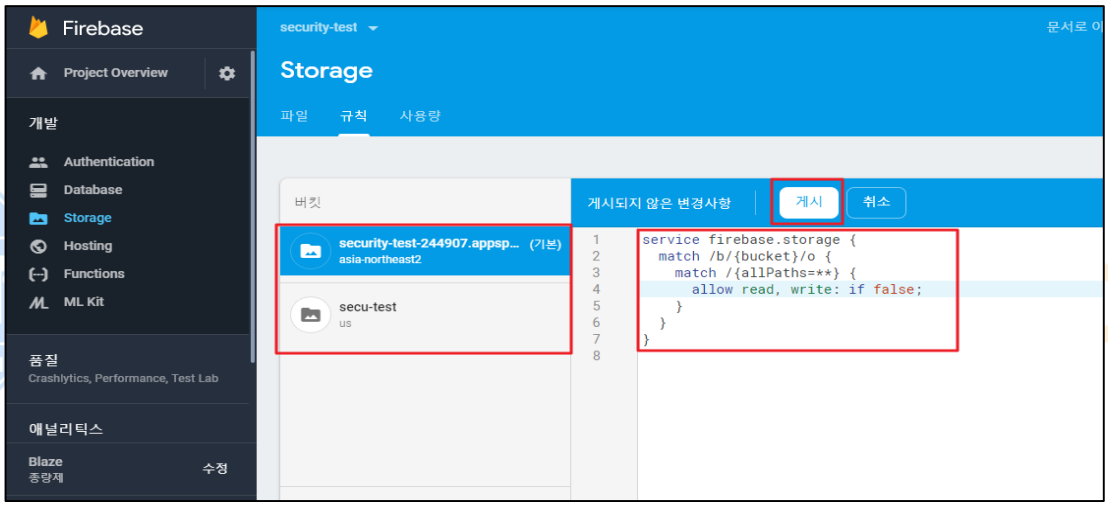
취약기준
: Storage 버킷 내 불필요한 공개 액세스 설정이 되어 있는 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

1.15 Firebase Storage 규칙 설정

분류	인증/인가	중요도	중
항목명	Firebase Storage 규칙 설정		
항목 설명	Firebase Storage는 모바일 및 웹 애플리케이션 개발 플랫폼으로서 사진, 동영상 등의 사용자 제작 콘텐츠를 저장하고 제공하며 Cloud Storage용 Firebase SDK를 사용하여 모바일 및 웹 앱에 대한 속성 기반의 세부적인 액세스제어를 제공합니다. 예를 들어, 객체를 업로드 또는 다운로드 할 수 있는 사용자, 객체의 최대 크기, 객체를 다운로드 할 수 있는 시기를 지정할 수 있습니다.		
설정 방법	**가. Firebase Storage** 1) Firebase 프로젝트 추가  2) Storage 추가  3) 규칙 설정		

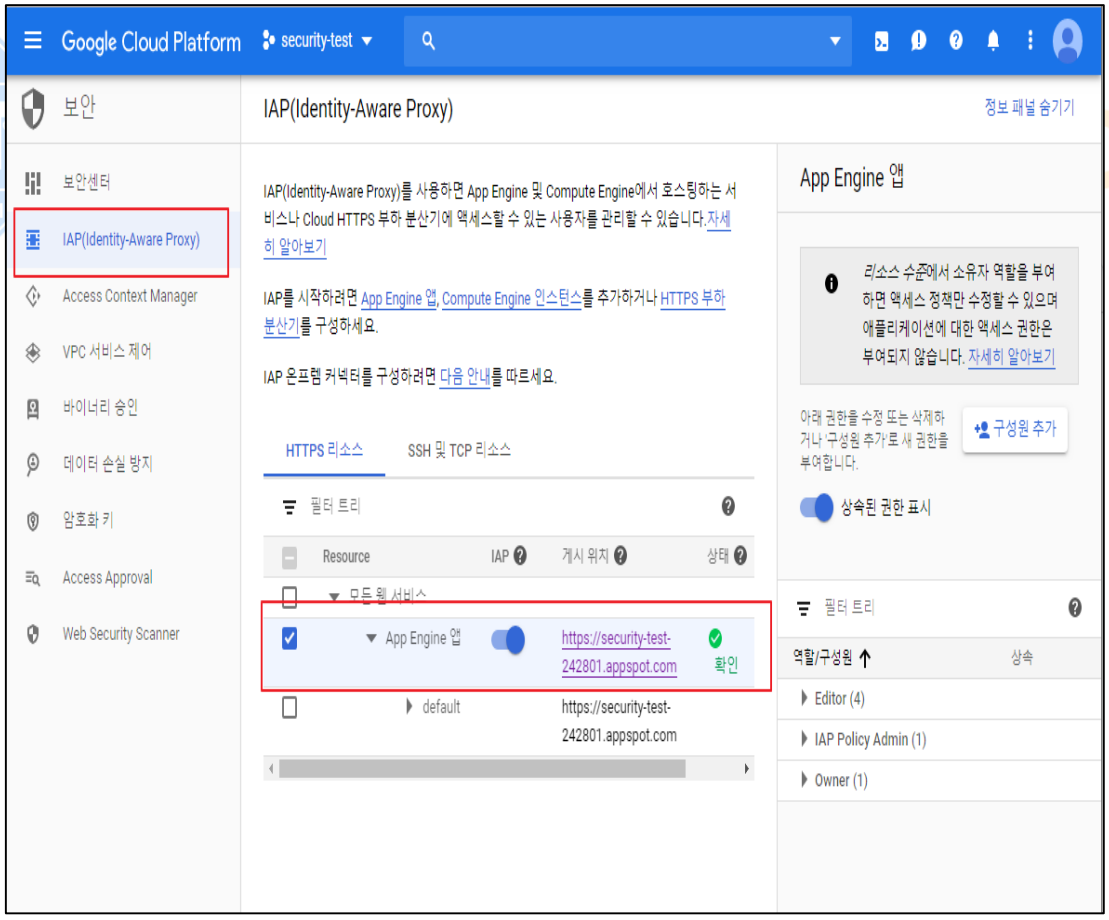


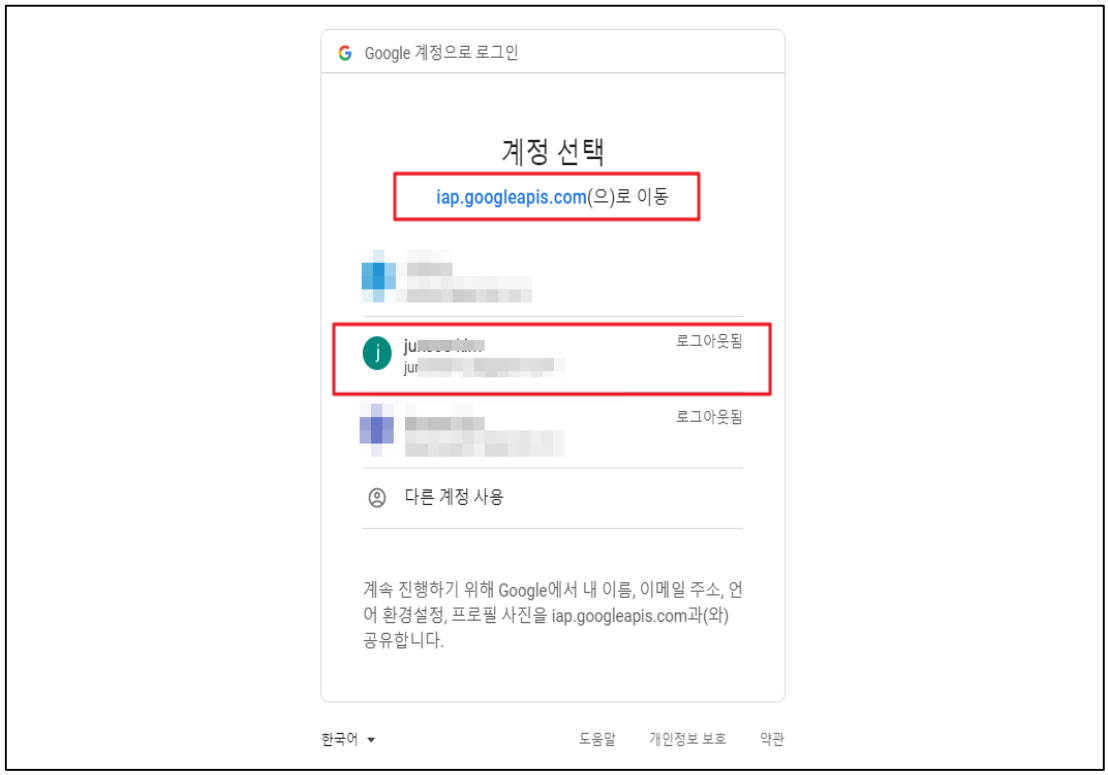
4) 임의의 규칙 설정(모두 공개 제외)



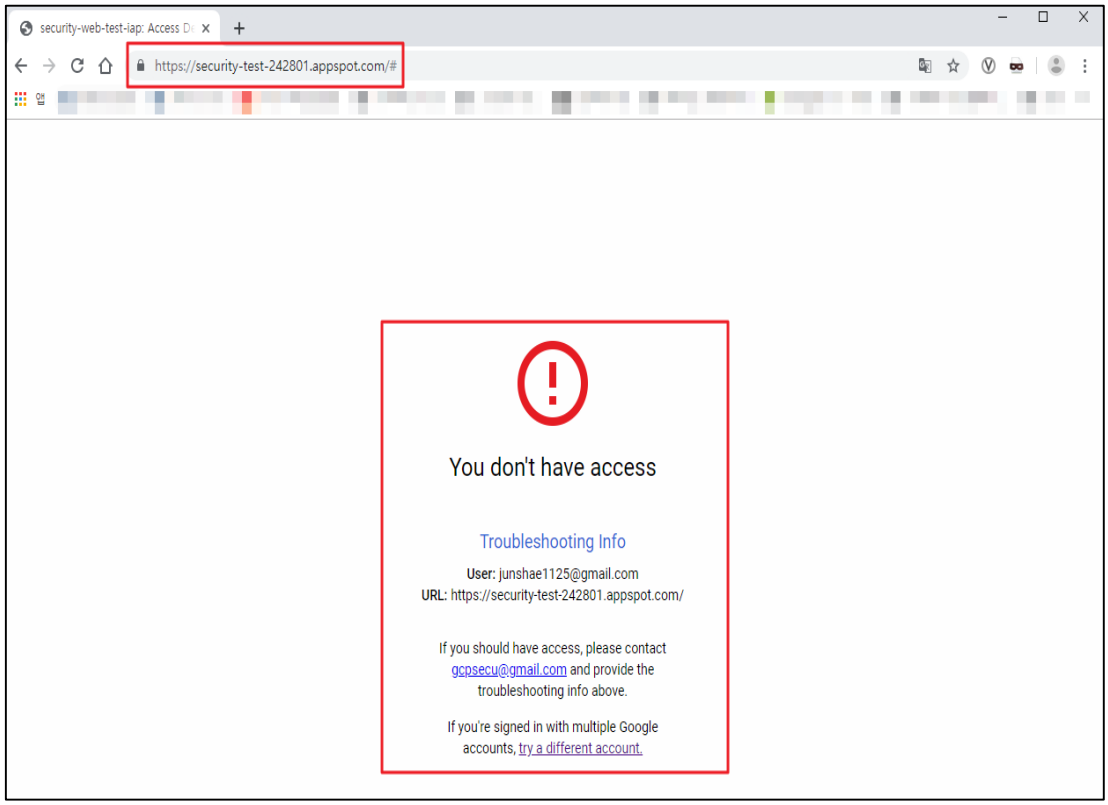
진단 기준	**양호기준** : Firebase Storage 사용 시 규칙이 모두 공개로 설정되어 있지 않은 경우 **취약기준** : Firebase Storage 사용 시 규칙이 모두 공개로 설정되어 있는 경우
비고	

1.16 IAP (Identity-Aware Proxy)

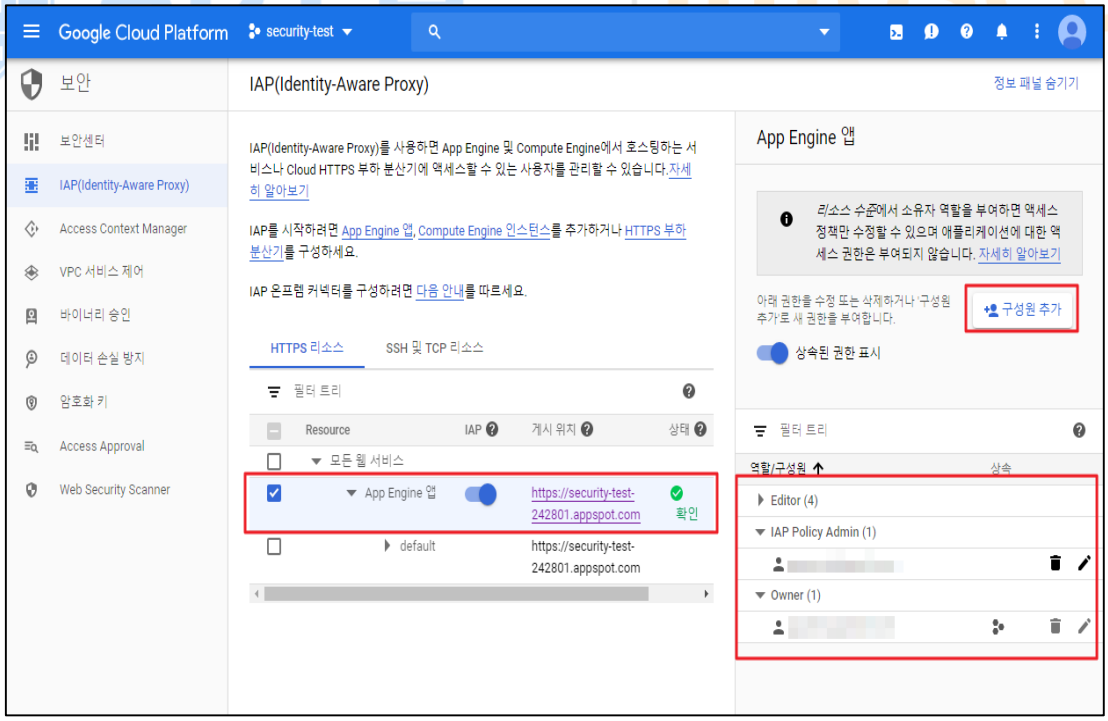
분류	인증/인가	중요도	하
항목명	IAP (Identity-Aware Proxy)		
항목 설명	App Engine 표준 환경, App Engine 가변형 환경, Compute Engine, GKE에서 실행 중인 애플리케이션에 대한 액세스를 관리할 수 있습니다. Cloud IAP는 HTTPS로 액세스되는 애플리케이션의 중앙 승인 레이어를 설정하므로, 개발자가 네트워크 수준의 방화벽을 사용하는 대신 애플리케이션 수준의 제어 모델을 채택할 수 있습니다. Cloud IAP를 사용할 때는 앱 보호를 위해 서명된 헤더 또는 App Engine 표준 환경 사용자 API도 사용해야 합니다. Cloud IAP는 GCP 프로젝트에서 개별 리소스에 대한 Cloud IAP 정책을 구성할 수 있으며, 한 프로젝트 내의 여러 앱은 각기 서로 다른 액세스 정책을 가질 수 있습니다. 해당하는 부분으로는 Compute Engine, App Engine 등의 앱이 있는 프로젝트가 포함됩니다.		
설정 방법	**가. Cloud IAP (Identity-Aware Proxy) 사용설정** 1) [보안] > [IAP(Identity-Aware Proxy)] - 추가하려는 사용자의 권한 확인을 위한 웹 서비스 접근 시도  2) [Google 계정 로그인] - IAP가 적용된 서비스 접근 시도 시 사용자 계정 확인		



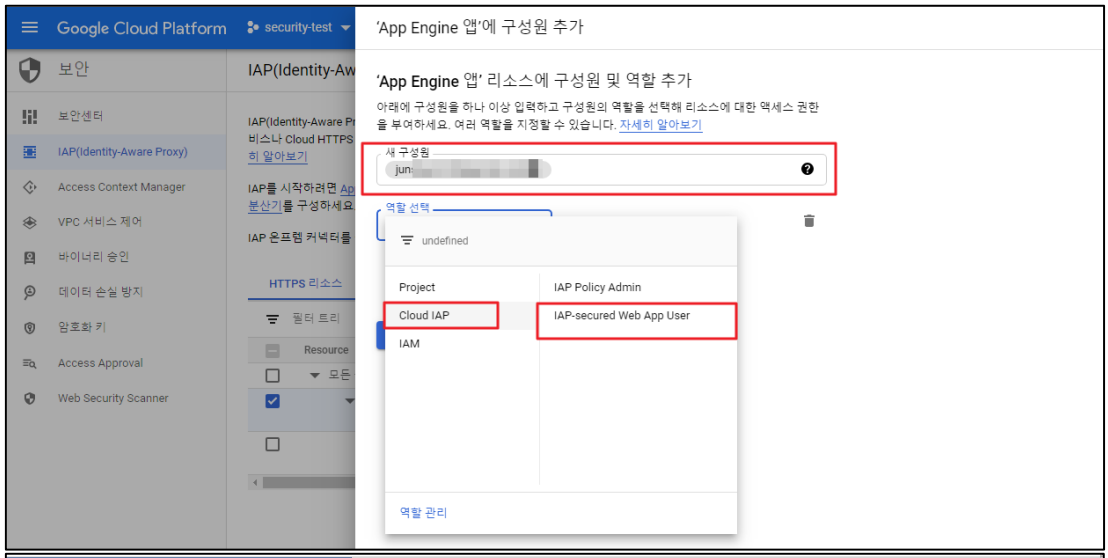
3) 로그인 사용자 웹 서비스에 대한 접근 권한 부재 확인

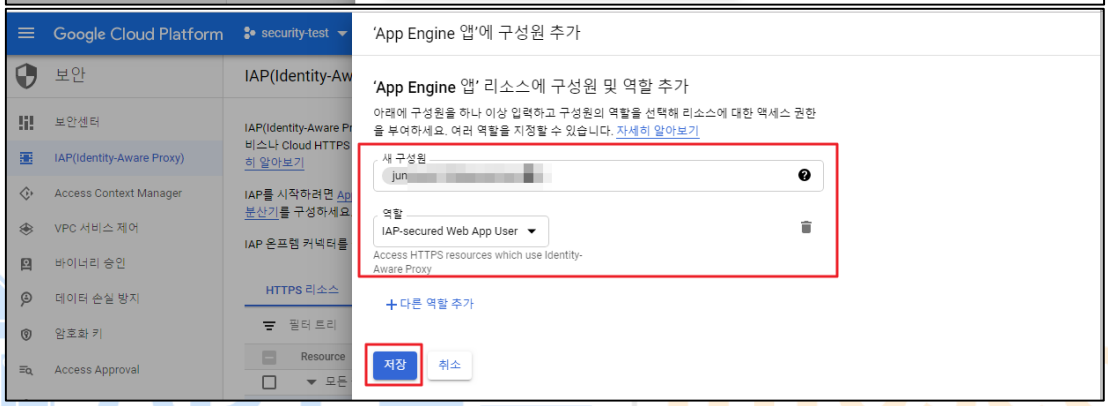


4) [보안] > [IAP(Identity-Aware Proxy] > [리소스 선택] > [구성원 추가]
- 이용하고자 하는 웹 서비스(리소스) 내 사용자 역할 및 구성원 정보 확인

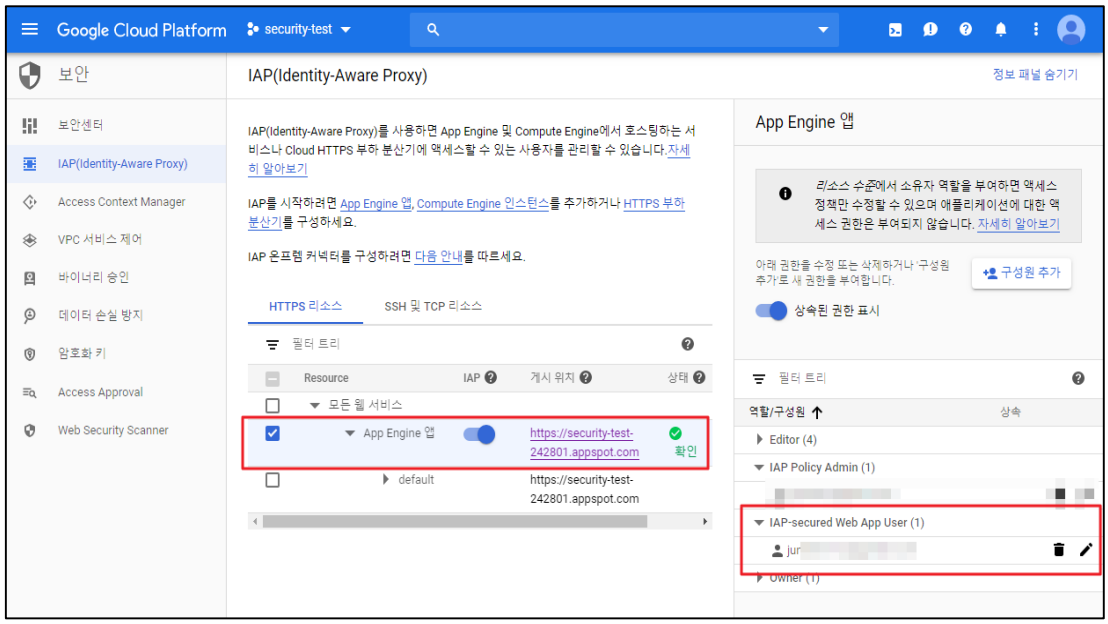


5) 새 구성원 검색 및 역할 할당

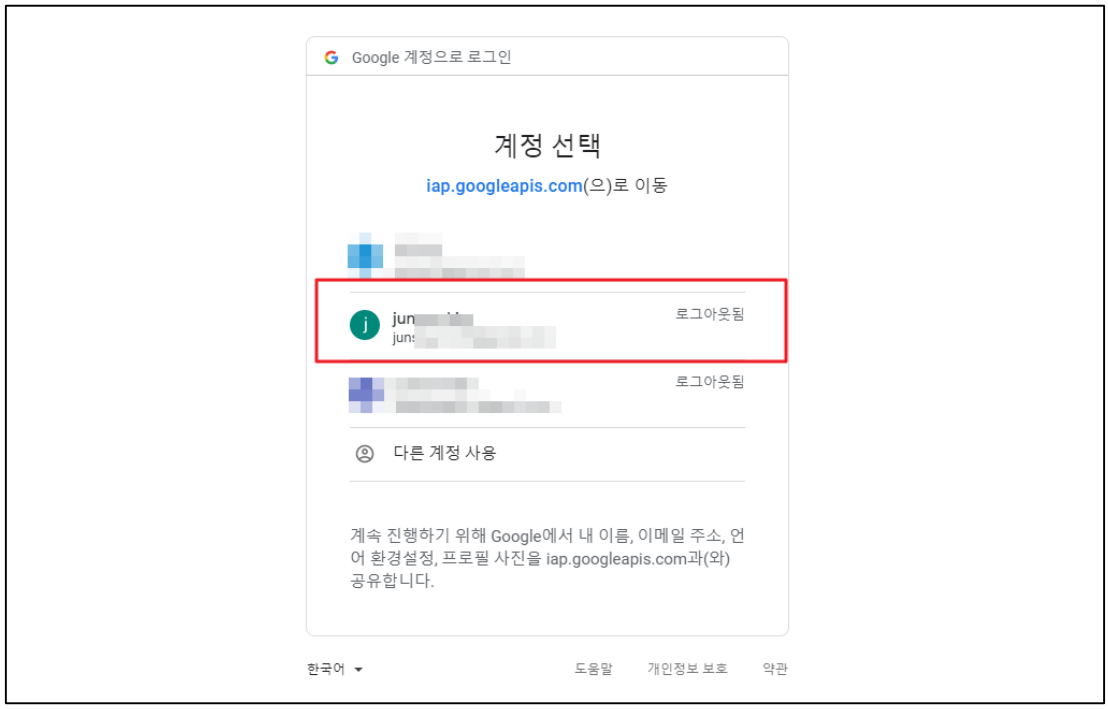


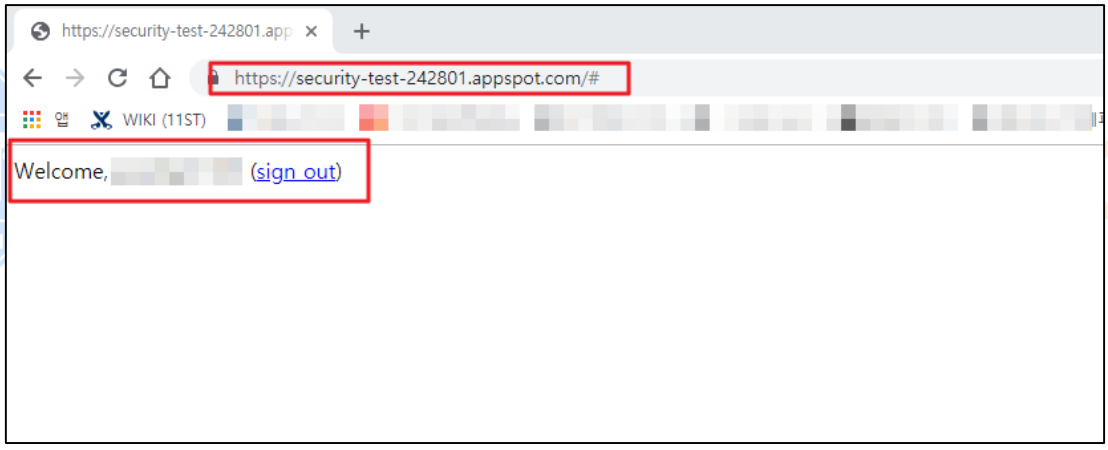


6) 추가된 사용자 계정/역할 확인 및 웹 서비스 재접근 시도



7) 추가된 사용자 서비스 정상 접근 확인





진단 기준	**양호기준** : 활성화 된 IAP 내 역할에 맞지 않는 비인가자 계정이 존재하지 않을 경우 **취약기준** : 활성화 된 IAP 내 역할에 맞지 않는 비인가자 계정이 존재할 경우
비고	

2. 데이터 보안

2.1 Compute Engine 디스크 암호화

<table>
<tr><td>분류</td><td>데이터 보안</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">Compute Engine 디스크 암호화</td></tr>
<tr><td>항목
설명</td><td colspan="3">Compute Engine 은 데이터가 인스턴스 외부에서 영구 디스크 저장소 공간으로 이동하기 전에 데이터를 자동으로 암호화합니다. 각 영구 디스크는 시스템 정의 키 또는 고객 제공 키를 사용하여 암호화된 상태로 유지됩니다. 또한, Google 은 사용자가 제어하지 않는 방식으로 영구 디스크 데이터를 여러 물리적 디스크에 분산시킵니다. 디스크 암호화에 사용되는 암호화 키는 Google 관리, 고객 제공, 고객 관리 등으로 나뉘어져 있습니다.

기본적으로 Compute Engine 은 모든 데이터를 암호화하여 저장하고 있으며, 사용 가능한 암호화 키로 "Google 관리 키", "고객 관리 키", "고객 제공 키"를 제공하고 있습니다. 기업 정책 및 내부 구성에 부합하는 암호화 키를 사용하여 저장 데이터를 안전하게 보호해야 합니다.

또한, "고객 관리 키"를 사용하는 경우 키에 대한 순환 주기를 설정하고, "고객 제공 키"를 사용하는 경우 암호화 키의 주기적 변경을 통해 키 유출 및 사용자 접근에 대한 보안 위협을 미연에 방지 할 수 있습니다.

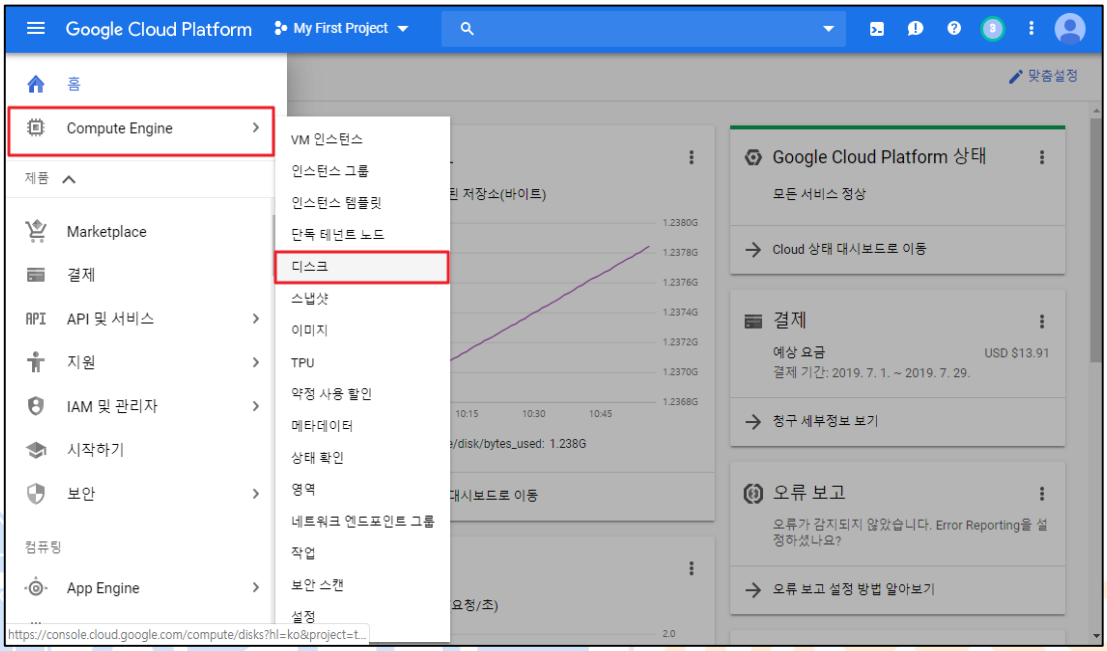
※ 암호화 키 방식
<table>
<tr><th>암호화 키</th><th>상세내용</th></tr>
<tr><td>Google 관리 암호화 키</td><td>Google 관리 암호화 키는 'Cloud Storage'에 데이터를 디스크에 쓰기 전에 서버 측에서 항상 암호화를 수행하며 추가 비용은 청구되지 않는 기능입니다. 암호화 방식은 AES-256 을 사용하여 저장된 사용자 데이터를 암호화합니다.</td></tr>
<tr><td>고객 제공 암호화 키</td><td>고객 제공 암호화 키는 표준 Base64 로 인코딩된 자체 AES-256 키를 추가로 제공됩니다. 고객 제공 암호화 키를 사용하는 경우'Cloud Storage'는 해당 키를 Google 서버에 영구적으로 저장하거나 키를 달리 관리하지 않습니다. 다만 사용자가 각'Cloud Storage' 작업에 키를 제공할 수 있으며, 작업이 완료되면 Google 서버에서 키가 삭제 됩니다.</td></tr>
<tr><td>고객 관리 암호화 키</td><td>고객 관리 암호화 키는 Google 관리 암호화 키에 Cloud Key Management Service 에서 생성한 키를 추가로 사용할 수 있는 키입니다. 고객 관리 암호화 키를 사용하면 암호화 키는 Cloud KMS 안에 저장됩니다.
Cloud KMS 는 클라우드에서 호스팅되는 키 관리 서비스로서 온프레미스와 동일한 방식으로 클라우드 서비스의 암호화 키를 관리할 수 있습니다. AES-256, RSA 2048, RSA 3072, RSA 4096,</td></tr>
</table>
</td></tr>
</table>

	EC P256, EC P384 암호화 키를 생성, 사용, 회전, 폐기할 수 있습니다. Cloud KMS 는 Cloud IAM 및 Cloud Audit Logging 과 통합되어 개별 키의 권한을 관리하고 어떻게 사용되는지 모니터링할 수 있습니다.

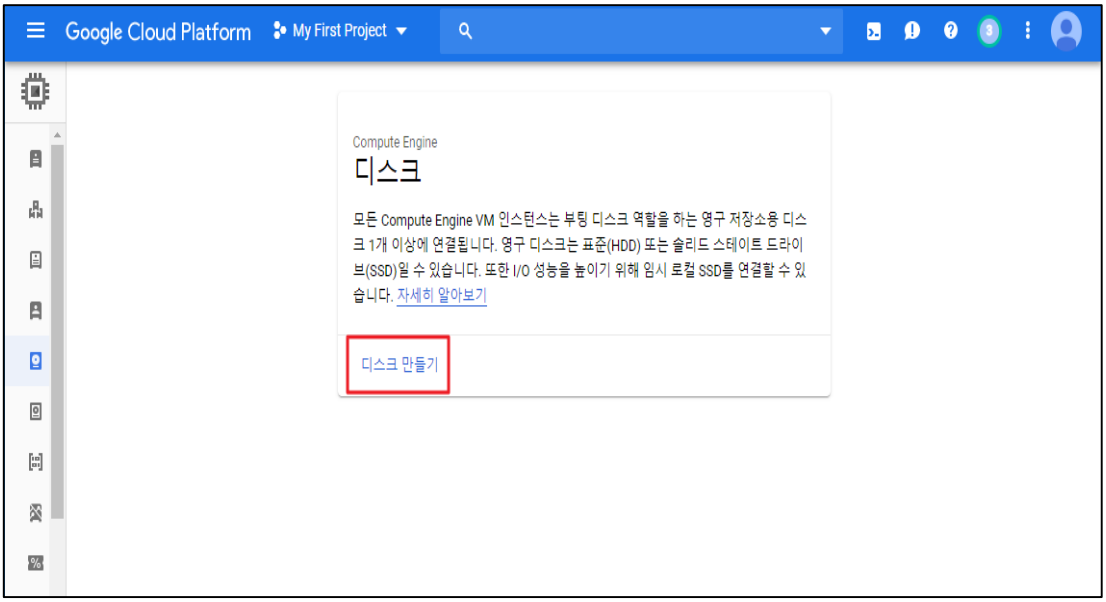
설정 방법

가. 디스크 암호화키 설정

1) [메인] > [Compute Engine] > [디스크]

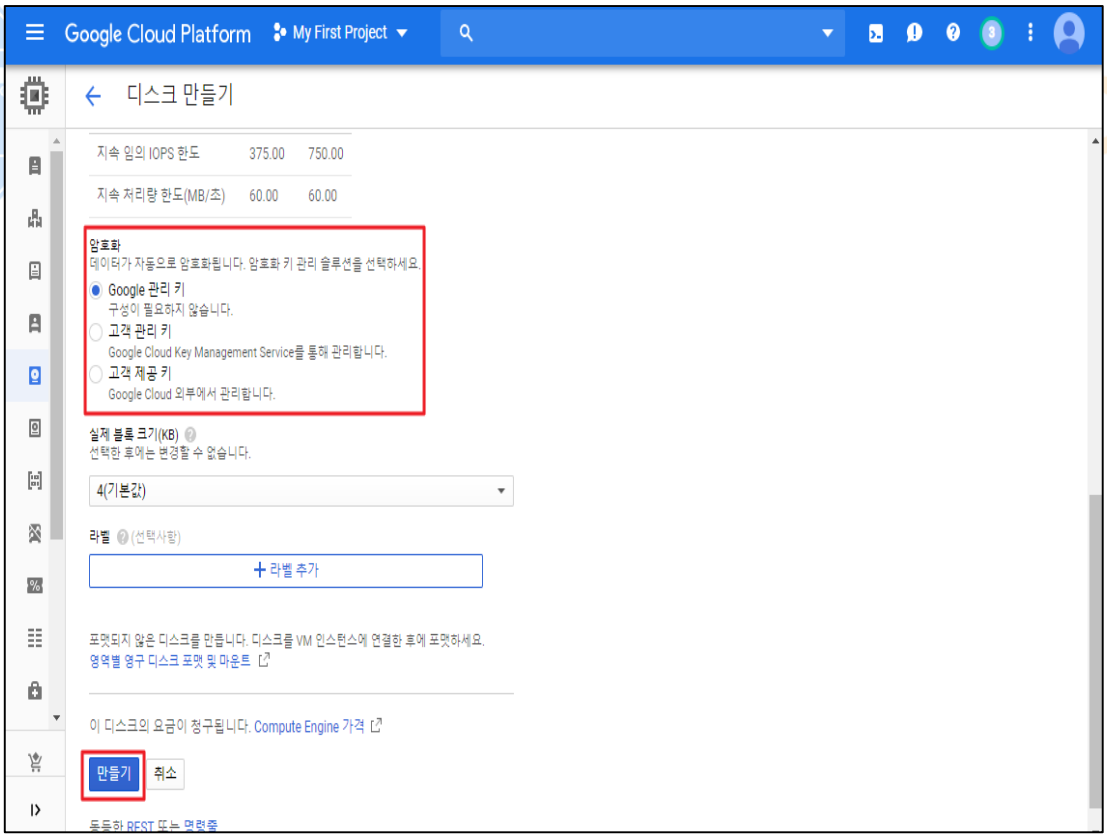


2) 디스크 만들기

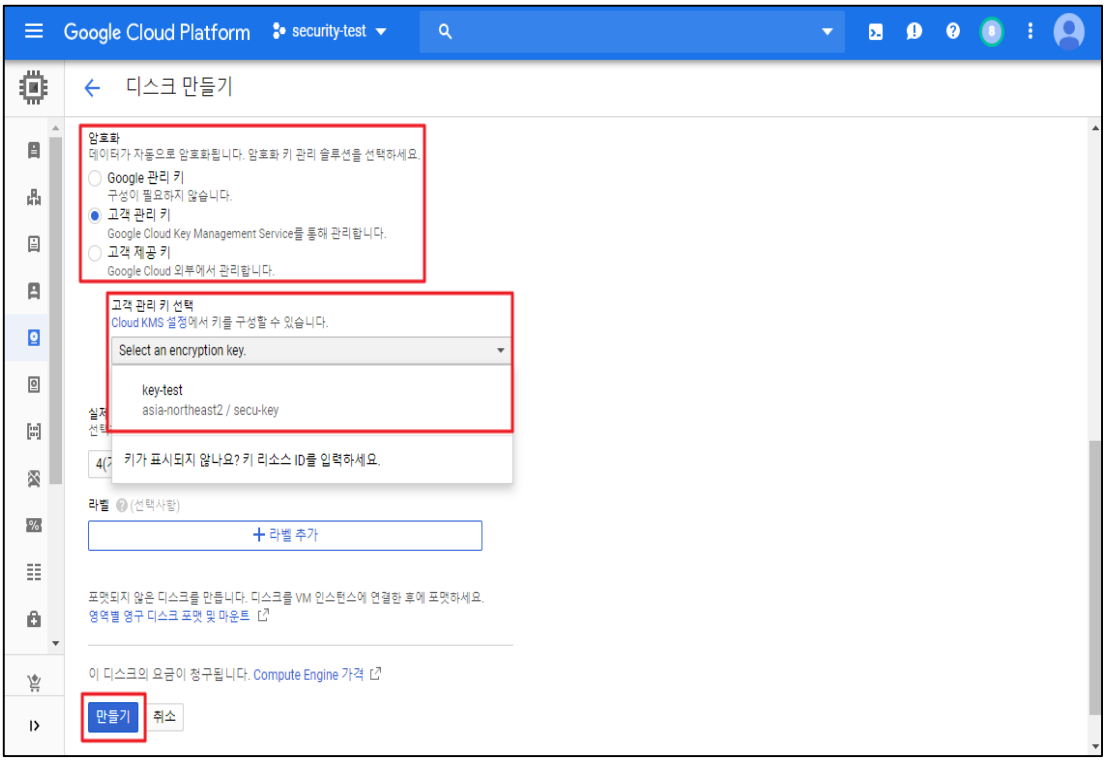


3) 디스크 정보 입력 및 리전 선택

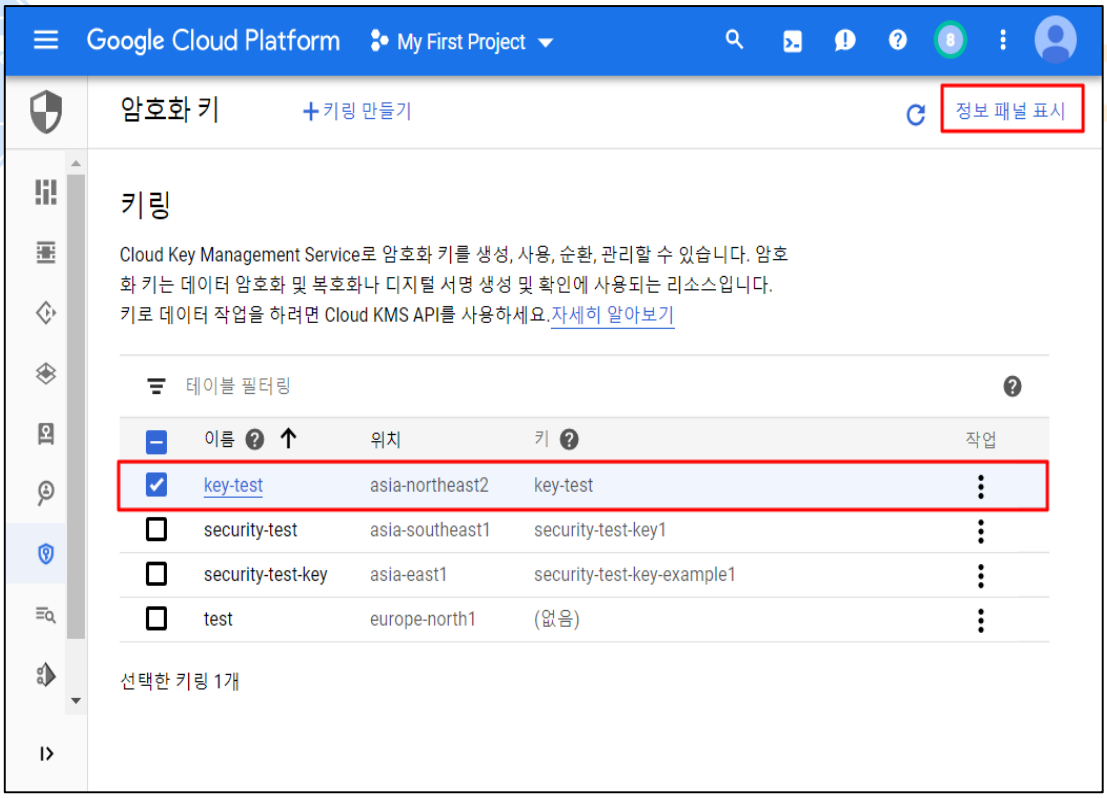
4) 'Google 관리 키' 암호화 방식 설정



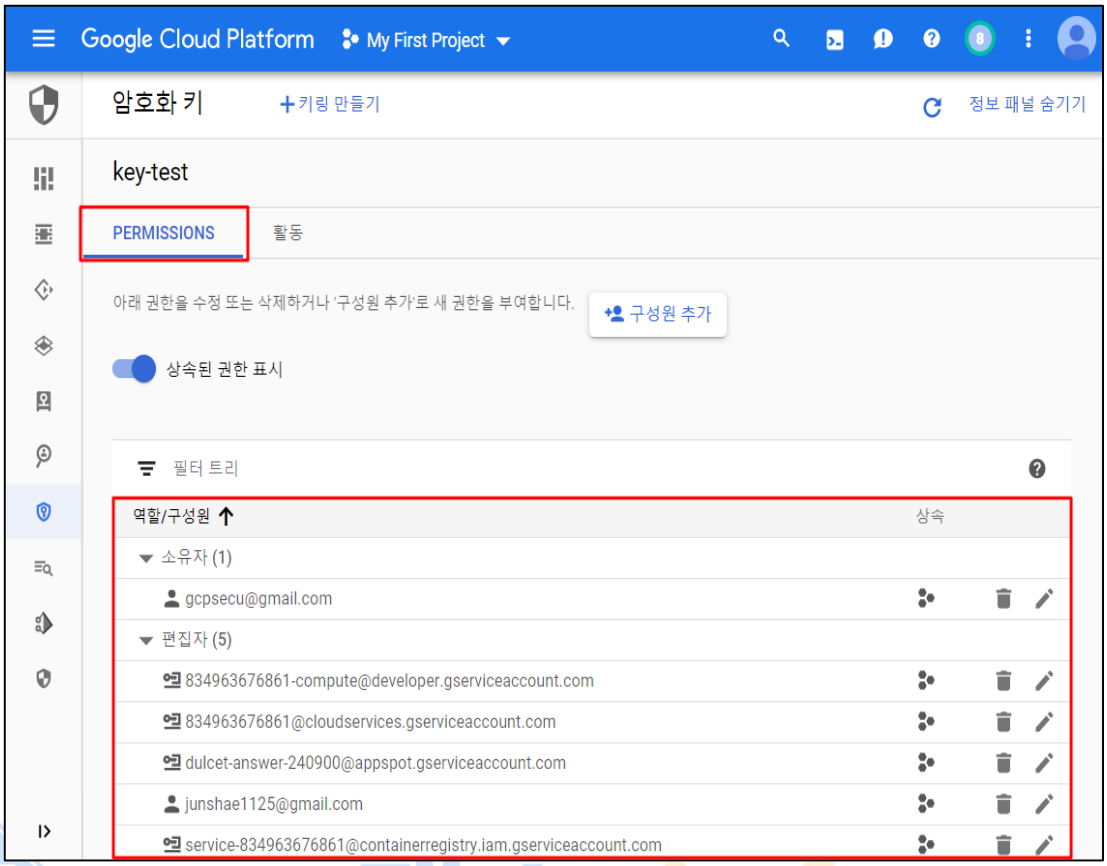
5) '고객 관리 키' 암호화 방식 설정



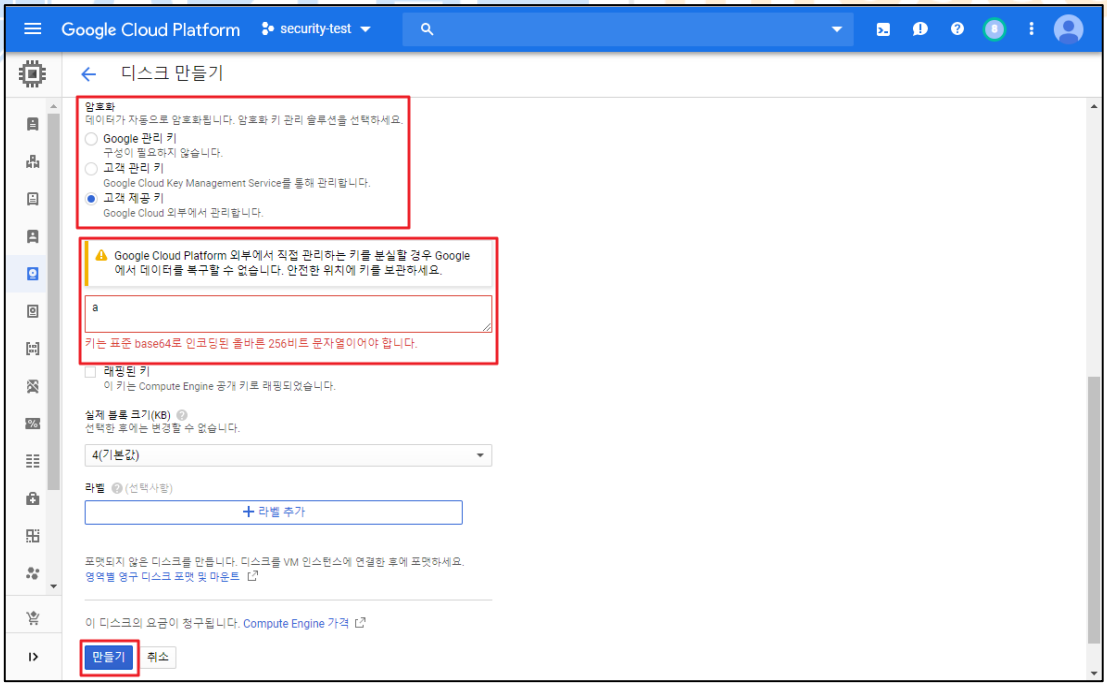
6) KMS 접근 후 사용 할 '고객 관리 키' 정보 패널 표시



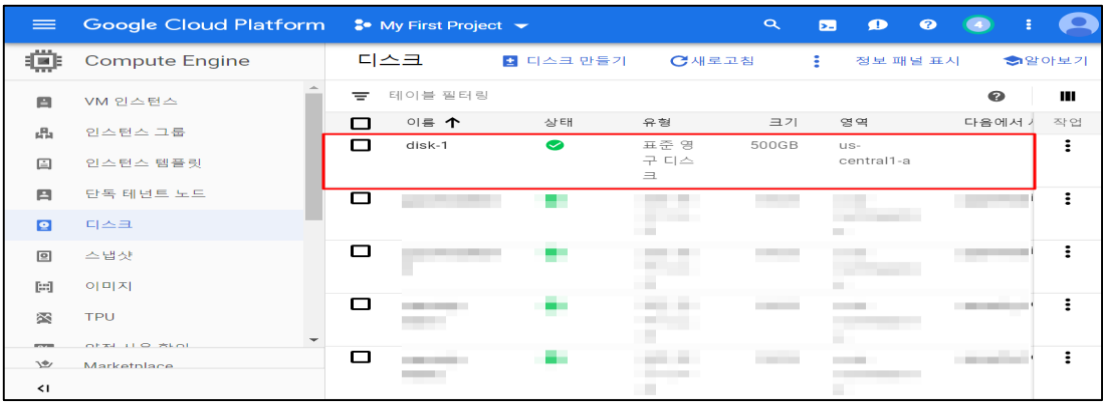
7) 키에 대한 접근 권한 확인



8) '고객 제공 키' 암호화 방식 설정 (256비트 키 사용)



9) 암호화된 디스크 생성 완료

	
진단 기준	**양호기준** : "고객 관리 키" 사용 시 키에 대한 순환 주기 설정이 되어 있을 경우 **취약기준** : "고객 관리 키" 사용 시 키에 대한 순환 주기 설정이 되어있지 않을 경우
비고	진단기준에서 하나라도 기준에 맞지 않는 설정을 보유하고 있을 경우 취약으로 간주함

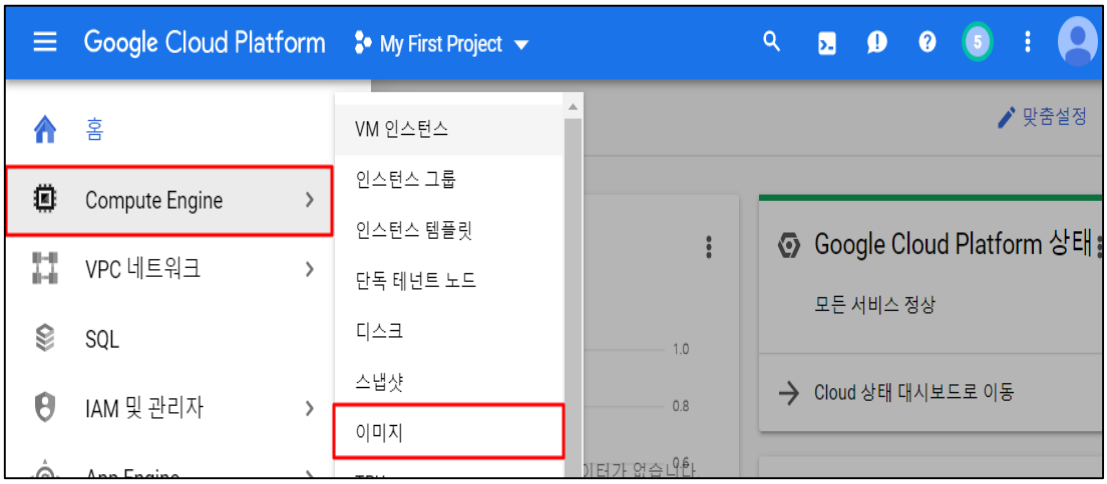
2.2 Compute Engine 이미지 암호화

<table>
<tr><td>분류</td><td>데이터 보안</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">Compute Engine 이미지 암호화</td></tr>
<tr><td>항목
설명</td><td colspan="3">Compute Engine 내 이미지는 변경할 수 없는 디스크에 대한 참조를 제공하는 클라우드 리소스로서, 운영체제(OS) 이미지를 이용하여 인스턴스의 부팅 디스크를 만드는데 사용되며, Compute Engine의 모든 디스크는 기본적으로 Google의 암호화 키를 사용하여 암호화됩니다. 디스크에서 빌드된 이미지도 암호화됩니다. 또는 디스크를 만들 때 자체 암호화 키를 제공할 수도 있습니다. 디스크를 만든 다음 이미지 생성 명령어에 암호화 키를 제공하여 암호화된 이미지를 만들 수 있습니다. 이미지는 아래 두가지 방식으로 생성이 가능합니다.

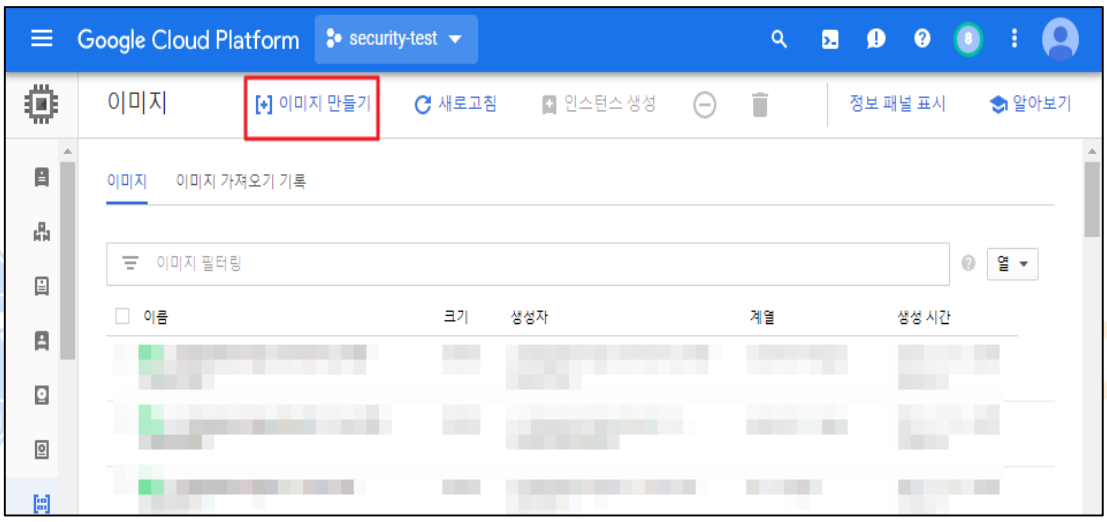
기본적으로 Compute Engine 은 생성된 이미지를 암호화 하여 저장하고 있으며, 사용 가능한 암호화 키로 "Google 관리 키", "고객 관리 키", "고객 제공 키"를 제공하고 있습니다. 기업 정책 및 내부 구성에 부합하는 암호화 키를 사용하여 저장 데이터를 안전하게 보호해야 합니다.

또한, "고객 관리 키"를 사용하는 경우 키에 대한 순환 주기를 설정하고, "고객 제공 키"를 사용하는 경우 암호화 키의 주기적 변경을 통해 키 유출 및 사용자 접근에 대한 보안 위협을 미연에 방지 할 수 있습니다.

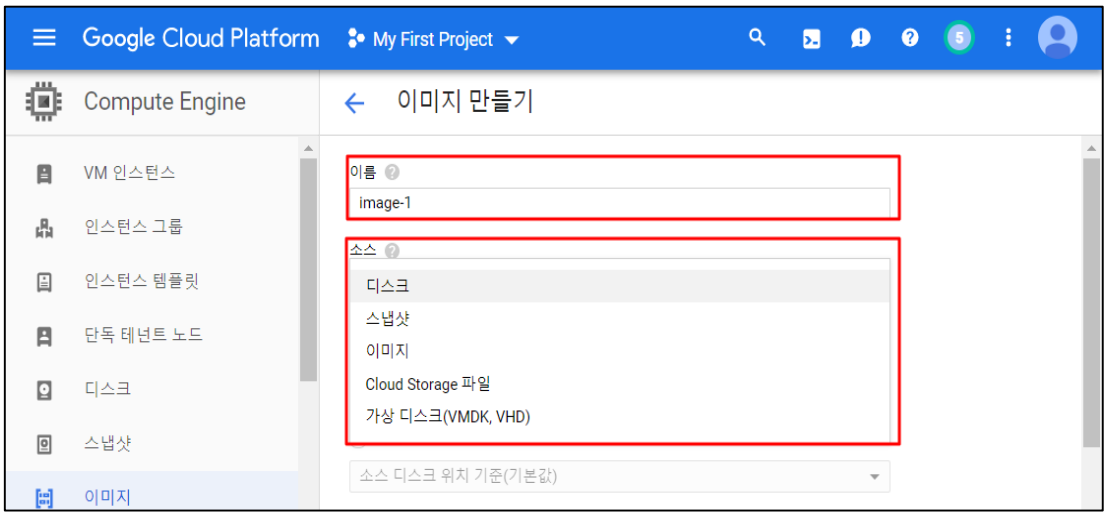
※ 이미지 생성 방식
<table>
<tr><th>이름</th><th>상세내용</th></tr>
<tr><td>공개 이미지</td><td>공개 이미지는 Google, 오픈소스 커뮤니티, 제3자 공급업체에서 제공하고 관리합니다. 기본적으로 모든 프로젝트에서 이러한 이미지에 액세스할 수 있으며 이를 사용하여 인스턴스를 만들 수 있으며 Google은 정기적으로 또는 중요한 영향을 주는 CVE 패치를 사용할 수 있을 때 공개 이미지를 업데이트합니다.</td></tr>
<tr><td>커스텀 이미지</td><td>커스텀 이미지는 사용자의 프로젝트에서만 사용할 수 있습니다. 부팅 디스크 및 다른 이미지에서 커스텀 이미지를 생성한 다음 해당 커스텀 이미지를 사용하여 인스턴스를 만들 수 있습니다.</td></tr>
</table>
</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. 이미지 암호화키 설정
1) [메인] > [Compute Engine] > [이미지]</td></tr>
</table>



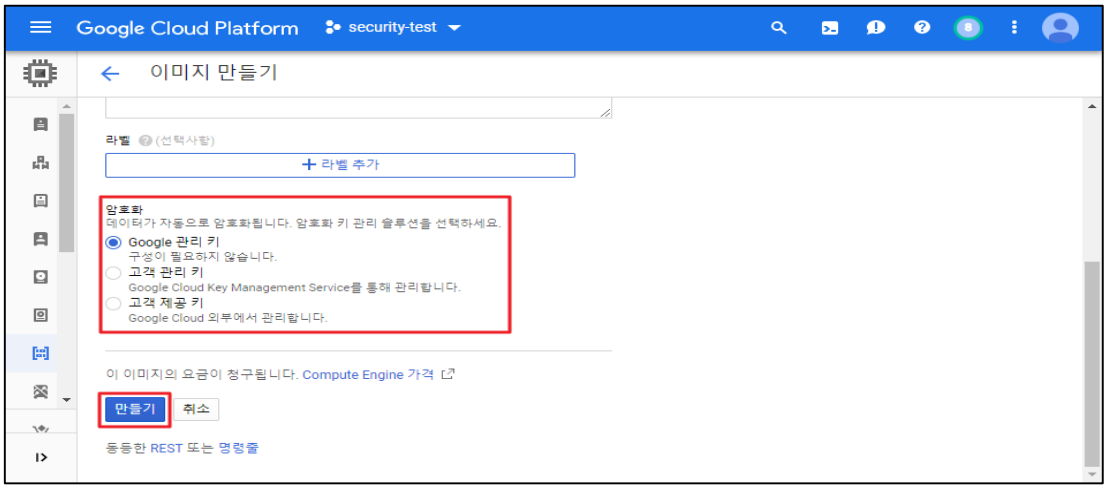
2) 이미지 만들기



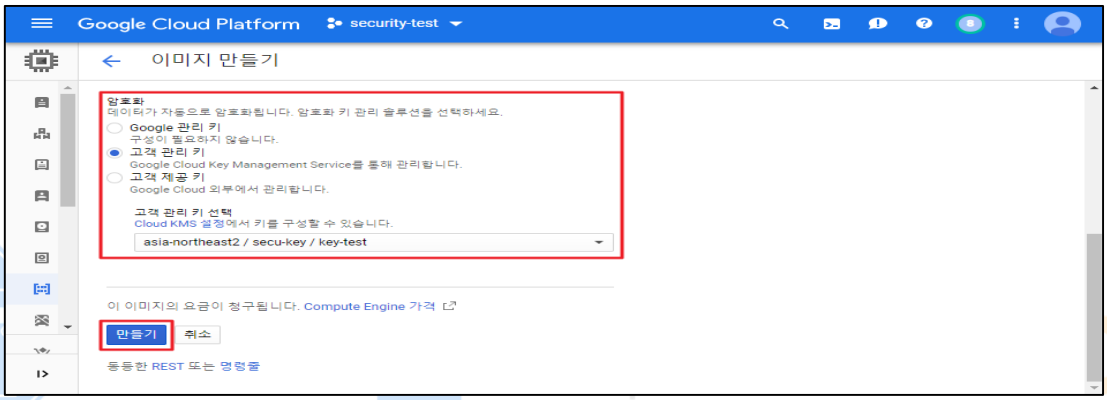
3) 이미지 정보 및 생성할 소스 대상 선택



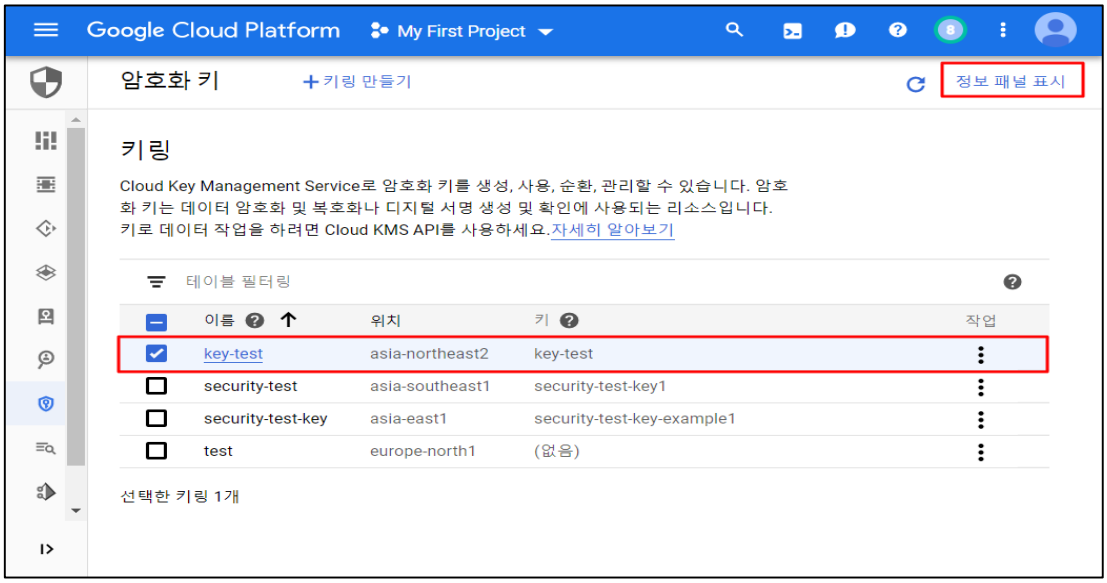
4) 'Google 관리 키' 암호화 방식 설정



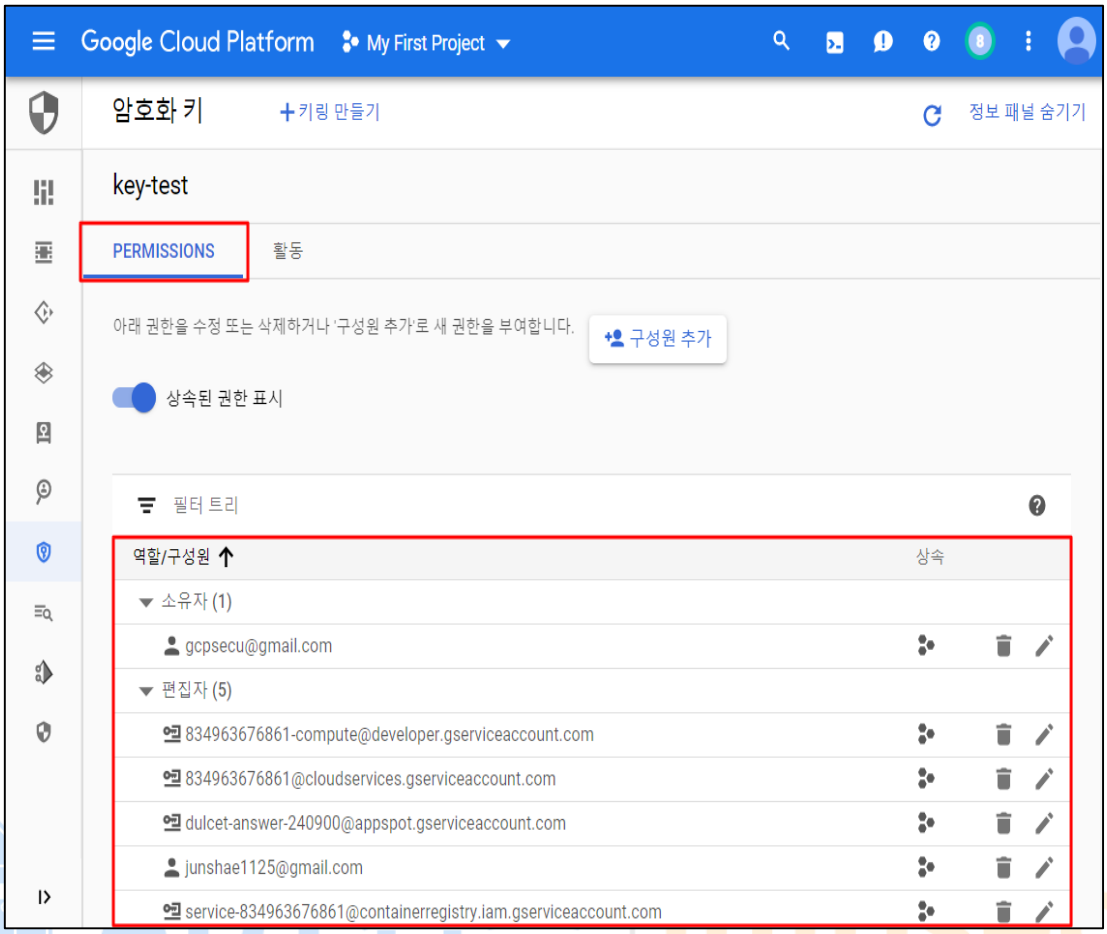
5) '고객 관리 키' 암호화 방식 설정



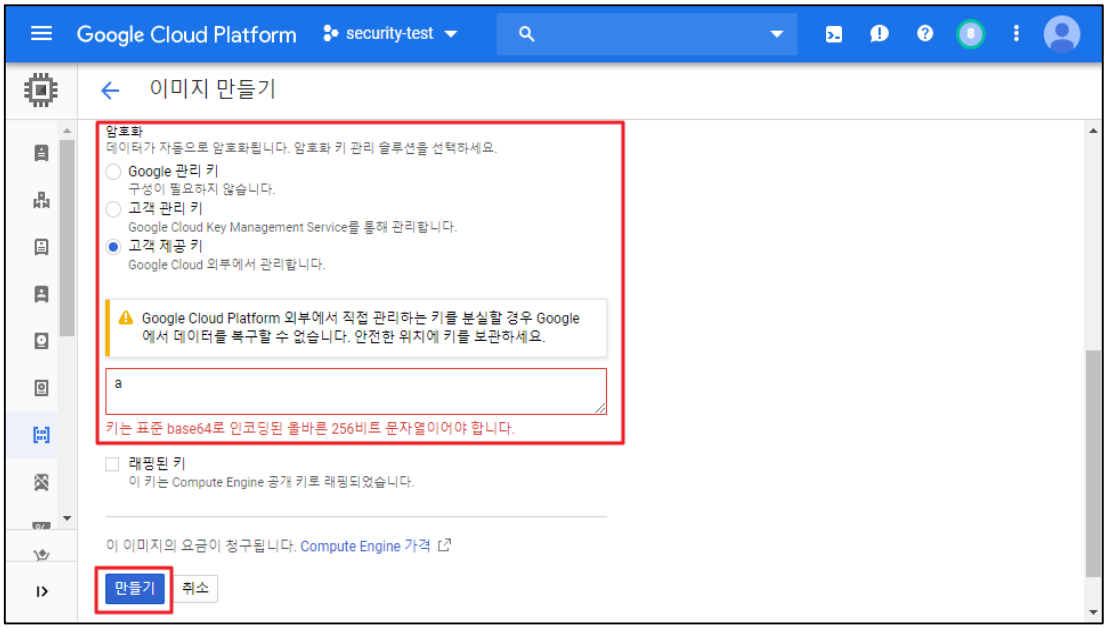
6) KMS 접근 후 사용 할 '고객 관리 키' 정보 패널 표시



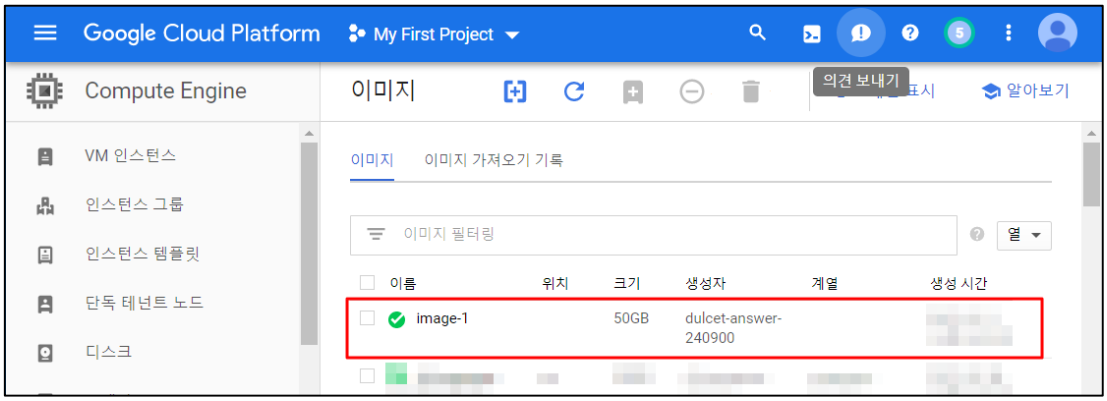
7) 해당 키에 대한 접근 권한 확인



8) '고객 제공 키' 암호화 방식 설정 (256비트 키 사용)



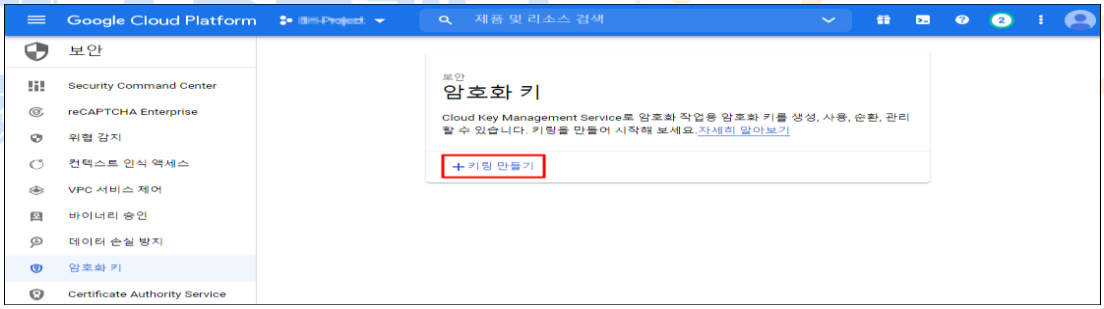
9) 암호화된 이미지 생성 완료

	
진단 기준	**양호기준** : "고객 관리 키" 사용 시 키에 대한 순환 주기 설정이 되어 있을 경우 **취약기준** : "고객 관리 키" 사용 시 키에 대한 순환 주기 설정이 되어있지 않을 경우
비고	

2.3 Cloud SQL 암호화

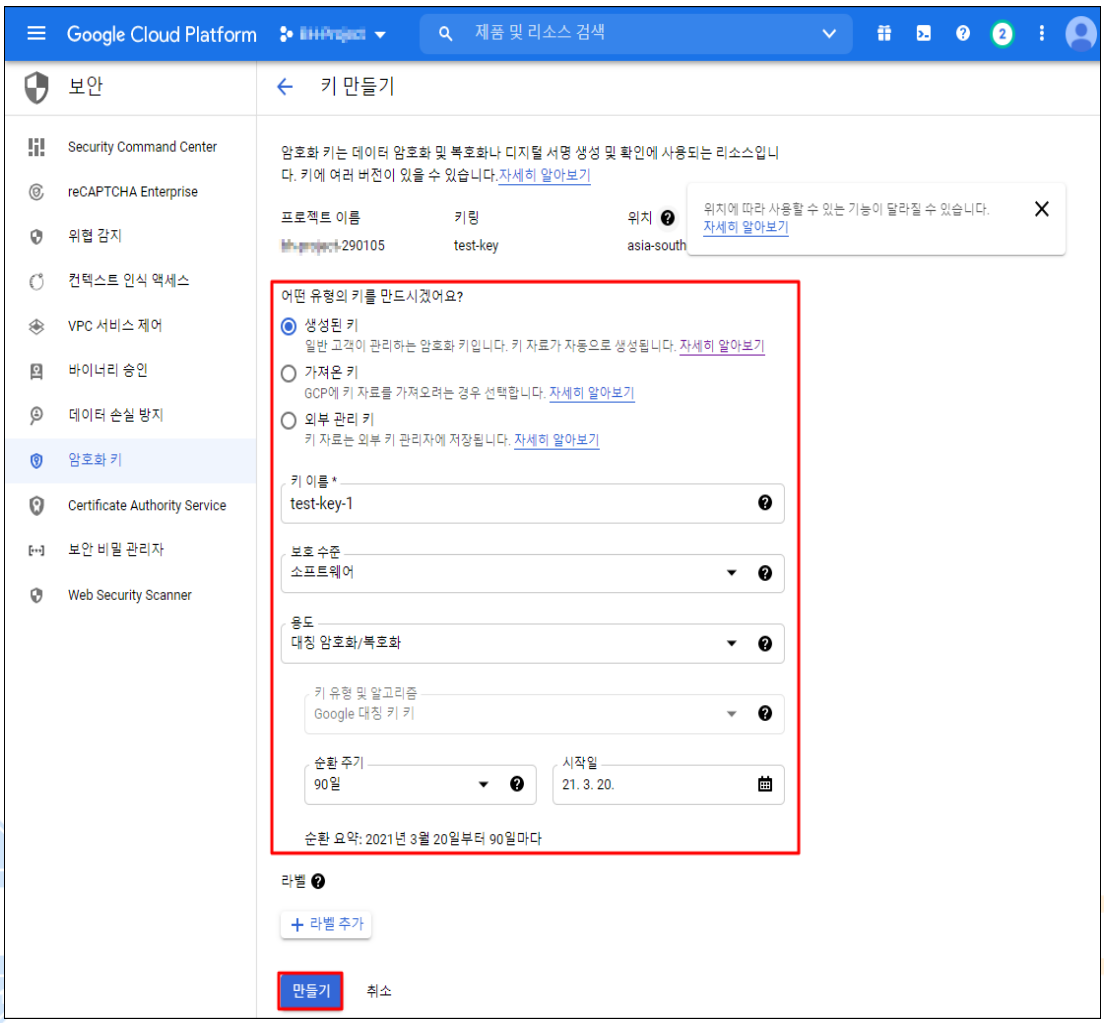
<table>
<tr><td>분류</td><td>데이터 보안</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">Cloud SQL 암호화</td></tr>
<tr><td>항목
설명</td><td colspan="3">기본적으로 Cloud SQL 인스턴스는 모든 데이터를 암호화하여 저장하고 있으며, 사용 가능한 암호화 키로 "Google 관리 키", "고객 관리 키"를 제공하고 있습니다. 기업 정책 및 내부 구성에 부합하는 암호화 키를 사용하여 저장 데이터를 안전하게 보호하는 것을 권고 드립니다.

"고객 관리 키"를 사용하는 경우 키에 대한 순환 주기 설정을 통해 키 유출 및 사용자 접근에 대한 보안 위협을 미연에 방지 할 수 있습니다.

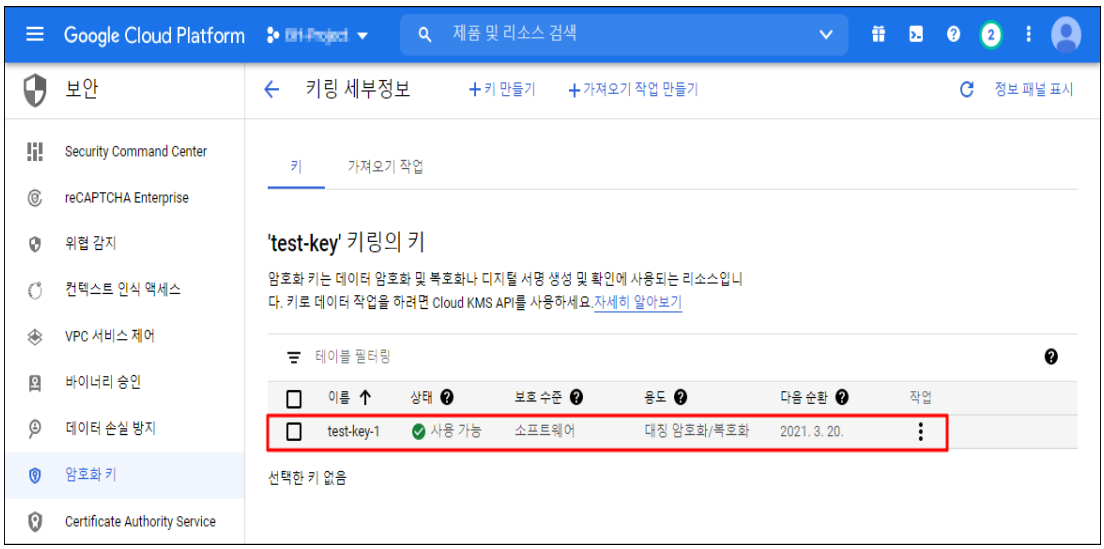
(*) 사용 가능한 암호화 키 종류
<table>
<tr><th>구분</th><th>내용</th></tr>
<tr><td>Google 관리 키</td><td>Google에서 제공하는 자체 암호화 키를 이용하여 데이터 암/복호화</td></tr>
<tr><td>고객 관리 키</td><td>CKMS(Cloud Key Management Service)를 이용하여 암호화 키 관리 및 데이터 암/복호화</td></tr>
</table></td></tr>
<tr><td>설정
방법</td><td colspan="3">가. CKMS(Cloud Key Management Service)를 통한 암호화 키 생성 방법
1) 보안 > 암호화 키 내 키링 만들기 클릭
 

2) 키링 이름 및 키링 위치 설정 후 만들기 클릭
 

3) 생성할 암호화 키의 유형, 이름, 보호 방법, 용도(순환 주기) 설정 후 만들기 클릭</td></tr>
</table>



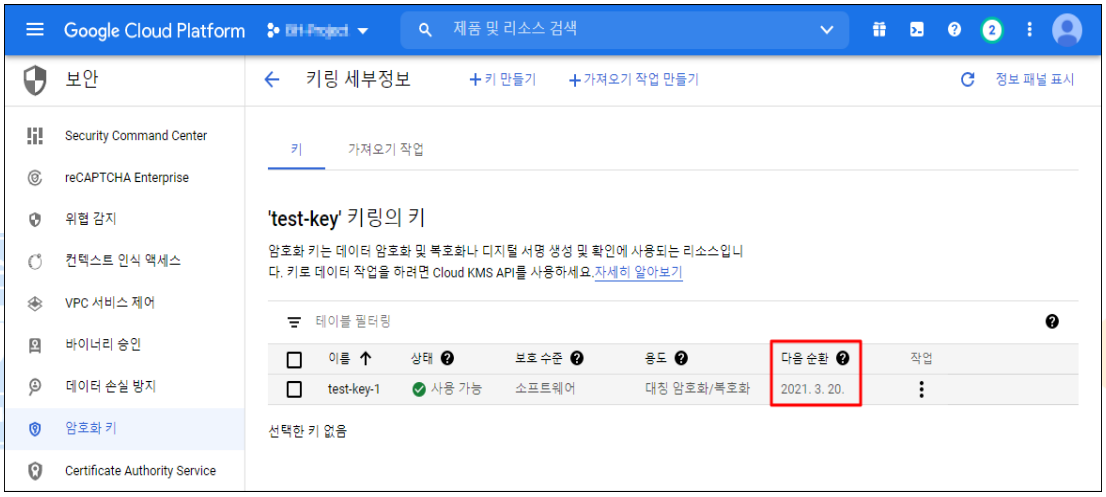
4) 생성된 암호화 키 확인



나. 등록되어 있는 암호화 키 확인 및 순환 주기 설정 확인

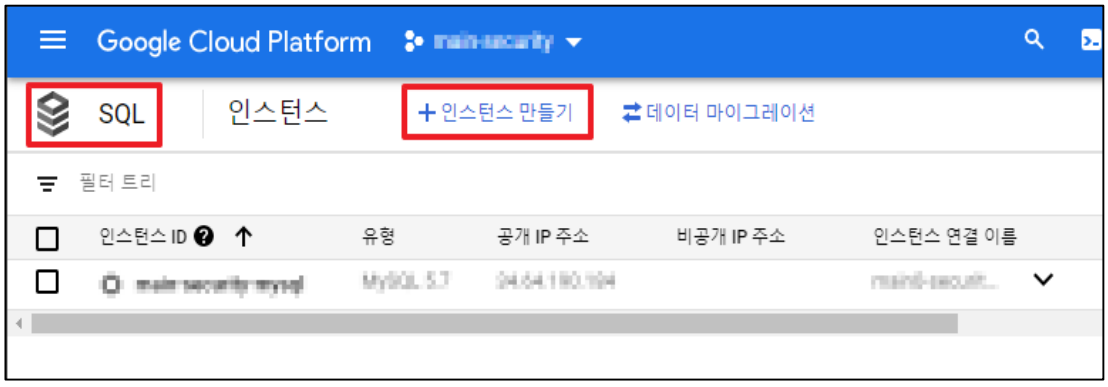
1) 보안 > 암호화 키 내 키링 클릭을 통해 등록되어 있는 암호화 키 확인

2) 보안 > 암호화 키 내 키링 클릭을 통해 순환 주기 설정 확인

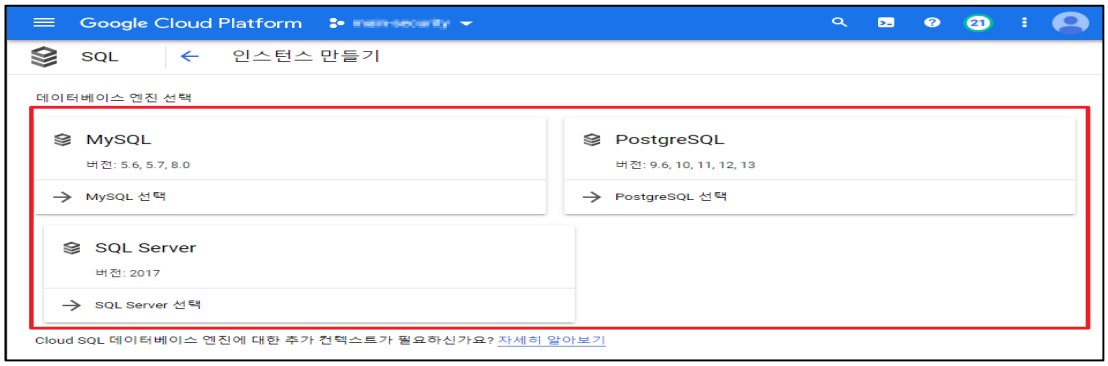


다. Cloud SQL 인스턴스 암호화 설정 방법

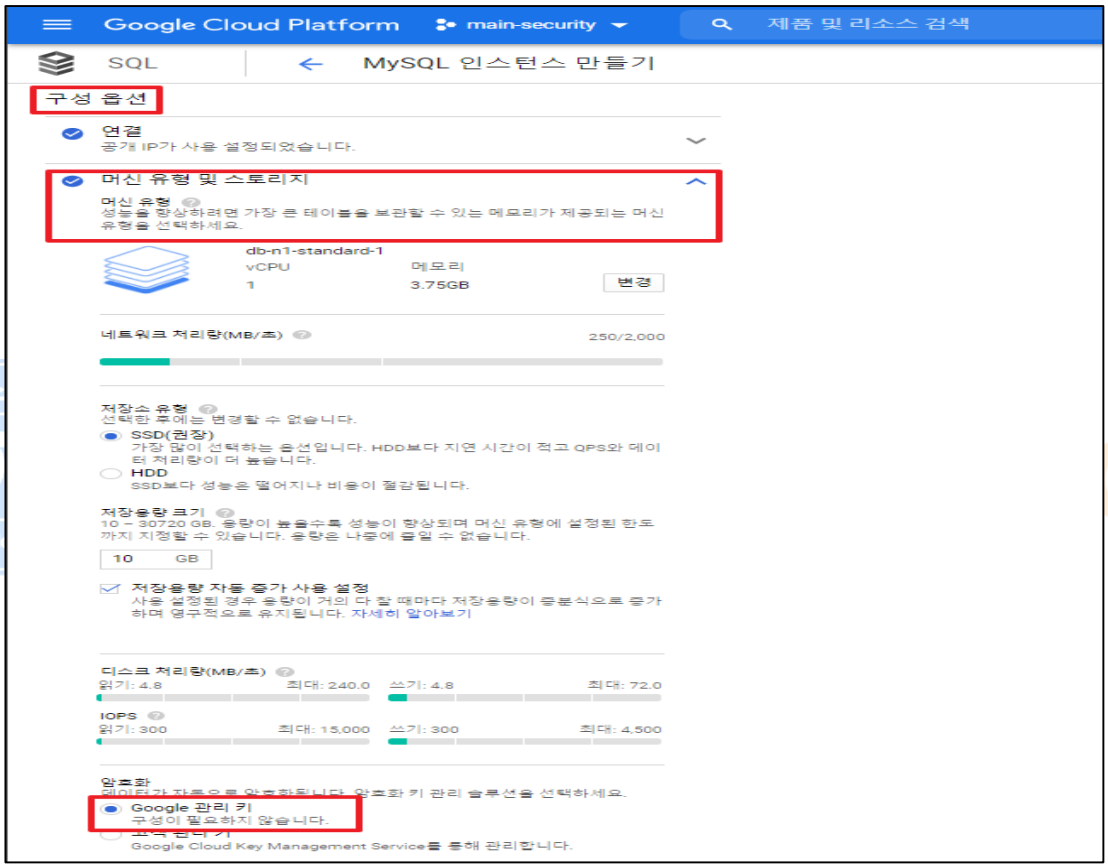
1) SQL 내 인스턴스 만들기 클릭



2) 데이터베이스 엔진 선택

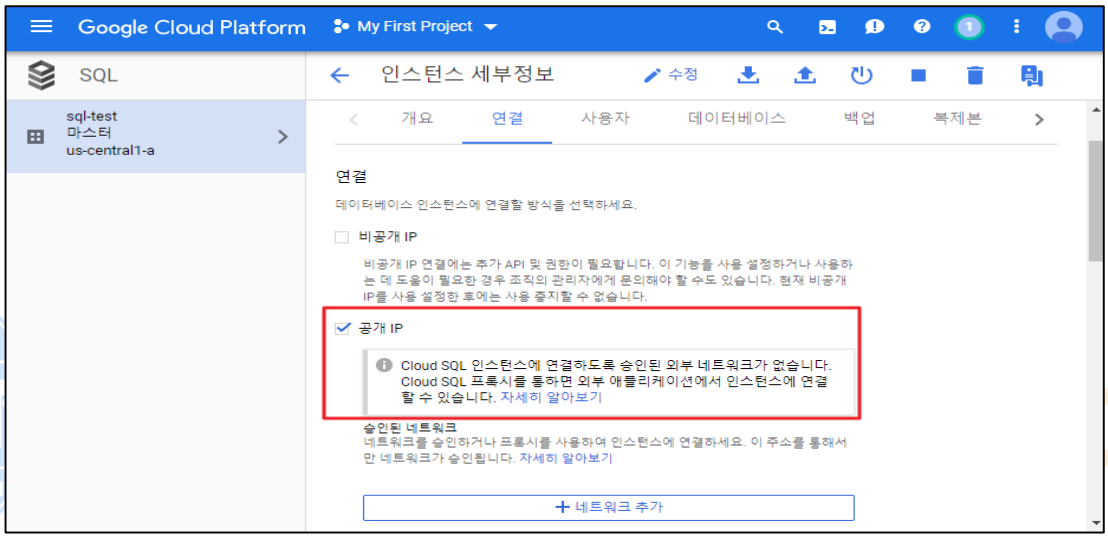
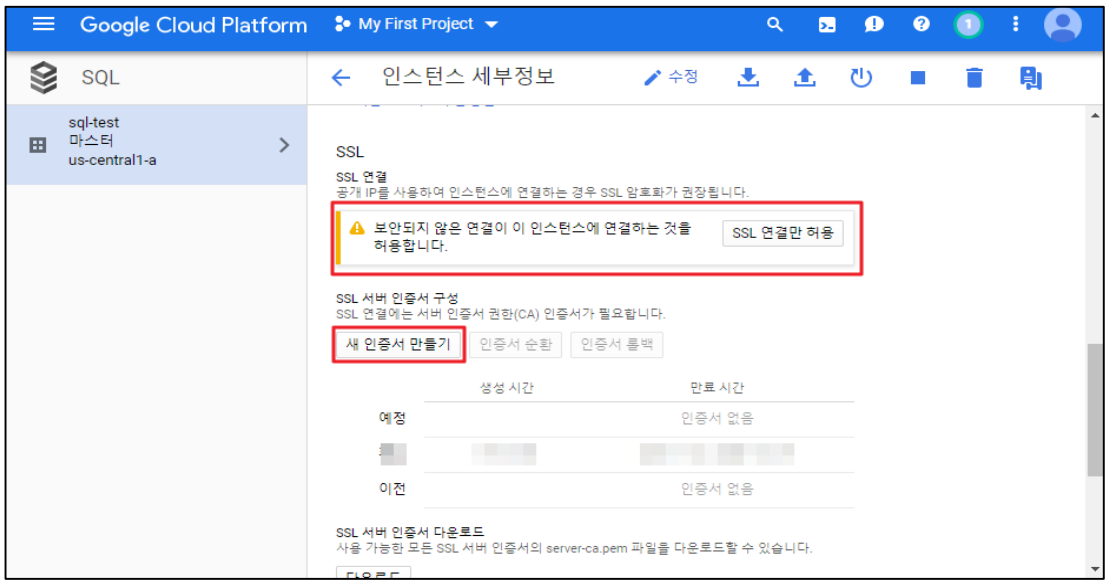


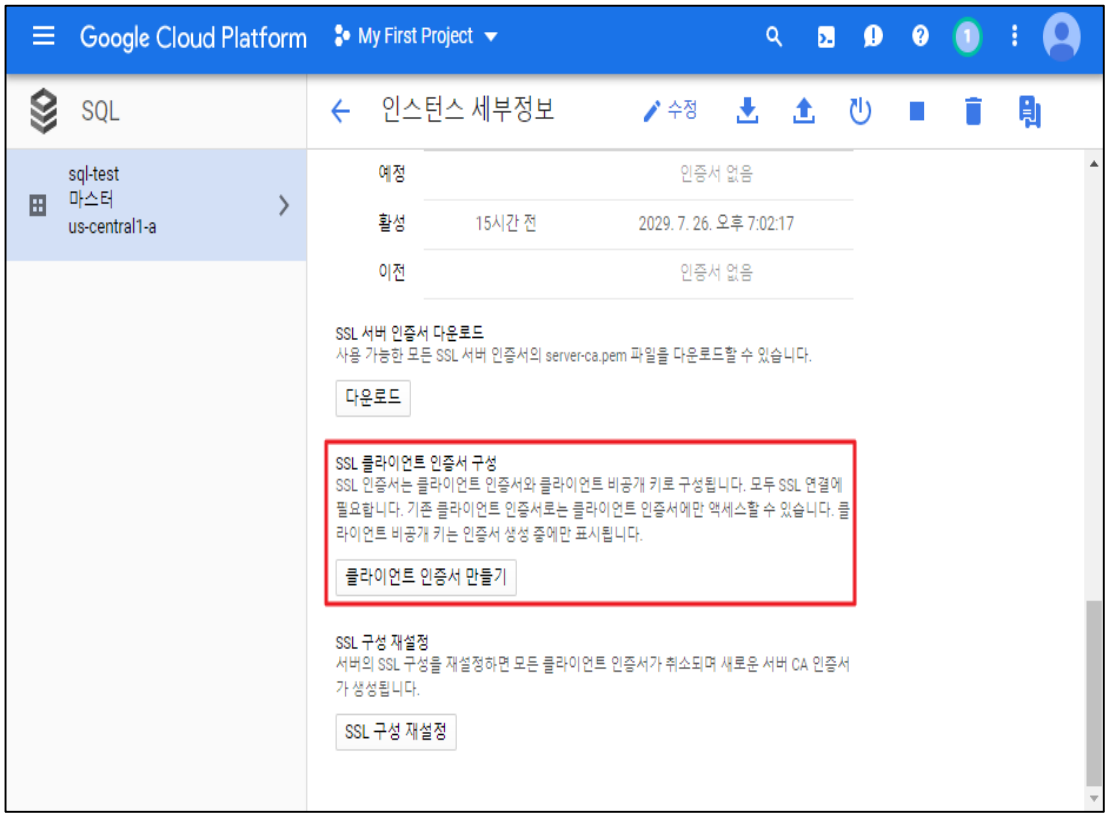
3) 구성 옵션 > 머신 유형 및 스토리지 내 암호화 유형 선택



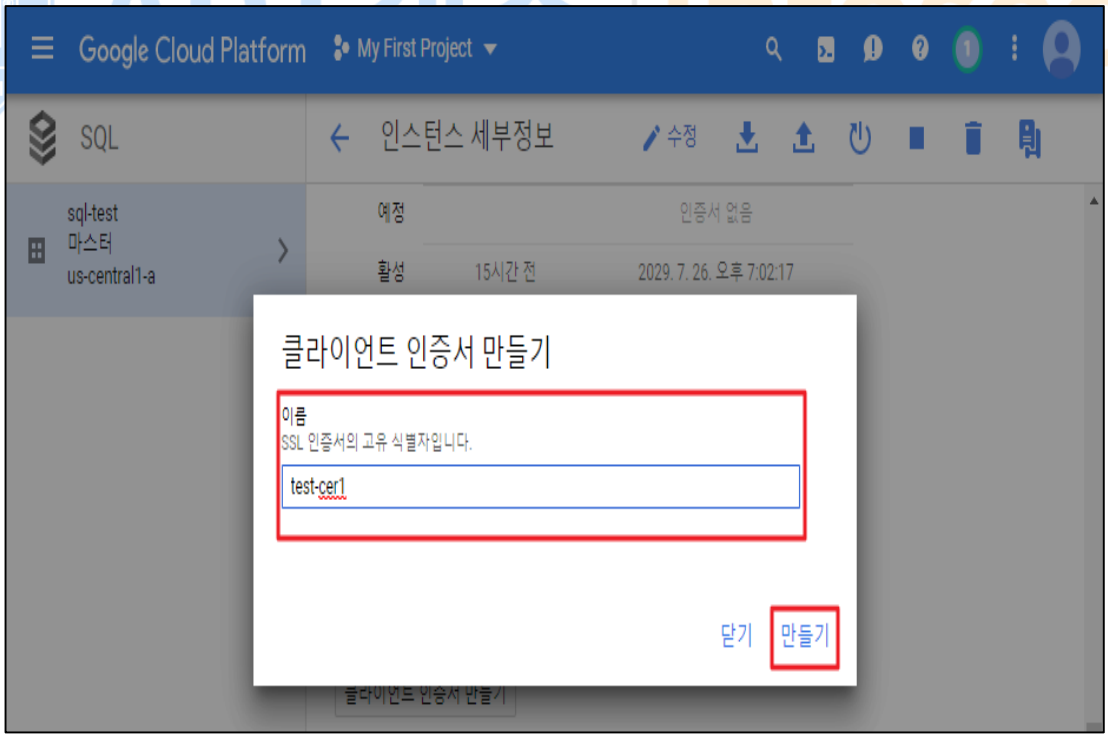
진단 기준	**양호기준** : "고객 관리 키" 사용 시 키에 대한 순환 주기 설정이 되어 있을 경우 **취약기준** : "고객 관리 키" 사용 시 키에 대한 순환 주기 설정이 되어있지 않을 경우
비고	

2.4 Cloud SQL 네트워크 통신 암호화 설정

분류	데이터 보안	중요도	중
항목명	Cloud SQL 네트워크 통신 암호화 설정		
항목 설명	Cloud SQL은 Google Cloud Platform에서 관계형 데이터베이스를 손쉽게 설정하고 유지하고 관리할 수 있게 해주는 완전 관리형 데이터베이스 서비스이며, GCP에서는 MySQL 및 PostgreSQL에서 Cloud SQL을 사용할 수 있습니다. Cloud SQL 내 공개 IP로 설정했을 경우, DB 인스턴스와 VM 연결 시 네트워크 내 보안을 위해 SSL 설정을 해야 데이터가 노출되지 않습니다.		
설정 방법	**가. SQL 접근 시 SSL 설정 방법** 1) [생성된 인스턴스] > [연결] > 공개 IP/비공개 IP 설정  2) SSL 새 인증서 만들기  3) SSL 클라이언트 인증서 구성		

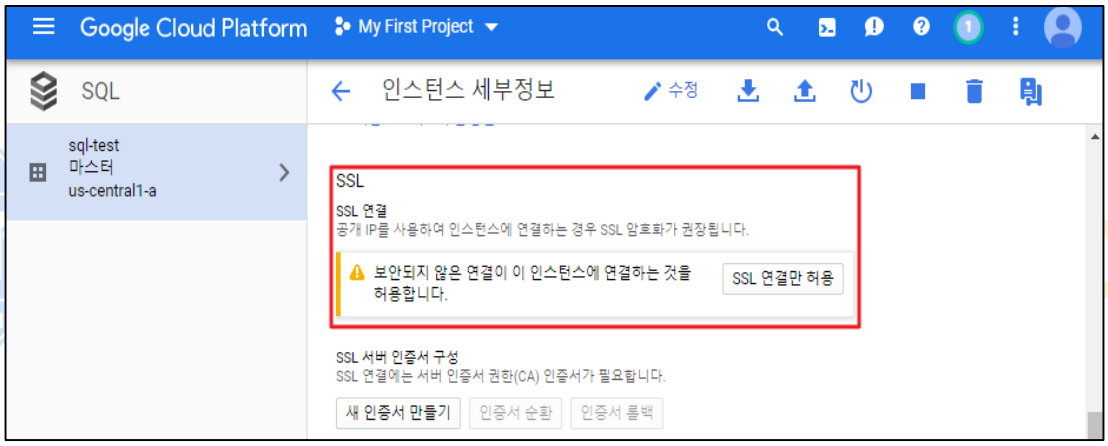


4) 클라이언트 인증서 만들기

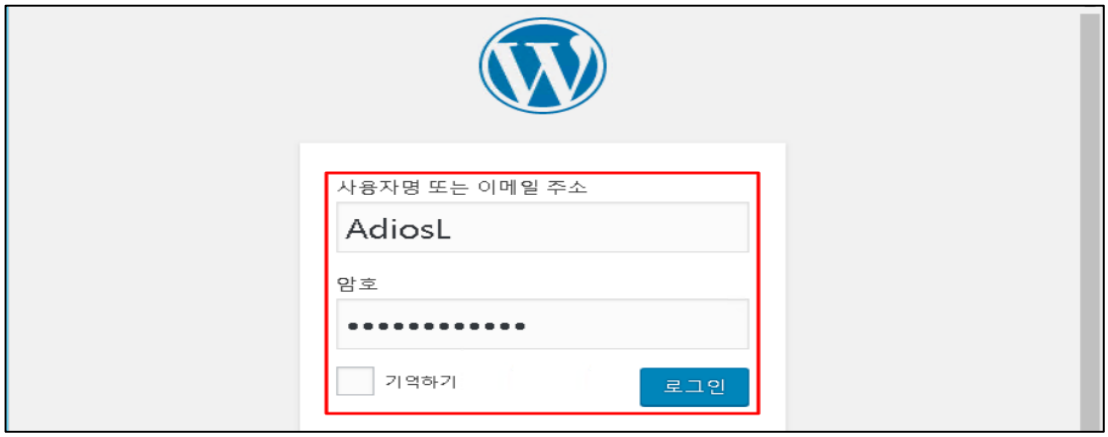


5) 생성된 새 SSL 인증서 확인

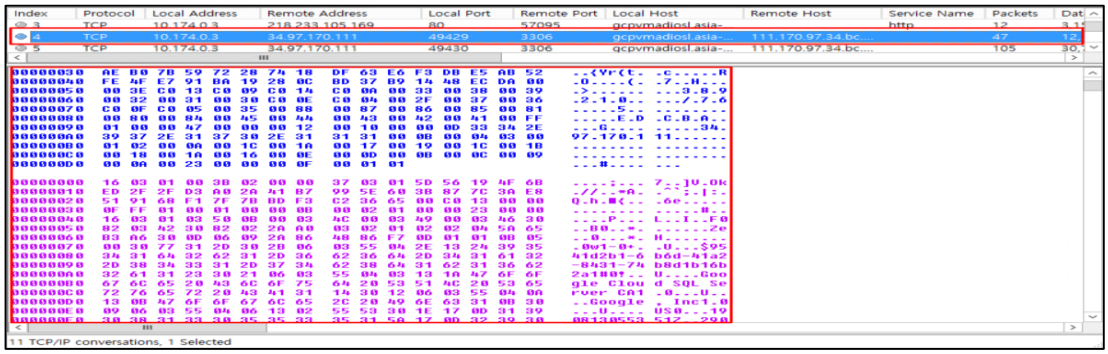
6) 'SSL 연결만 허용' 설정



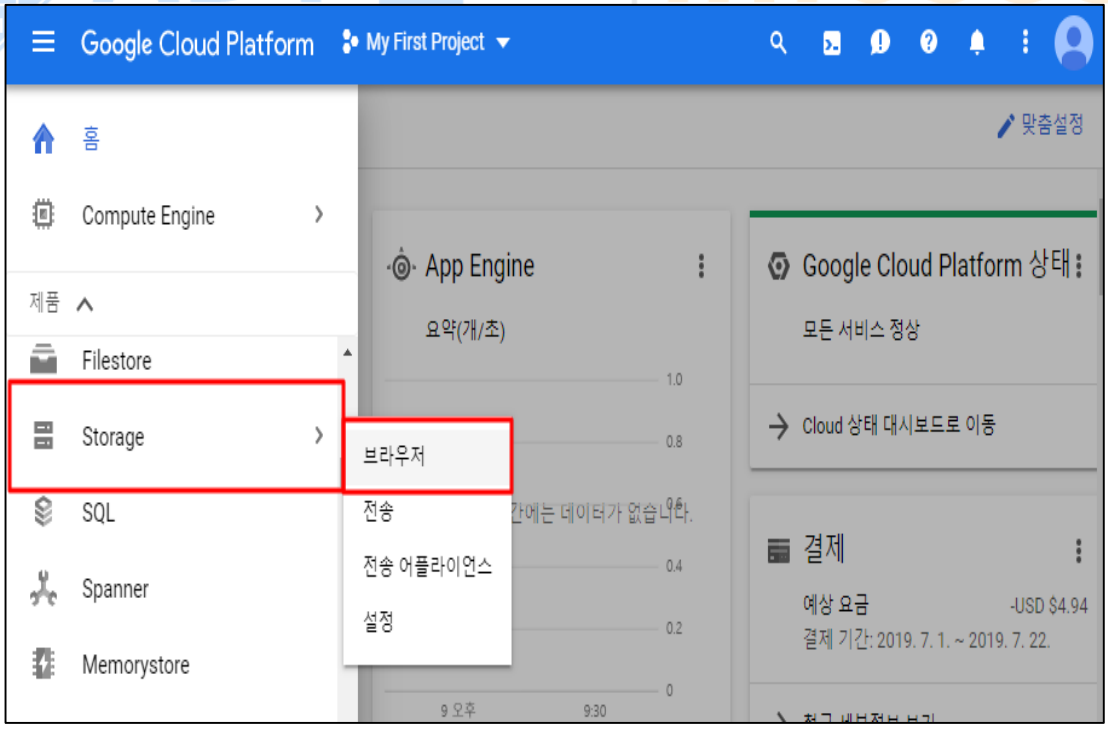
7) 웹 서비스 로그인 시도

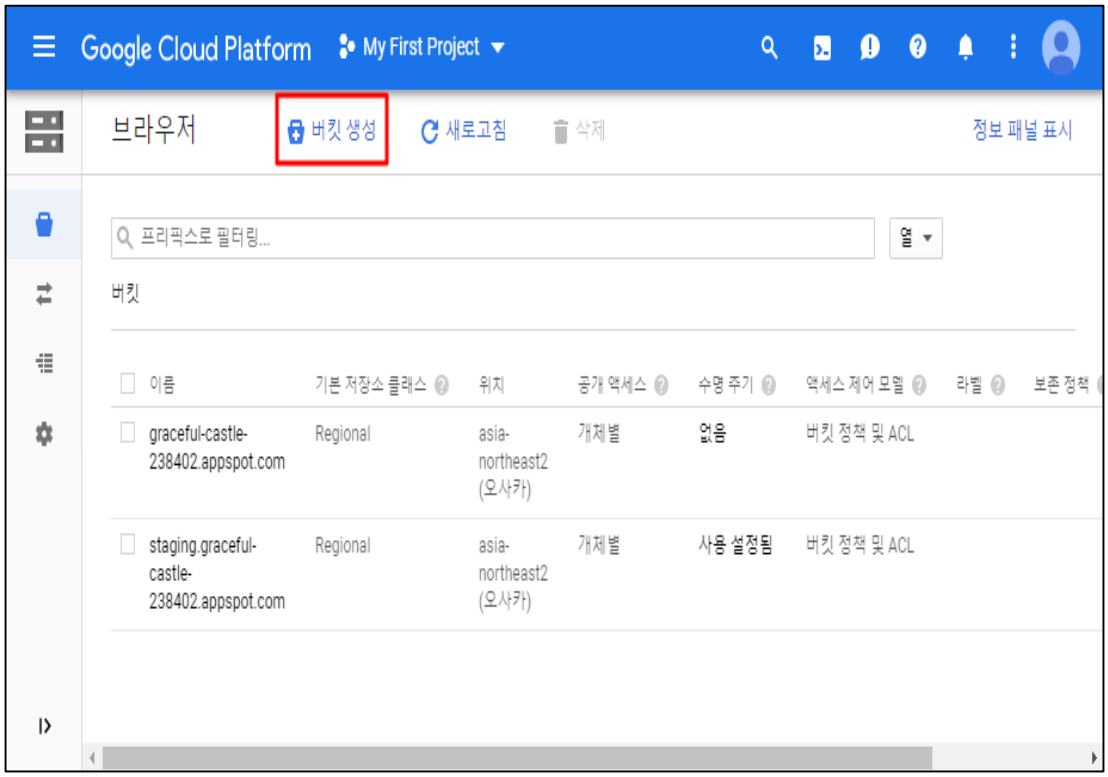


8) 암호화된 SQL 쿼리 확인

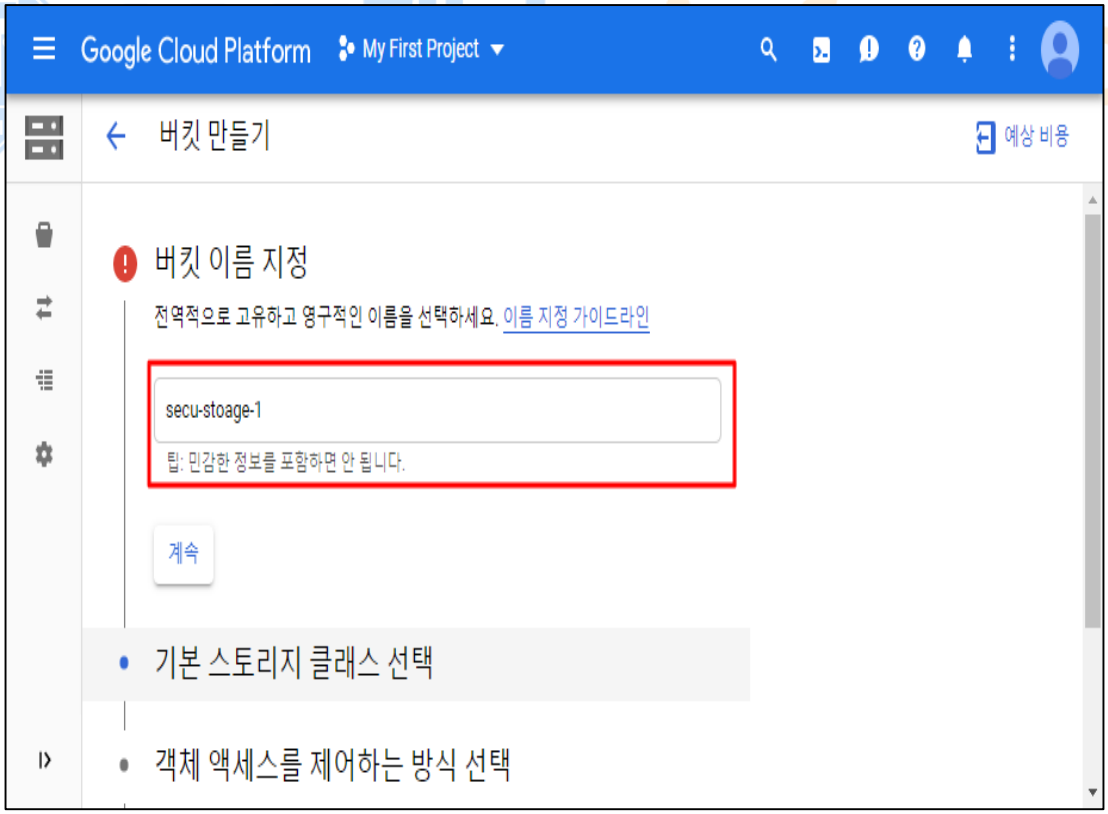
	
진단 기준	**양호기준** : 공개 IP를 통한 DB 인스턴스와 VM 연결 시 SSL 연결 설정이 존재할 경우 **취약기준** : 공개 IP를 통한 DB 인스턴스와 VM 연결 시 SSL 연결 설정이 존재하지 않을 경우
비고	

2.5 Storage 데이터 보안 관리

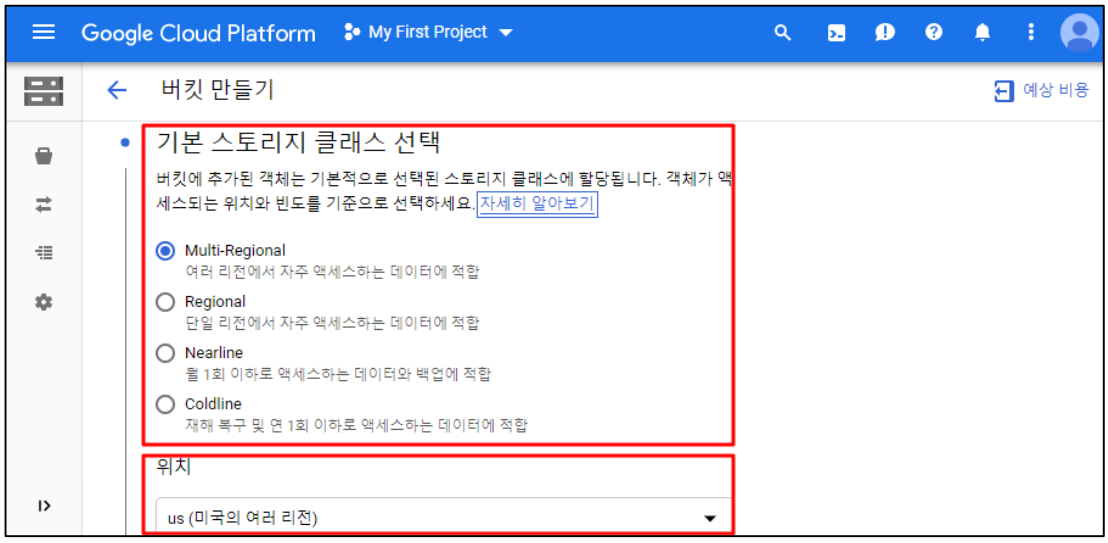
분류	데이터 보안	중요도	중
항목명	Storage 데이터 보안 관리		
항목 설명	Cloud Storage를 사용하면 데이터 양에 관계없이 언제 어디서나 데이터를 저장하고 가져올 수 있습니다. Cloud Storage를 통해 웹사이트 콘텐츠를 제공하거나, 보관 및 재해 복구를 위해 데이터를 저장하거나, 직접 다운로드를 통해 사용자에게 대량의 데이터 객체를 배포하는 등 다양한 용도로 사용할 수 있으며 Storage 내 보관 정책을 설정하여 이 버킷의 객체가 업로드된 후 삭제되거나 수정되지 않도록 보호해야 하는 최소 기간을 지정합니다. 또한, 기본적으로 Cloud Storage 는 모든 데이터를 암호화하여 저장하고 있으며, 사용 가능한 암호화 키로 "Google 관리 키", "고객 관리 키"를 제공하고 있습니다. 기업 정책 및 내부 구성에 부합하는 암호화 키를 사용하여 저장 데이터를 안전하게 보호해야합니다. "고객 관리 키"를 사용하는 경우 키에 대한 순환 주기 설정을 통해 키 유출 및 사용자 접근에 대한 보안 위협을 미연에 방지 할 수 있습니다. **※ 일정 기간을 정해두고 필수로 보관해야 하는 자료(계약서, 개인정보 등)는 장기간 보관을 고려 해야 합니다.**		
설정 방법	**가. Storage 암호화 및 데이터 보존 정책 설정** 1) [관리 콘솔] > [Storage] > [브라우저]  2) 버킷 생성		



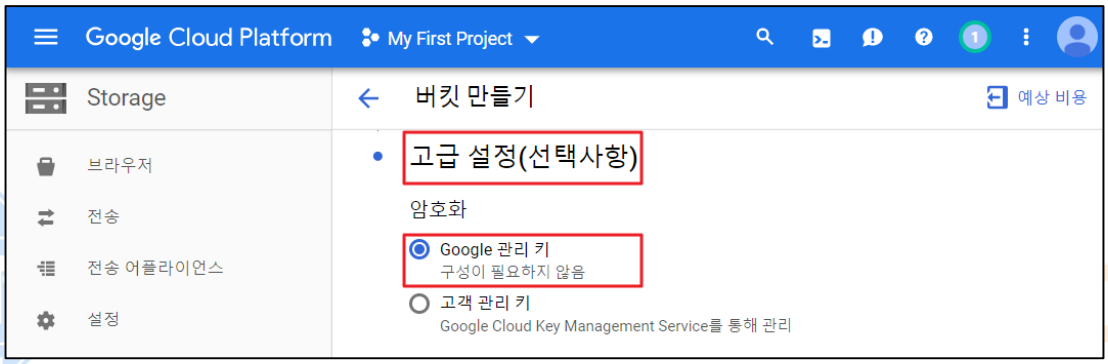
3) 버킷 정보 입력



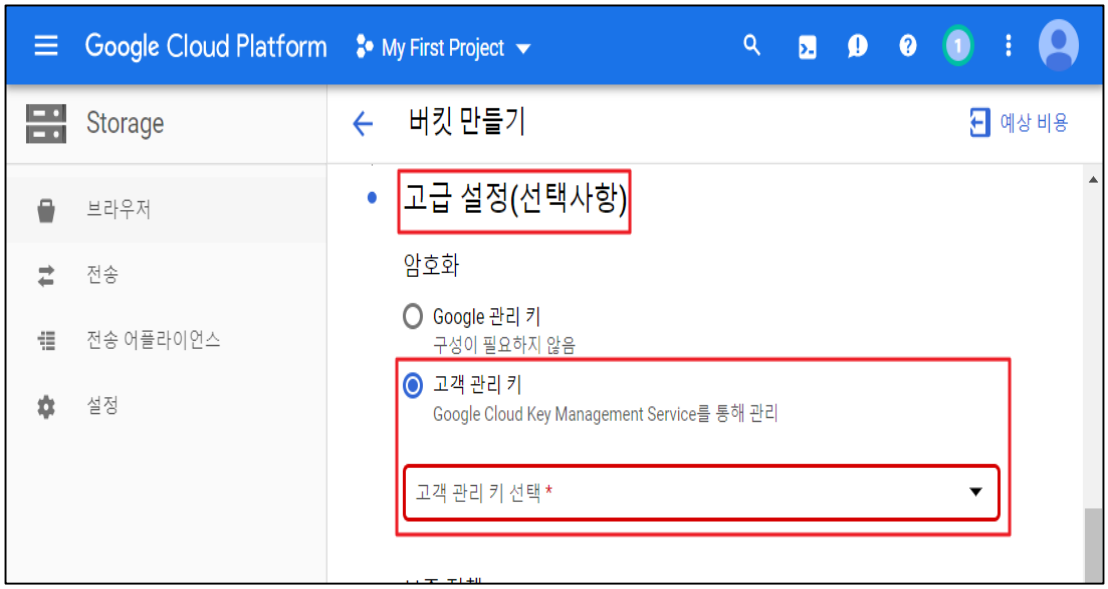
4) 기본 스토리지 클래스 선택



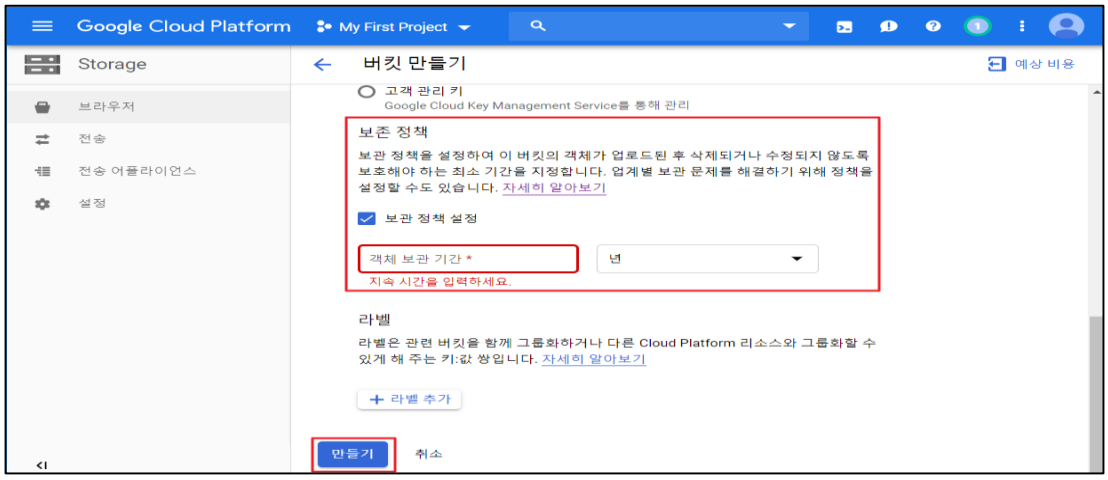
5) 'Google 관리 키' 암호화 방식 설정



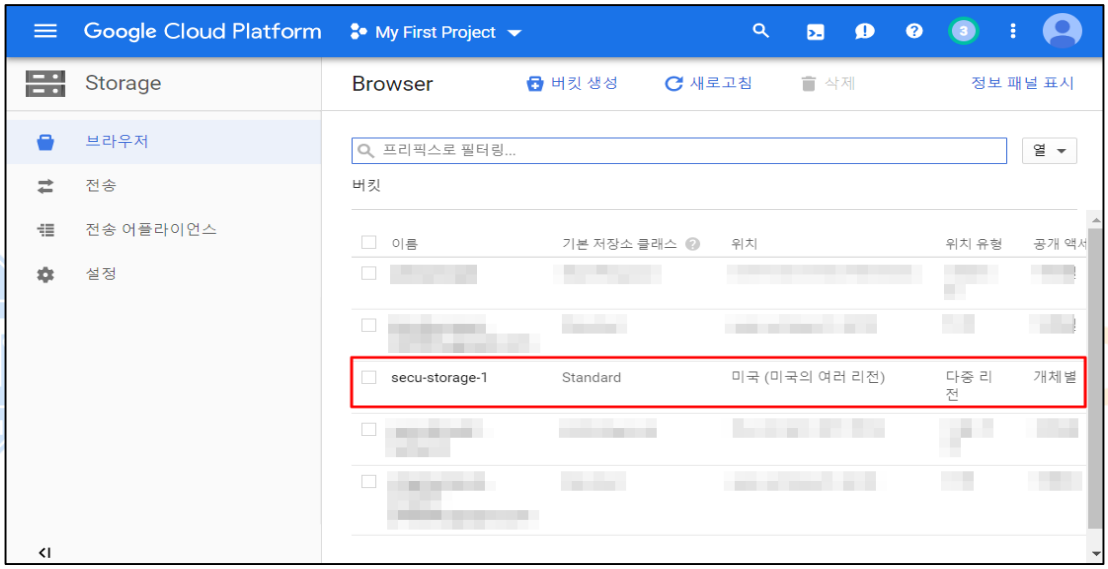
6) '고객 관리 키' 암호화 방식 설정



7) 데이터 보존 정책 설정

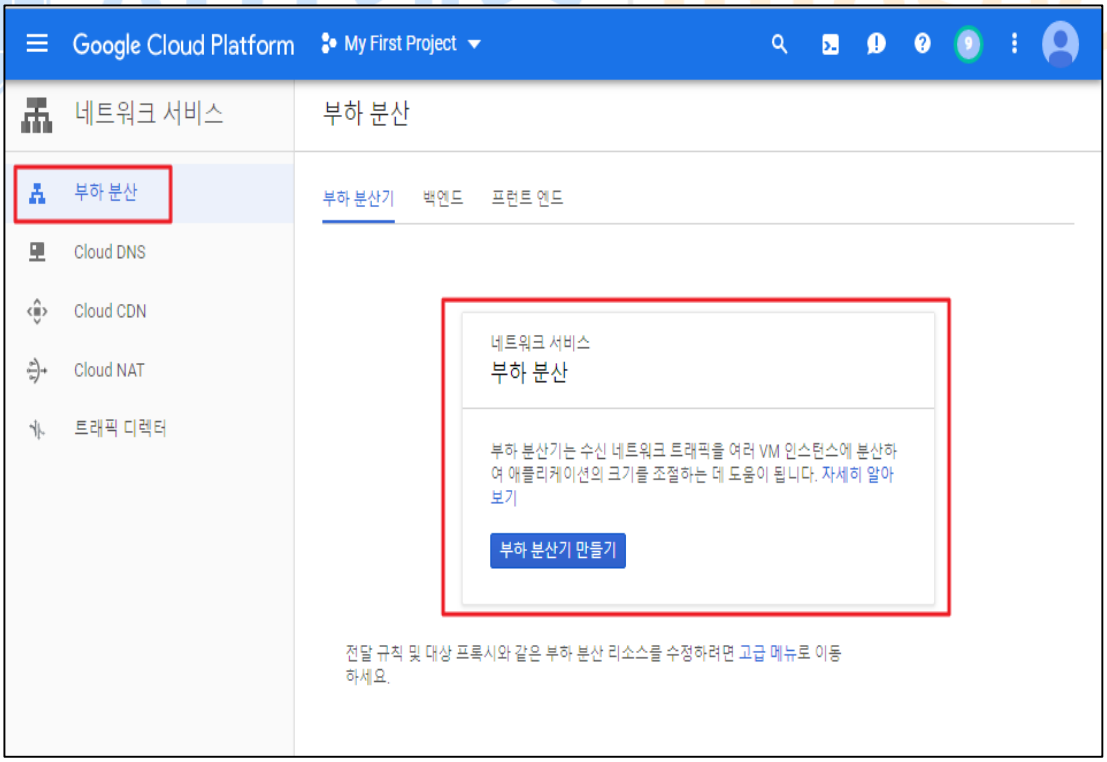


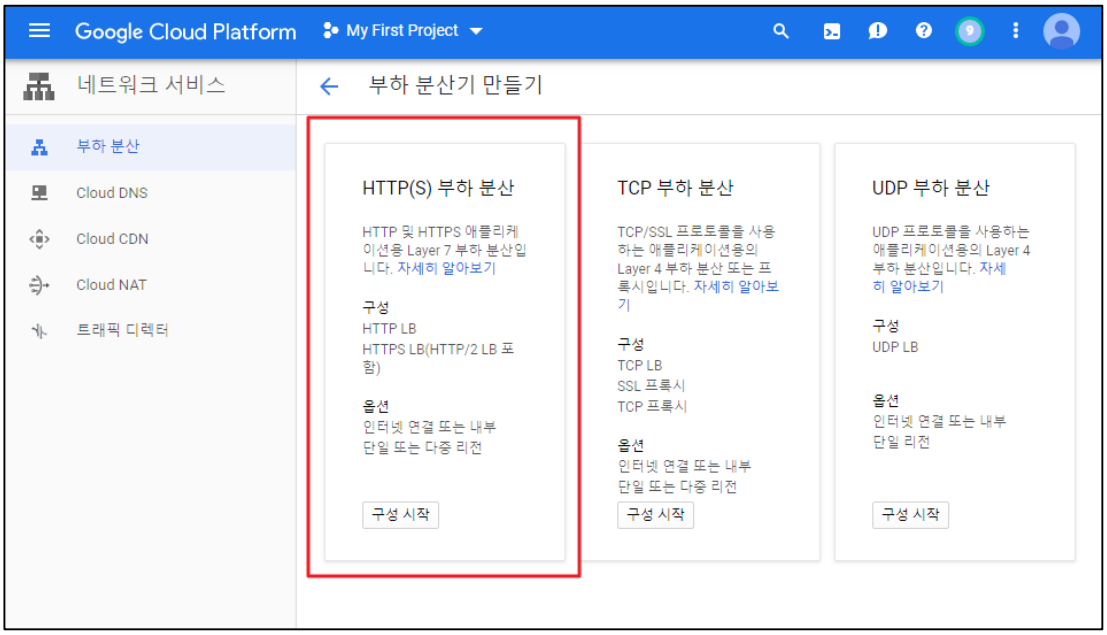
8) 버킷 생성 완료



진단 기준	**양호기준** : 장기간 보관해야 하는 객체(데이터)에 보존 정책이 설정되어 있는 경우 **취약기준** : 장기간 보관해야 하는 객체(데이터)에 보존 정책이 설정되어 있지 않은 경우
비고	

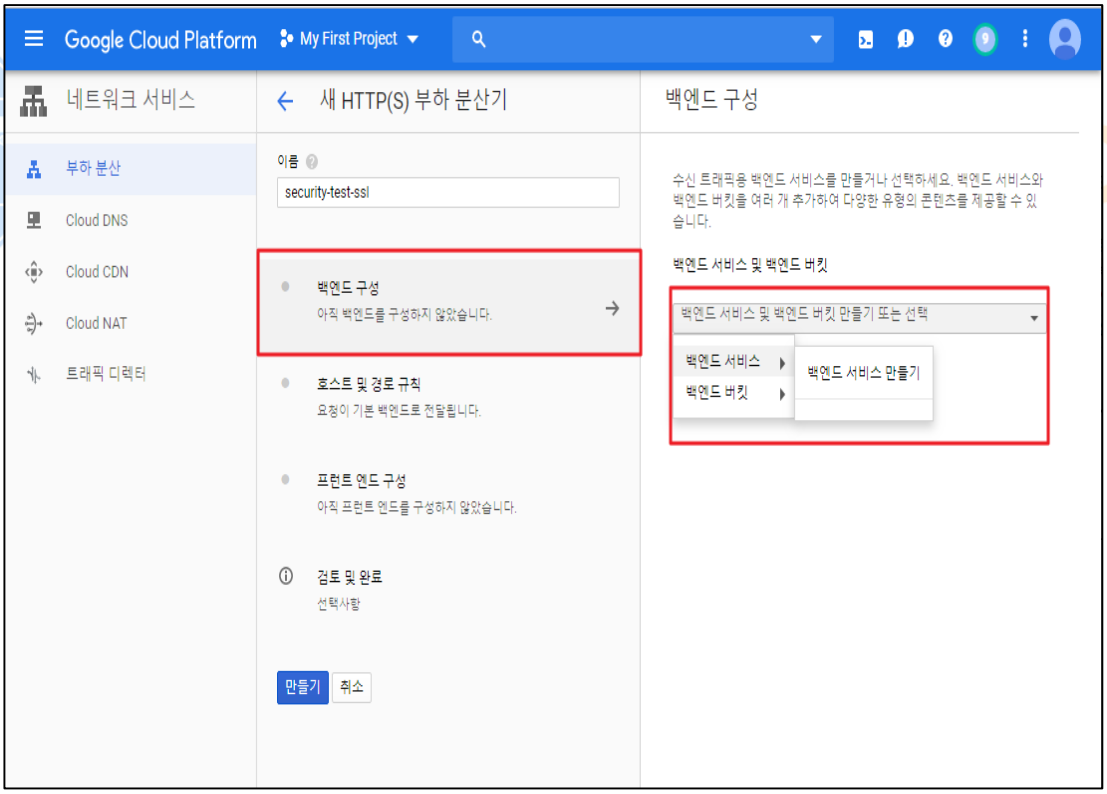
2.6 Compute Engine SSL 정책 관리

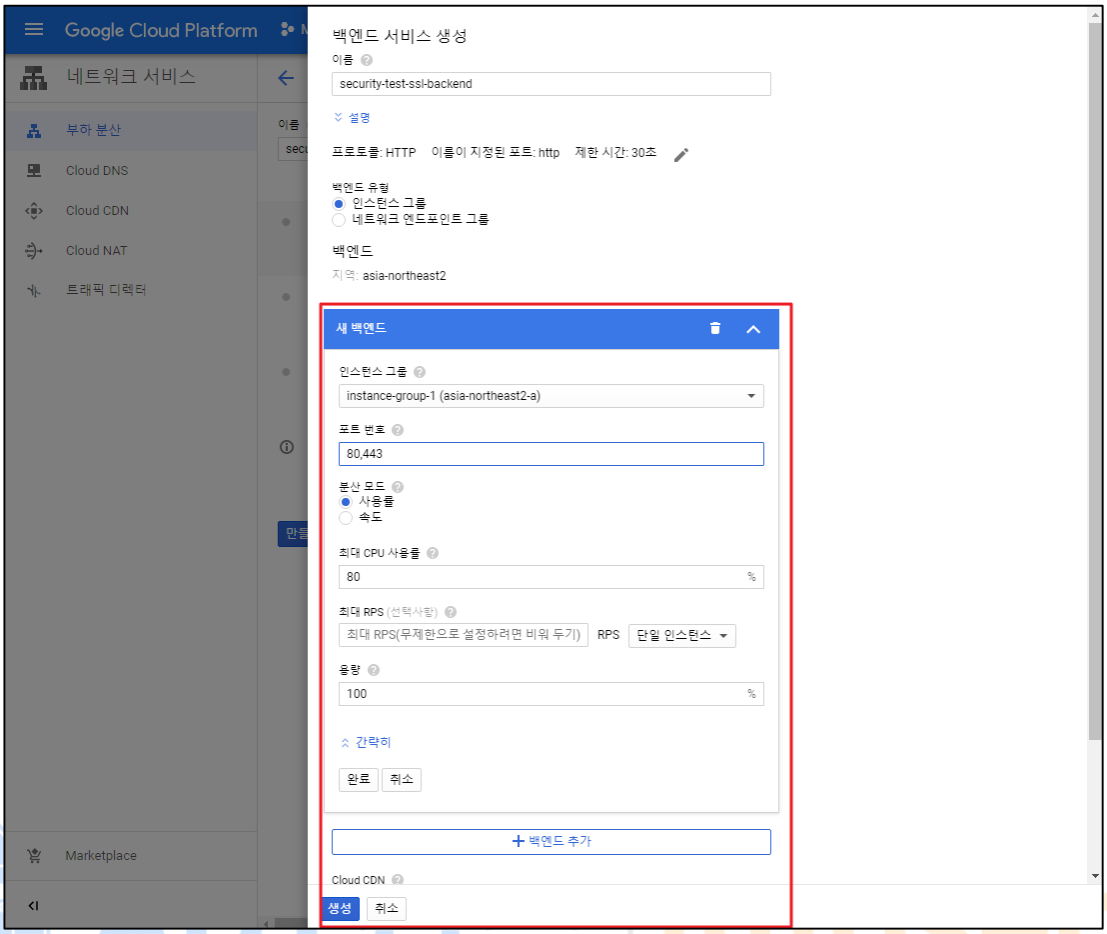
분류	데이터 보안	중요도	상
항목명	Compute Engine SSL 정책 관리		
항목 설명	Google Cloud Platform 에서의 통신 구간의 데이터 보호는 크게 아래 두가지(Compute Engine / App Engine) 환경에서 설정하여 SSL을 사용합니다. **※ Compute Engine** Compute Engine 내 SSL 설정은 부하 분산기가 클라이언트와 SSL을 협상하는 방식으로 제어를 하며, SSL/TLS 버전 및 암호화의 세밀한 제어를 위해 정책을 만들고 HTTPS 및 SSL 부하 분산기에 정책을 연결할 수 있습니다. 기본적으로 HTTPS로드 균형 조정과 SSL 프록시로드 균형 조정은 훌륭한 보안 및 광범위한 호환성을 제공하는 SSL 기능 세트를 사용합니다. 일부 응용 프로그램은 HTTPS 또는 SSL 연결에 사용되는 SSL 버전 및 암호를보다 많이 제어해야합니다. SSL 정책을 정의하여로드 밸런서가 클라이언트와 협상하는 SSL 기능을 제어 할 수 있습니다.		
설정 방법	**가. 구글 관리형 SSL - Compute Engine** 1) [네트워크 서비스] > [부하 분산] > [부하 분산기 만들기] - Compute Engine 리소스 내 구글 관리형 SSL 인증서 발급 및 확인을 위한 부하 분산기 생성  2) HTTP(S) 부하 분산으로 부하 분산기 구성		



3) [백엔드 구성]

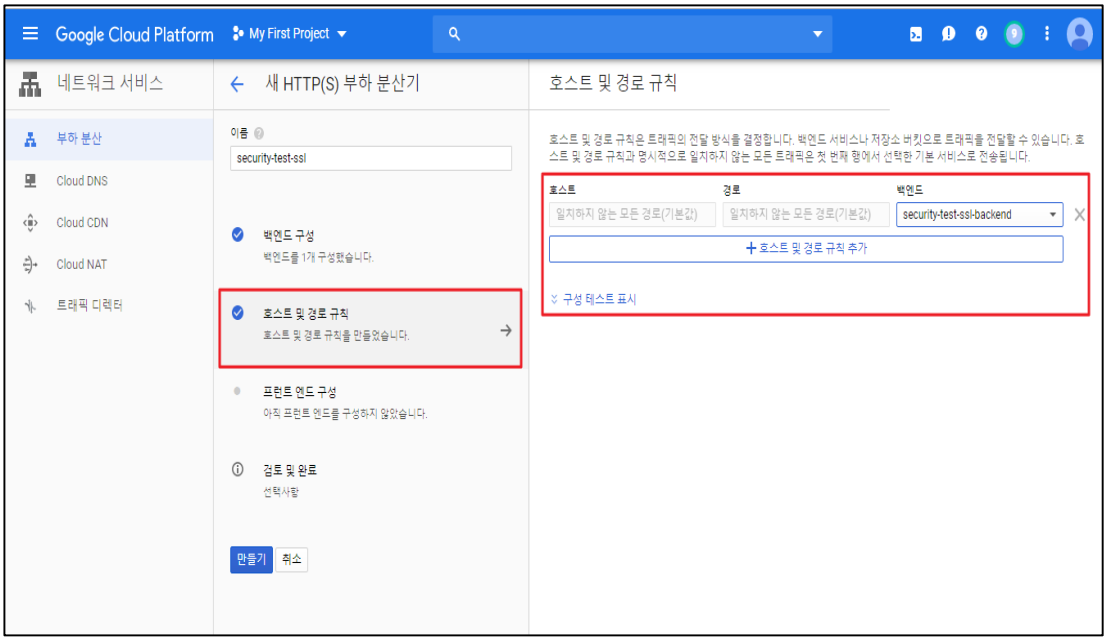
- VM 인스턴스 그룹을 이용해 백엔드 서비스 생성





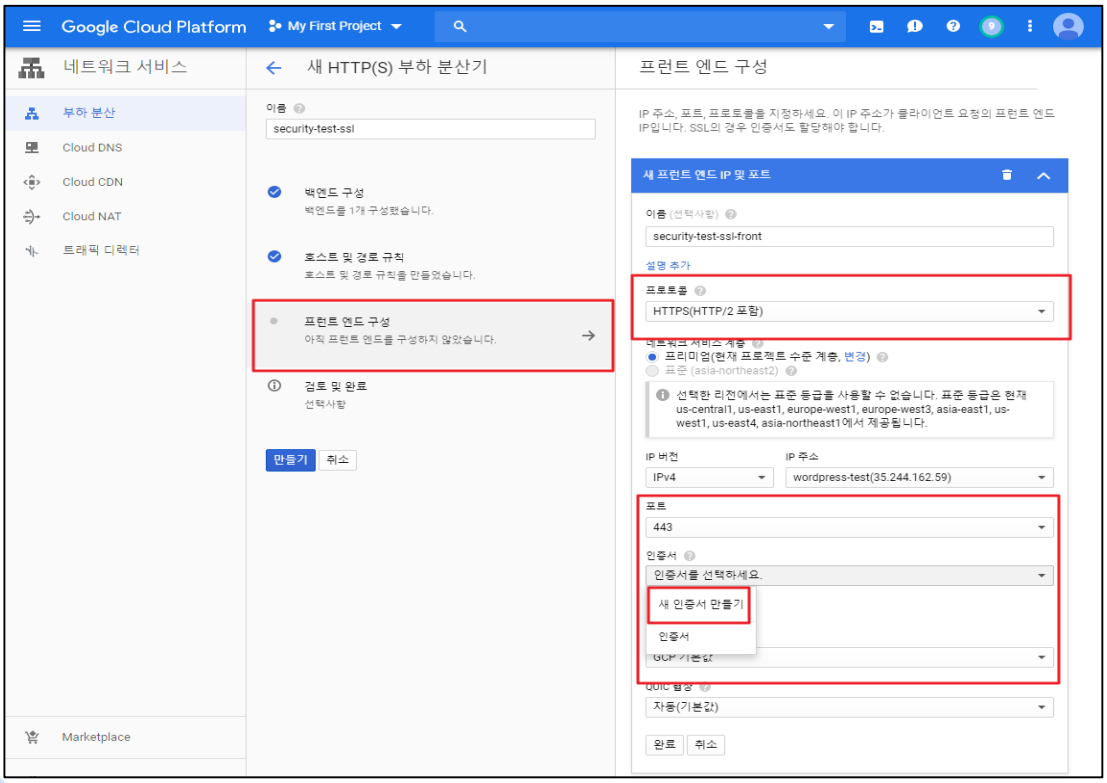
4) [호스트 경로 및 규칙]

- 호스트 및 경로 규칙은 기본값(일치하지 않은 모든 경로)으로 설정



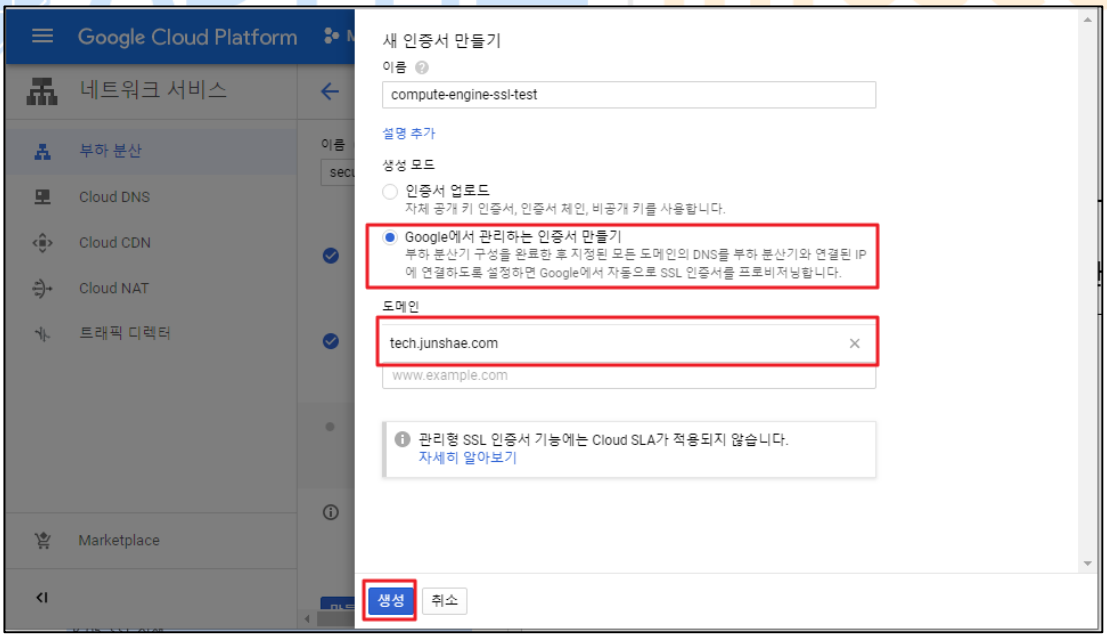
5) [프런트엔드 구성]

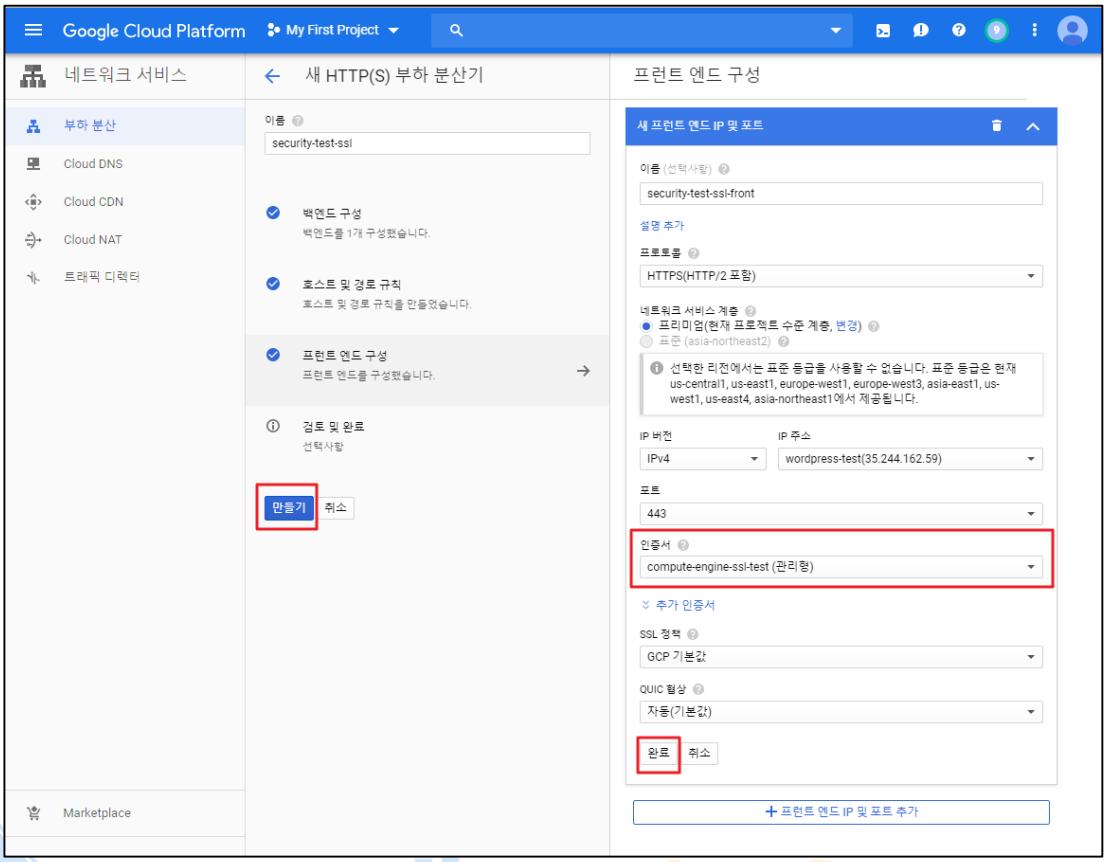
- 부하 분산기 이용을 위한 설정 (IP / 포트 / SSL 인증서)



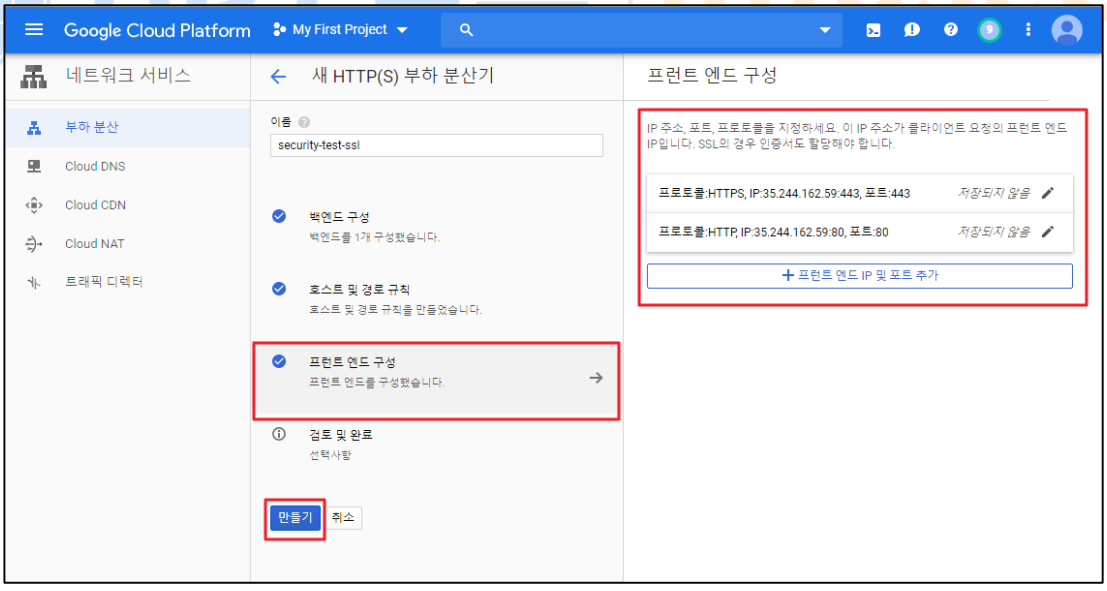
6) [SSL 인증서 생성]

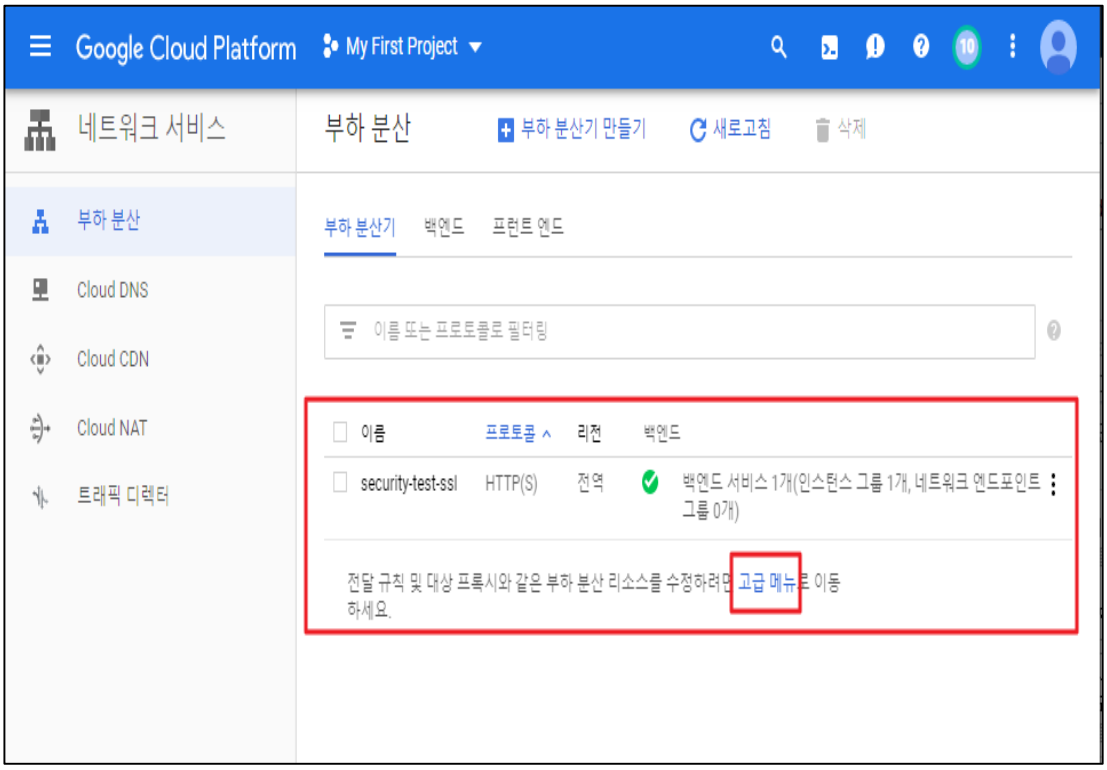
- 구글 관리형 인증서 생성 및 도메인 지정





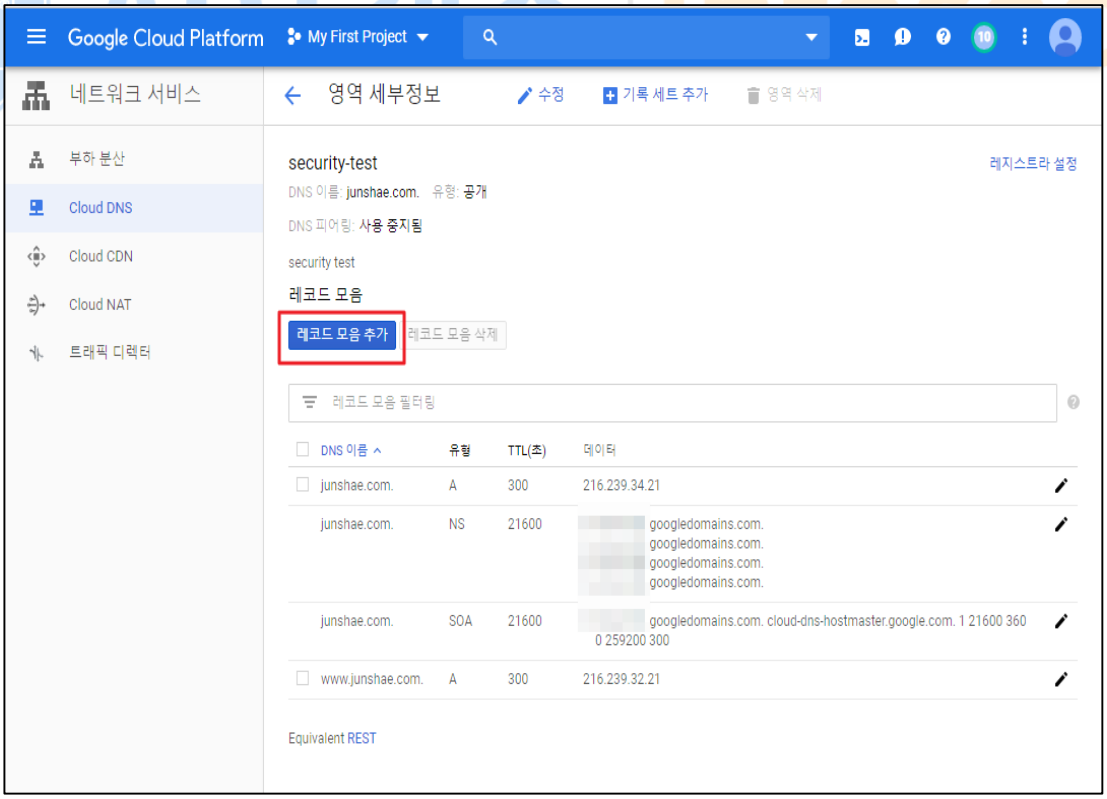
7) 부하 분산기 최종 설정 완료 및 생성





8) [네트워크 서비스] > [Cloud DNS] > [레코드 모음 추가]

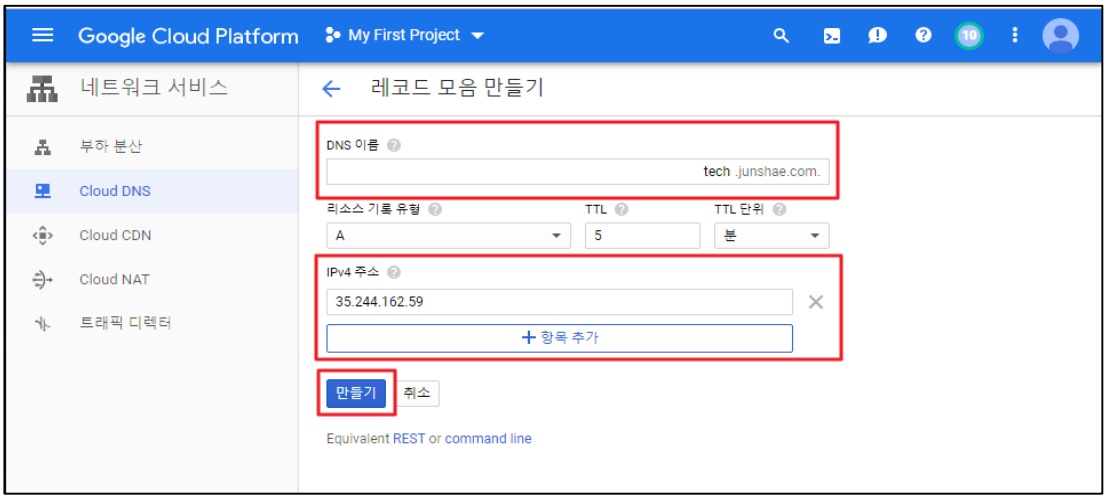
- 부하 분산기를 통한 웹서비스 접근 및 SSL 인증서 등록을 위한 Cloud DNS 설정



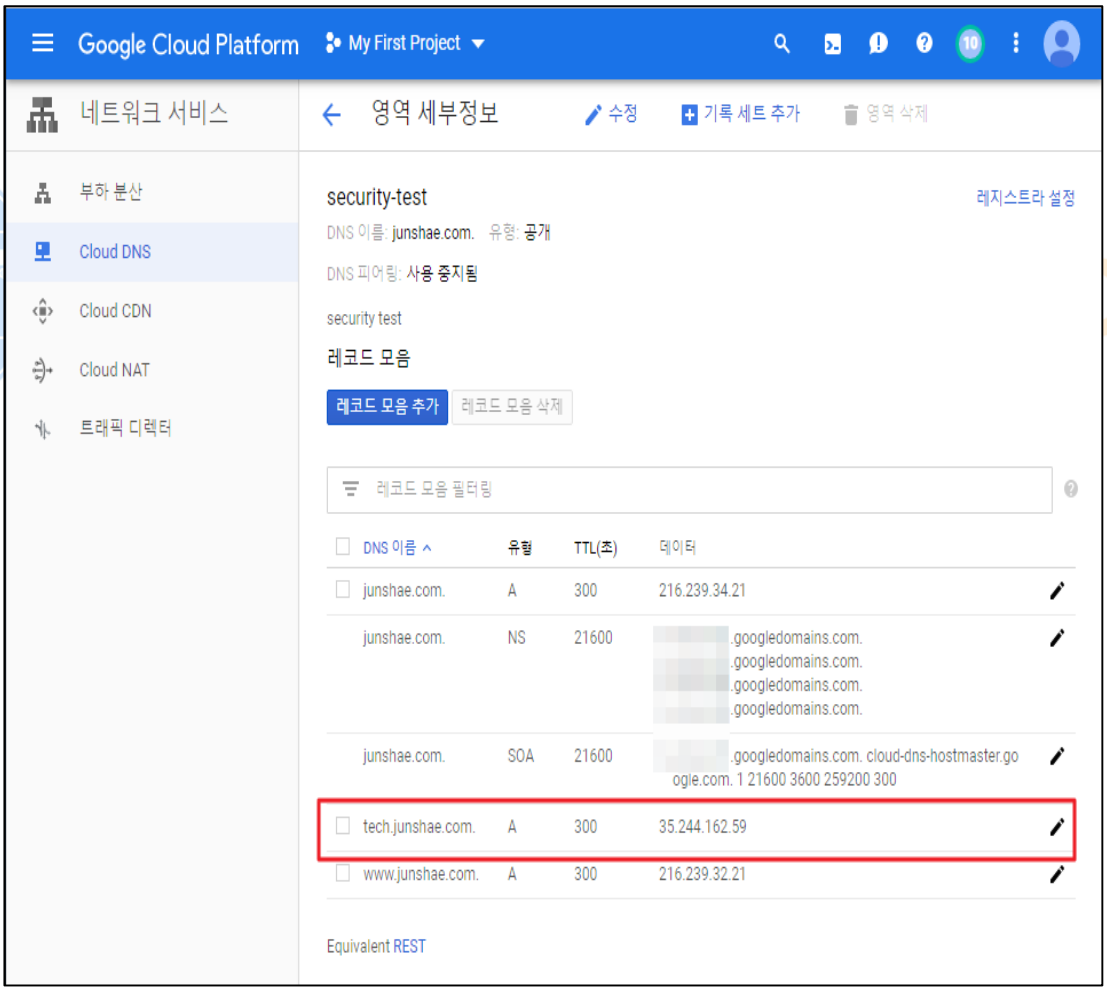
9) 웹서비스 연결에 사용할 도메인 및 IP(부하 분산기 외부 IP) 등록

※ 이때 DNS 이름은 부하 분산기 내 구글 관리형 SSL 인증서 생성 시 등록한 도메인과 동일

해야함

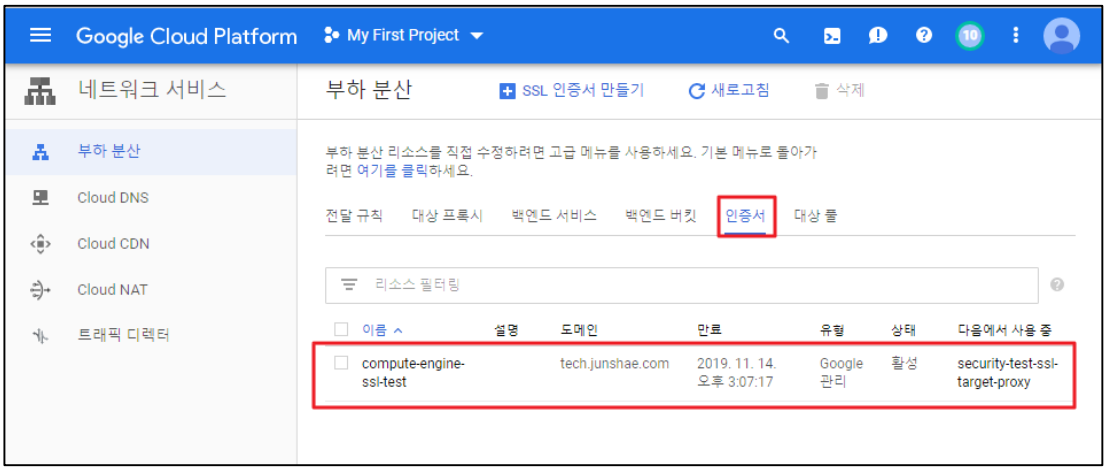


10) 레코드 정상 등록 확인

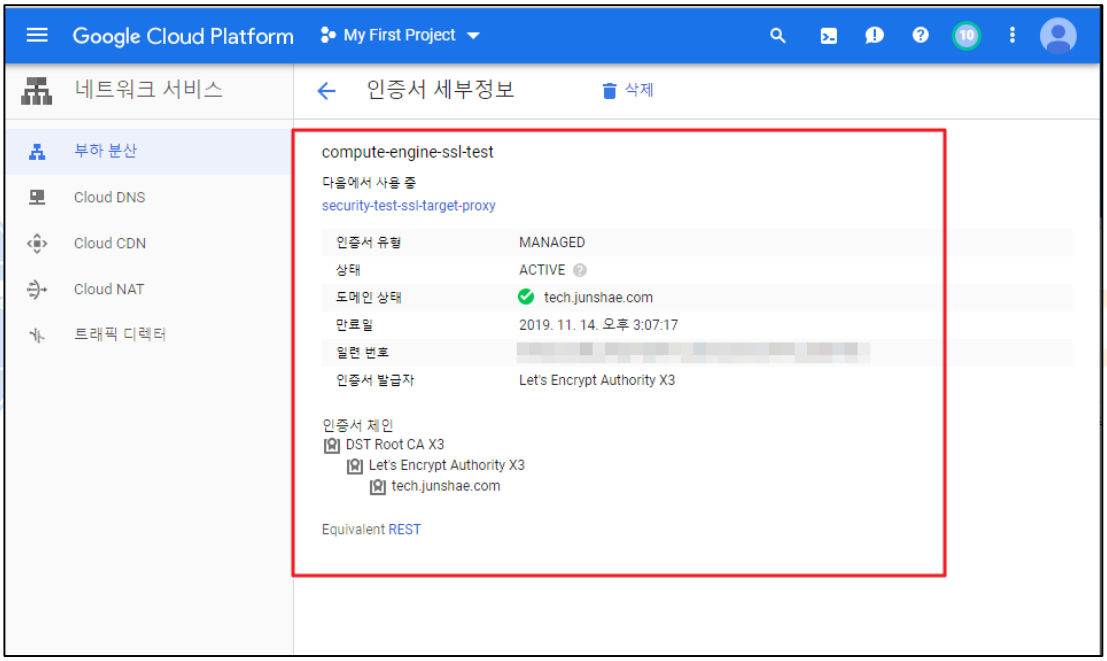


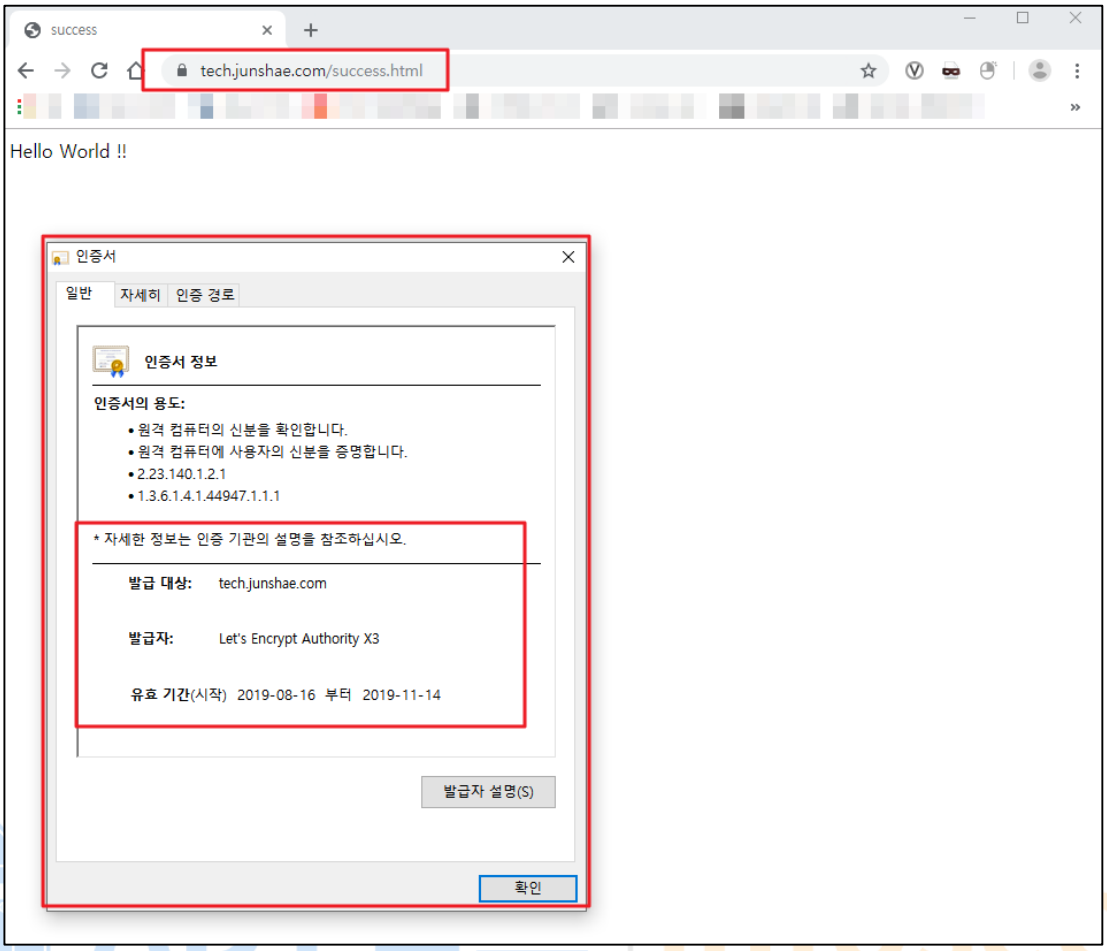
11) [네크워크 서비스] > [부하 분산] > [고급 설정] > [인증서]
- 부하 분산기를 통한 웹서비스 접근 및 SSL 인증서 등록을 위한 Cloud DNS 설정 (레코드 추가)

※ 등록한 SSL 인증서의 정상 이용은 Cloud DNS 레코드 등록 후 30~60분 정도 소요



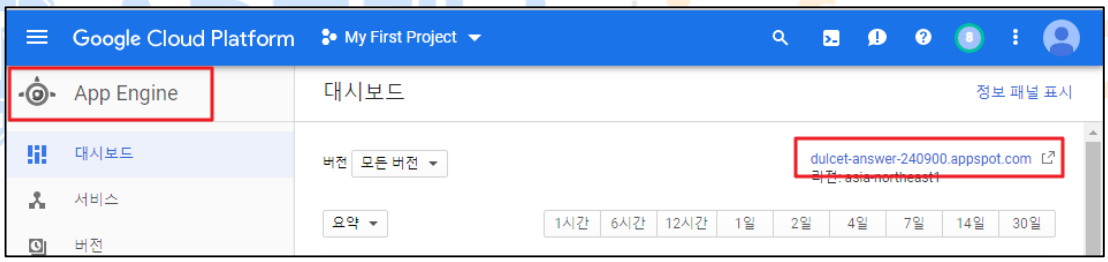
12) 구글 관리형 SSL 인증서 정상 등록 및 이용 가능 상태 확인 (상태: Active)

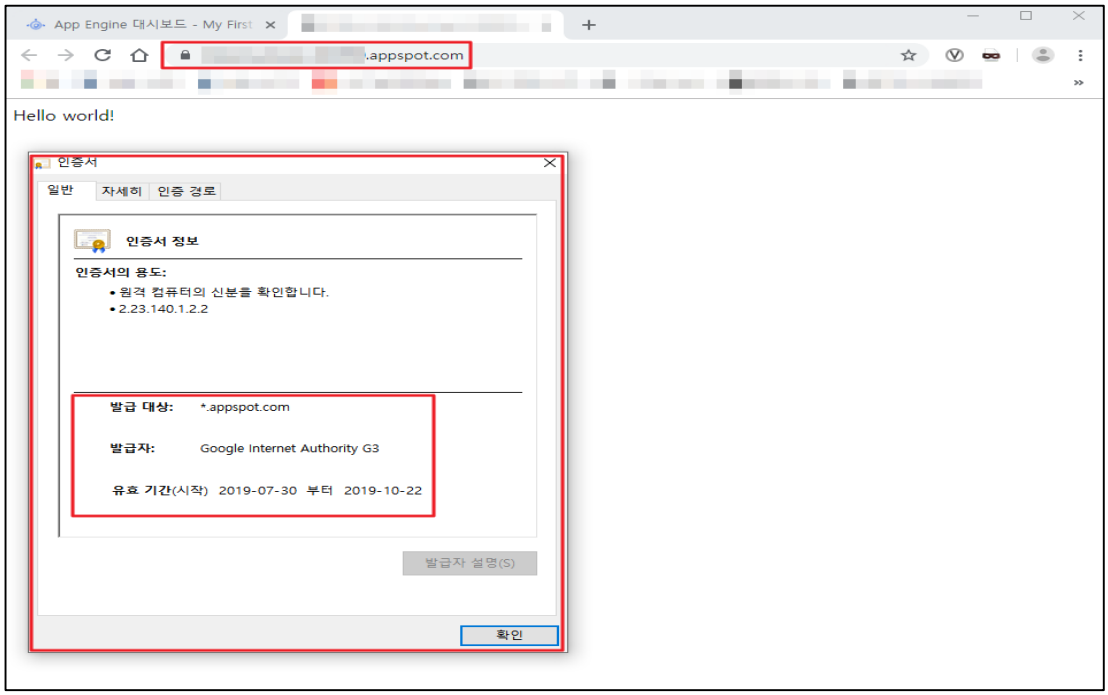


<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단
기준</td><td>양호기준
: SSL 인증서를 Google에서 관리하고 있을 경우

취약기준
: SSL 인증서를 외부에서 관리하며 직접 다운로드가 가능할 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

2.7 App Engine SSL 정책 관리

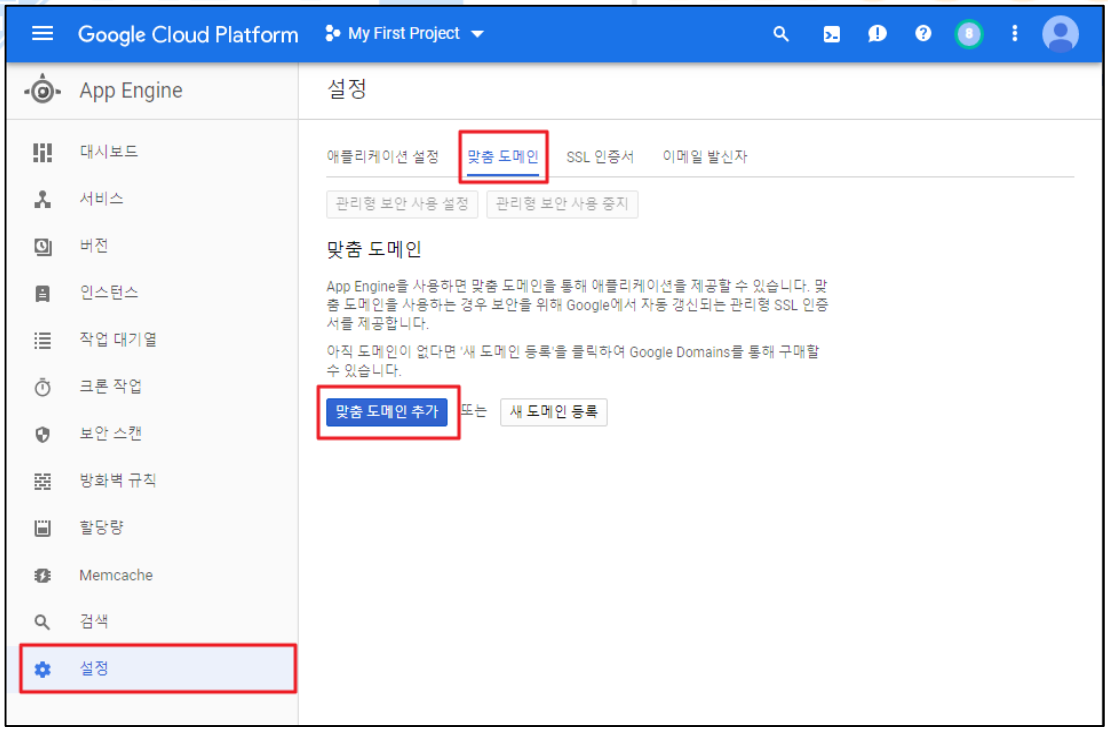
분류	데이터 보안	중요도	상
항목명	SSL 정책 관리 (App Engine)		
항목 설명	Google Cloud Platform 에서의 통신 구간의 데이터 보호는 크게 아래 두가지(Compute Engine / App Engine) 환경에서 설정하여 SSL을 사용합니다. **※ App Engine** App Engine 앱에 기본적인 SSL보다 높은 수준으로 SSL을 지원하기 위해 전 세계에 분산된 SSL 엔드포인트가 제공되고 부하 분산이 기본적으로 사용되므로 전 세계의 사용자에게 빠르고 안전하며 안정적으로 앱을 제공할 수 있습니다. 기본적으로 HTTPS로드 균형 조정과 SSL 프록시로드 균형 조정은 훌륭한 보안 및 광범위한 호환성을 제공하는 SSL 기능 세트를 사용합니다. 일부 응용 프로그램은 HTTPS 또는 SSL 연결에 사용되는 SSL 버전 및 암호를보다 많이 제어해야합니다. SSL 정책을 정의하여로드 밸런서가 클라이언트와 협상하는 SSL 기능을 제어 할 수 있습니다.		
설정 방법	**가. 구글 관리형 SSL – App Engine (기본 적용)** 1) [App Engine] > [대시보드] - App Engine 내 구동 서비스 확인  2) App Engine 내 구동 서비스 접근 및 인증서 확인 - 기본적으로 App Engine을 통해 서비스를 운영할 경우 아래 그림과 같이 구글에서 자체적으로 SSL 인증서를 발급 해 *.appspot.com 도메인을 사용해 HTTPS 통신이 가능하게 해줍니다.		



나. 구글 관리형 SSL – App Engine (커스텀 적용)

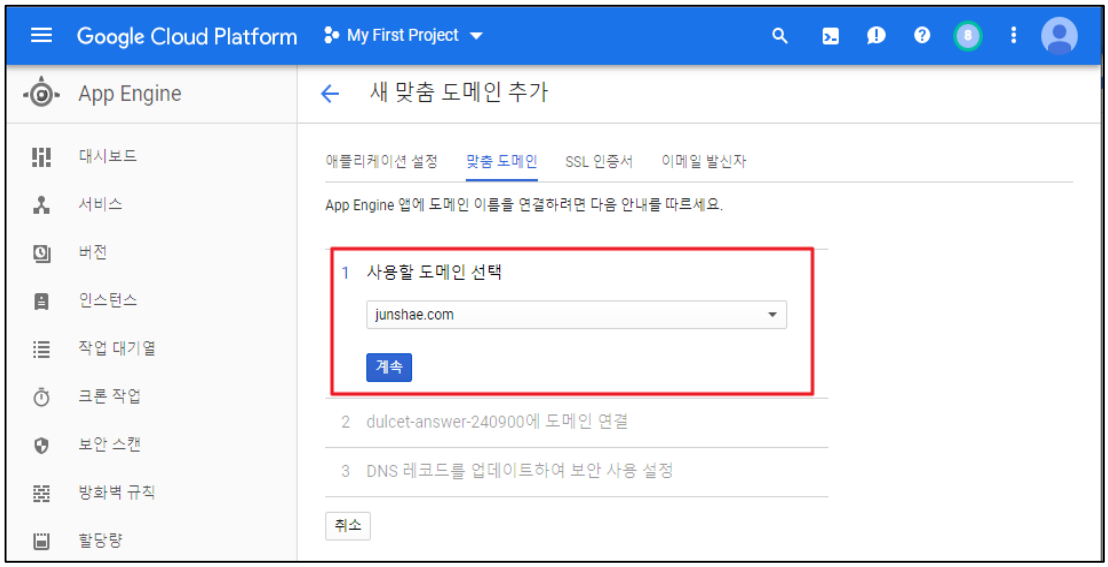
- App Engine 내 사용자가 별도 지정한 도메인에 대해 구글 관리형 SSL 인증서를 받기 위해서는 아래 그림을 참고해 주시기 바랍니다.

1) [App Engine] > [설정] > [맞춤 도메인] > [맞춤 도메인 추가]

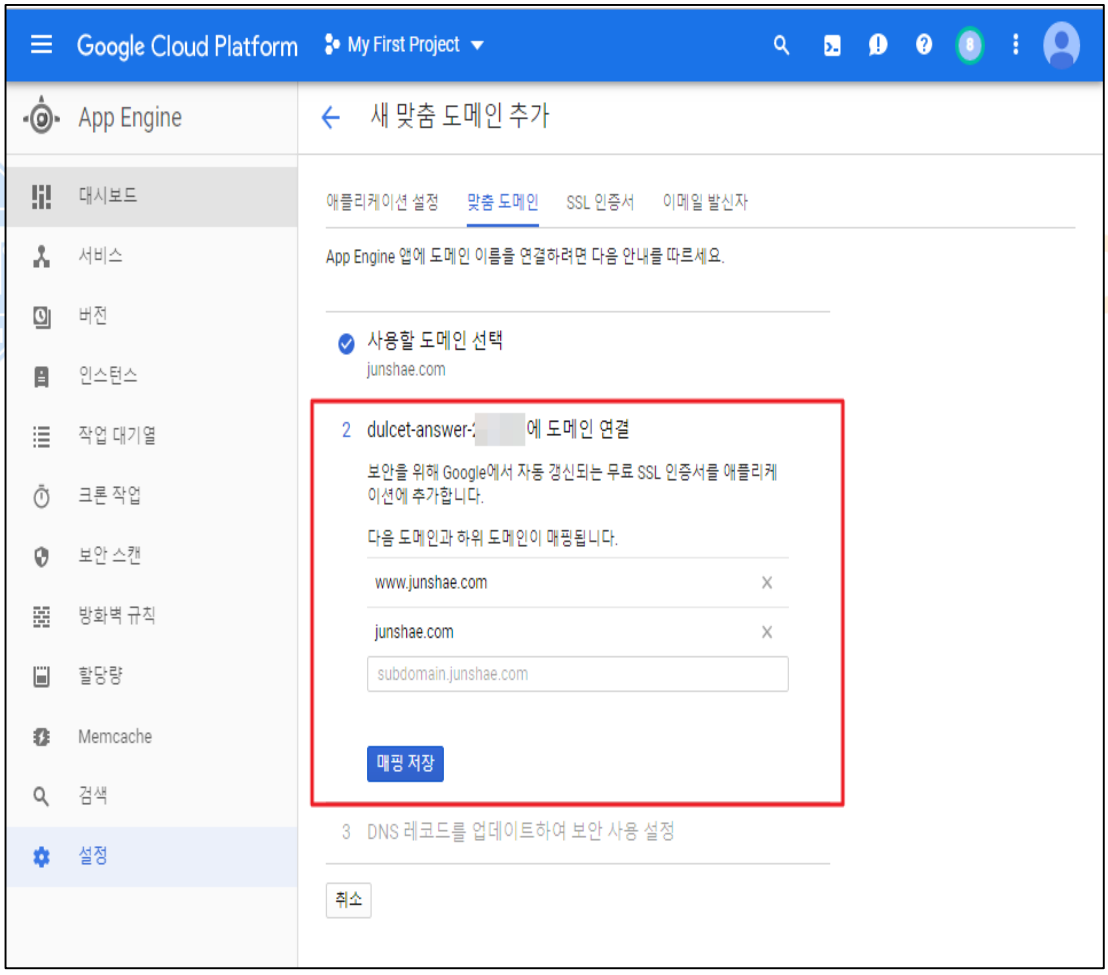


2) 사용할 도메인 선택

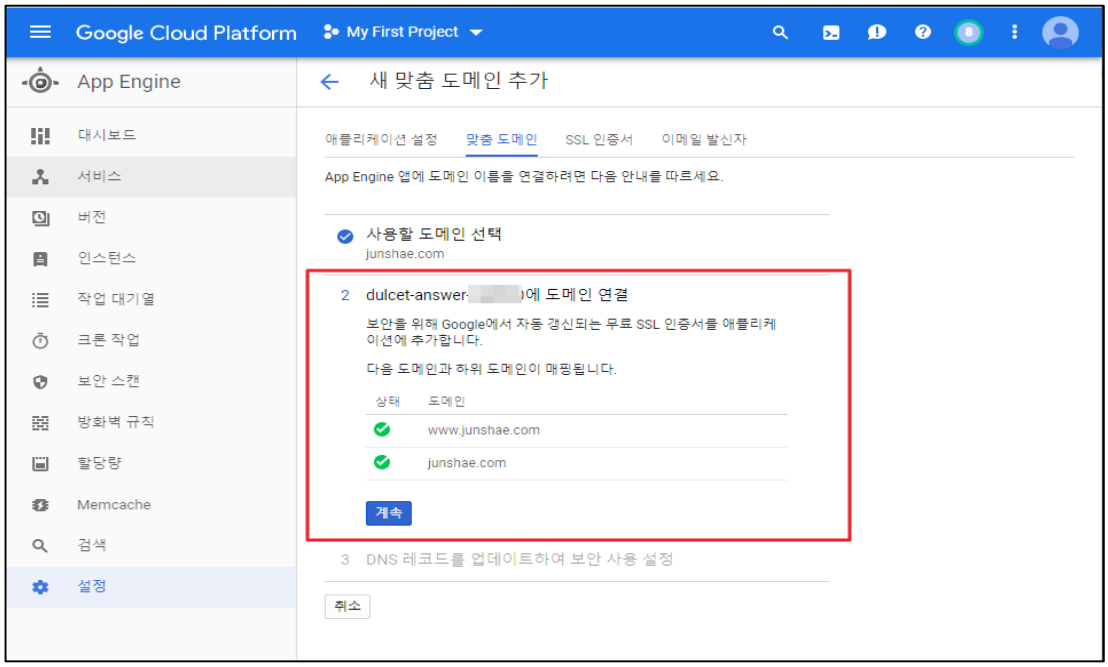
- Google Domain 및 기타 도메인 제공 업체 등에서 등록한 도메인 입력 설정



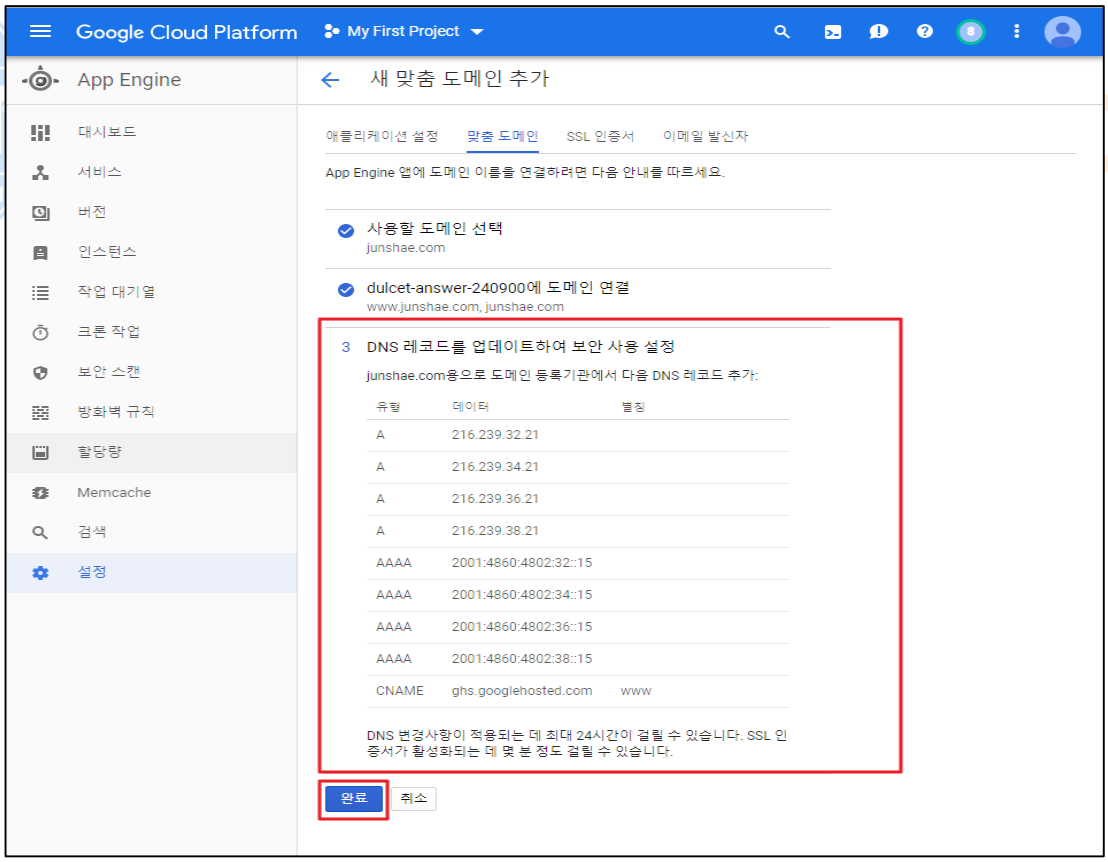
3) 사용할 하위 도메인 주소 등록



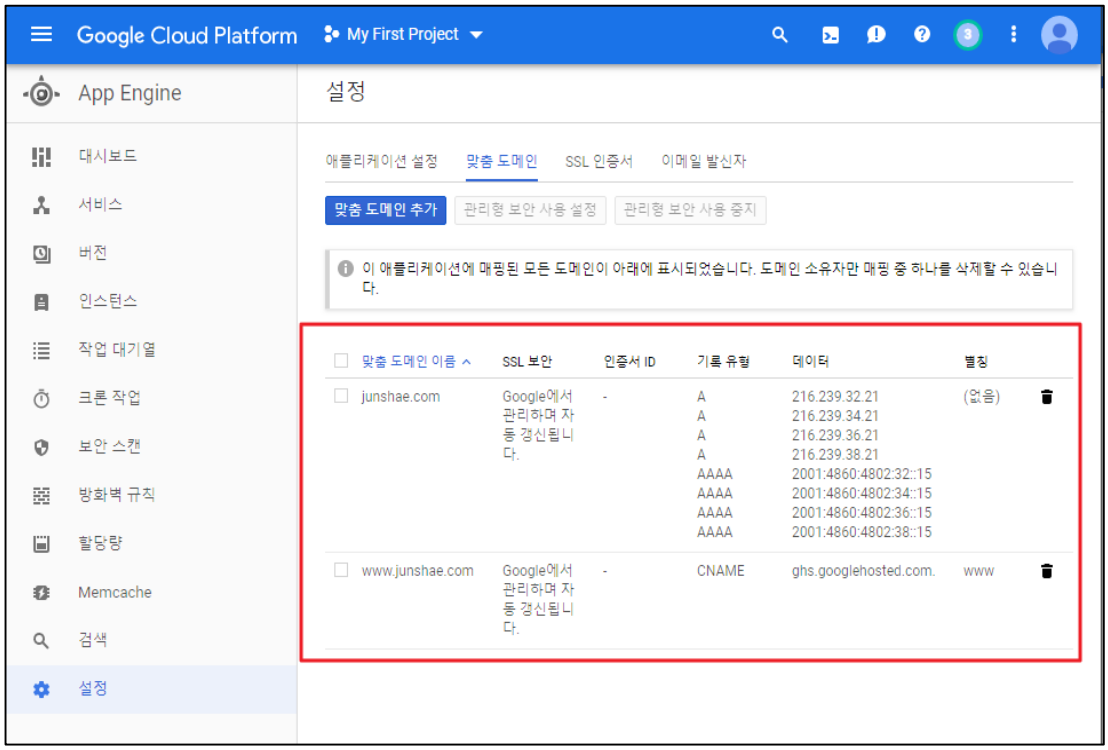
4) 하위 도메인 유효성 확인



5) App Engine 내에서 해당 도메인으로 매칭하여 사용하게 될 DNS 레코드(IPv4 / IPv6) 확인 및 맞춤 도메인 추가

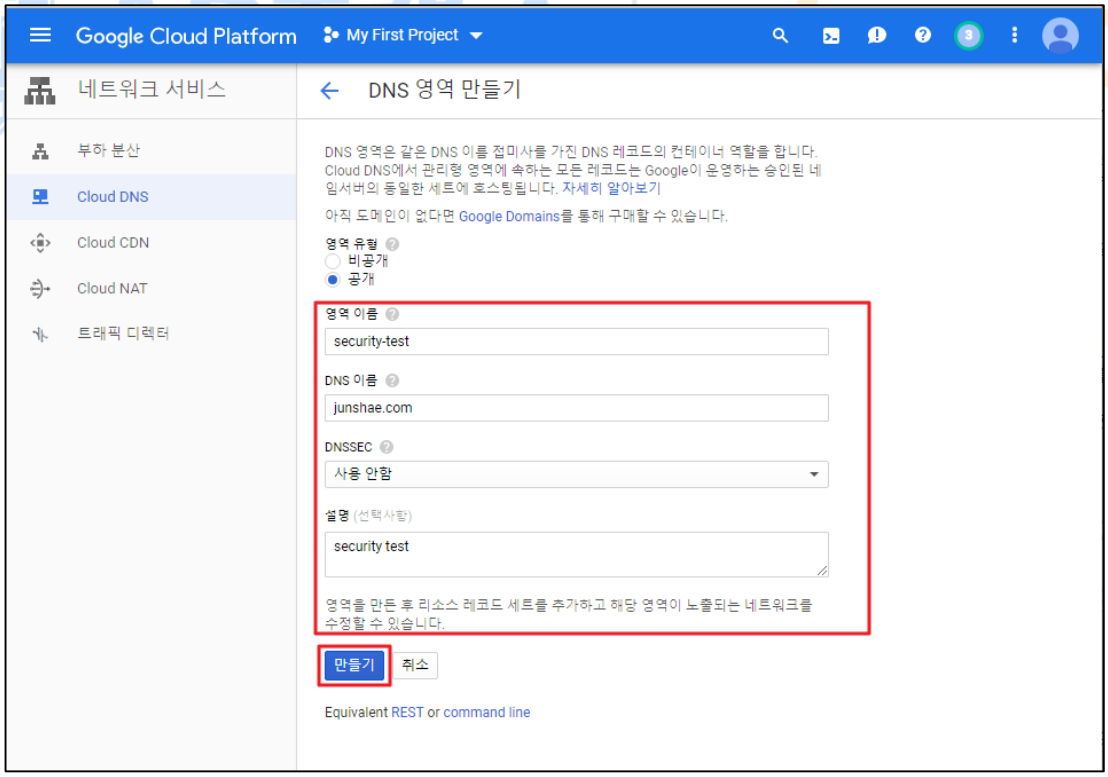


6) 맞춤 도메인 추가 완료



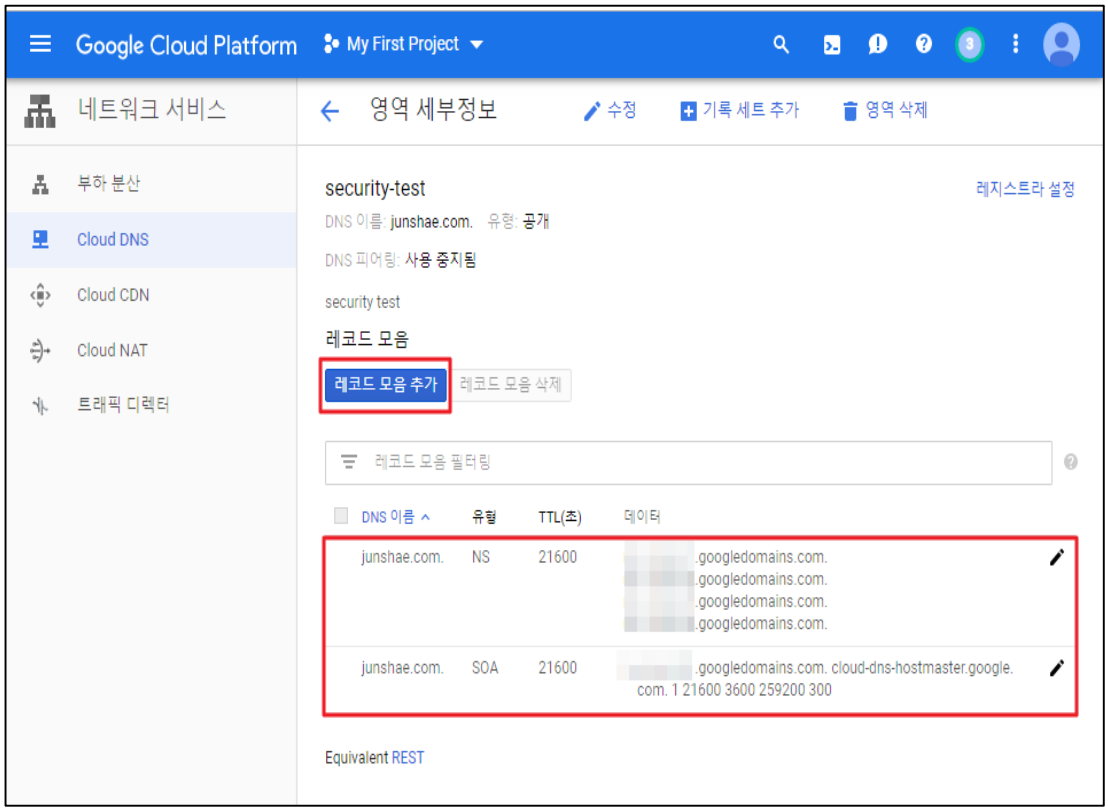
7) [네트워크 서비스] > [Cloud DNS] > [DNS 영역 만들기]

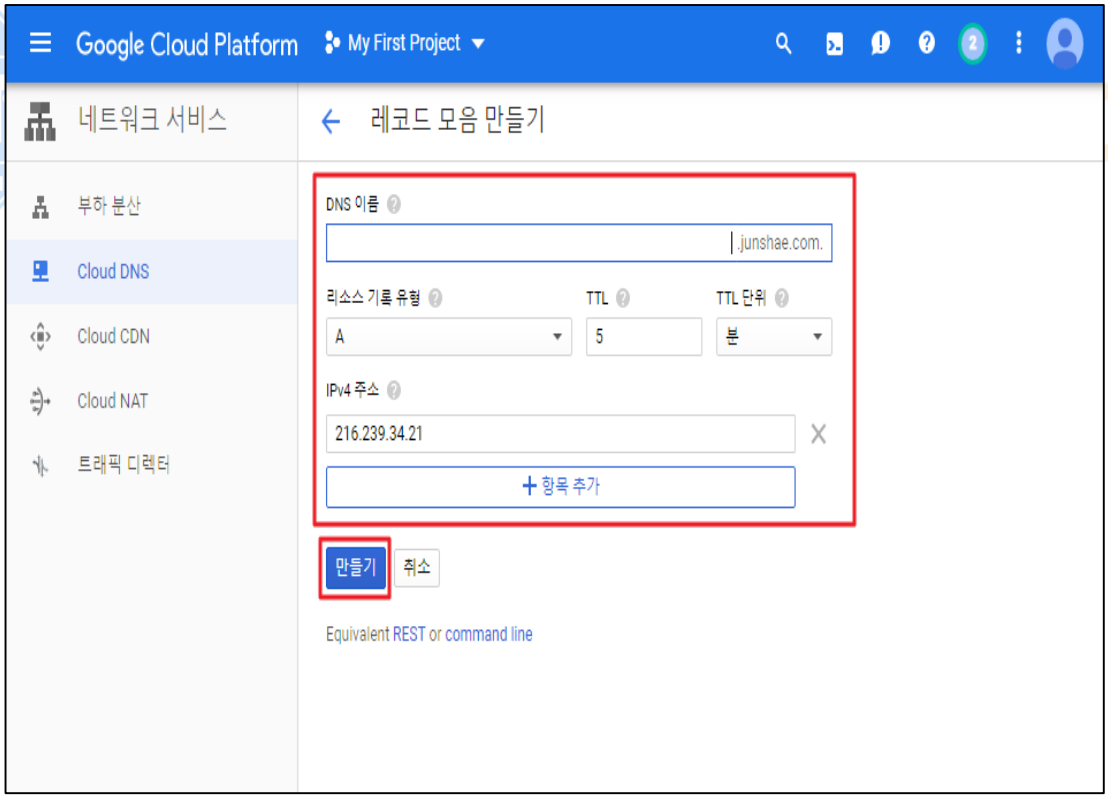
- App Engine 서비스에서 생성된 맞춤 도메인 사용을 위해 Cloud DNS 생성



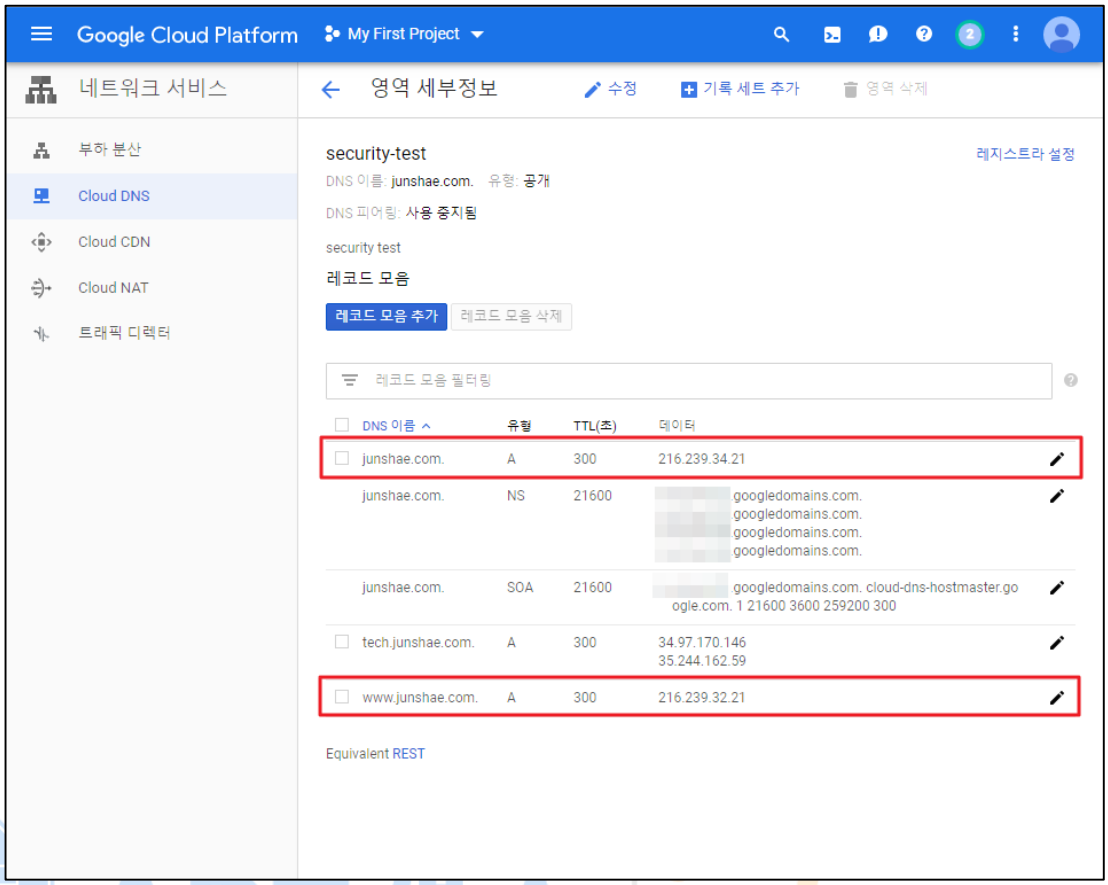
8) [레코드 모음 추가]

- App Engine 서비스에서 생성된 맞춤 도메인의 정보를 Cloud DNS에 등록 시도



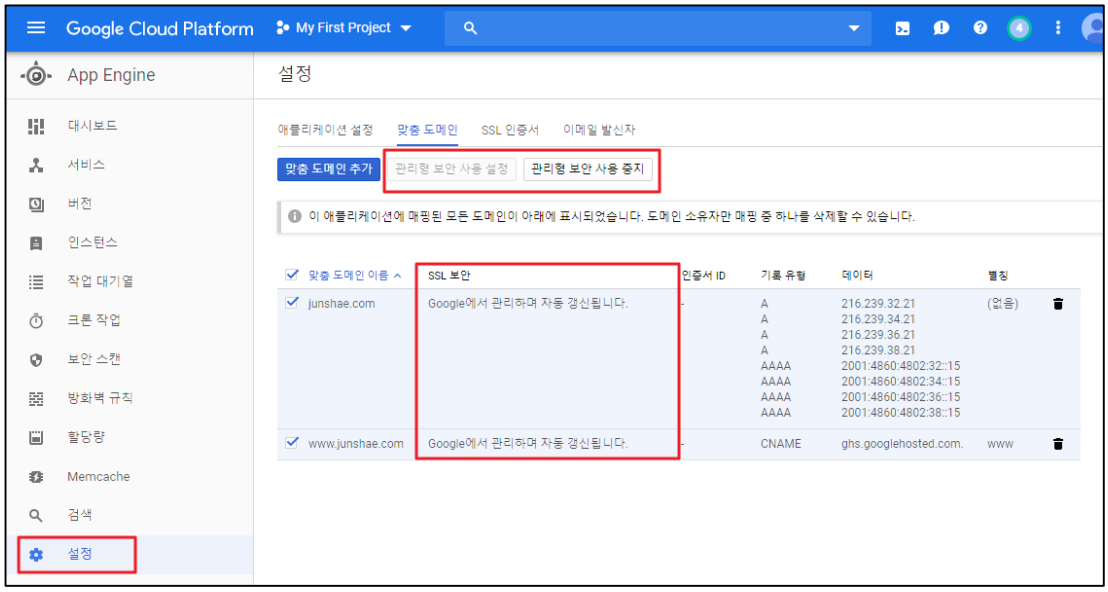


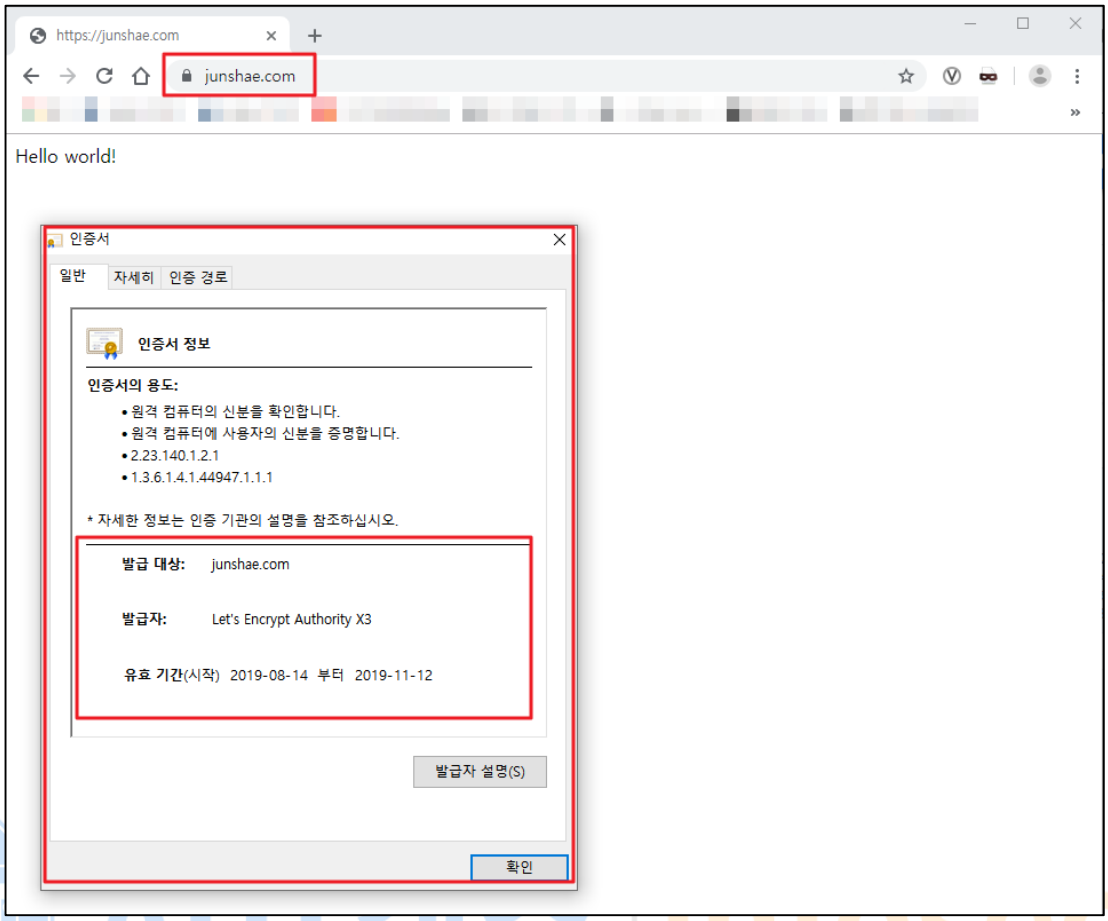
9) Cloud DNS 내 AppEngine 서비스와 연결하여 사용할 레코드 (도메인/IP) 추가 완료 확인



10) [App Engine] > [설정] > [맞춤 도메인]

- 맞춤 도메인 설정과 Cloud DNS의 설정이 정상적일 경우 아래 그림과 같이 별다른 에러 없이 구글 관리형 SSL 인증서(Let's Encrypt Authority) 사용이 가능함



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

※ 상기 설정 방법은 구글 관리형 SSL 인증서에 대해 다루어 졌으며, SSL 인증서 설정 시 참고용으로 이용하시기 바랍니다.</td></tr>
<tr><td>진단 기준</td><td>양호기준
: App Engine을 사용할 때 SSL(TLS)의 설정이 적용되어 있을 경우

취약기준
: App Engine을 사용할 때 SSL(TLS)의 설정이 적용되어 있지 않을 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

3. 가상 리소스 관리

3.1 ID 및 API 액세스

<table>
<tr><td>분류</td><td>가상 리소스 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">ID 및 API 액세스</td></tr>
<tr><td>항목
설명</td><td colspan="3">VM에서 실행되는 애플리케이션은 서비스 계정을 사용하여 Google Cloud API를 호출합니다. 사용할 서비스 계정과 허용할 API 액세스 수준을 선택할 수 있다.

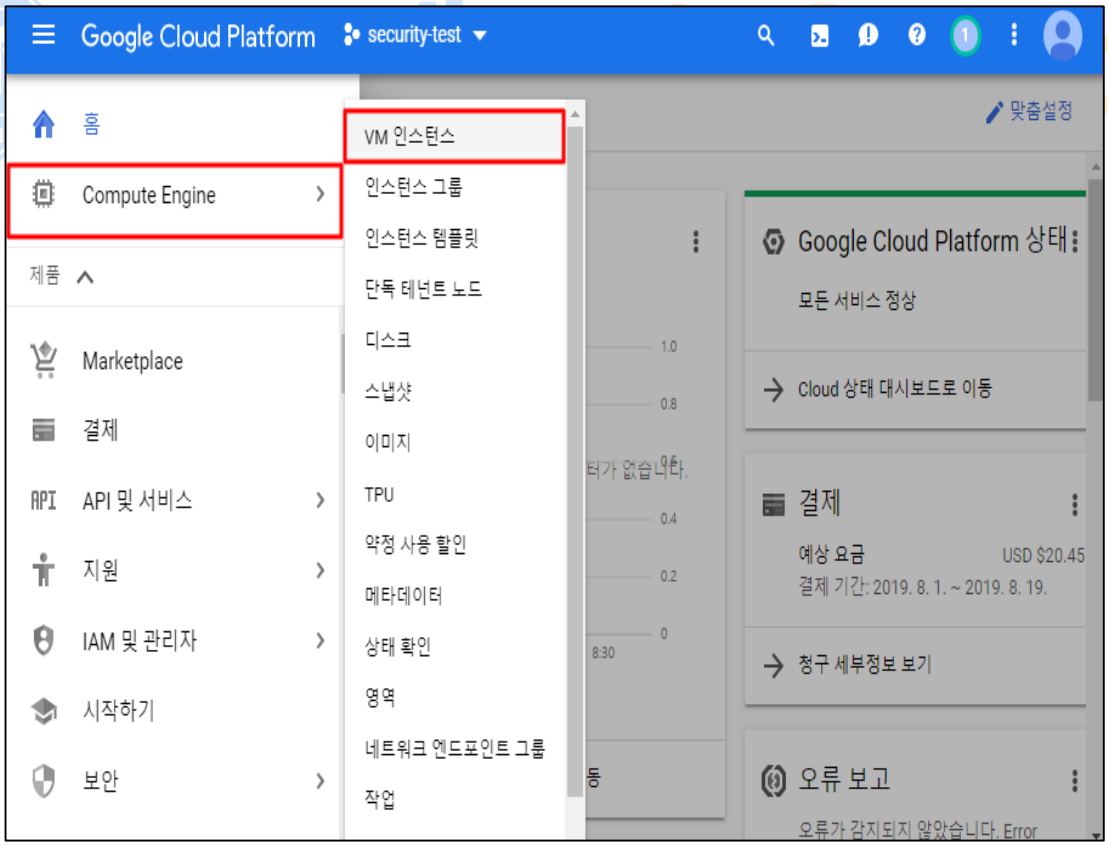
※ 액세스 설정 Google Cloud API 리스트
<table>
<tr><th>구분</th><th>상세내용</th></tr>
<tr><td>사용자 정보</td><td>임대 단위 생성 및 관리 기능을 포함하여 관리형 서비스 제작자가 서비스 소비자와의 관계를 관리할 수 있도록 지원하는 유틸리티를 제공합니다.</td></tr>
<tr><td>서비스 관리</td><td>관리형 서비스 게시 및 서비스 구성 관리 메소드를 제공합니다.</td></tr>
<tr><td>서비스 제어</td><td>액세스 제어, 로깅 및 모니터링 서비스와의 통합 등, 관리형 서비스에 대한 제어부 기능을 제공합니다.</td></tr>
<tr><td>작업 대기열</td><td>Google Cloud Platform 프로젝트에서 API 를 나열, 활성화, 비활성화하는 메소드를 제공합니다.</td></tr>
<tr><td>저장소</td><td>대량의 불변 데이터 객체를 저장하고 가져옵니다.</td></tr>
<tr><td>클라우드 소스 저장소</td><td>외부 데이터 소스의 데이터를 Google Cloud Storage 버킷에 전송하거나, Google Cloud Storage 버킷 사이에서 데이터를 전송합니다.</td></tr>
<tr><td>BigQuery</td><td>데이터 생성, 관리, 공유, 쿼리 기능을 제공합니다.</td></tr>
<tr><td>Bigtable 관리자</td><td>Cloud Bigtable 인스턴스, 클러스터, 테이블을 관리합니다.</td></tr>
<tr><td>Bigtable 데이터</td><td>테라바이트, 페타바이트 단위의 스키마 없는 데이터를 저장하는 NoSQL 빅데이터 솔루션에 액세스합니다.</td></tr>
<tr><td>Cloud 게시/구독</td><td>애플리케이션 사이에서 안정적인 다대다 비동기 메시징 기능을 제공합니다.</td></tr>
<tr><td>Cloud Datastore</td><td>스키마 없는 NoSQL 문서 데이터베이스에 액세스하여 애플리케이션을 위한 강력하고 확장성이 뛰어난 완전 관리형 저장소를 제공합니다.</td></tr>
</table></td></tr>
</table>

Cloud Debugger	실행 중인 애플리케이션을 중단하거나 지연시키지 않고, 애플리케이션의 호출 스택과 변수를 조사합니다.
Cloud SQL	완전 관리형 MySQL 데이터베이스를 제공하는 Cloud SQL 인스턴스를 생성하고 구성합니다.
Compute Engine	Google Cloud Platform 에서 가상 머신을 생성하고 실행합니다.
Stackdriver 추적	Stackdriver Trace 에 추적 데이터를 보내고 가져옵니다. App Engine 애플리케이션은 기본값으로 데이터를 생성하므로, 별도의 작업 없이 이용할 수 있습니다. 다른 애플리케이션의 데이터는 Stackdriver Trace 에 기록하여 표시, 보고, 분석 등의 기능을 이용할 수 있습니다.
Stackdriver Logging API	로그 항목을 쓰고 로그, 로그 내보내기, 로그 기반 측정항목을 관리합니다.
Stackdriver Monitoring API	Stackdriver Monitoring 데이터 및 구성을 관리합니다.

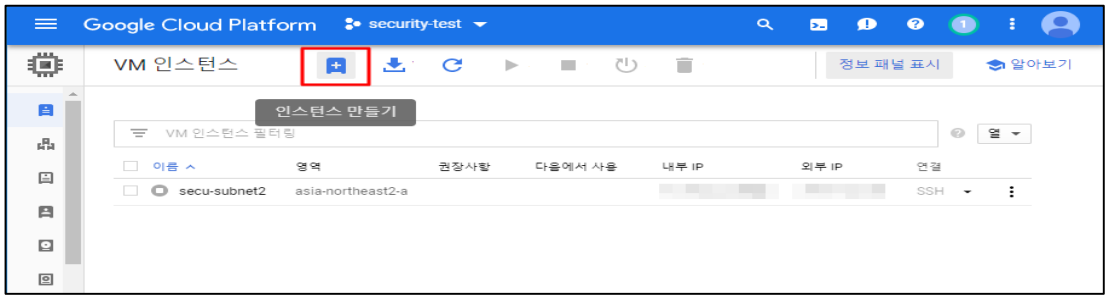
설정 방법

가. ID 및 API 액세스 설정

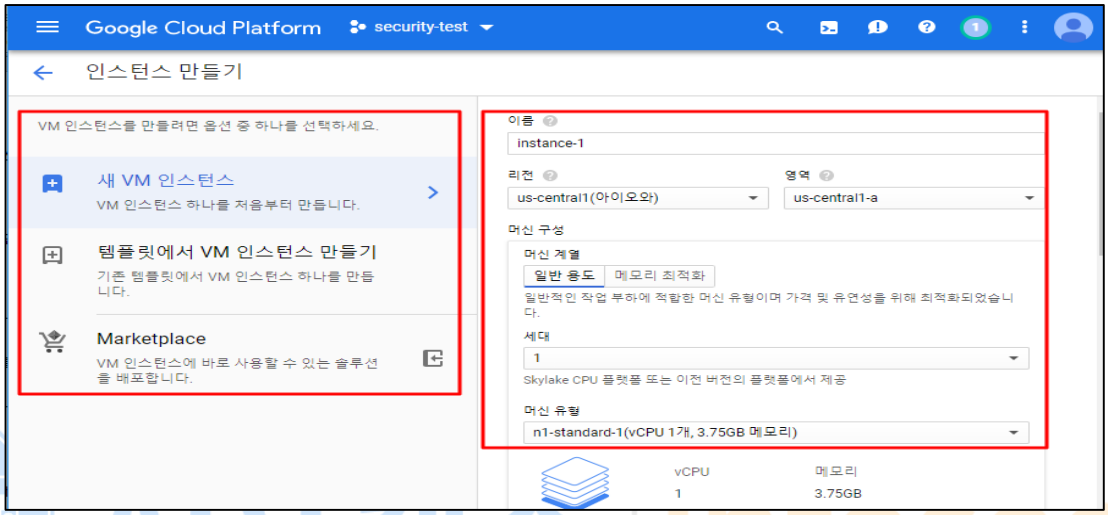
1) [메인] > [Compute Engine] > [VM 인스턴스]



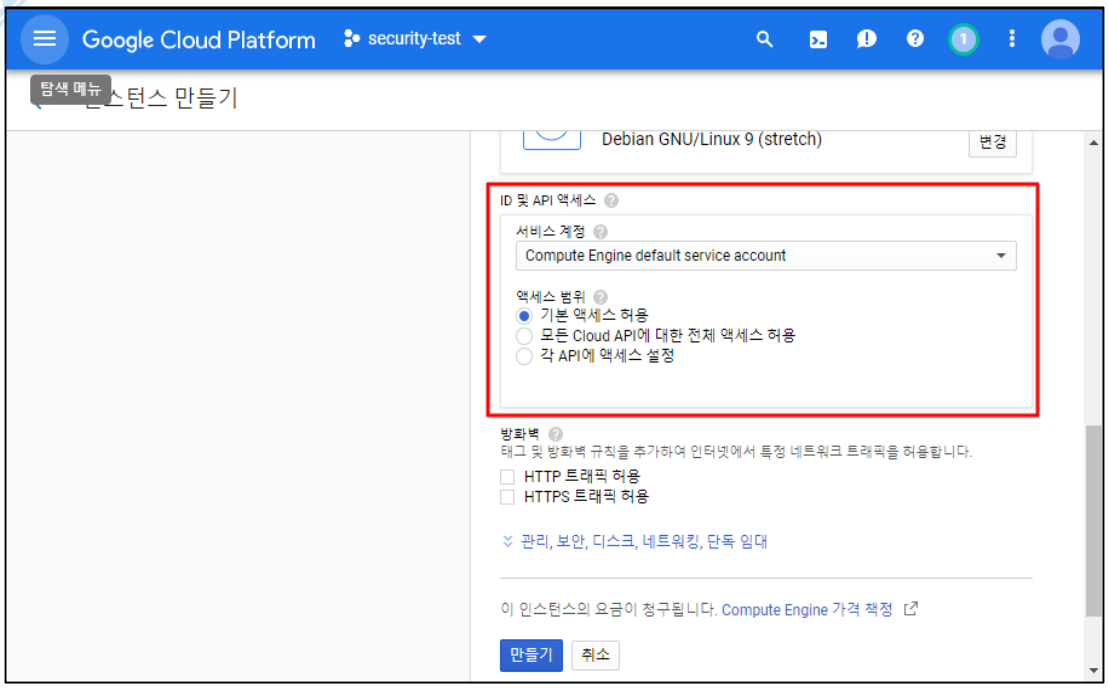
2) 인스턴스 만들기



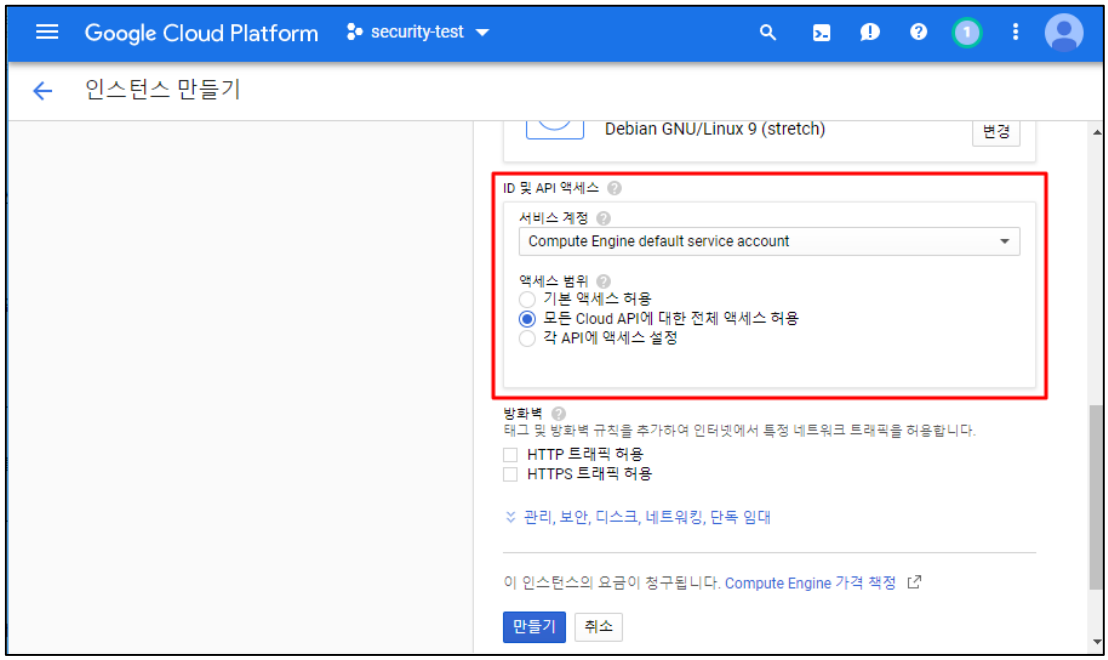
3) VM 인스턴스 옵션 및 정보 입력



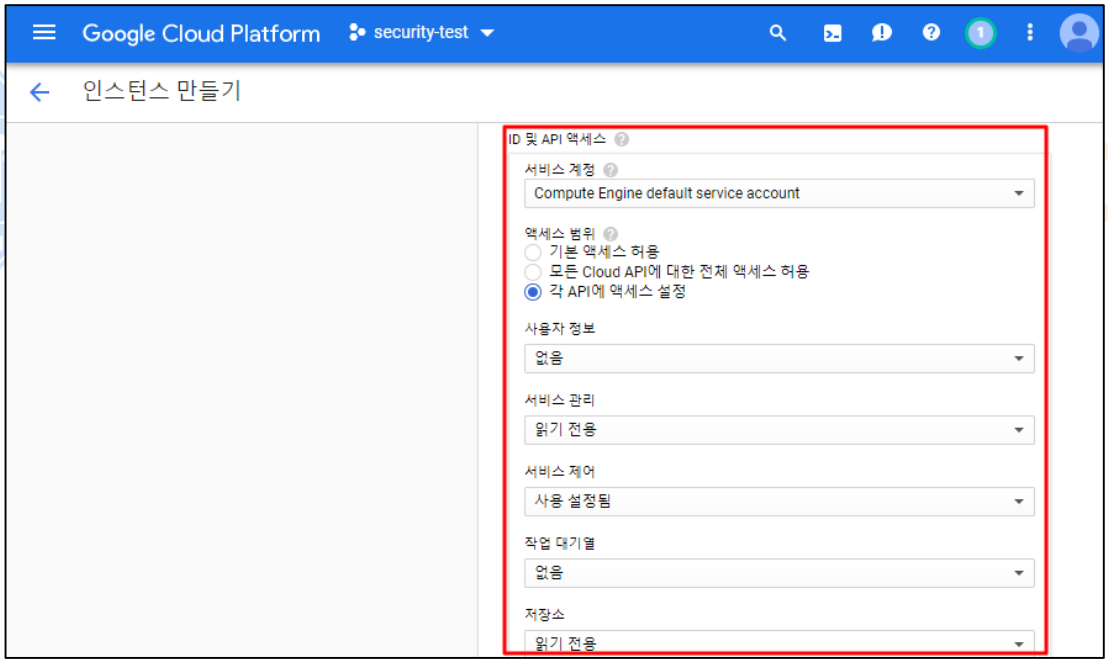
4) '기본 액세스 허용' 액세스 범위 설정

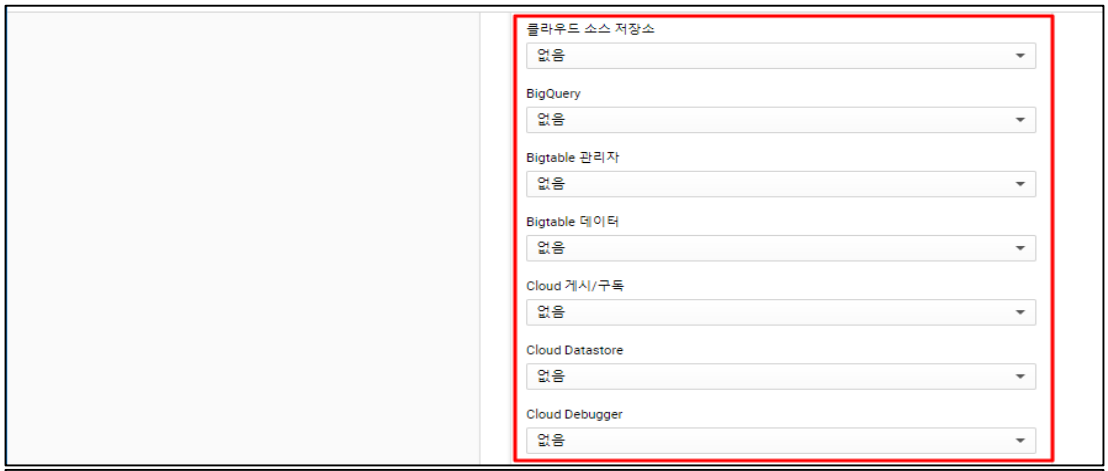


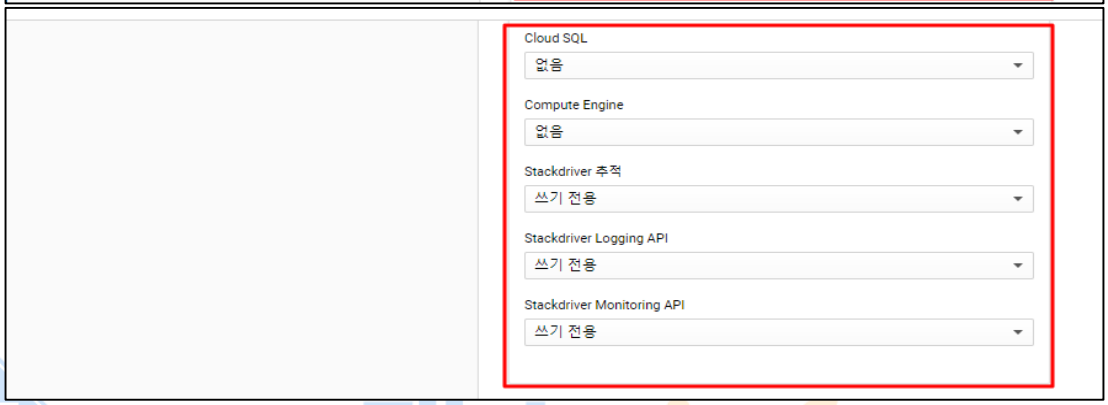
5) '모든 Cloud API 에 대한 전체 액세스 허용' 액세스 범위 설정

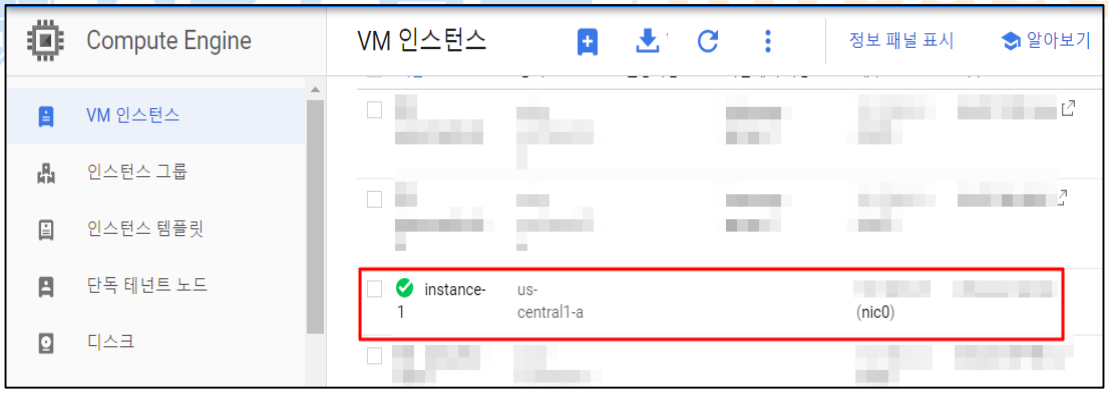


6) '각 API 에 액세스 설정' 액세스 범위 설정



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




7) 인스턴스 생성 완료


</td>
</tr>
<tr>
<td>진단 기준</td>
<td>
양호기준
: 서비스 역할에 맞게 API 액세스 설정이 되어 있는 경우

취약기준
: 서비스 역할에 맞게 API 액세스 설정이 되어 있지 않은 경우
</td>
</tr>
<tr>
<td>비고</td>
<td></td>
</tr>
</table>

3.2 VM 인스턴스 관리 및 보안

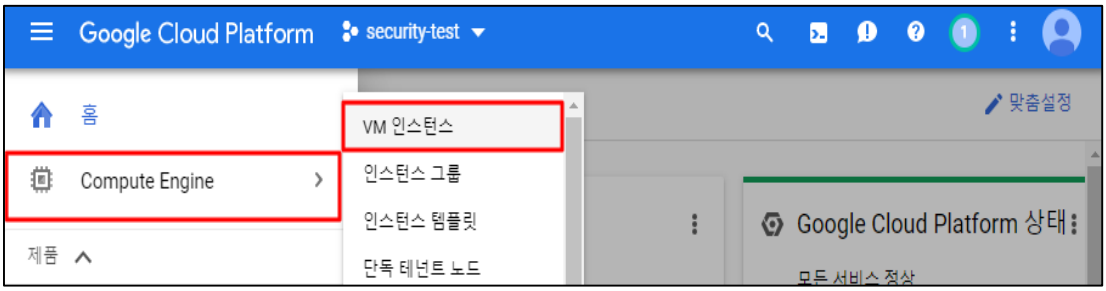
<table>
<tr><td>분류</td><td>가상 리소스 관리</td><td>중요도</td><td>하</td></tr>
<tr><td>항목명</td><td colspan="3">VM 인스턴스 관리 및 보안</td></tr>
<tr><td>항목
설명</td><td colspan="3">VM 인스턴스 삭제 작업 부하 중에는 SQL 서버를 실행하는 인스턴스, 라이선스 관리자로 사용되는 서버 등과 같이 애플리케이션 또는 서비스를 실행하는 데 필수적인 특정 VM 인스턴스가 존재할 수 있습니다. 이러한 VM 인스턴스는 지속적으로 실행되어야 하므로, VM이 삭제되지 않도록 보호할 수 있는 방법이 필요하며, VM 삭제보호 (deletionProtection 속성)를 설정하면 VM 인스턴스가 실수로 삭제되지 않도록 보호할 수 있습니다. deletionProtection 플래그가 설정된 VM 인스턴스를 다른 사용자가 삭제하려고 시도하면 삭제 요청이 실패합니다. compute.instances.create 권한이 부여된 사용자만 이 플래그를 재설정하여 리소스 삭제를 허용할 수 있습니다.

또한, 보안 설정된 VM은 Compute Engine VM 인스턴스의 검증 가능한 무결성을 제공하므로, 부팅 또는 커널 수준의 멀웨어나 루트킷으로 인한 침해로부터 인스턴스의 안전을 보장합니다. 보안 설정된 VM의 검증 가능한 무결성은 안전한 부팅, vTPM(virtual Trusted Platform Module)이 지원되는 신중한 부팅, 무결성 모니터링 등을 통해 얻을 수 있습니다.

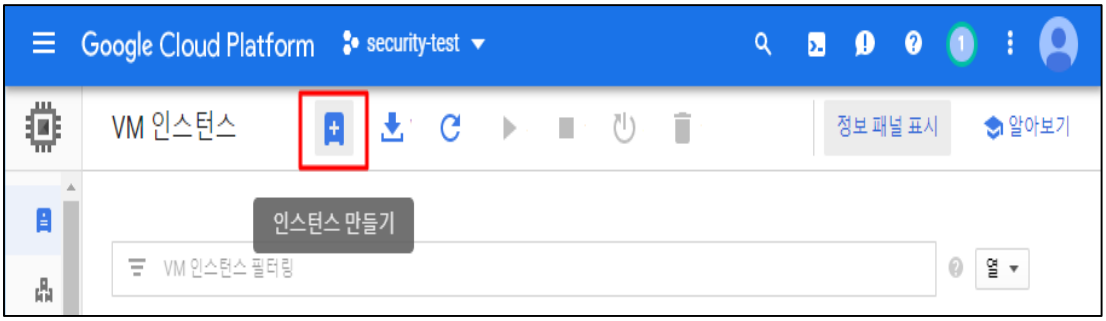
※ VM 인스턴스 보안 설정
<table>
<tr><th>제목</th><th>설명</th></tr>
<tr><td>보안 부팅 설정</td><td>안전한 부팅에서는 모든 부팅 구성요소의 디지털 서명을 확인하고 서명 확인에 실패할 경우 부팅 프로세스를 중단하여 시스템에서 인증된 소프트웨어만 실행하도록 보장합니다.</td></tr>
<tr><td>vTPM 설정</td><td>vTPM은 가상화된 신뢰할 수 있는 플랫폼 모듈로서 키 및 인증서 등 시스템 액세스 인증에 사용하는 객체를 보호하는 데 사용할 수 있는 특수한 컴퓨터 칩입니다. 보안 설정된 VM vTPM은 TPM(Trusted Computing Group) 라이브러리 사양 2.0과 완벽하게 호환되며 FIPS 140-2 L1 인증을 받은 BoringSSL을 사용합니다.</td></tr>
<tr><td>무결성 모니터링 사용 설정</td><td>무결성 모니터링은 VM 인스턴스의 상태를 파악하고 결정을 내리도록 도와주며, 최신 부팅 측정을 무결성 정책 기준과 비교하고 일치 여부에 따라 이전 부팅 시퀀스와 이후 부팅 시퀀스로 이루어진 한 쌍의 성공/실패 결과를 반환합니다.</td></tr>
</table>
※ 무결성 모니터링은 신중한 부팅에서 수집하는 데이터를 기반으로 하기 때문에 vTPM을 사용 중지하면 무결성 모니터링도 사용 중지됩니다. 또한, ‘보안 설정된 VM’ 기능은 현재 베타 기능으로 적용 시 참고바랍니다.</td></tr>
<tr><td>설정</td><td colspan="3">가. VM 인스턴스 보안 설정</td></tr>
</table>

방법

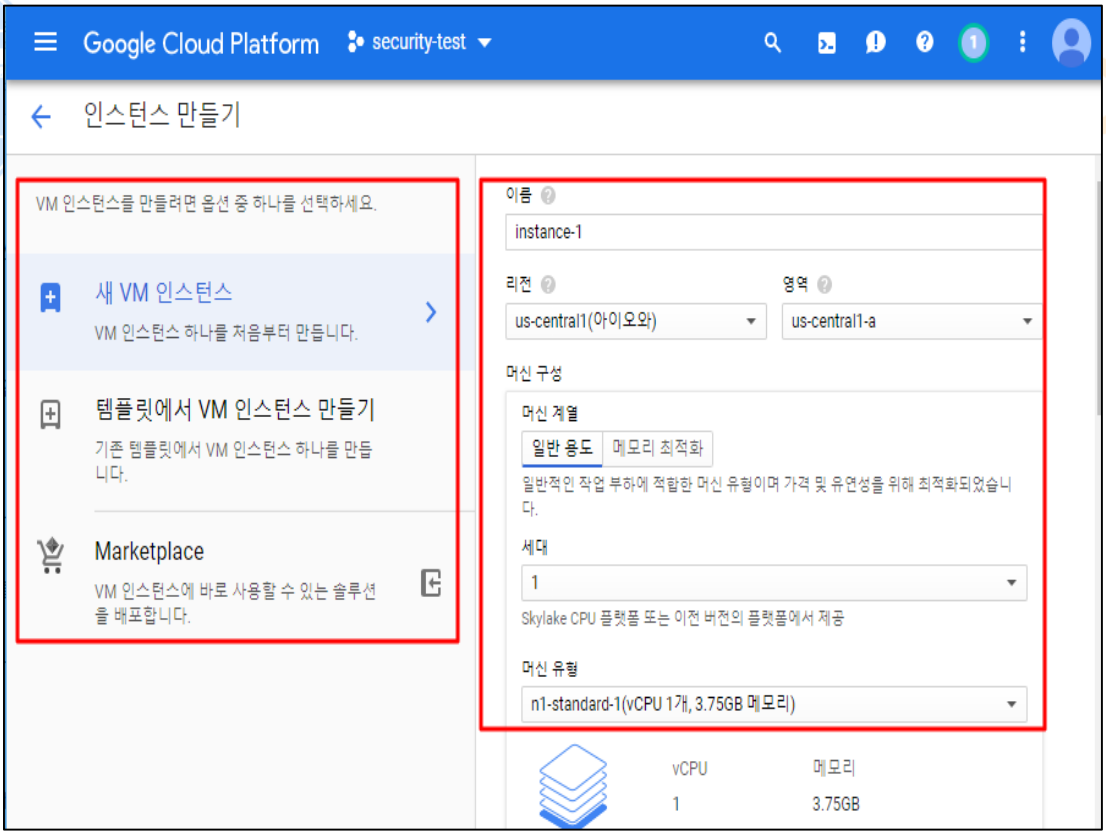
1) [메인] > [Compute Engine] > [VM 인스턴스]



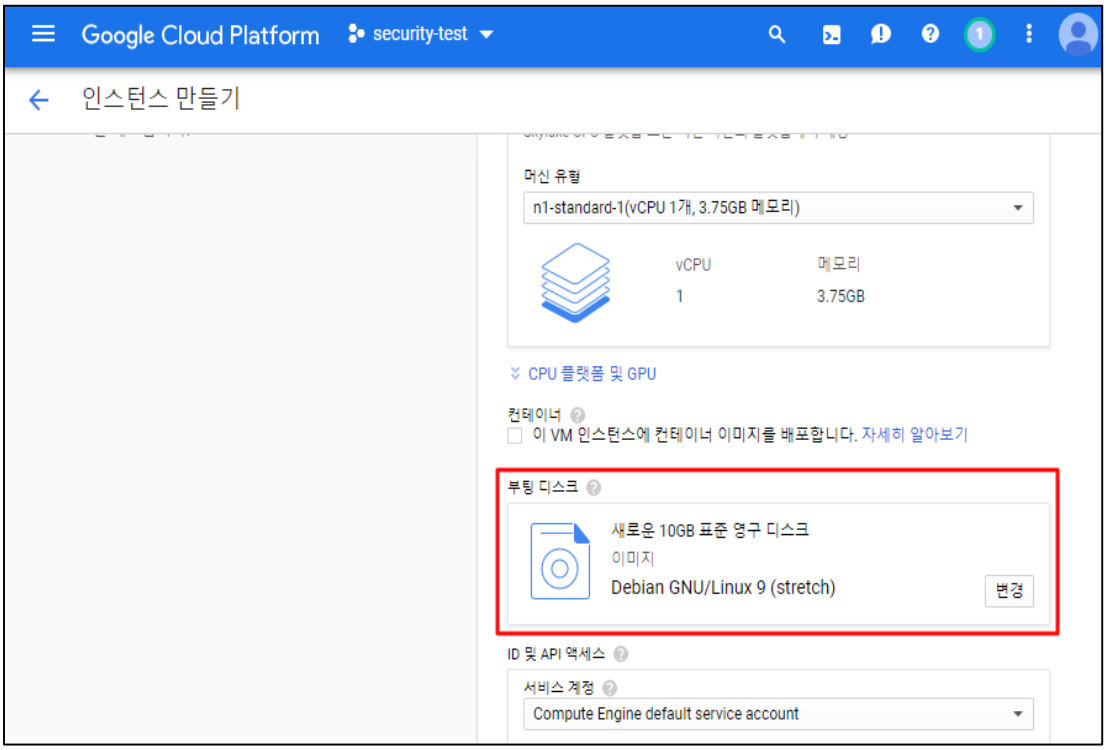
2) 인스턴스 만들기



3) VM 인스턴스 옵션 및 정보 입력

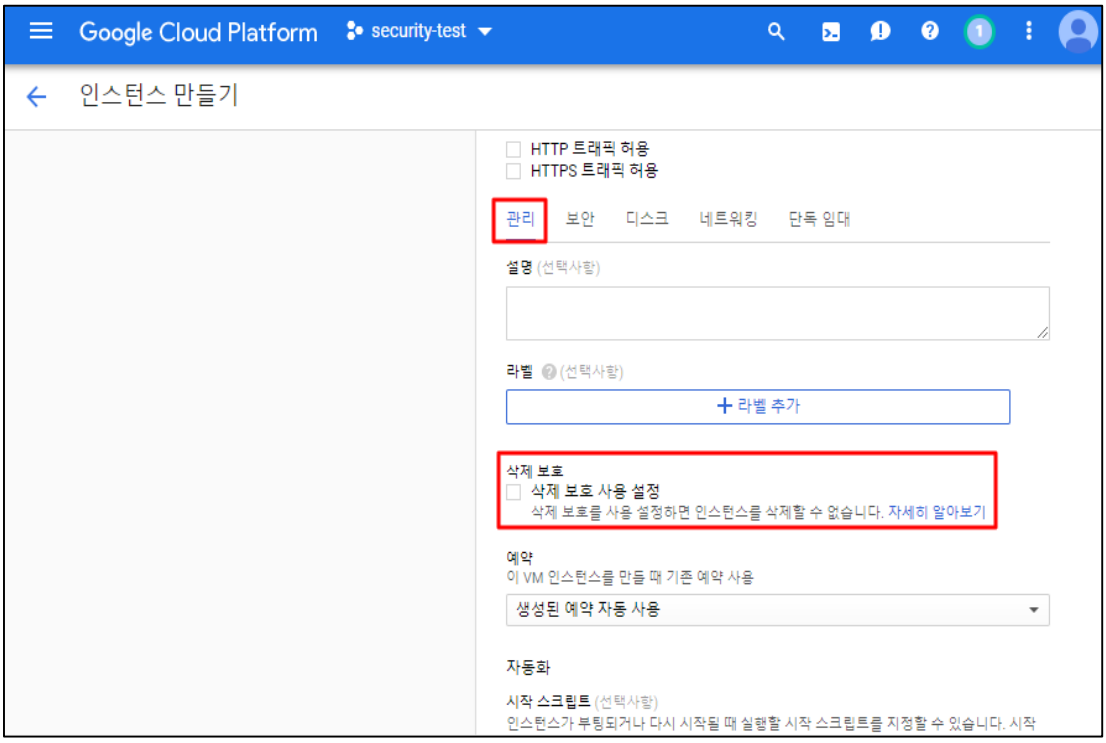


4) 부팅 디스크 변경

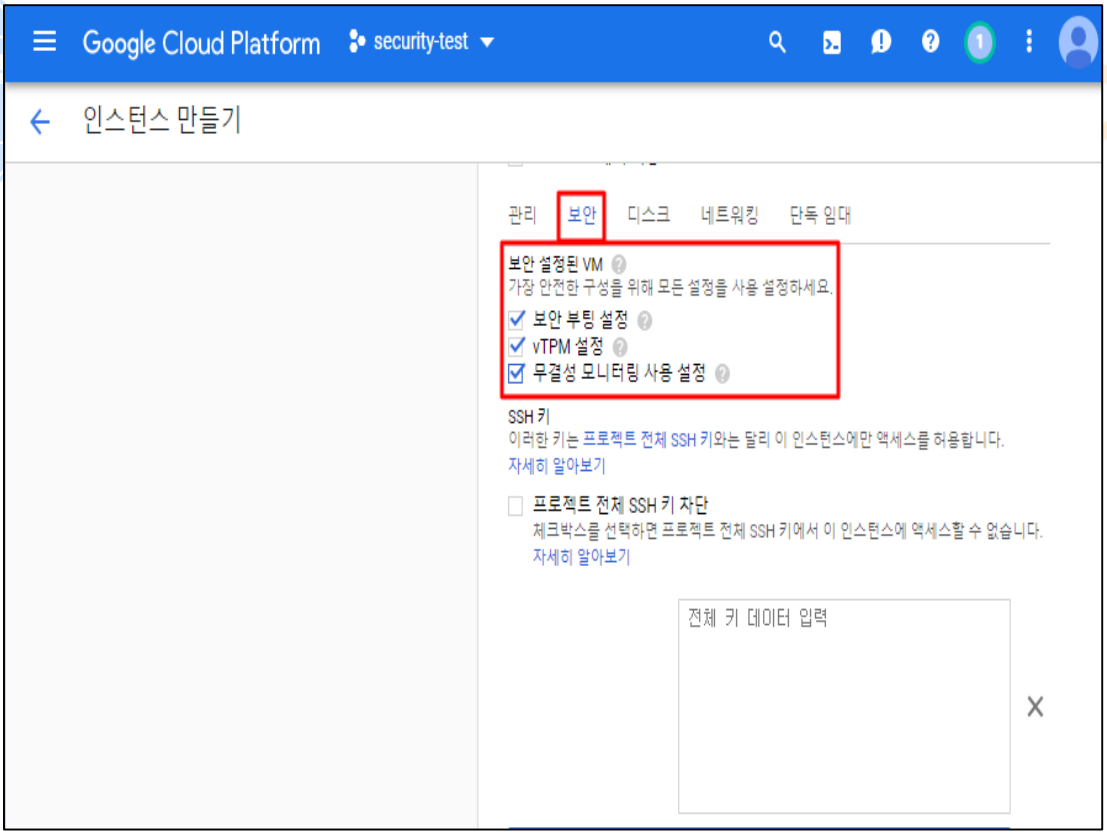


5) 보안 설정된 VM 이미지 설정

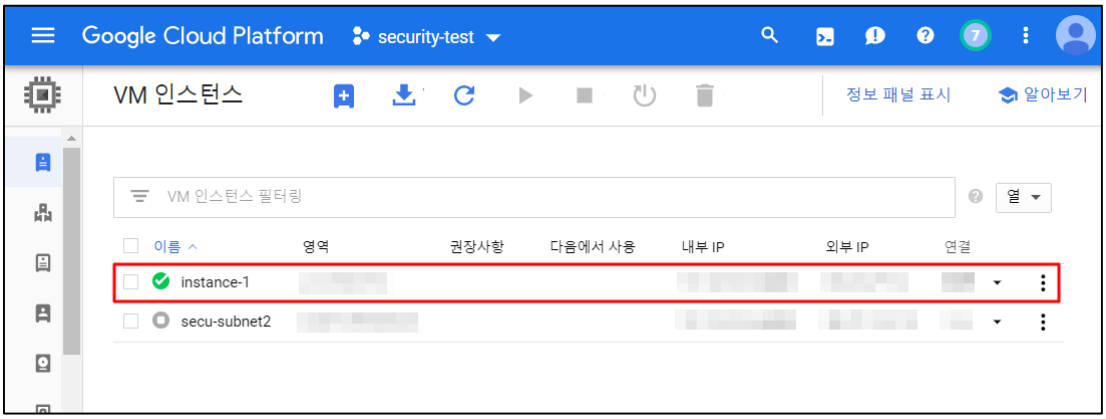
6) [관리] > [삭제 보호 사용 설정]



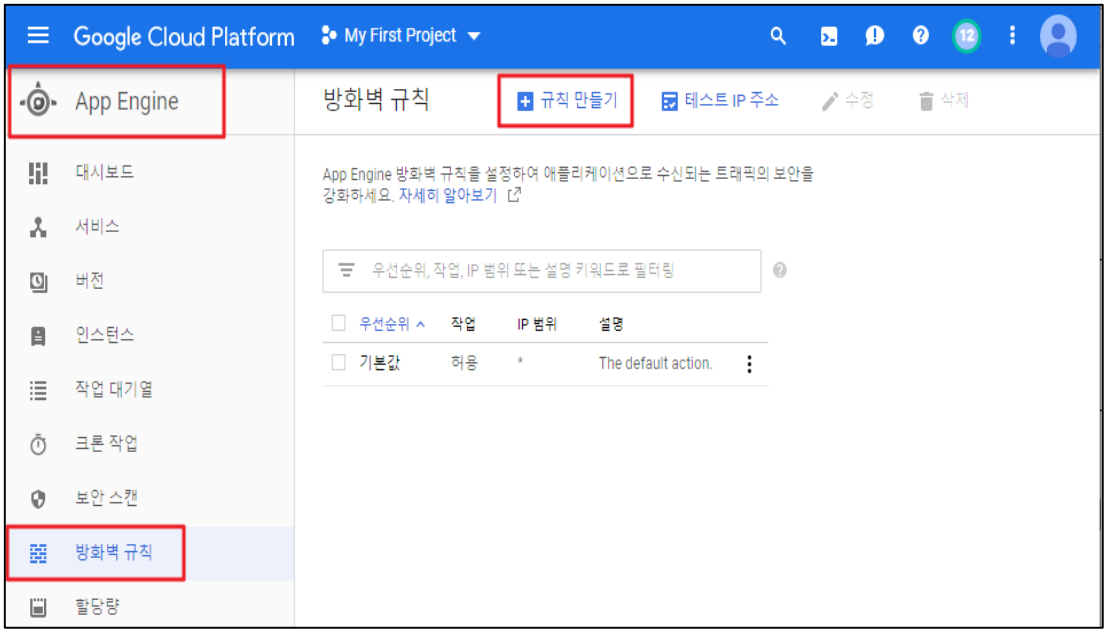
7) [보안] > [보안 설정된 VM] > [보안부팅 설정], [vTPM 설정], [무결성 모니터링 사용 설정]

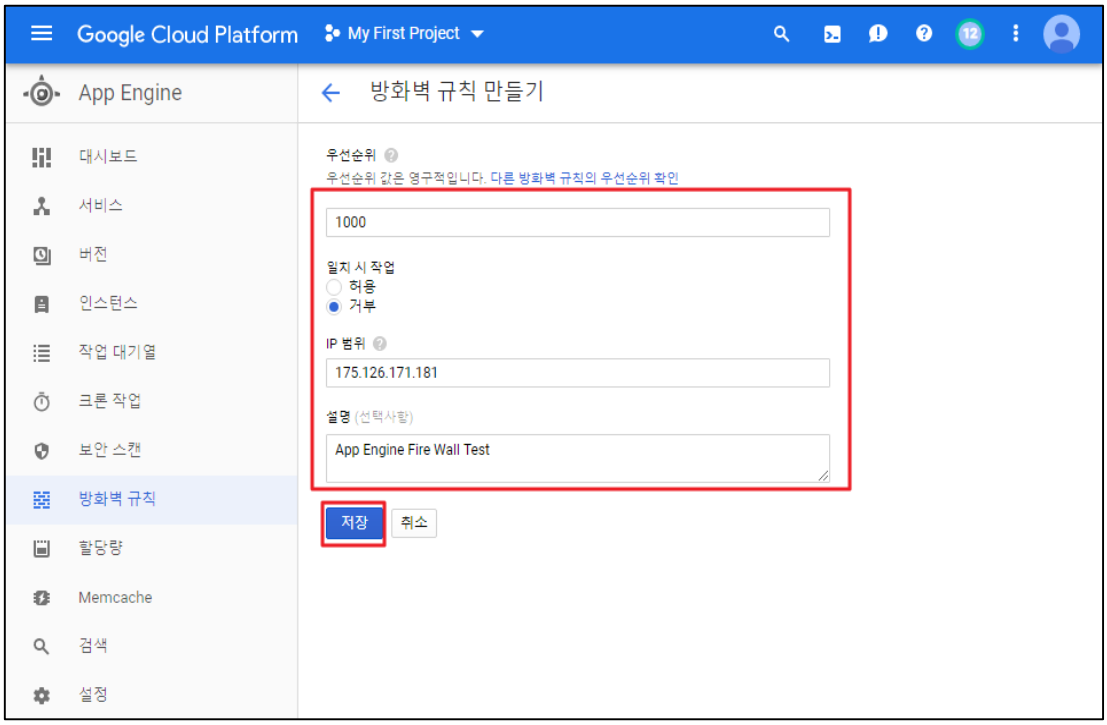


8) 보안 설정된 인스턴스 생성 완료

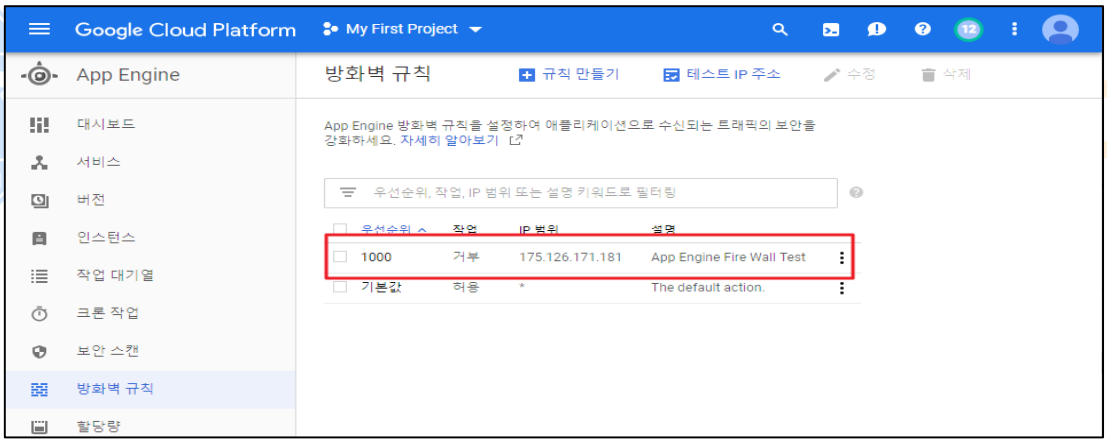
	
진단 기준	**양호기준** : 인스턴스 보안 부팅 설정을 사용하고 있을 경우 **취약기준** : 인스턴스 보안 부팅 설정을 사용하고 있지 않을 경우
비고	

3.3 애플리케이션 방화벽 (App Engine)

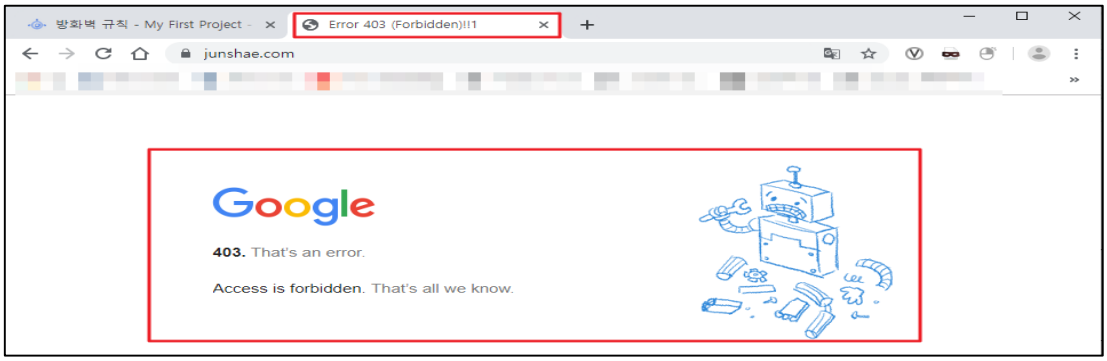
분류	가상 리소스 관리	중요도	중
항목명	애플리케이션 방화벽 (App Engine)		
항목 설명	App Engine 방화벽을 사용하면 사용자가 지정된 IP 주소 범위의 요청을 허용하거나 거부할 수 있는 규칙 집합을 통해 App Engine 앱에 대한 액세스를 제어할 수 있습니다. 방화벽에서 차단된 트래픽 또는 대역폭은 요금이 청구되지 않습니다. 또한, 방화벽 규칙은 중요도에 따라 정렬되며, 중요도는 각 규칙의 우선순위에 숫자 값으로 정의합니다. 각 규칙에 고유한 우선순위 값을 지정해야 합니다. 이 값은 방화벽의 다른 규칙에 대한 상대적인 중요도를 정의합니다. 규칙의 우선순위 값은 가장 중요한 값인 1 부터 가장 중요하지 않은 값인 2147483647 까지입니다. 각 방화벽은 2147483647 우선순위로 자동 생성되는 default 규칙을 포함하며 앱의 전체 IP 범위에 적용됩니다. default 규칙은 항상 방화벽의 다른 모든 규칙 이후에 평가되고 모든 IP 주소의 모든 요청에 적용됩니다. 방화벽은 우선순위가 가장 높은 규칙을 가장 먼저 평가합니다. 방화벽의 나머지 모든 규칙은 규칙이 해당 요청의 IP 범위와 일치할 때까지 순차적으로 평가됩니다. 일치하는 규칙이 발견되면 연결이 허용되거나 거부되고 방화벽의 나머지 모든 규칙은 건너뛰게 됩니다. 요청과 일치하는 방화벽에 수동으로 정의된 규칙이 없으면 default 규칙이 평가됩니다.		
설정 방법	**가. App Engine 방화벽 내 규칙 생성** 1) [App Engine] > [방화벽 규칙] > [규칙 만들기] - App Engine 서비스 내 방화벽 규칙 생성 시도  2) 적용하고자 하는 서비스에 대해 방화벽 규칙 설정		



3) 방화벽 규칙 생성 확인

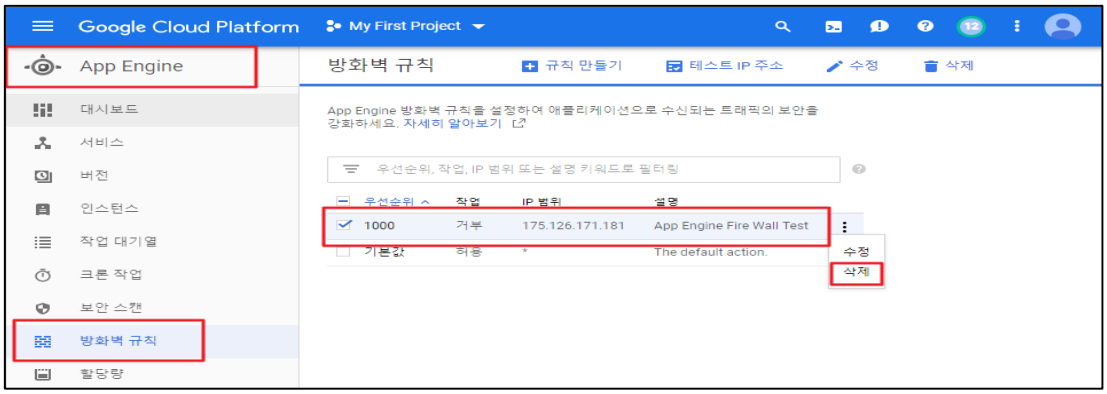
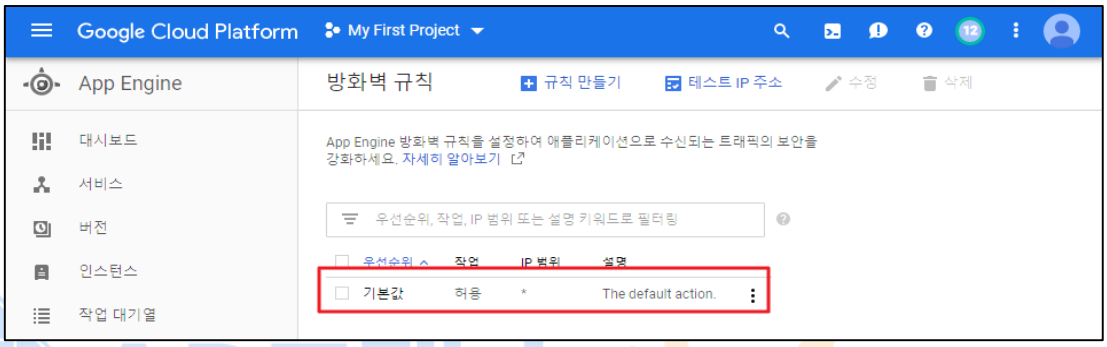
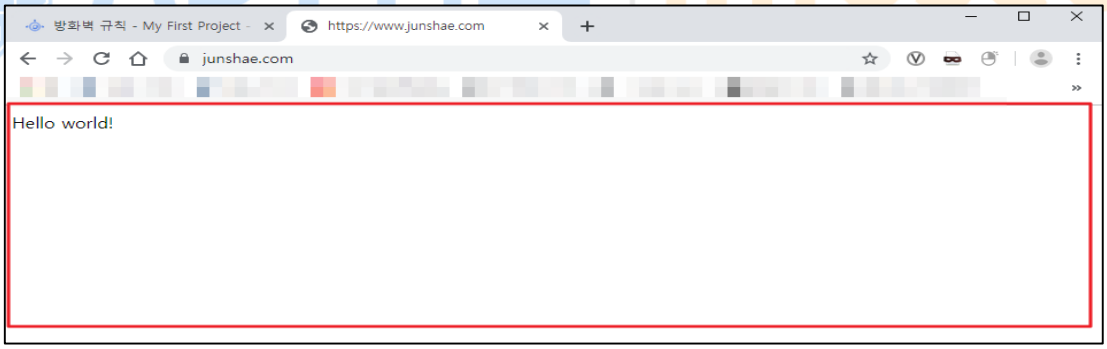


4) App Engine 방화벽 규칙 적용 확인



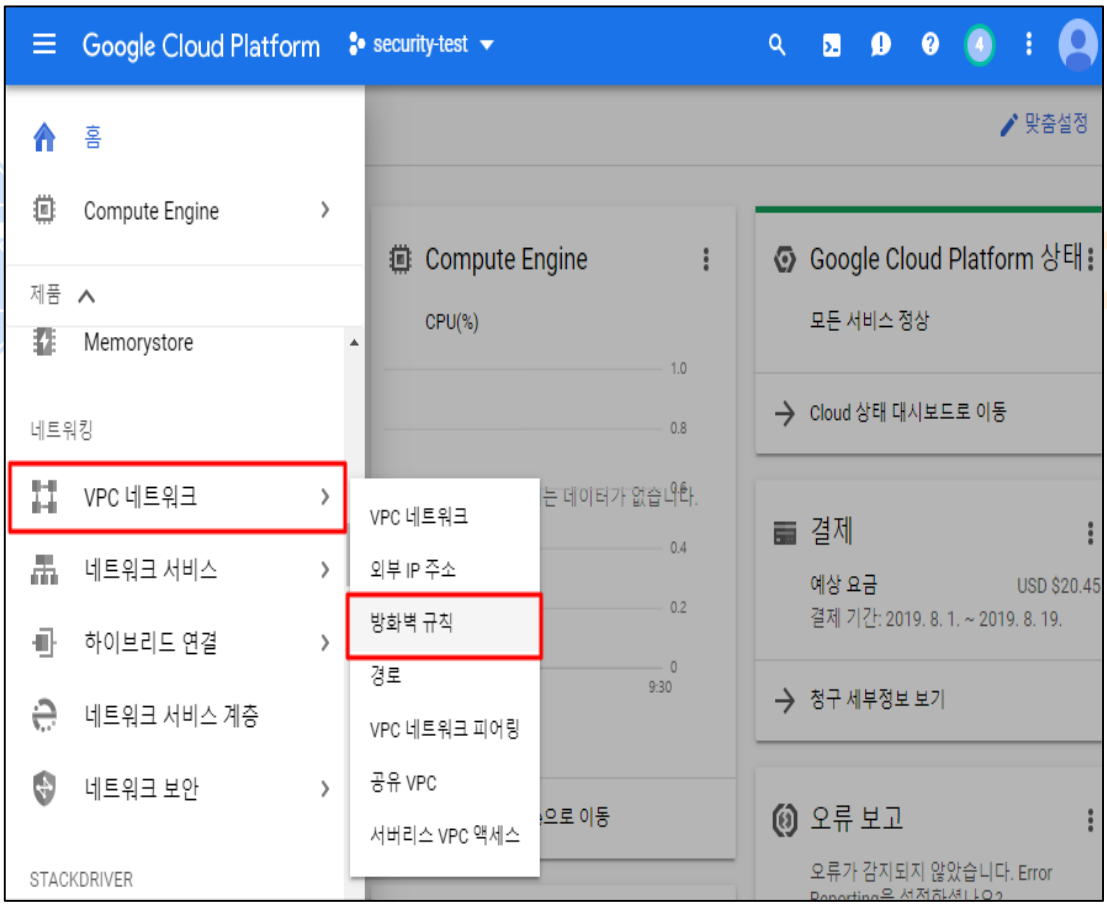
나. App Engine 방화벽 내 규칙 삭제

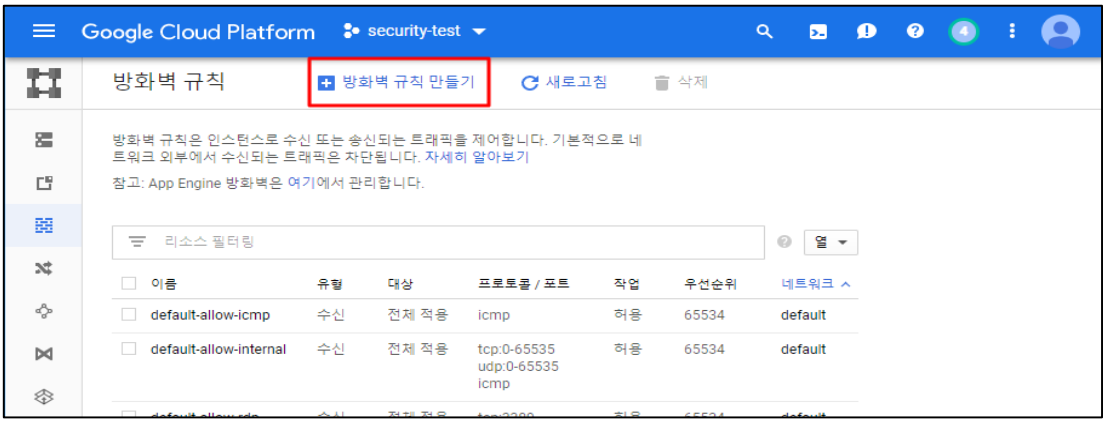
1) [App Engine] > [방화벽 규칙] > [규칙 선택] > [삭제]

	- 방화벽 규칙 삭제 시도  2) 방화벽 규칙 삭제 확인  3) 방화벽 규칙 적용 확인 
진단 기준	**양호기준** : IP 범위가 모두 허용(*) 설정이 되어 있지 않는 경우 **취약기준** : IP 범위가 모두 허용(*) 설정이 되어 있는 경우
비고	

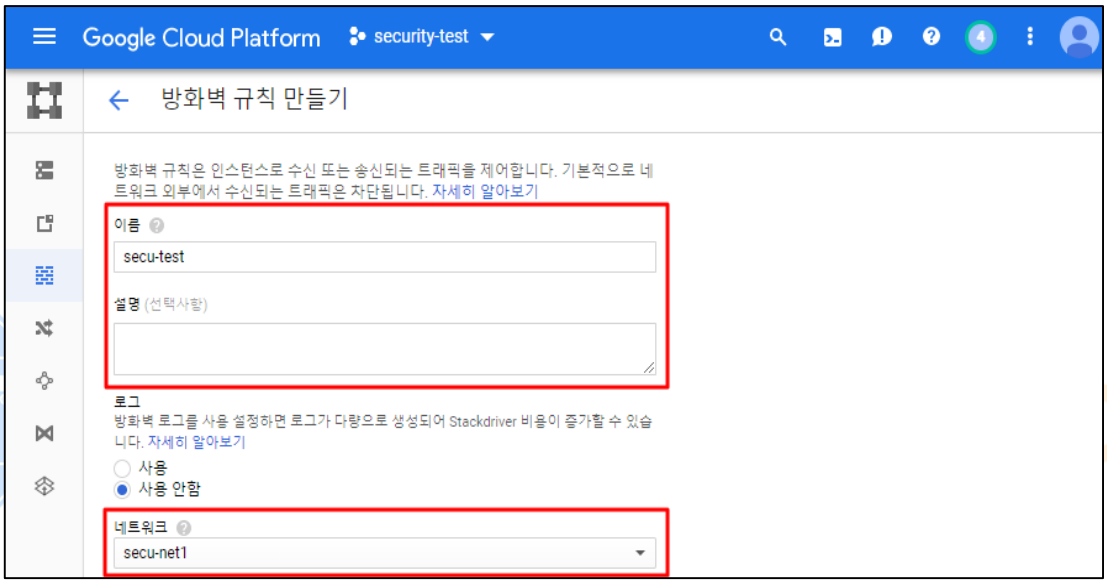
3.4 네트워크 방화벽 규칙 관리

분류	가상 리소스 관리	**중요도**	중
항목명	네트워크 방화벽 규칙 관리		

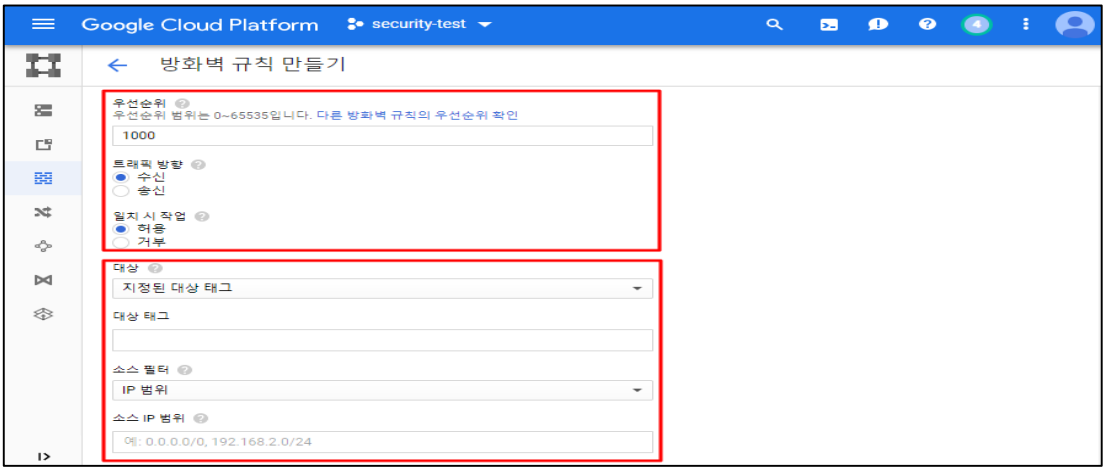
항목 설명	방화벽 규칙은 네트워크에서 나가는(송신) 트래픽과 들어오는(수신) 트래픽 모두에 적용됩니다. 방화벽 규칙은 VM 인스턴스 간의 통신을 포함하여 전적으로 네트워크 내에서 이루어지는 트래픽도 제어(허용/거부)합니다. 또한, 사용 설정한 GCP 방화벽 규칙은 인스턴스의 구성 및 운영 체제와 상관없이 인스턴스를 보호할 수 있도록 항상 실행됩니다. 모든 네트워크에는 수신 트래픽에 적용되는 묵시적 거부 방화벽 규칙이 있으므로 인스턴스 간 통신을 위해서는 적절한 방화벽 규칙도 구성해야 합니다. default 네트워크를 제외하고 인스턴스 간 통신을 허용하려면 우선순위가 더 높은 수신 방화벽 규칙을 명시적으로 만들어야 합니다. default 네트워크에는 네트워크 내에서 인스턴스 간 통신을 허용하는 default-allow-internal 규칙을 포함하여 묵시적 규칙 외에도 여러 가지 방화벽 규칙이 포함되어 있습니다. default 네트워크에는 RDP 및 SSH와 같은 프로토콜을 허용하는 수신 규칙도 있습니다.
설정 방법	**가. Compute Engine 네트워크 방화벽 설정** 1) [메인] > [VPC 네트워크] > [방화벽 규칙]  2) 방화벽 규칙 만들기



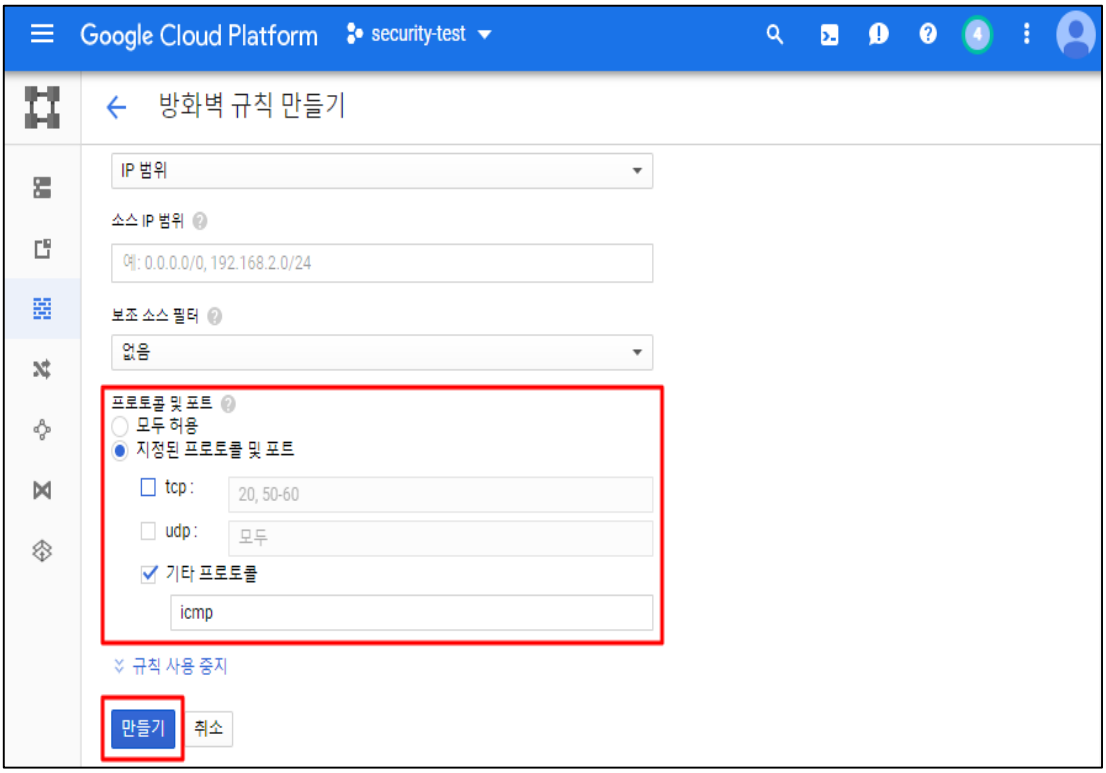
3) 방화벽 이름 및 네트워크 설정



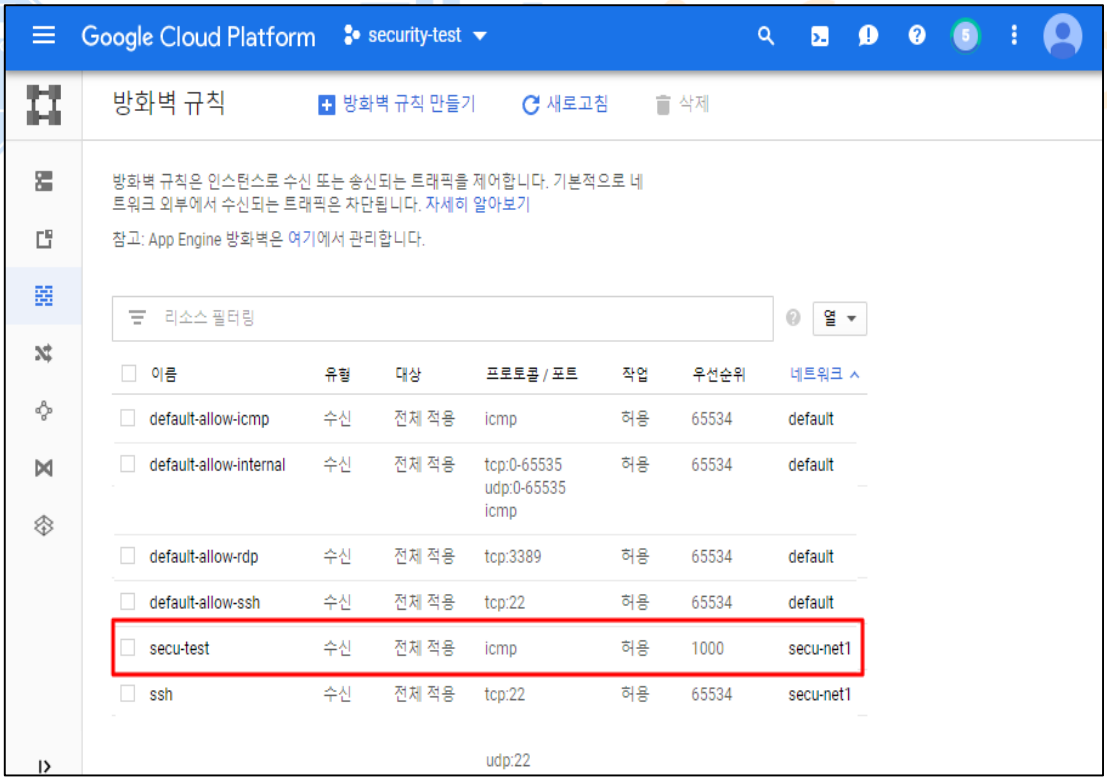
4) 트래픽 방향 및 일치 시 작업, IP 대역 설정



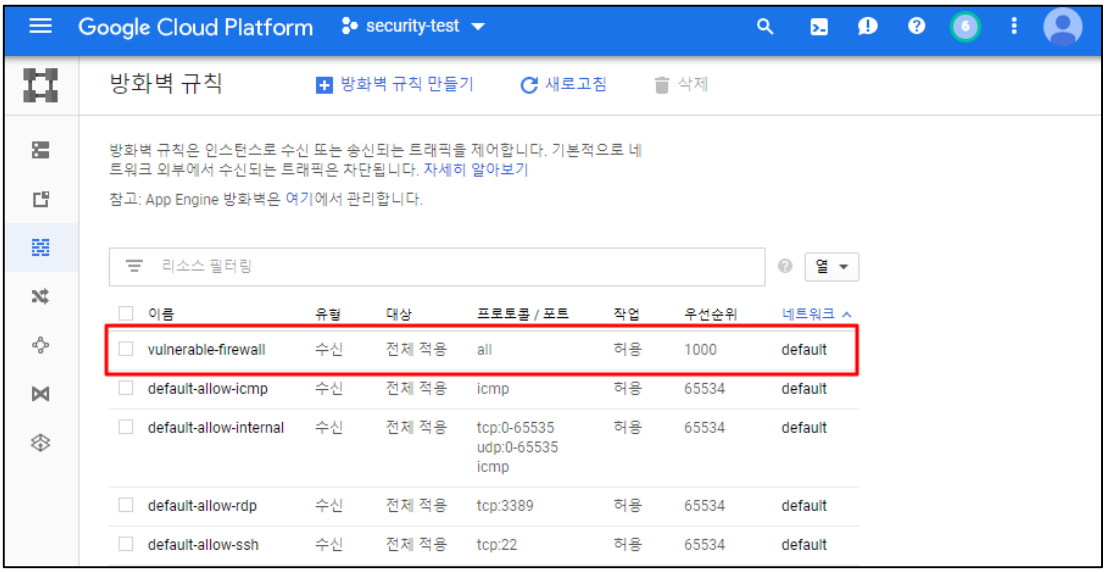
5) 프로토콜 및 포트 설정 및 만들기



6) 생성된 방화벽 규칙 확인

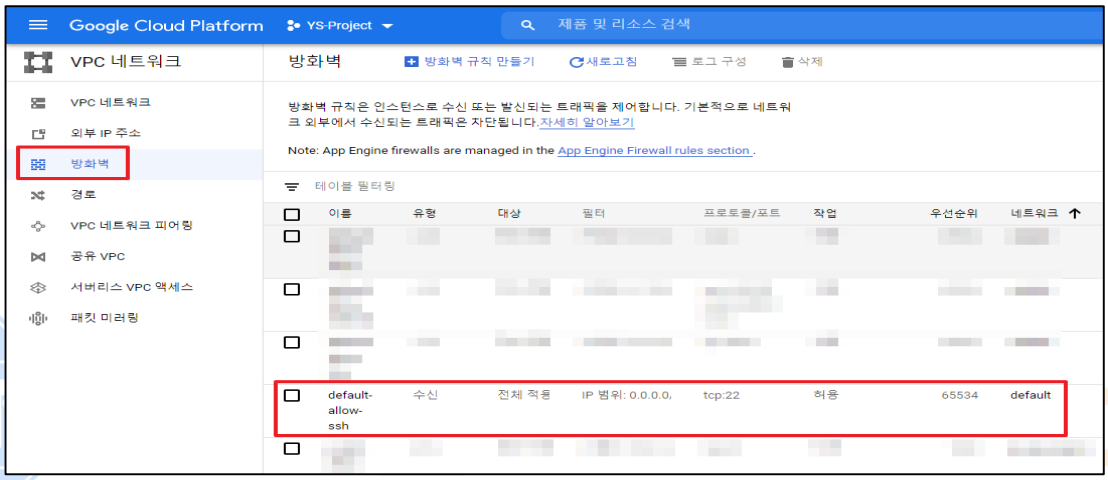
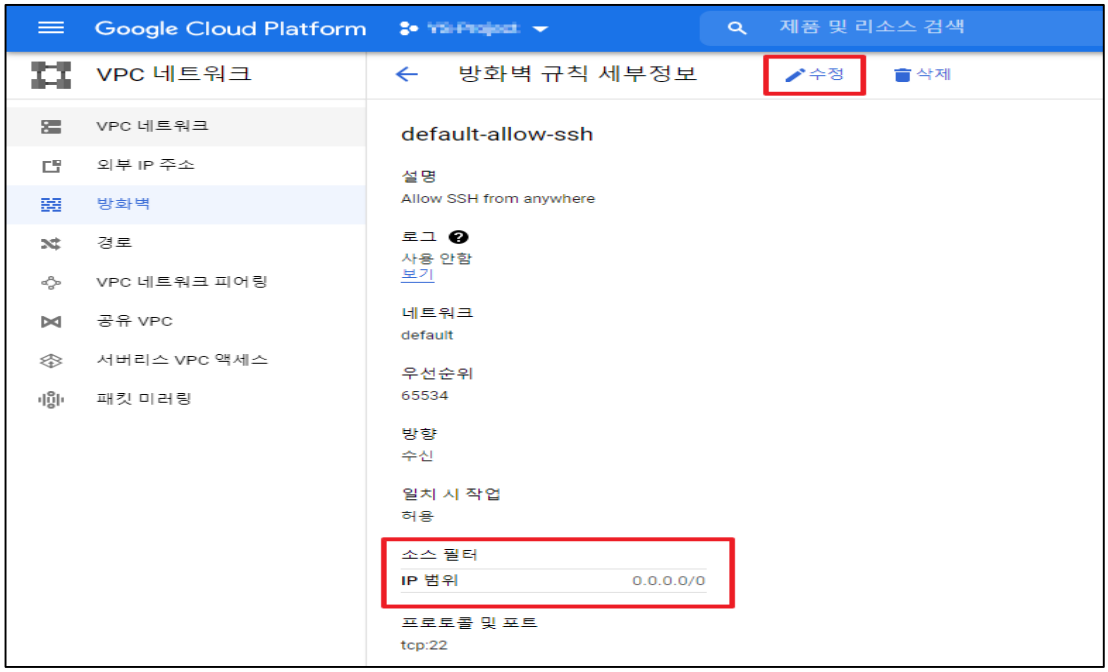


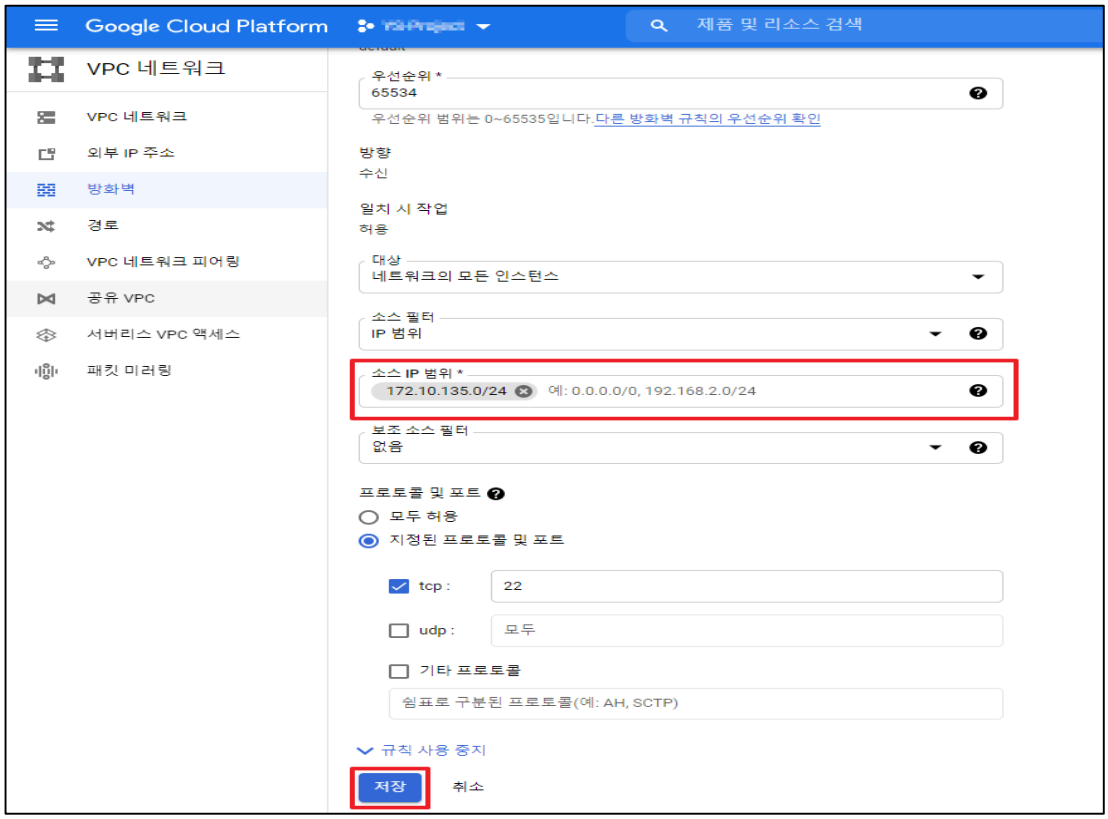
7) 취약한 방화벽 설정(ALL/ALL 설정)

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단
기준</td><td>양호기준
: 불필요한 방화벽 규칙이 있지 않는 경우

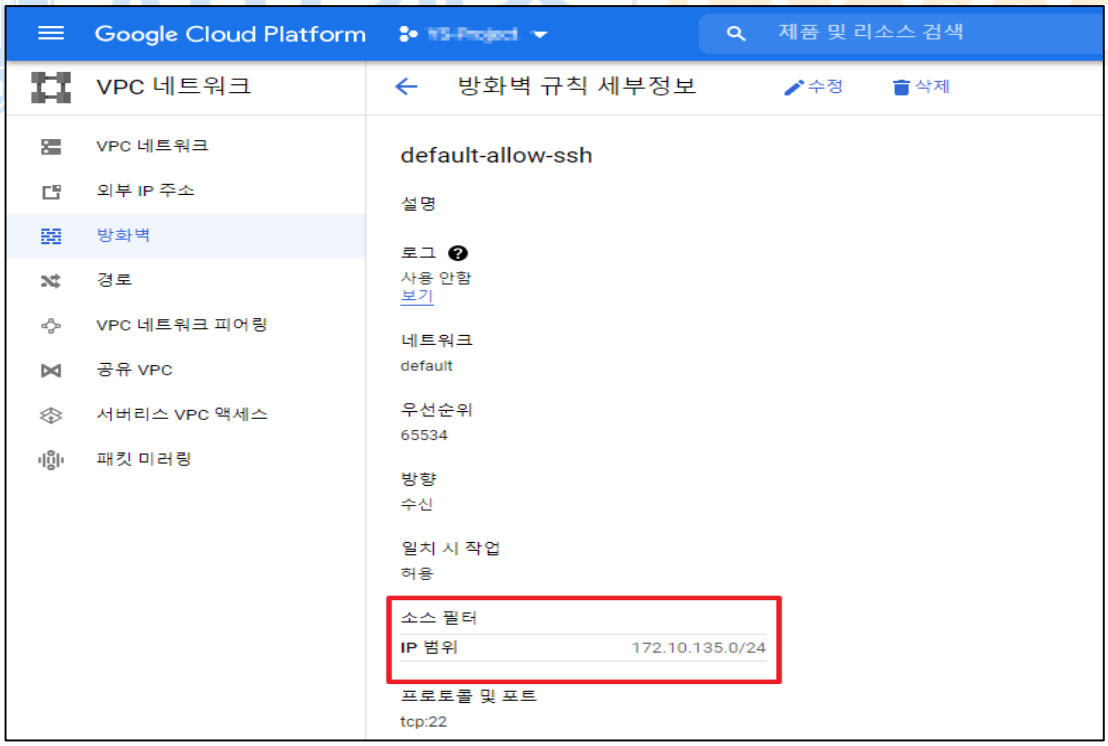
취약기준
: 불필요한 방화벽 규칙을 사용하고 있는 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

3.5 네트워크 방화벽 IP Address 및 Port 관리

분류	가상 리소스 관리	중요도	중
항목명	네트워크 방화벽 IP Address 및 Port 관리		
항목 설명	GCP 방화벽 서비스는 프로젝트 내 인스턴스에 대한 인바운드 및 아웃바운드 트래픽을 제어하는 기능을 제공하며, 접근을 허용/차단할 IP 주소 제어 및 프로젝트 별 Port 규칙을 추가하거나 제거가 가능합니다. In/OutBound 트래픽 내 불필요하게 Any로 허용된 IP주소 및 Port가 존재할 경우 GCP 리소스에 비정상적인 접근 또는 2차 공격에 활용될 수 있습니다.		
설정 방법	**가. 방화벽 정책 내 IP Address ANY 정책 확인 방법** 1) 방화벽 정책 내 IP Address ANY 정책 확인  2) 방화벽 정책 내 IP Address ANY 정책 수정  3) 방화벽 정책 내 허용하는 IP 대역으로 수정		

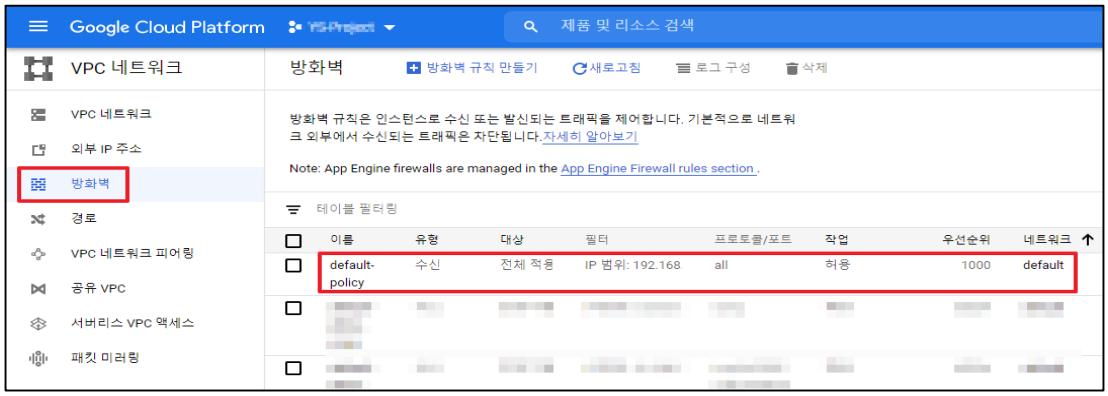


4) 방화벽 정책 수정 확인

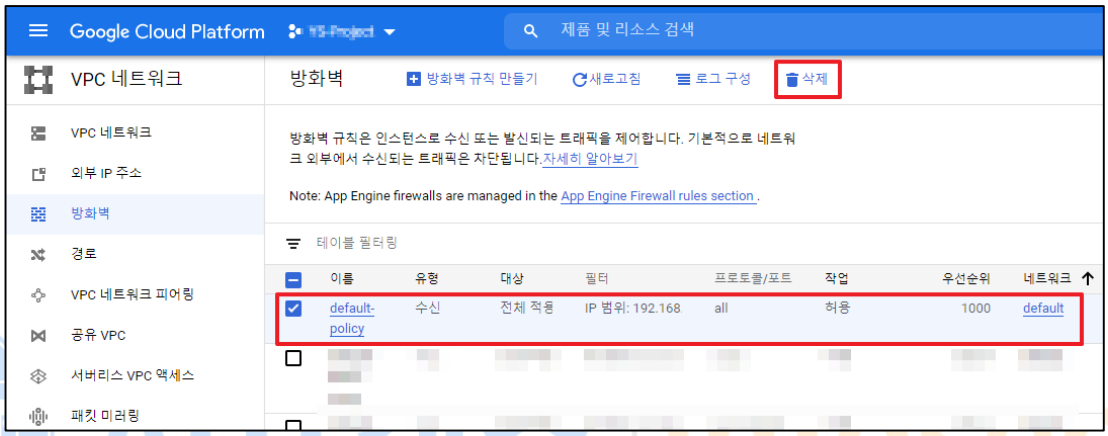


나. 방화벽 정책 내 Port ALL 정책 확인 방법

1) 방화벽 정책 내 port ALL 정책 확인



2) 방화벽 정책 내 Port ALL 정책 삭제



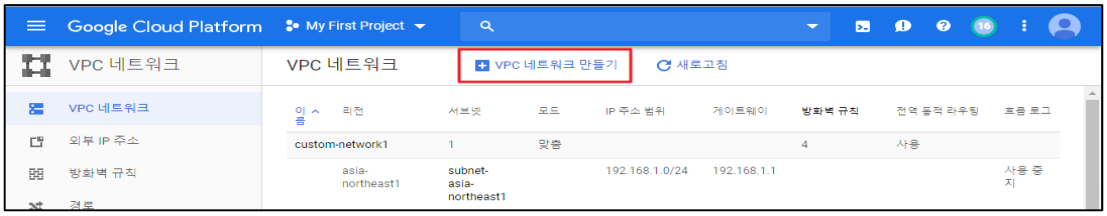
진단 기준	**양호기준** : 방화벽 In/OutBound 규칙 내 Source 또는 Destination 설정 및 port가 Any로 허용되어 있지 않을 경우 **취약기준** : 방화벽 In/OutBound 규칙 내 Source 또는 Destination 설정 및 port가 Any로 허용되어 있을 경우
비고	

3.6 VPC 네트워크 서브넷 관리

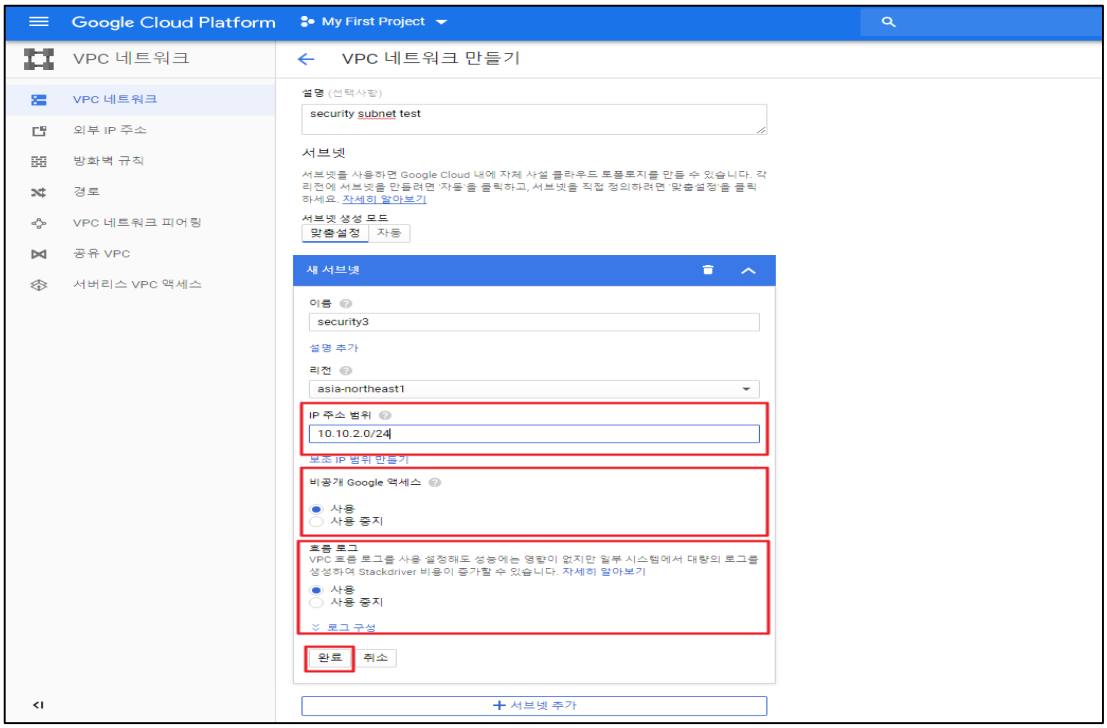
<table>
<tr><td>분류</td><td>가상 리소스 관리</td><td>중요도</td><td>상</td></tr>
<tr><td>항목명</td><td colspan="3">VPC 네트워크 서브넷 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">VPC 네트워크는 Compute Engine 가상 머신(VM) 인스턴스, Kubernetes Engine 클러스터, App Engine 가변형 인스턴스, 프로젝트의 다른 리소스를 위한 연결을 제공하며 하위 네트워크 또는 서브넷이라는 유용한 IP 범위 파티션 하나나 그 이상으로 구성됩니다.

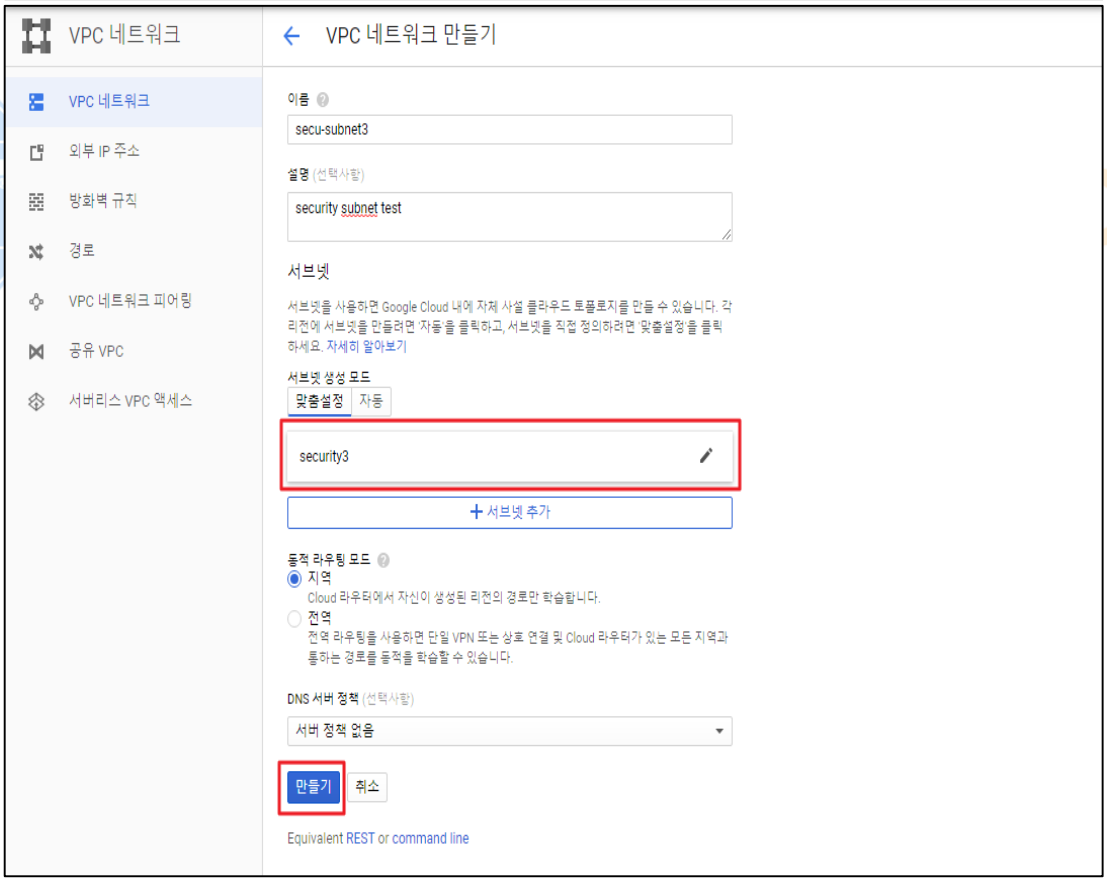
※ 서브넷 속성
<table>
<tr><th>속성</th><th>설명</th></tr>
<tr><td>서브넷</td><td>네트워크를 사용하려면 네트워크에 한 개 이상의 서브넷이 있어야 합니다. 자동 모드 네트워크는 각 리전에 자동으로 서브넷을 만듭니다. 커스텀 모드 네트워크는 서브넷 없이 시작되므로 서브넷 만들기를 전적으로 제어할 수 있습니다. 한 리전에 두 개 이상의 서브넷을 만들 수 있습니다. 서브넷 생성은 아래 두 가지 방법으로 생성이 가능합니다.

자동 모드
네트워크가 생성될 때는 네트워크 내의 리전마다 서브넷이 하나씩 자동 생성됩니다. 자동으로 생성되는 이러한 서브넷은 10.128.0.0/9 CIDR 블록에 속하는 사전 정의된 IP 범위 집합을 사용합니다. 새 GCP 리전을 사용할 수 있게 되면 이 블록의 IP 범위를 사용하여 리전의 새 서브넷이 자동으로 자동 모드 네트워크에 추가됩니다. 자동으로 생성되는 서브넷 외에도, 자동 모드 네트워크의 선택한 리전에 10.128.0.0/9 이외의 IP 범위를 사용하여 수동으로 서브넷을 추가할 수 있습니다.

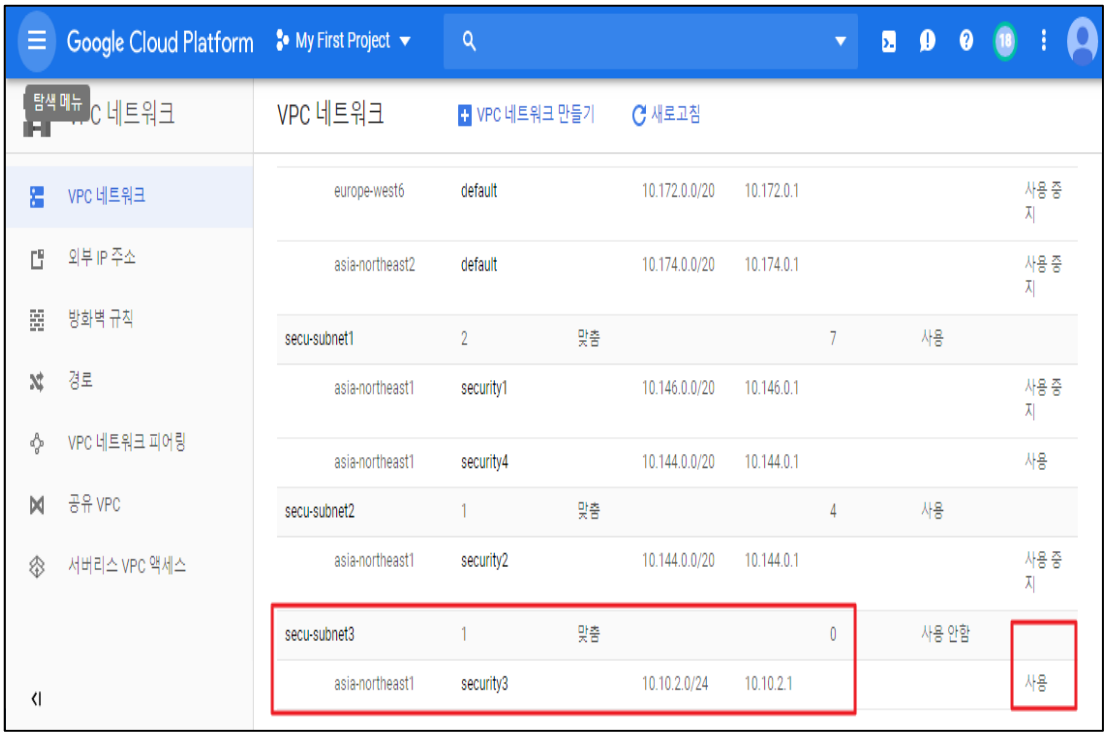
커스텀 모드
네트워크가 만들어질 때는 서브넷이 자동 생성되지 않습니다. 이 네트워크 유형에서는 개발자가 서브넷과 IP 범위를 완전히 제어할 수 있습니다. 선택한 리전에 만들 서브넷을 결정하고 직접 지정한 IP 범위를 사용합니다.</td></tr>
</table></td></tr>
<tr><td>설정
방법</td><td colspan="3">가. VPC 네트워크 생성 방법
1) [VPC 네트워크] > [VPC 네트워크 만들기]
- VPC 네트워크 생성 시도
 

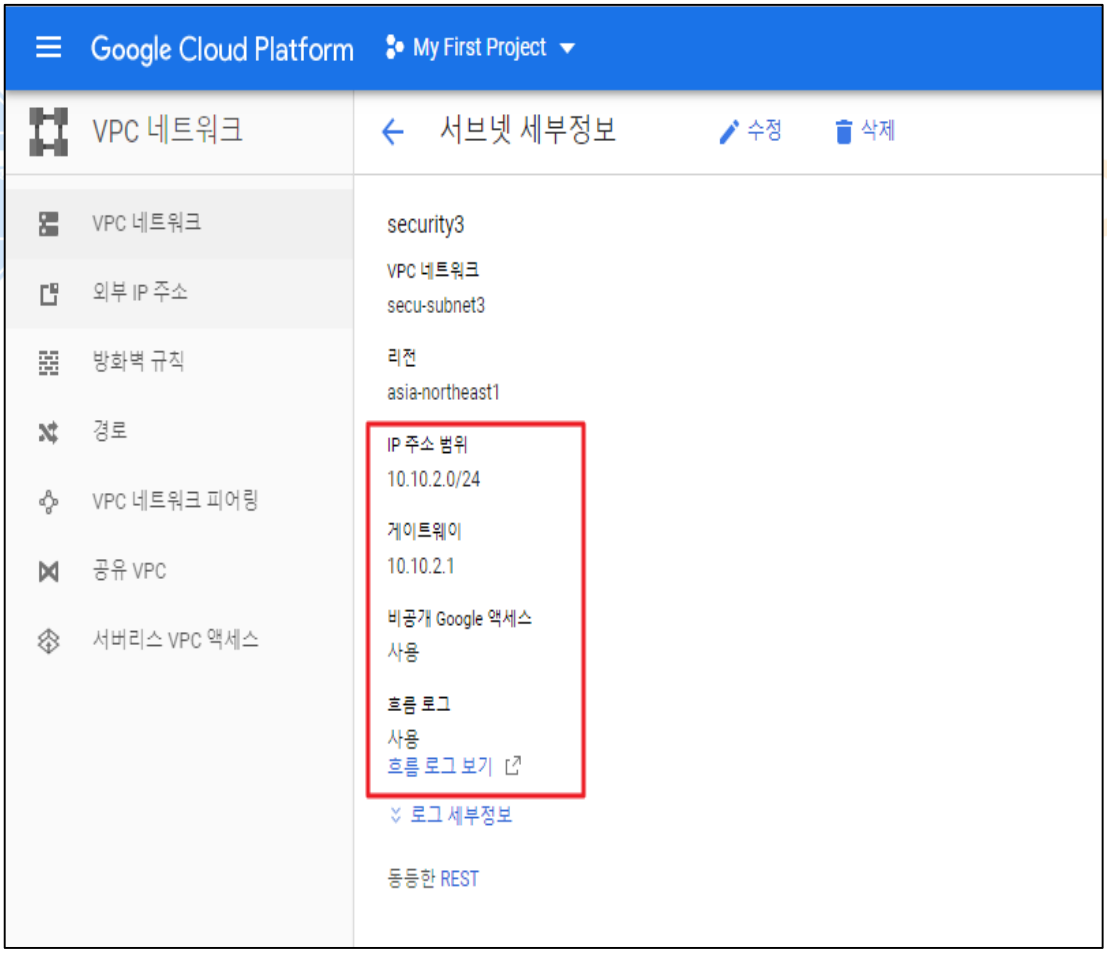
2) [VPC 네트워크 만들기] > [서브넷] > [새 서브넷]
- 맞춤 설정을 통한 커스텀 서브넷 및 흐름로그 사용 설정</td></tr>
</table>





3) 생성된 VPC 네트워크 및 서브넷 내용 확인

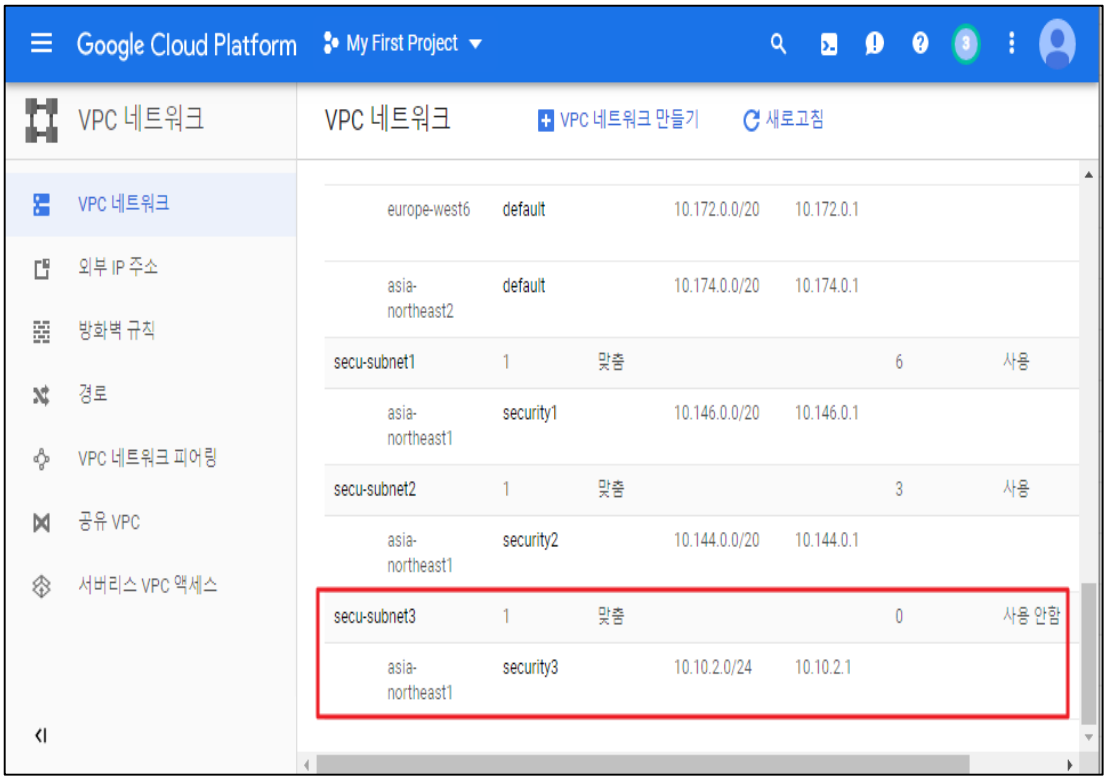




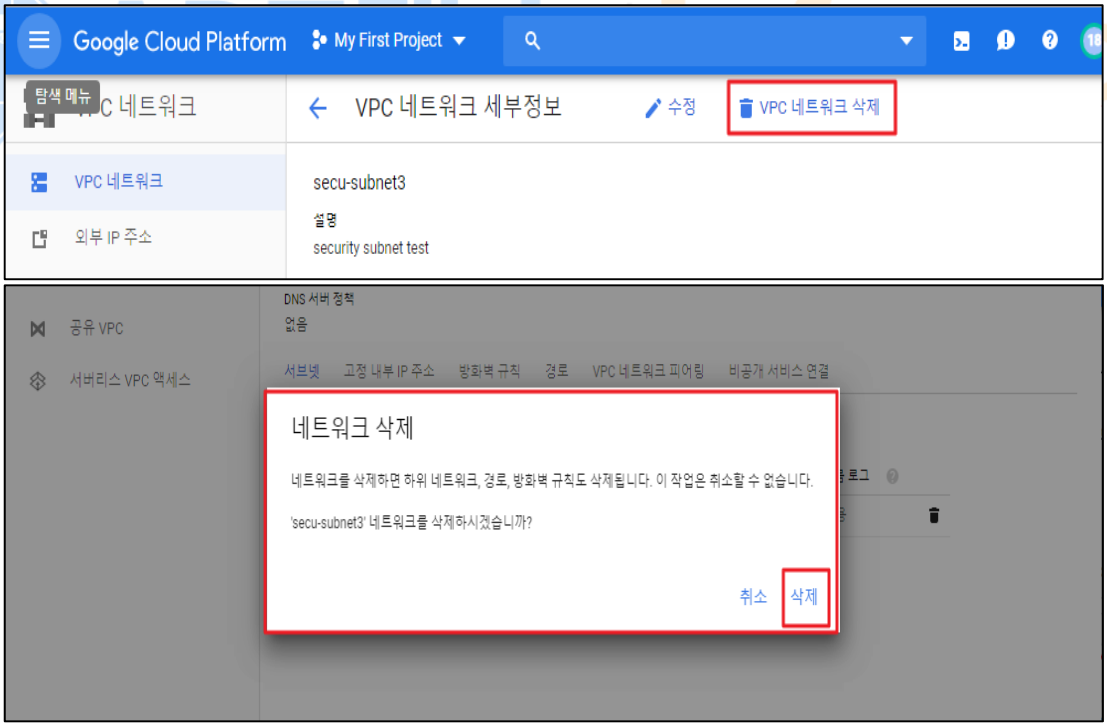
나. VPC 네트워크 삭제 방법

1) [VPC 네트워크] > [VPC 네트워크]

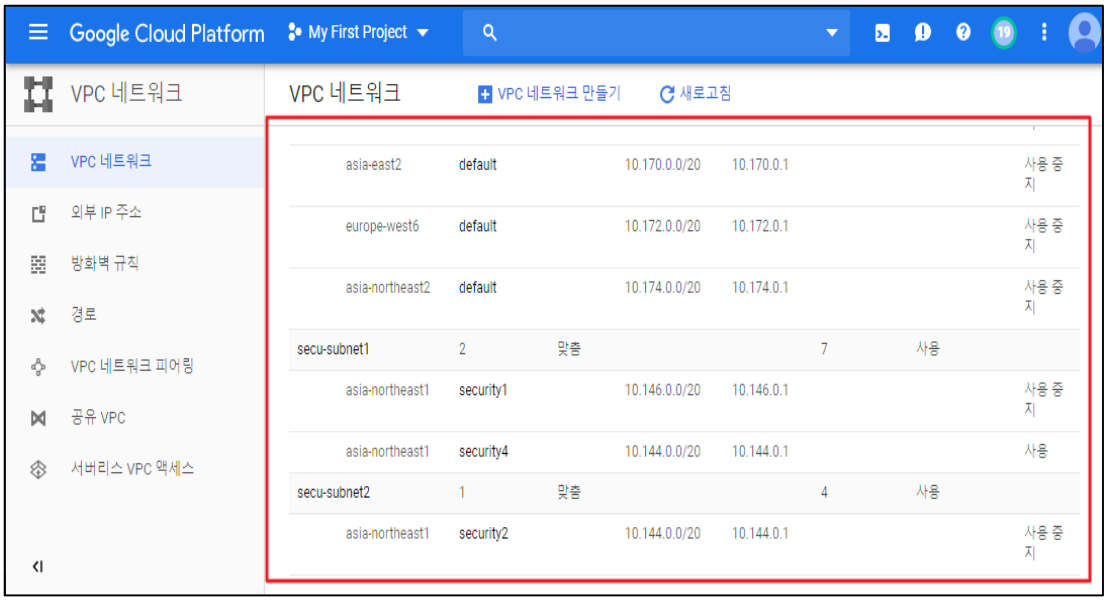
- 삭제 하고자 하는 VPC 네트워크 선택



2) VPC 네트워크 삭제 시도

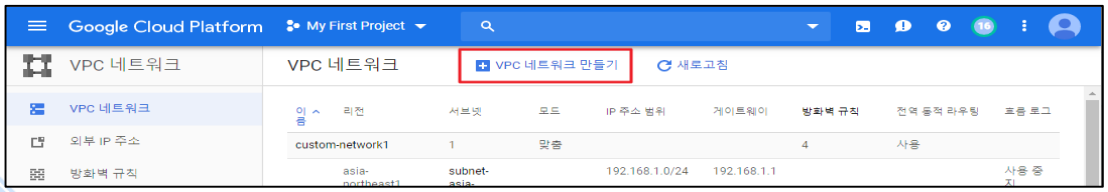
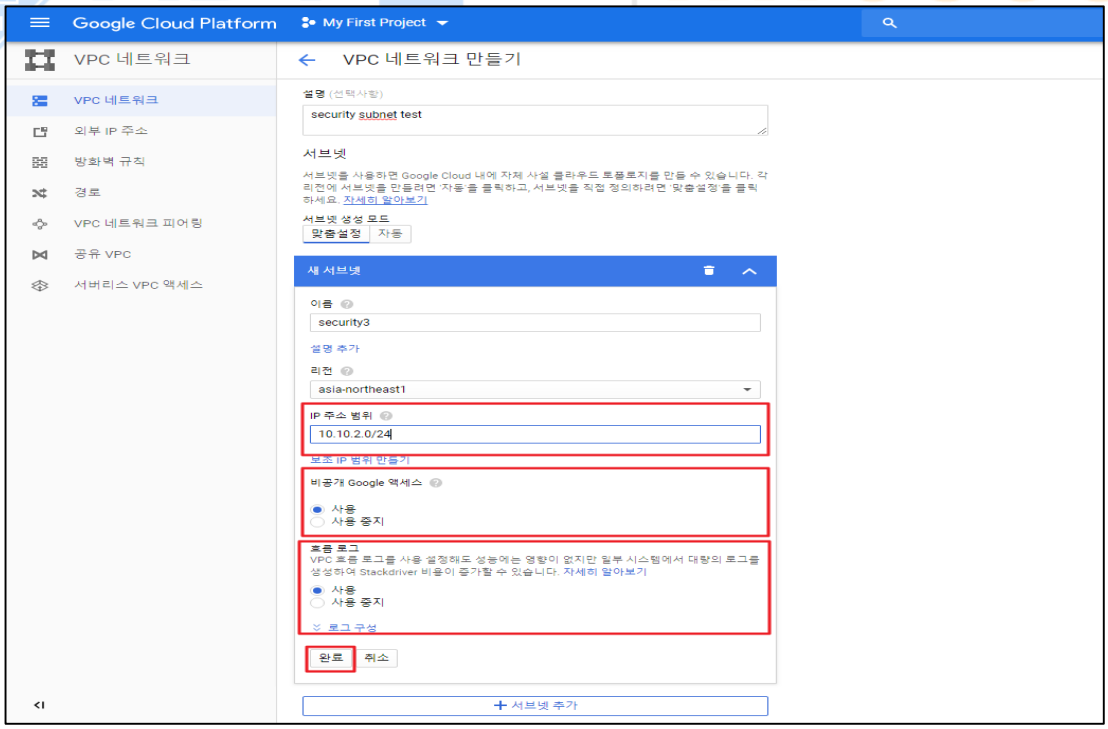


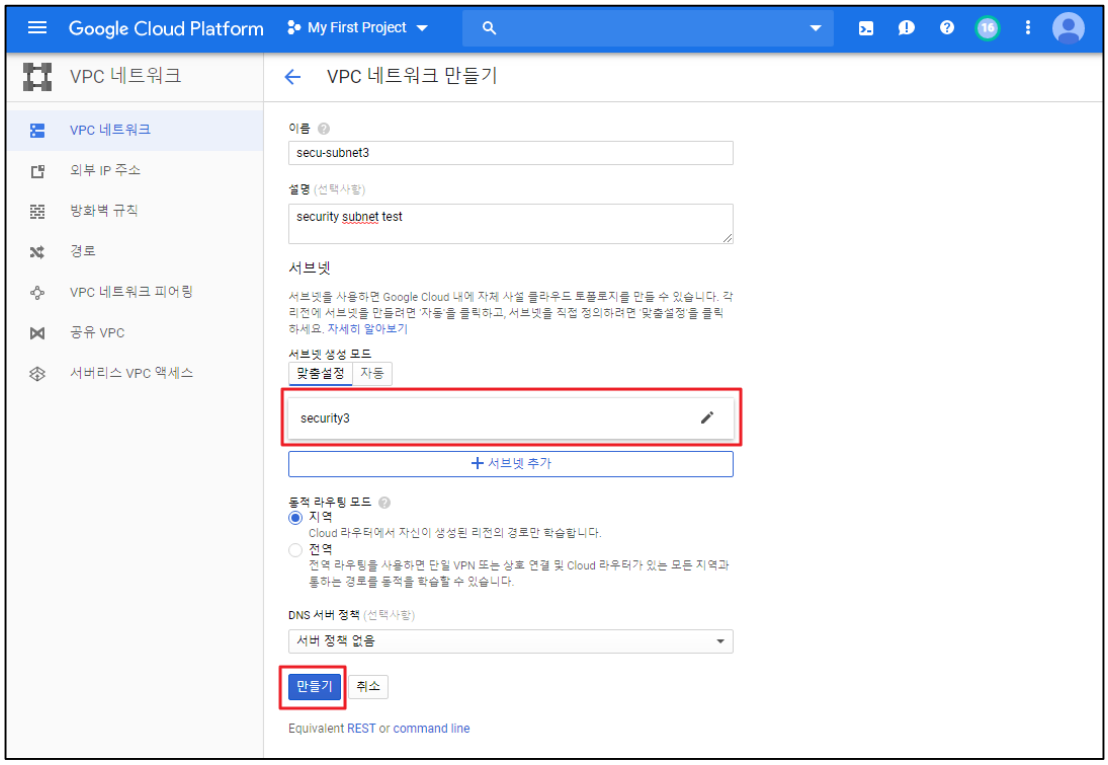
3) VPC 네트워크 삭제 완료 (secu-subnet3)

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단 기준</td><td>양호기준
: 사용 목적에 맞게 서브넷이 사용 중일 경우

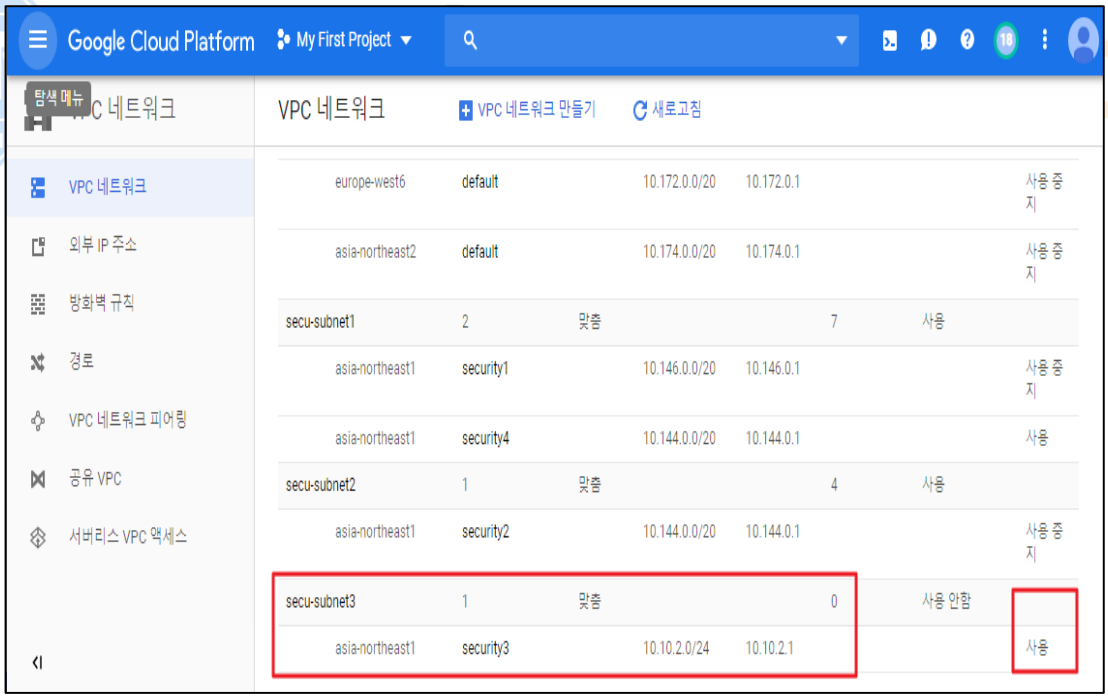
취약기준
: 사용 목적에 맞지 않는 서브넷이 존재할 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

3.7 VPC 네트워크 서브넷 비공개 구글 액세스 설정

분류	가상 리소스 관리	중요도	중
항목명	VPC 네트워크 서브넷 비공개 구글 액세스 설정		
항목 설명	비공개 Google 액세스를 사용하면 내부(비공개) IP 주소만 있고 외부 IP 주소는 없는 VM 인스턴스가 Google API 및 서비스의 공개 IP 주소에 연결할 수 있습니다. 서브넷 수준에서 비공개 Google 액세스를 사용 설정할 수 있습니다. 비공개 Google 액세스를 사용 설정하면 서브넷에서 비공개 IP 주소만 있는 인스턴스가 기본 인터넷 게이트웨이에 대한 다음 홉으로 기본 경로(0.0.0.0/0)를 통해 Google API 및 서비스로 트래픽을 전송할 수 있습니다. 또한, 비공개 Google Access를 사용 중지하면 VM 인스턴스가 더 이상 Google API 및 서비스에 도달할 수 없으며 VPC 네트워크 내에서만 트래픽을 전송할 수 있습니다.		
설정 방법	**가. 비공개 구글 액세스 설정** 1) [VPC 네트워크] > [VPC 네트워크 만들기] - VPC 네트워크 생성 시도  2) [VPC 네트워크 만들기] > [서브넷] > [새 서브넷] - 비공개 Google 액세스 사용 설정  		



3) 생성된 VPC 네트워크 및 서브넷 내용 확인



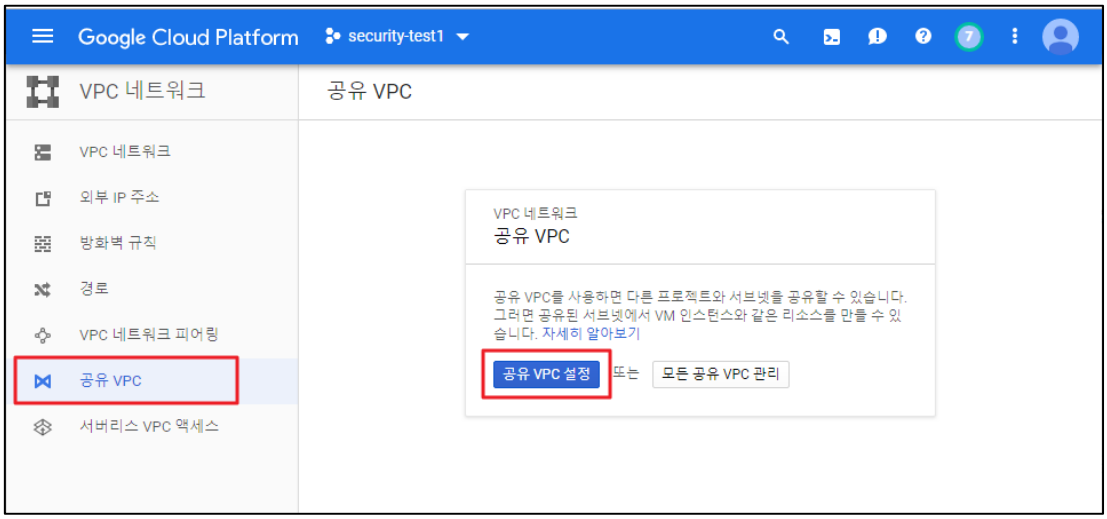
<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단
기준</td><td>양호기준
: 비공개 구글 액세스를 사용하는 경우

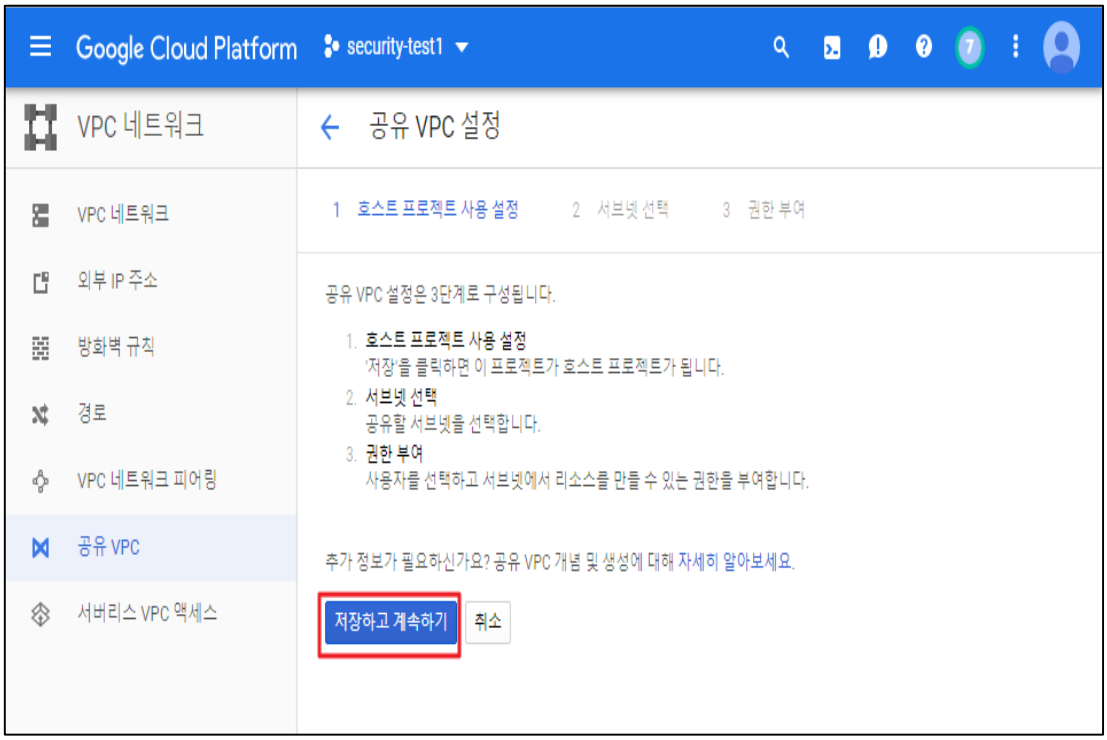
취약기준
: 비공개 구글 액세스를 사용하지 않는 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

3.8 공유 VPC 관리

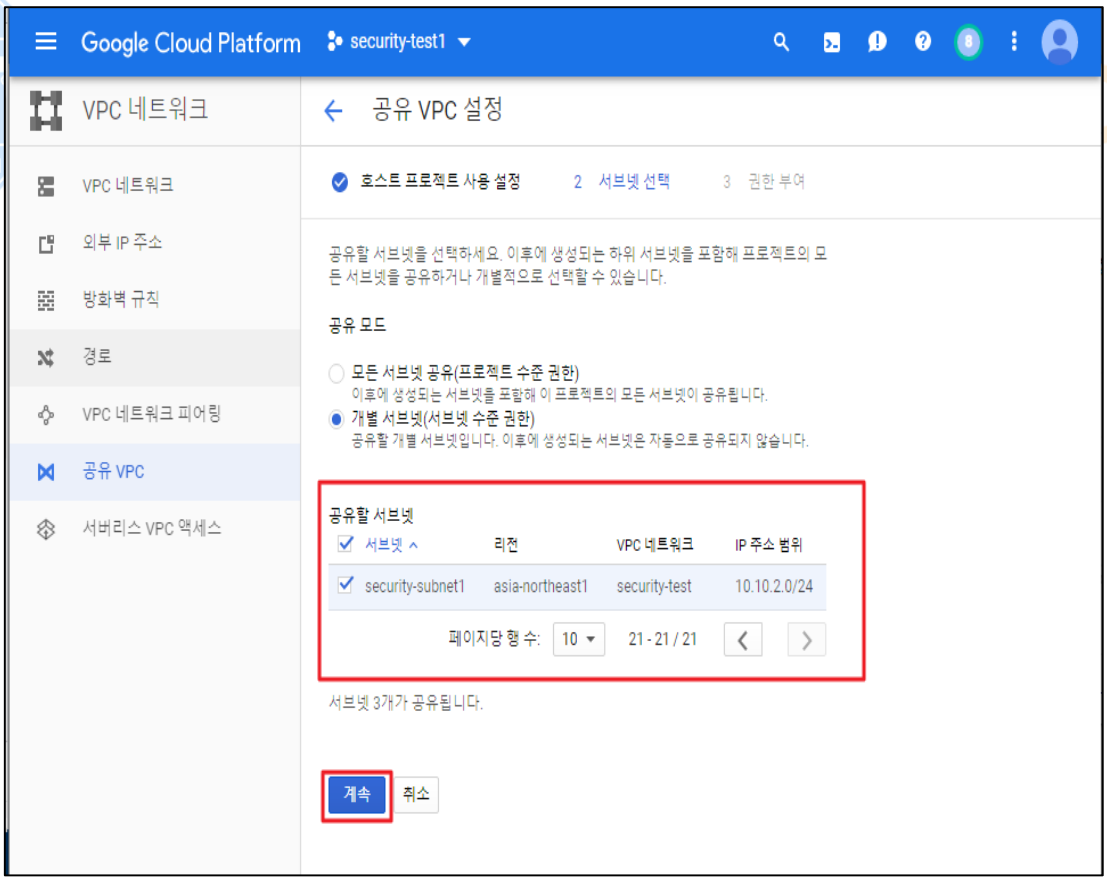
<table>
<tr><td>분류</td><td>가상 리소스 관리</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">공유 VPC 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">공유 VPC 는 동일한 조직 내에서 프로젝트를 연결합니다. 참여하는 호스트 및 서비스 프로젝트는 다른 조직에 속할 수 없습니다. 연결된 프로젝트는 같거나 다른 폴더 모두에 있을 수 있지만 다른 폴더에 있는 경우에는 관리자에게 두 폴더에 대한 공유 VPC 관리자 권한이 있어야 합니다.

또한, 공유 VPC 를 사용하는 조직은 여러 프로젝트의 리소스를 공통 VPC 네트워크에 연결할 수 있으므로 해당 네트워크의 내부 IP 를 사용하여 서로 안전하고 효율적으로 통신할 수 있으며, 공유 VPC 를 사용하면 조직 관리자가 서브넷, 경로, 방화벽과 같은 네트워크 리소스를 중앙에서 제어하면서 서비스 프로젝트 관리자에게 인스턴스 생성 및 관리와 같은 관리 책임을 위임할 수 있습니다.

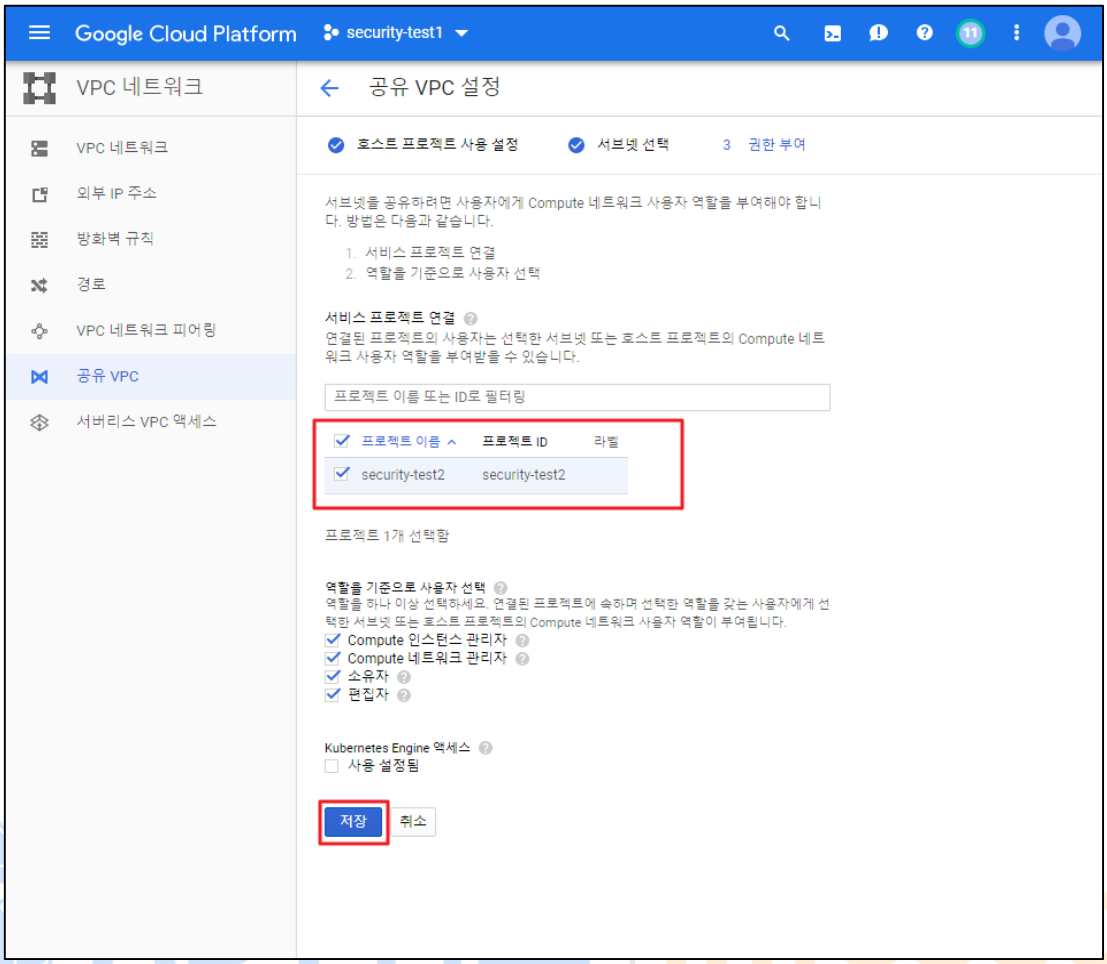
※ 공유 VPC List (예시)
<table>
<tr><th>호스트
프로젝트</th><th>연결된(서비스)
프로젝트</th><th>서브넷 명</th><th>IP 주소범위</th><th>사용목적</th><th>취약
유/무</th></tr>
<tr><td>ex) host-project</td><td>ex) project1</td><td>ex)dafult_subnet</td><td>ex)192.168.0.
0/24</td><td>ex)사용목적</td><td>N/A</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>N/A</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>N/A</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>N/A</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>설정
방법</td><td colspan="3">가. 공유 VPC를 통한 조직 내 프로젝트 간 서브넷 공유
1) [VPC 네트워크] > [공유 VPC] > [공유 VPC 설정]
- 조직 내 프로젝트 간의 서브넷 공유를 위한 공유 VPC 설정 시도
 
</td></tr>
</table>



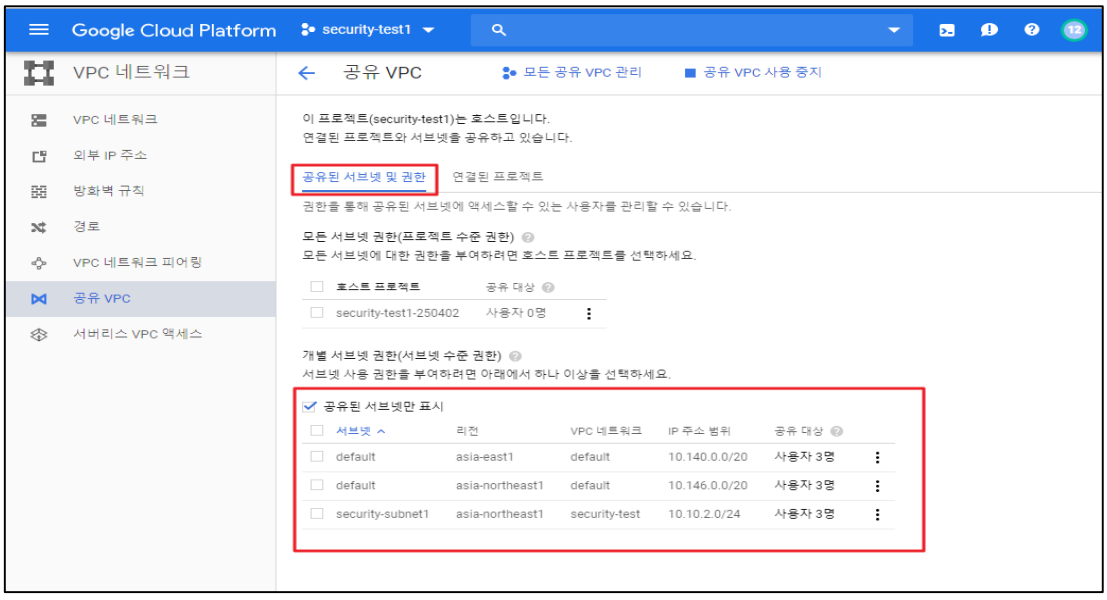
2) 조직 내 타 프로젝트와 공유할 서브넷 설정

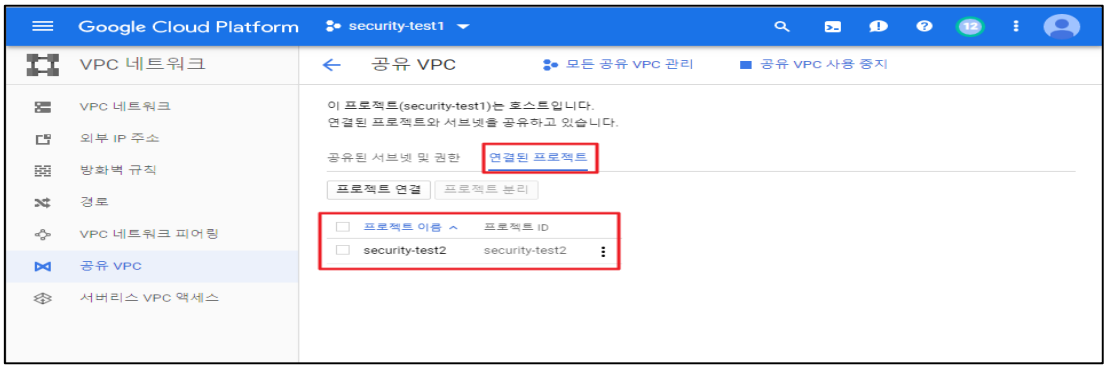


3) 연결할 프로젝트 설정



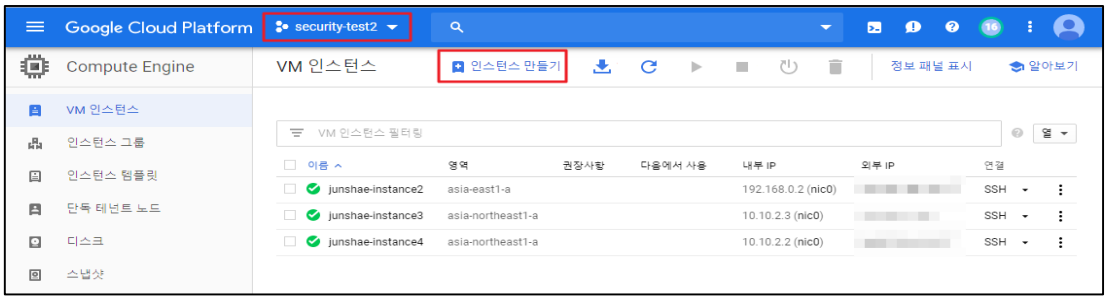
4) 설정된 공유 VPC 정보 확인





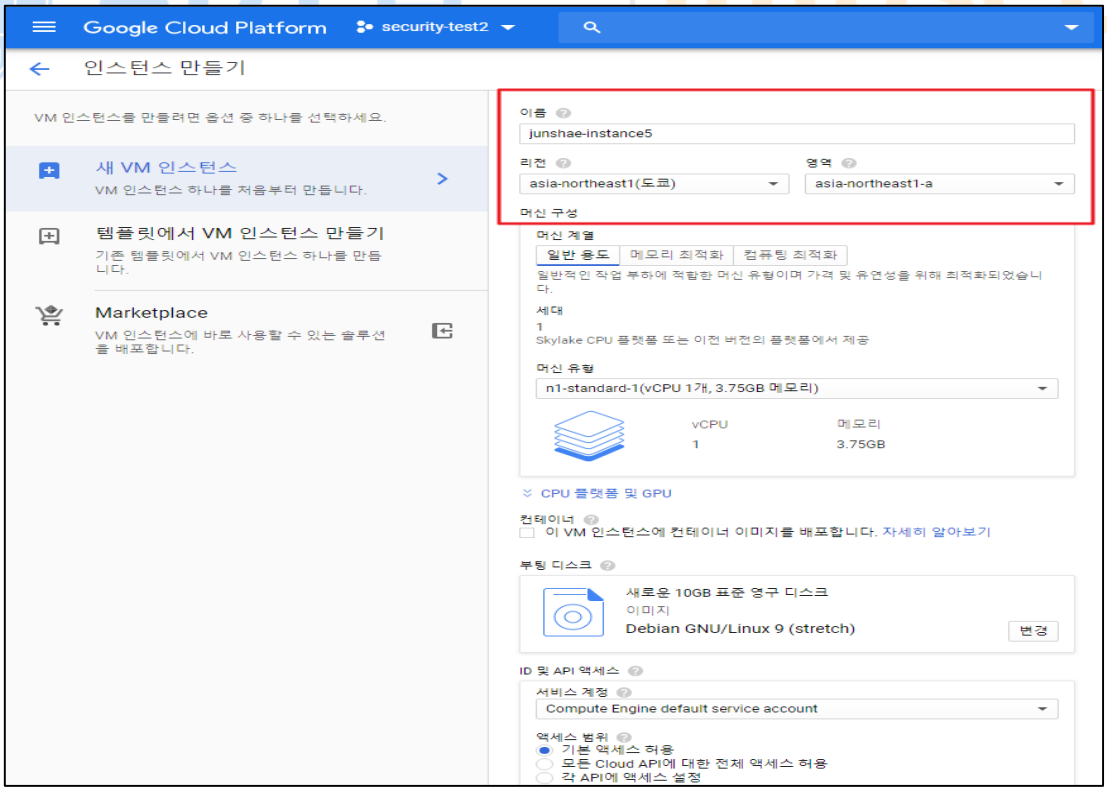
5) [Compute Engine] > [VM 인스턴스] > [인스턴스 만들기]

- 공유된 VPC 를 통한 VM 인스턴스 생성

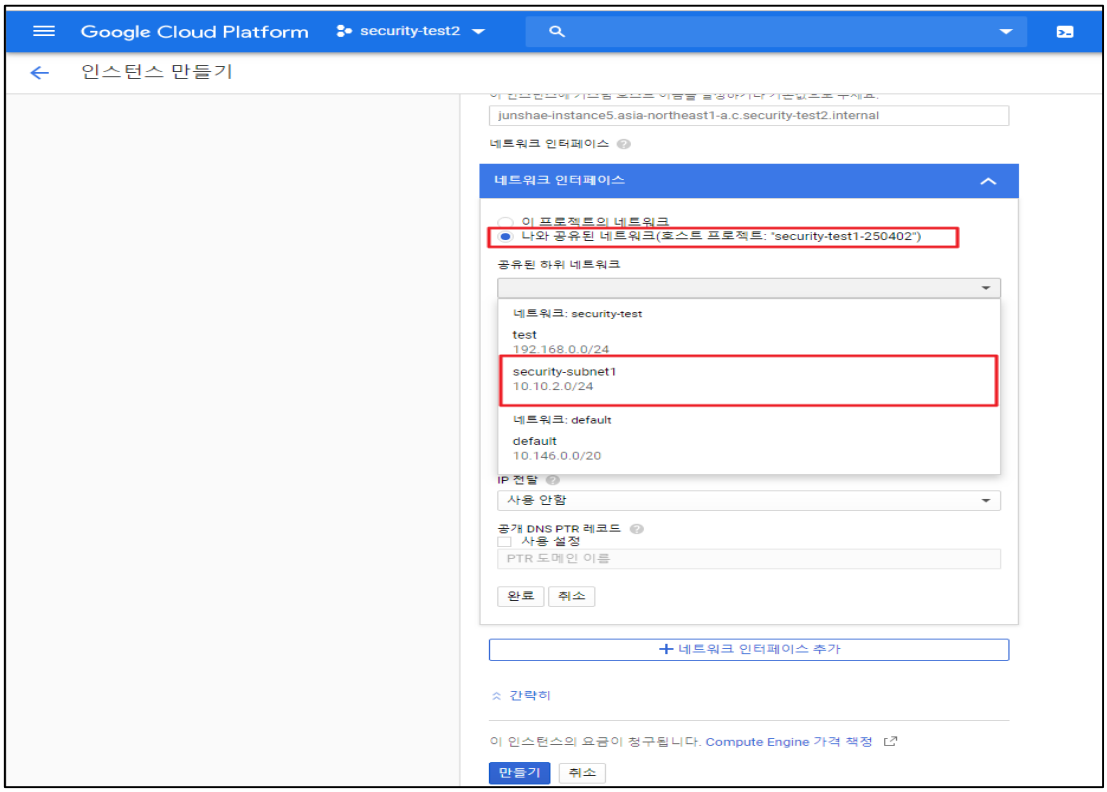


6) 새 VM 인스턴스 만들기

- 인스턴스 생성 시 리전을 공유 하려는 서브넷과 동일하게 설정되어야 함

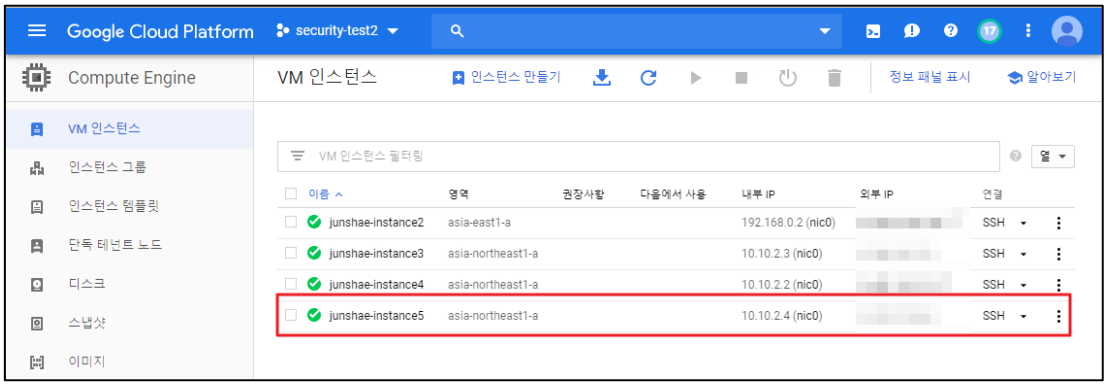


7) 네트워크 인터페이스 설정 시 '나와 공유된 네트워크' 선택



8) 공유된 서브넷들 중 사용하고자 하는 서브넷 선택 및 인스턴스 생성

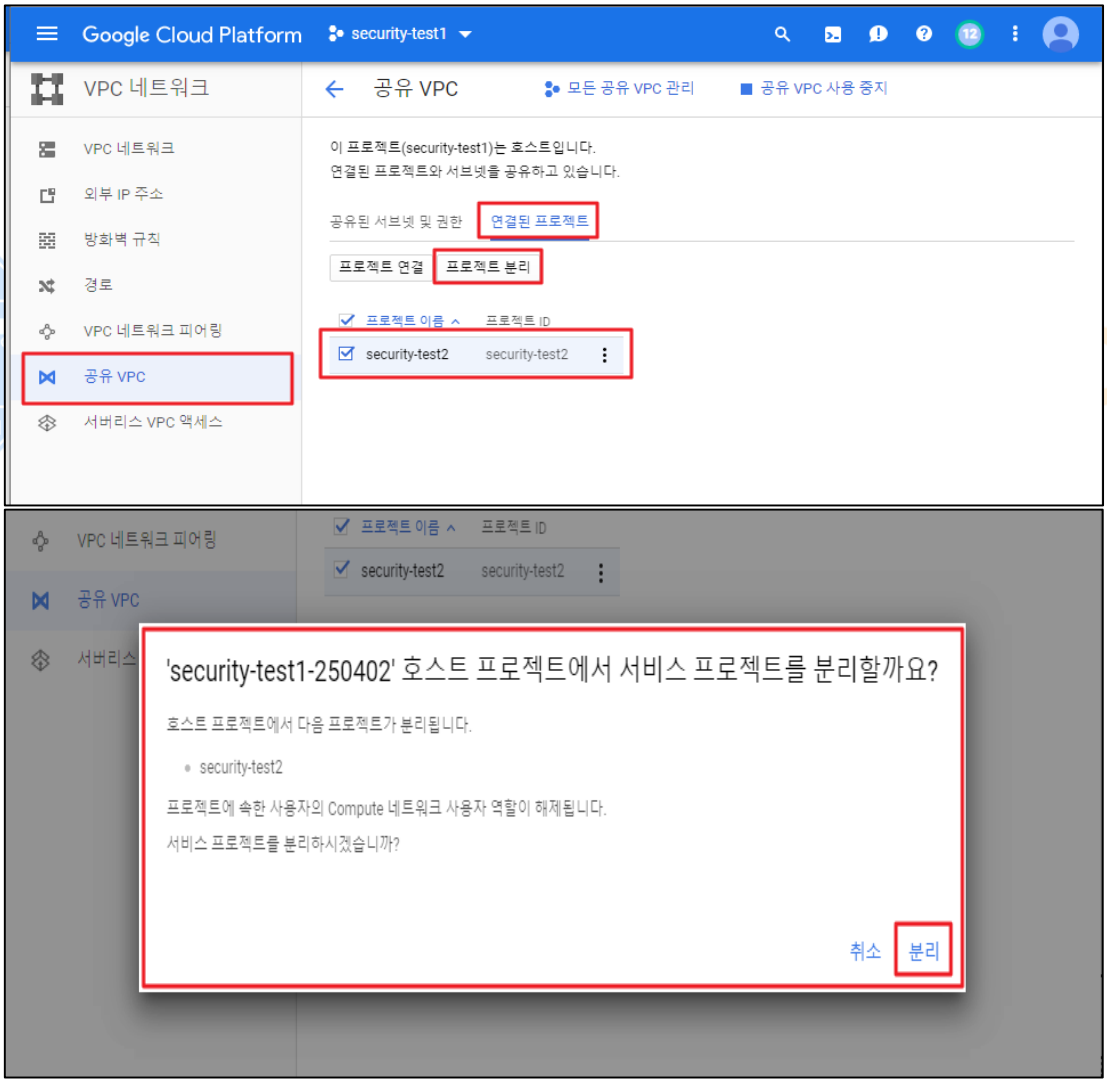
9) 공유된 서브넷을 통한 VM 인스턴스 생성 완료



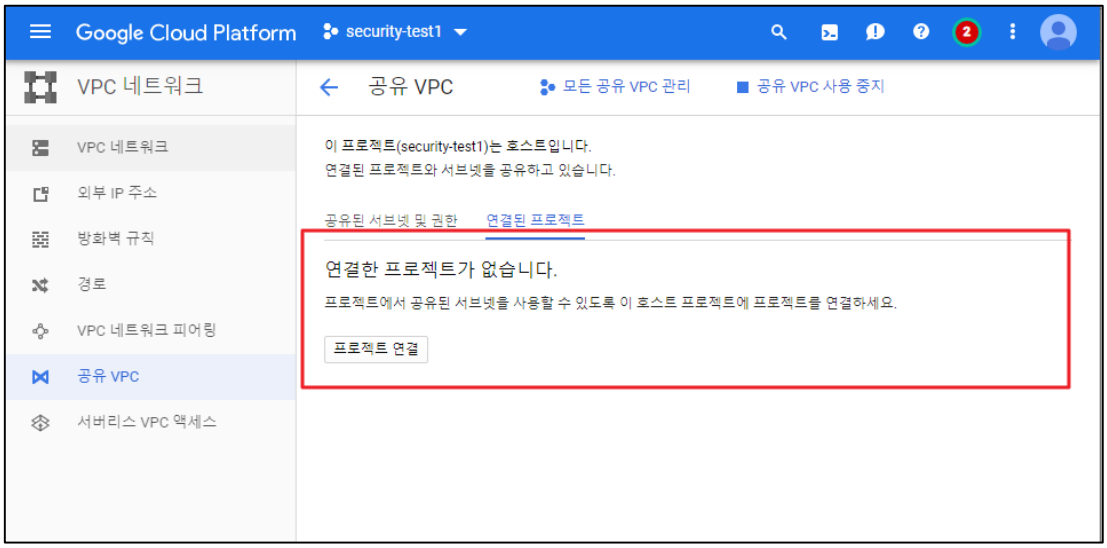
나. 공유 VPC 내 프로젝트 연결 해제

1) [VPC 네트워크] > [공유 VPC] > [연결된 프로젝트] > [프로젝트 분리]

- 조직 내 불필요한 프로젝트 연결 해제를 위해 프로젝트 분리 시도



2) 프로젝트 연결 해제 확인

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단
기준</td><td>양호기준
: 사용 목적에 맞게 호스트 프로젝트와 서비스 프로젝트 서브넷이 공유되고 있을 경우

취약기준
: 사용 목적 없이 호스트 프로젝트와 서비스 프로젝트 서브넷이 공유되고 있을 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

3.9 VPN 연결 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">VPN 연결 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">
Cloud VPN 은 IPsec VPN 연결을 통해 온프레미스 네트워크를 Google Cloud Platform Virtual Private Cloud(GCP VPC) 네트워크에 안전하게 연결합니다. 두 개의 네트워크 사이로 이동되는 트래픽은 하나의 VPN 게이트웨이에서 암호화된 후 다른 VPN 게이트웨이에서 암호 해독됩니다. 인터넷에서 전송되는 데이터는 이러한 방식으로 보호됩니다.

또한, Cloud VPN 은 온프레미스 VPN 장치 및 VPN 서비스를 위해 사전 공유 키(공유 보안 비밀 또는 PSK 라고도 부름)라는 암호화 및 구성 매개변수를 지원합니다. Cloud VPN 은 온프레미스 측이 지원되는 IKE 암호화 설정을 사용하는 한 연결을 자동 협상하며, 보안 권장사항에 따라 강력한 32 자 공유 보안 비밀을 생성하는 것을 권고합니다.

※ IKEv1 지원되는 암호화
<table>
<tr><th>단계</th><th>암호화 역할</th><th>암호화</th></tr>
<tr><td rowspan="6">1 단계</td><td>암호화</td><td>AES-CBC-128</td></tr>
<tr><td>무결성</td><td>HMAC-SHA1-96</td></tr>
<tr><td>PFS 알고리즘(필수)</td><td>그룹 2(modp_1024)</td></tr>
<tr><td>PRF(의사 난수 함수)</td><td>PRF-SHA1-96</td></tr>
<tr><td>DH(Diffie-Hellman)</td><td>그룹 2(modp_1024)</td></tr>
<tr><td>1 단계 수명</td><td>36,600 초(10 시간, 10 분)</td></tr>
<tr><td rowspan="4">2 단계</td><td>암호화</td><td>AES-CBC-128</td></tr>
<tr><td>무결성</td><td>HMAC-SHA1-96</td></tr>
<tr><td>DH(Diffie-Hellman)</td><td>일부 장치에는 2 단계에 대해 DH 값이 필요합니다. 이 경우 1 단계에 사용한 값을 사용하세요.</td></tr>
<tr><td>2 단계 수명</td><td>10,800 초(3 시간)</td></tr>
</table>
※ IKEv2 지원되는 암호화
<table>
<tr><th>단계</th><th>암호화 역할</th><th>암호화</th></tr>
<tr><td>1 단계</td><td>암호화</td><td>- 3DES
- AES-CBC-128, AES-CBC-192, AES-CBC-256
- AES-GCM-128-8, AES-GCM-192-8, AES-GCM-256-8
- AES-GCM-128-12, AES-GCM-192-12, AES-GCM-256-12
- AES-GCM-128-16, AES-GCM-192-16, AES-GCM-256-16
일부 플랫폼에서 GCM 알고리즘은 비트(각각 64, 96, 128)로 지정된 해당 ICV 매개변수 옥텟(8, 12, 16)을 포함할 수 있습니다.</td></tr>
</table>
</td></tr>
</table>

		무결성	- HMAC-MD5-96 - HMAC-SHA1-96 - AES-XCBC-96, AES-CMAC-96 - HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256 이러한 이름은 플랫폼에 따라 달라집니다. 예를 들어 HMAC-SHA2-512-256 은 자르기 길이 번호 및 기타 여분의 정보를 모두 삭제하고 단순히 SHA-512 로 표시할 수 있습니다.
		PRF(의사 난수 함수)	- PRF-MD5-96 - PRF-SHA1-96 - PRF-AES-XCBC-96, PRF-AES-CMAC-96 - PRF-SHA2-256, PRF-SHA2-384, PRF-SHA2-512 많은 장치에서 명시적인 PRF 설정이 필요하지 않습니다.
		DH(Diffie-Hellman)	- 그룹 2(modp_1024), 그룹 5(modp_1536), 그룹 14(modp_2048), 그룹 15(modp_3072), 그룹 16(modp_4096) - modp_1024s160, modp_2048s224, modp_2048s256
		1 단계 수명	36,000 초(10 시간)
	2 단계	암호화	- 3DES - AES-CBC-128, AES-CBC-192, AES-CBC-256 - AES-GCM-128-8, AES-GCM-192-8, AES-GCM-256-8 - AES-GCM-128-12, AES-GCM-192-12, AES-GCM-256-12 - AES-GCM-128-16, AES-GCM-192-16, AES-GCM-256-16 일부 플랫폼에서 GCM 알고리즘은 비트(각각 64, 96, 128)로 지정된 해당 ICV 매개변수 옥텟(8, 12, 16)을 포함할 수 있습니다.
		무결성	- HMAC-MD5-96 - HMAC-SHA1-96 - AES-XCBC-96, AES-CMAC-96 - HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256 이러한 이름은 플랫폼에 따라 달라집니다. 예를 들어 HMAC-SHA2-512-256 은 자르기 길이 번호 및 기타 여분의 정보를 모두 삭제하고 단순히 SHA-512 로 표시할 수 있습니다.
		PFS 알고리즘(필수)	- 그룹 2(modp_1024), 그룹 5(modp_1536), 그룹 14(modp_2048), 그룹 15(modp_3072), 그룹 16(modp_4096), 그룹 18(modp_8192)

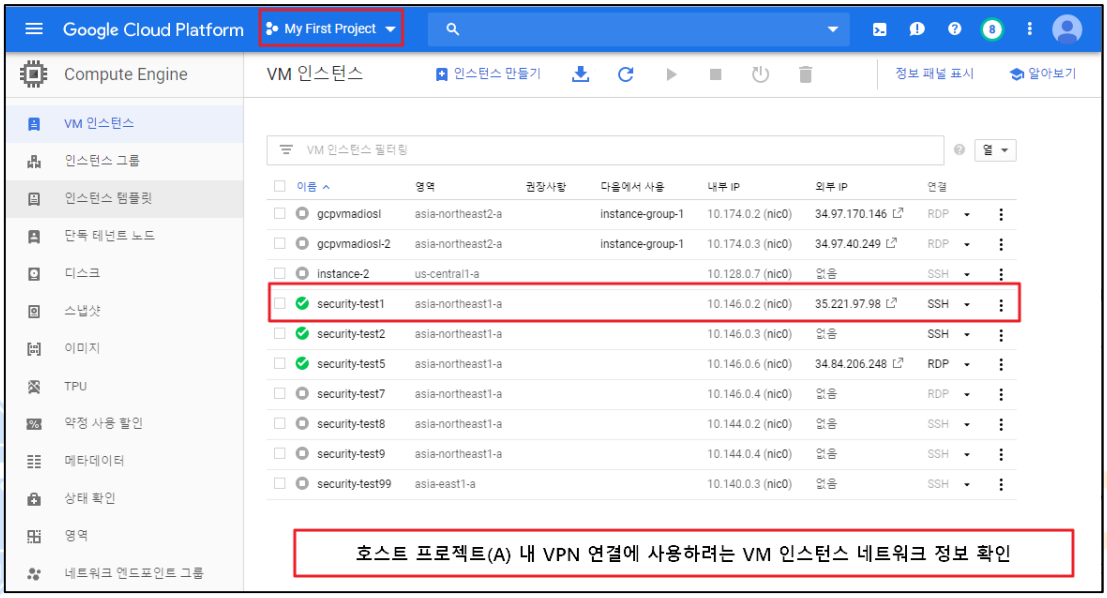
		- modp_1024s160, modp_2048s224, modp_2048s256
	DH(Diffie-Hellman)	일부 장치에는 2 단계에 대해 DH 값이 필요합니다. 이 경우 1 단계에 사용한 값을 사용하세요.
	2 단계 수명	10,800 초(3 시간)

설정 방법

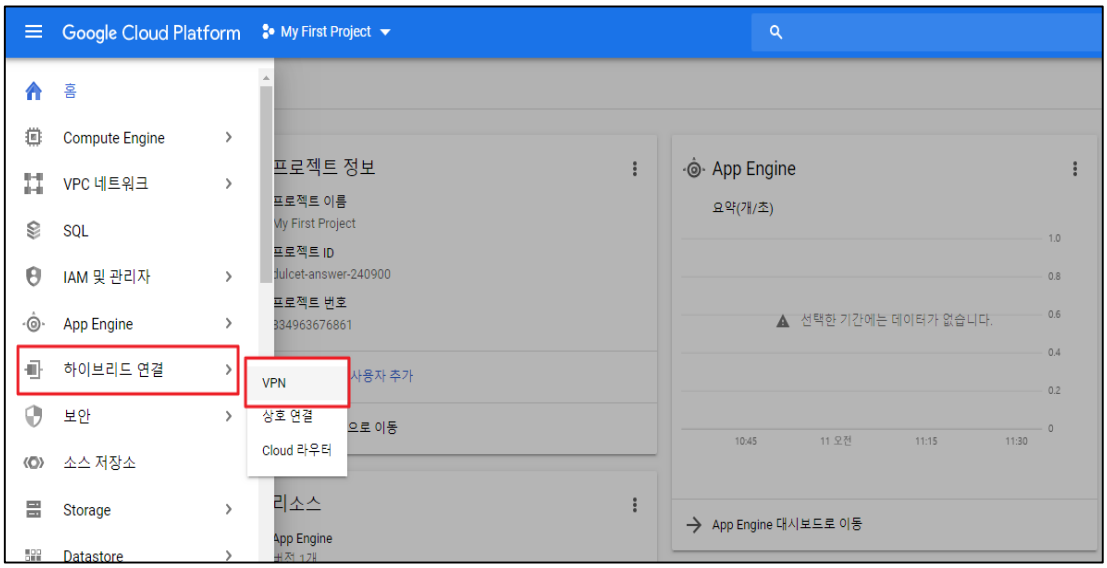
가. Cloud VPN 설정 방법

(호스트 프로젝트 (A): My First Project / 대상 프로젝트 (B): security-test)

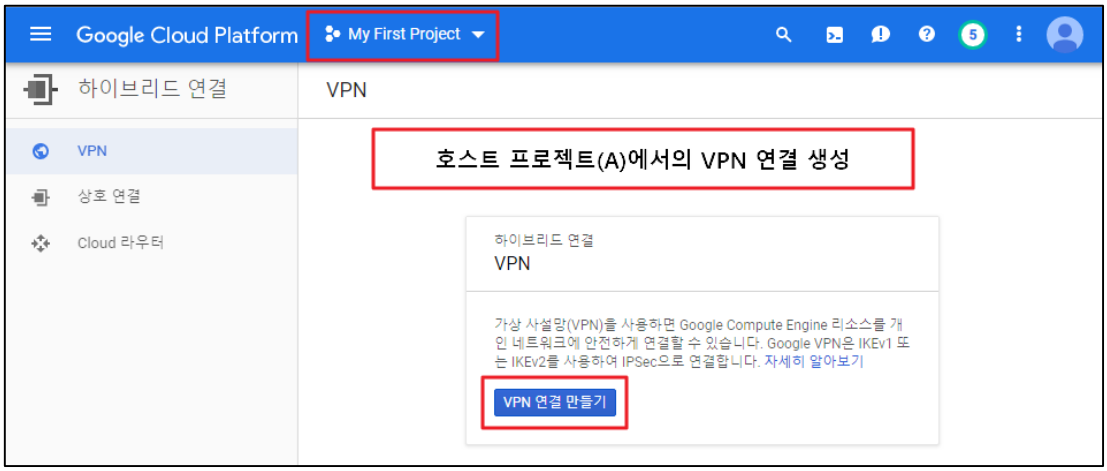
1) [Compute Engine] > [VM 인스턴스]



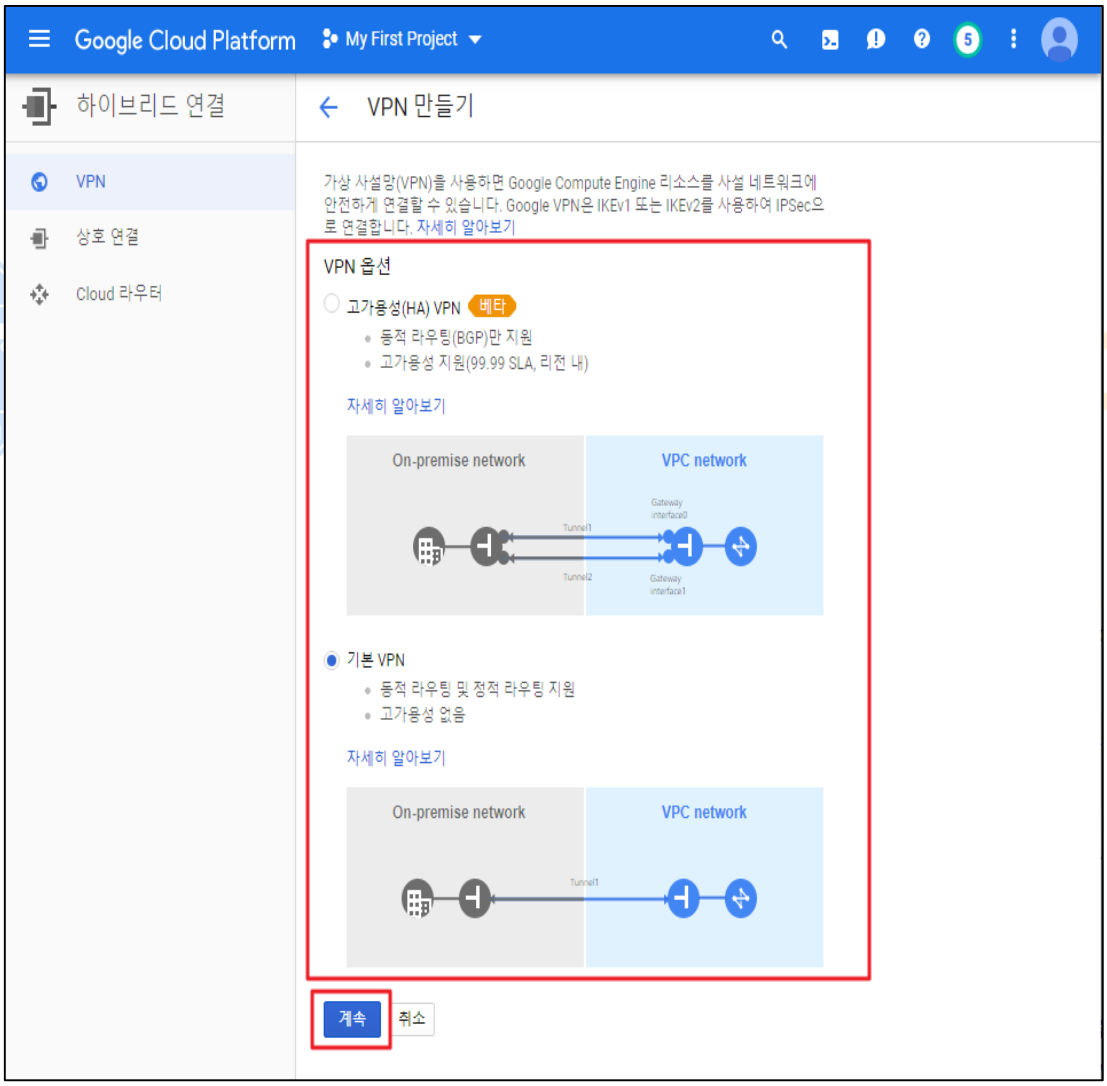
2) [하이브리드 연결] > [VPN]



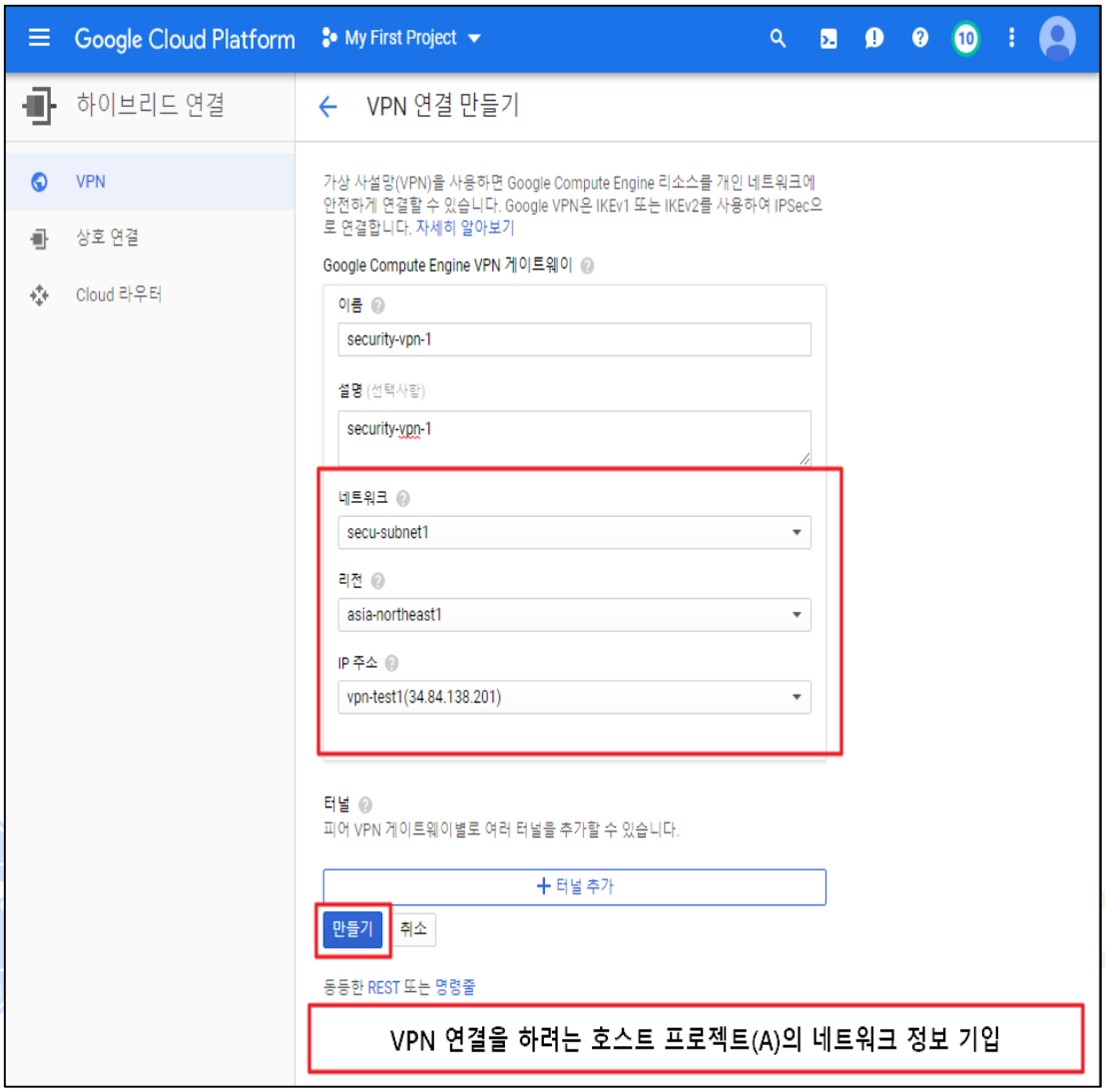
3) [VPN 연결 만들기]



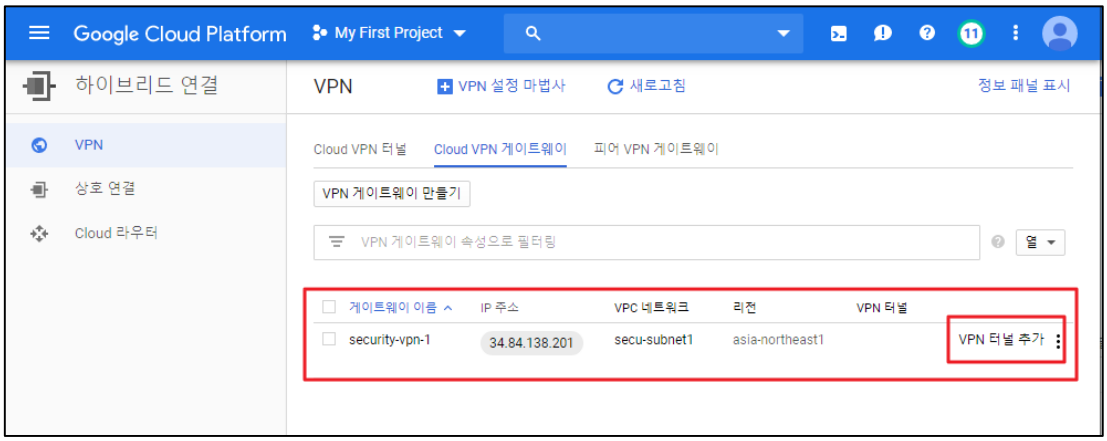
4) VPN 옵션 선택 (기본 VPN)



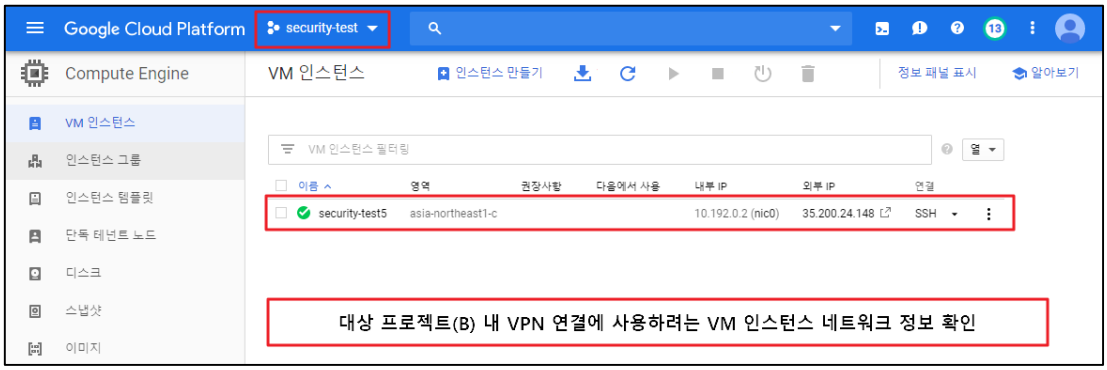
5) 호스트 프로젝트(A) 내 VPN 연결을 하려는 네트워크 정보 기입 및 VPN 에 공개 IP 주소 할당



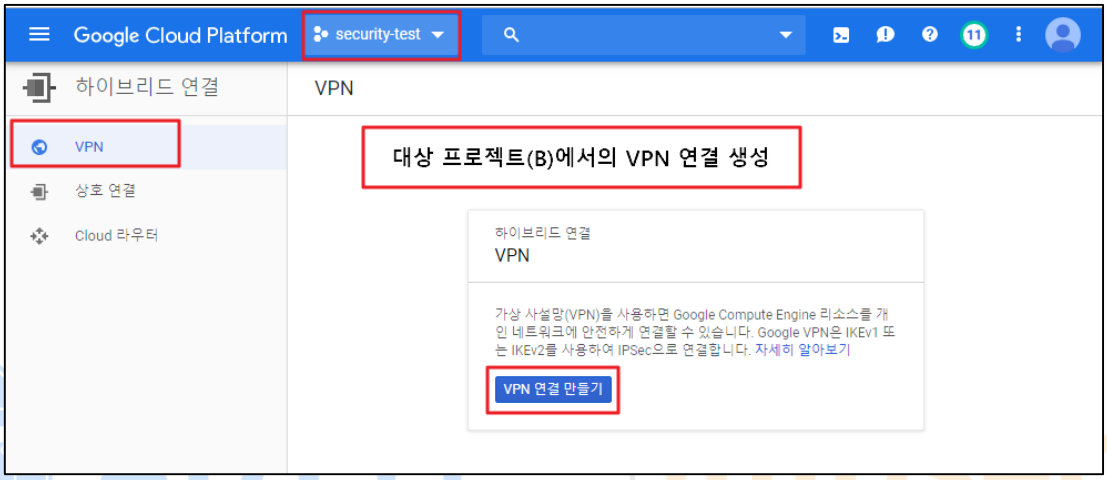
6) 호스트 프로젝트(A) Cloud VPN 게이트웨이 생성 확인



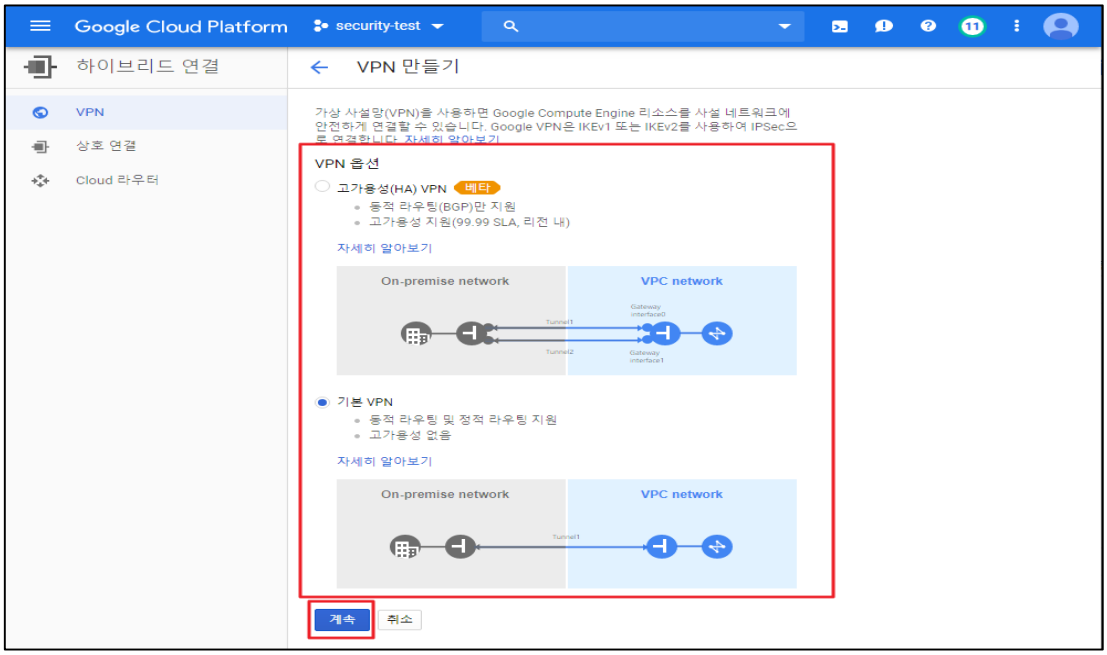
7) 대상 프로젝트(B) 내 VPN 연결을 하려는 네트워크 정보 확인



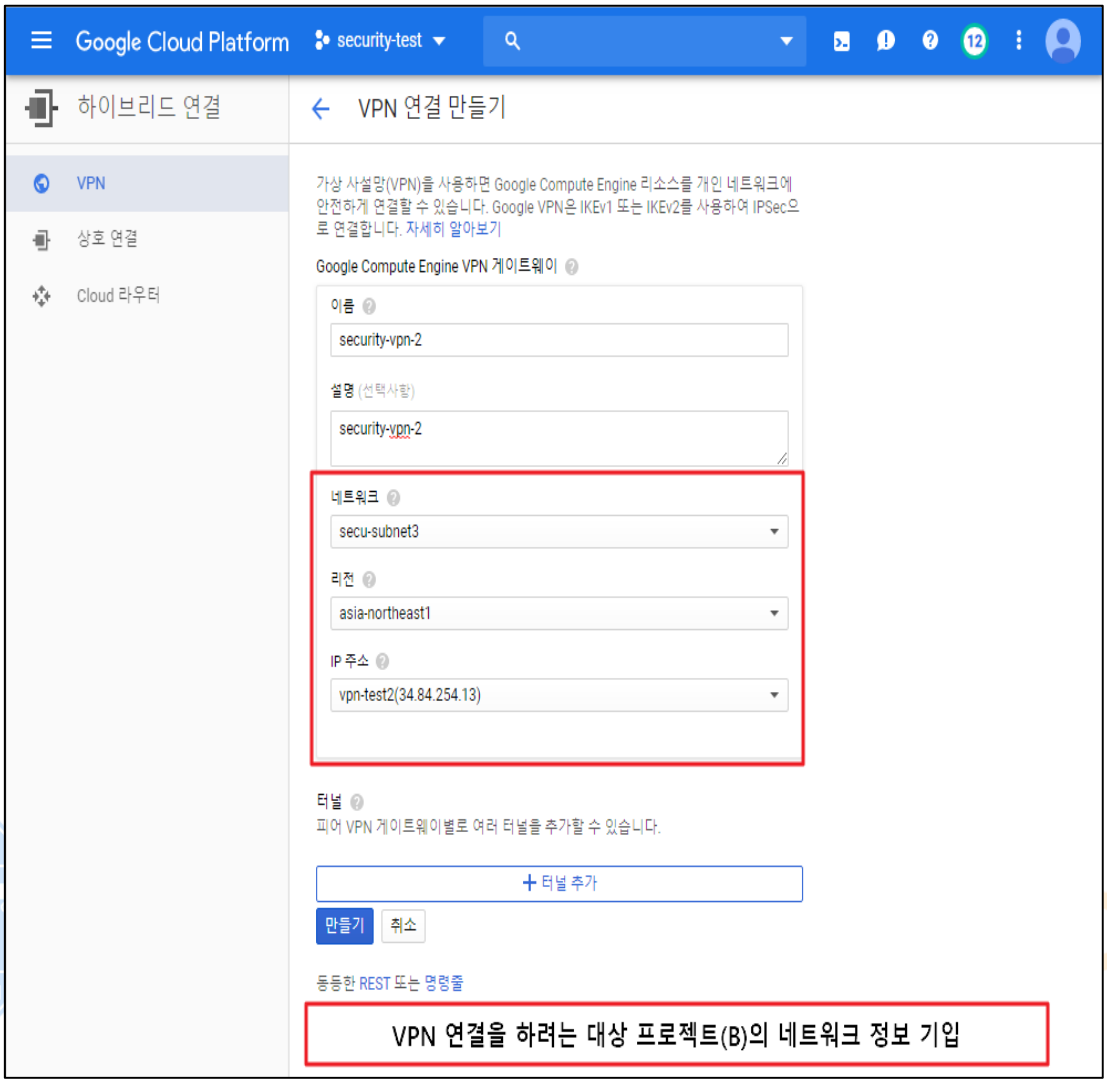
8) 대상 프로젝트(B)에서의 VPN 연결 만들기



9) VPN 연결 생성 옵션 선택



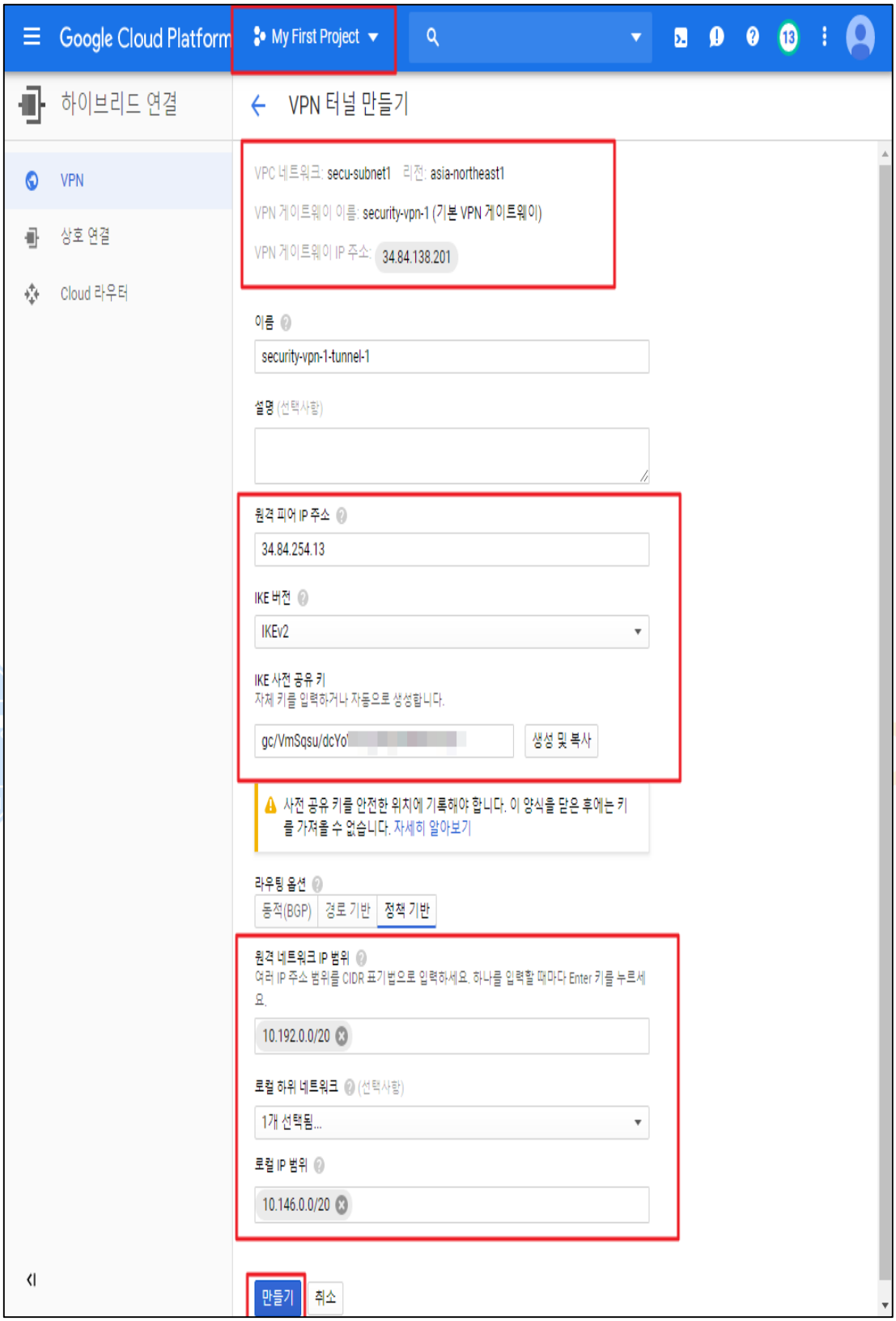
10) 대상 프로젝트(B) 내 VPN 연결을 하려는 네트워크 정보 기입 및 VPN 에 공개 IP 주소 할당



11) 대상 프로젝트(B) Cloud VPN 게이트웨이 생성 확인

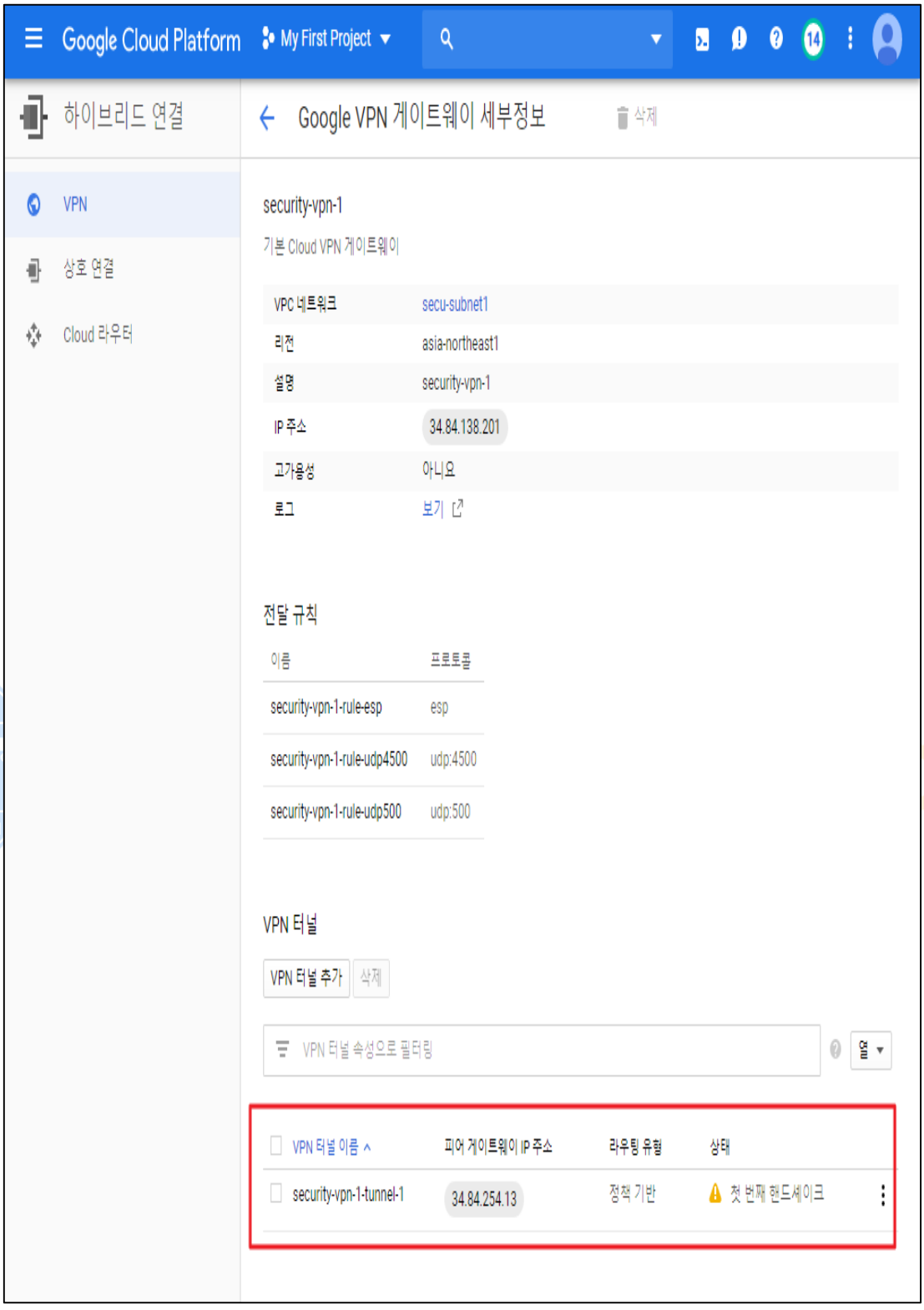
12) 호스트 프로젝트(A) 내 VPN 터널 추가

- IKE 키 생성 및 대상 프로젝트(B)의 원격 주소 / 호스트 프로젝트(B) 로컬 주소 입력



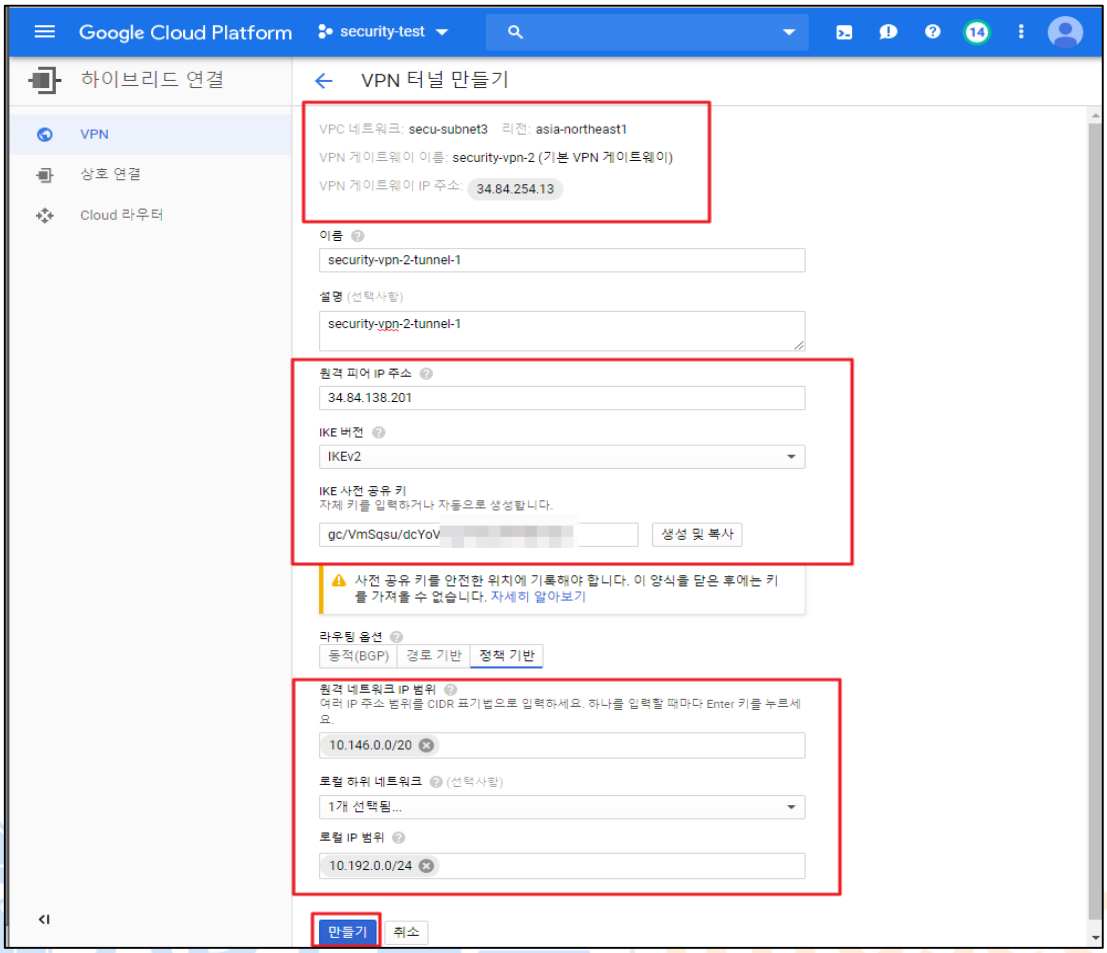
13) 호스트 프로젝트(A) 내 VPN 터널 생성 및 상태 값 확인

※ 상태 값이 '첫 번재 핸드셰이크'이 이유는 대상 프로젝트(B)의 VPN 터널 미 생성으로 인한 상태 값이며 설정이 정상 완료 될 경우 '설정됨' 표시가 됩니다.

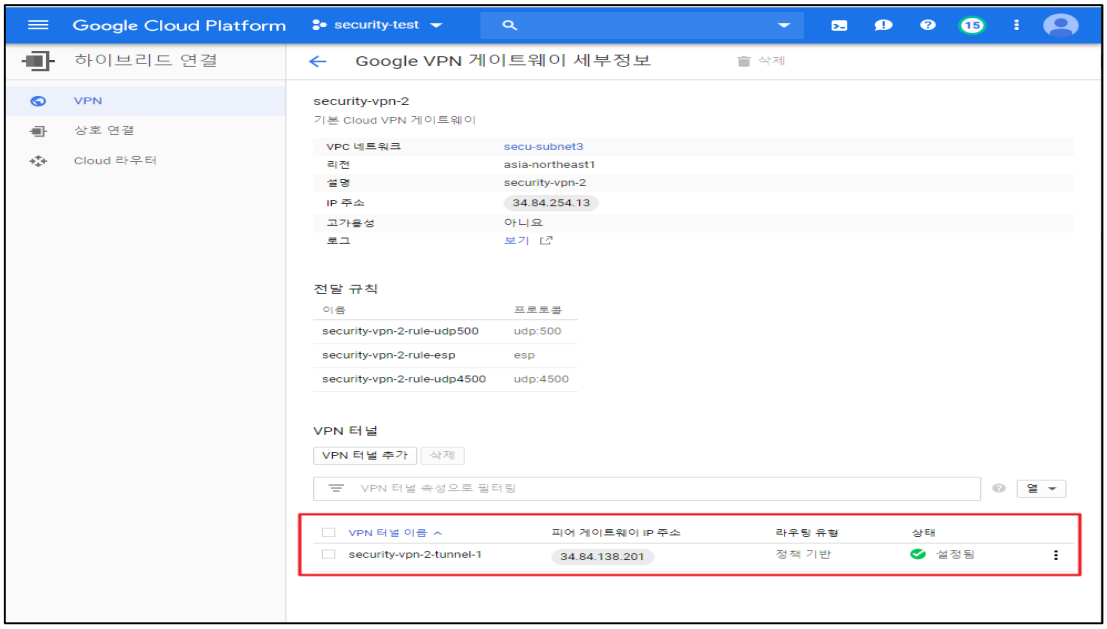


14) 대상 프로젝트(B) 내 VPN 터널 추가

- IKE 키 생성 및 호스트 프로젝트(A)의 원격 주소 / 대상 프로젝트(B) 로컬 주소 입력.



15) 대상 프로젝트(B) 내 VPN 터널 생성 및 상태 값 확인

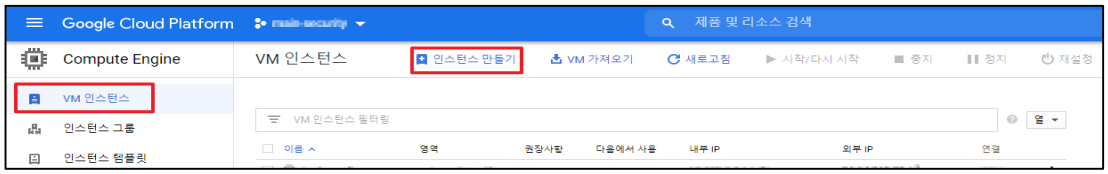
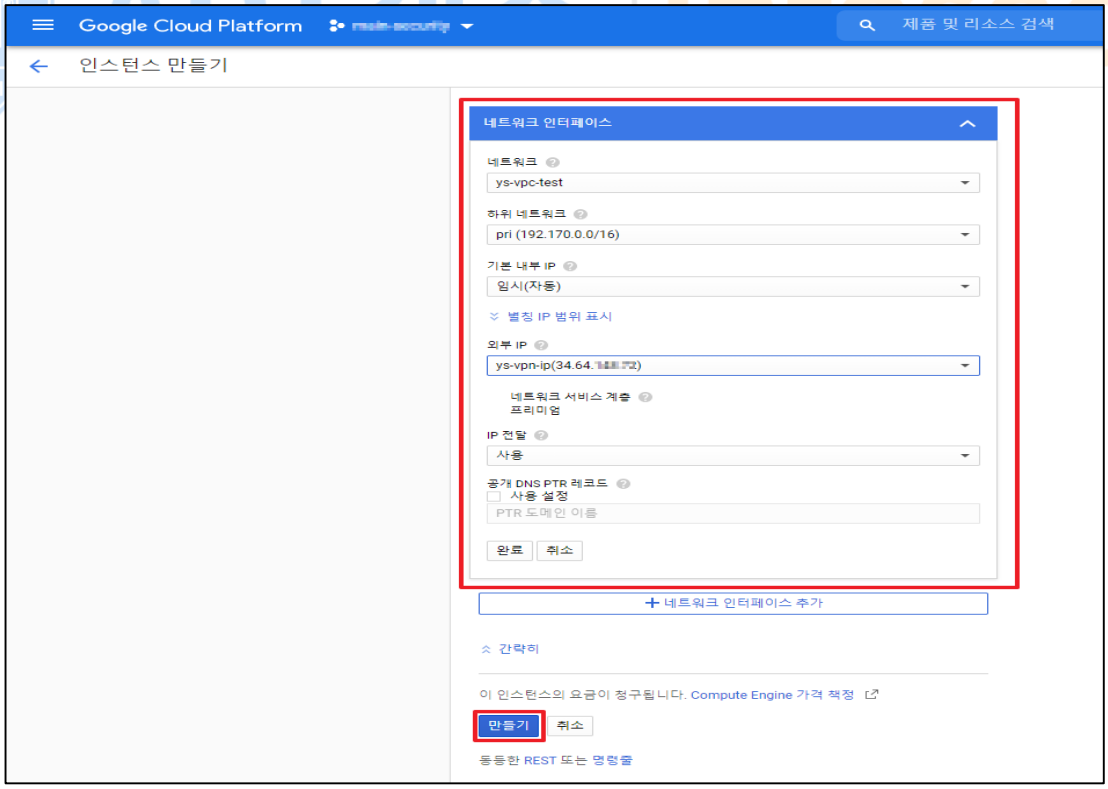


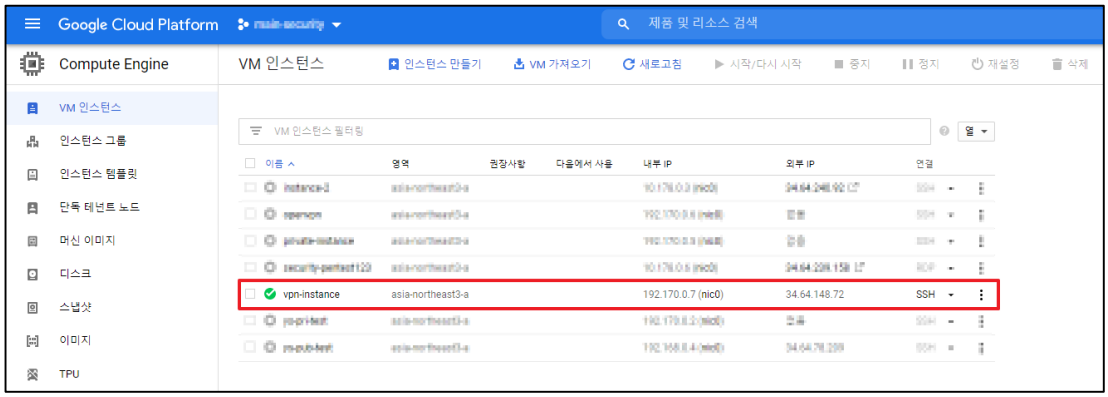
16) 호스트 프로젝트(A) 및 대상 프로젝트(B)의 VPN 연결 최종 확인

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단 기준</td><td>양호기준
: On-Demend(Private Cloud)와 Public Cloud 환경 간에 Cloud VPN 터널 및 게이트웨이를 연결하고 있지 않을 경우

취약기준
: On-Demend(Private Cloud)와 Public Cloud 환경 간에 Cloud VPN 터널 및 게이트웨이를 연결하고 있을 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

3.10 VPN 공용 IP 설정

분류	가상 리소스 관리	중요도	하
항목명	VPN 공용 IP 설정		
항목 설명	Cloud VPN 은 IPsec VPN 연결을 통해 온프레미스 네트워크를 Google Cloud Platform Virtual Private Cloud(GCP VPC) 네트워크에 안전하게 연결합니다. 두 개의 네트워크 사이로 이동되는 트래픽은 하나의 VPN 게이트웨이에서 암호화된 후 다른 VPN 게이트웨이에서 암호 해독됩니다. 인터넷에서 전송되는 데이터는 이러한 방식으로 보호됩니다. 하지만, VPN 내 공용 IP가 설정된 인스턴스 존재 시 VPN 연결을 통한 접근이 아닌 외부 어디서든 접근이 가능한 인스턴스가 존재하고 있어, 공용 IP 인스턴스에 접근할 경우 VPN이 허용되지 않은 사용자더라도 VPN 내 인스턴스 등에 접근할 수 있습니다.		
설정 방법	**가. VPN 인스턴스 내 공용 IP 설정** 1) VPN 서버 내 VM 인스턴스 생성  2) 네트워크 인터페이스 설정 내 공용 IP 설정  3) VPN 서버 내 공용 IP VM 인스턴스 생성 완료		

	
진단 기준	**양호기준** : VPN에 연결된 대상 네트워크 내 공용IP를 할당 받은 리소스가 존재하지 않을 경우 **취약기준** : VPN에 연결된 대상 네트워크 내 공용IP를 할당 받은 리소스가 존재할 경우
비고	사용하고 있는 서비스가 대외적으로 Open 해도 영향도가 없을 경우에는 예외사항으로 함

4. 감사/추적

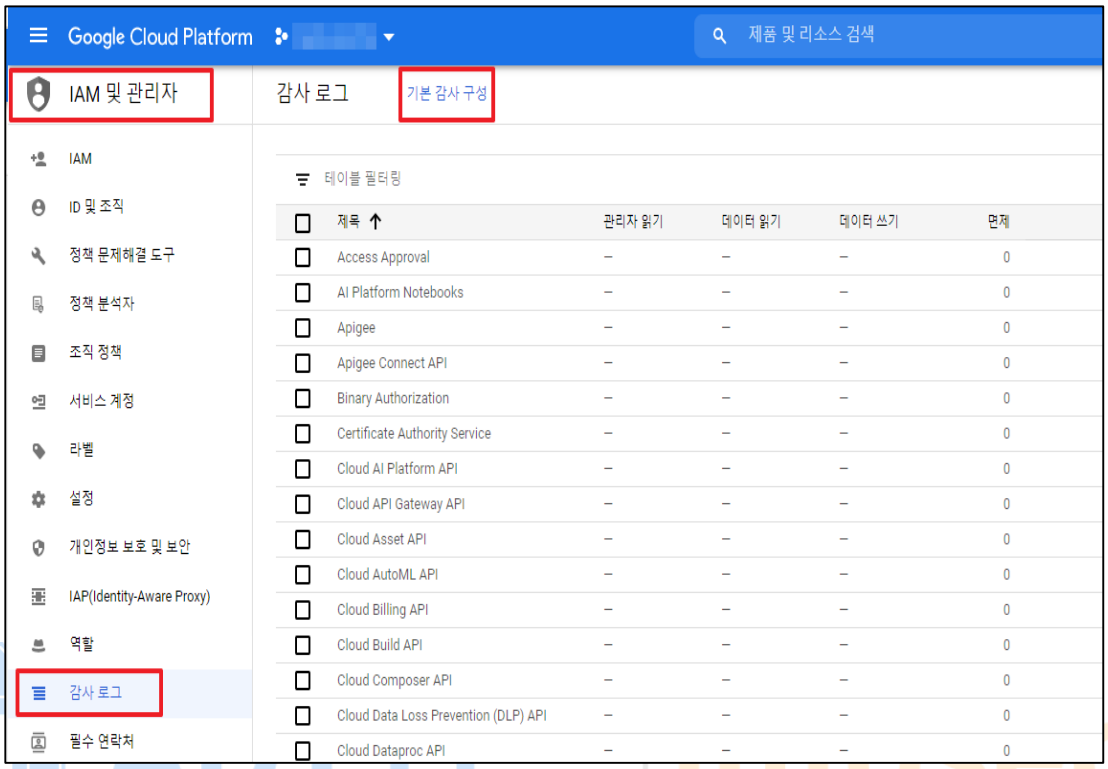
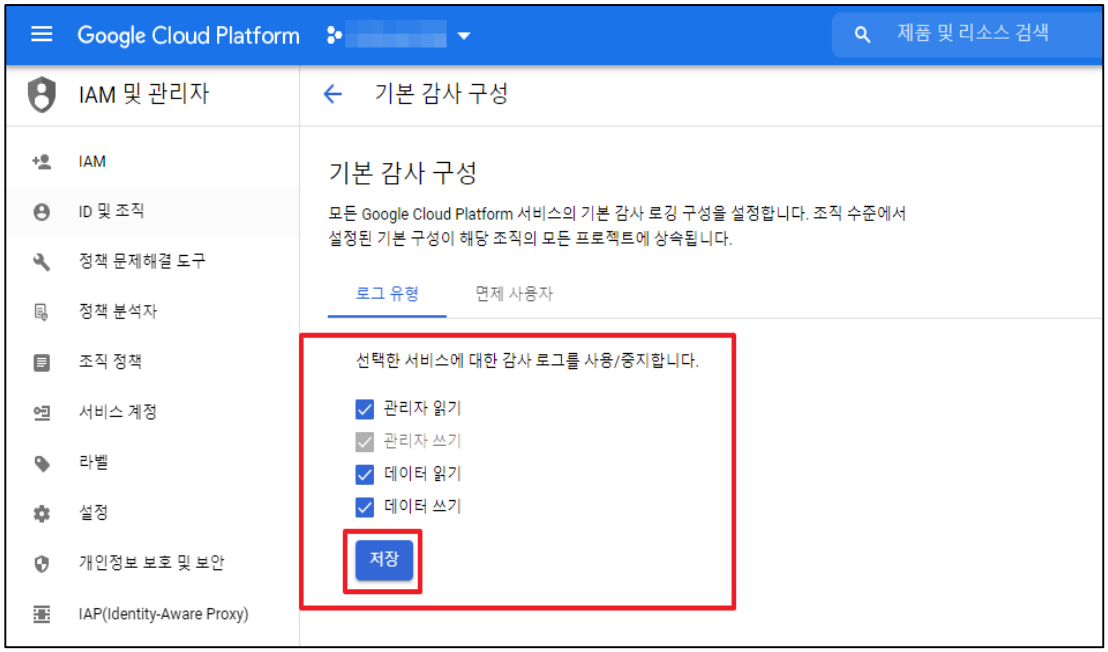
4.1 감사 로그 기록 및 관리

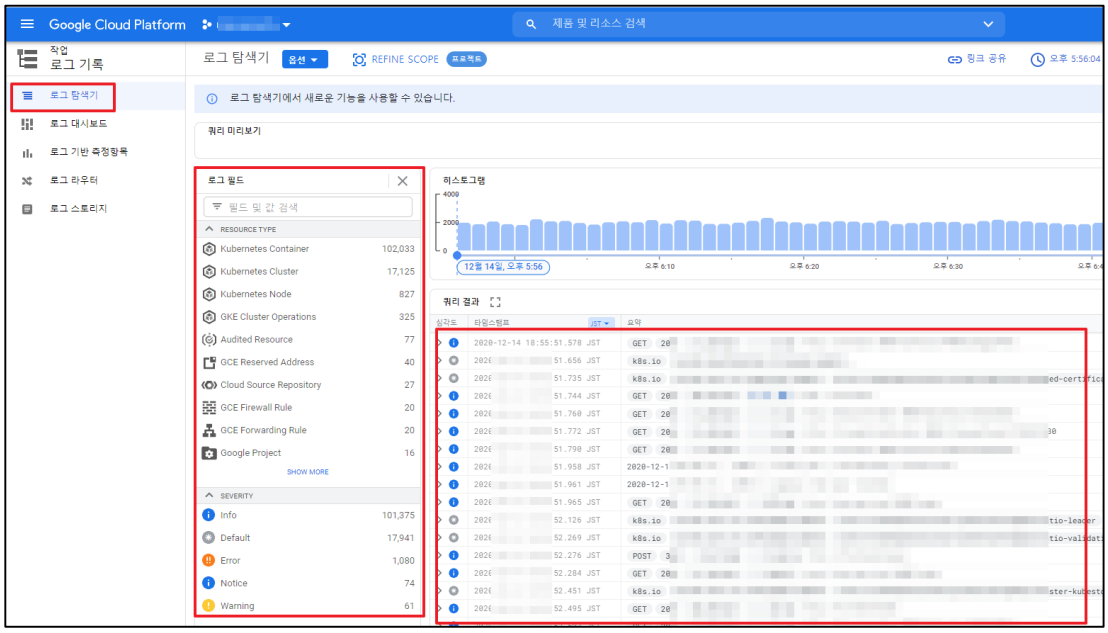
<table>
<tr><td>분류</td><td>감사/추적</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">감사 로그 기록 및 관리</td></tr>
<tr><td>항목
설명</td><td colspan="3">Cloud 감사 로그 설정을 통해 Google Cloud 리소스에 '누가, 언제, 어디서, 무엇을 했는지' 파악할 수 있습니다.

Cloud 감사 로그로 관리자 활동, 시스템 이벤트, 데이터 액세스, 정책 거부에 대한 로그가 저장되며, 관리자 활동 및 시스템 이벤트 감사 로그의 경우 기본적으로 항상 기록되므로 사용을 중지시킬 수 없습니다. 데이터 액세스 감사 로그는 Cloud Console의 [IAM 및 관리자] - [감사 로그] 메뉴에서 설정 가능합니다.

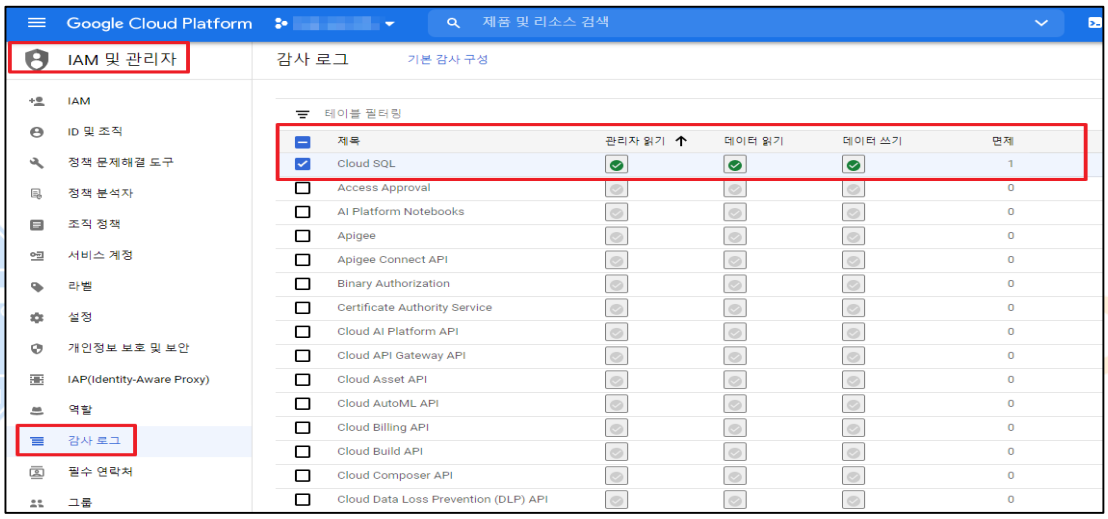
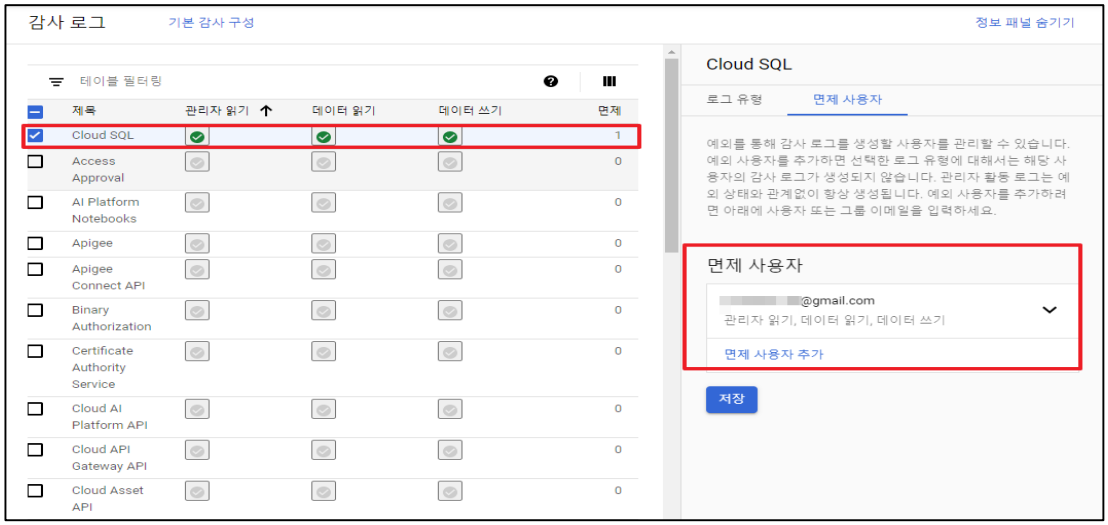
Cloud 감사 로그로 관리자 활동, 시스템 이벤트, 데이터 액세스, 정책 거부에 대한 로그가 저장되며, Cloud Console의 [IAM 및 관리자] - [감사 로그] 메뉴에서 설정 가능합니다. 설정된 Cloud 감사 로그는 Cloud Console의 [로그 기록] - [로그 탐색기] 메뉴에서 확인할 수 있습니다.

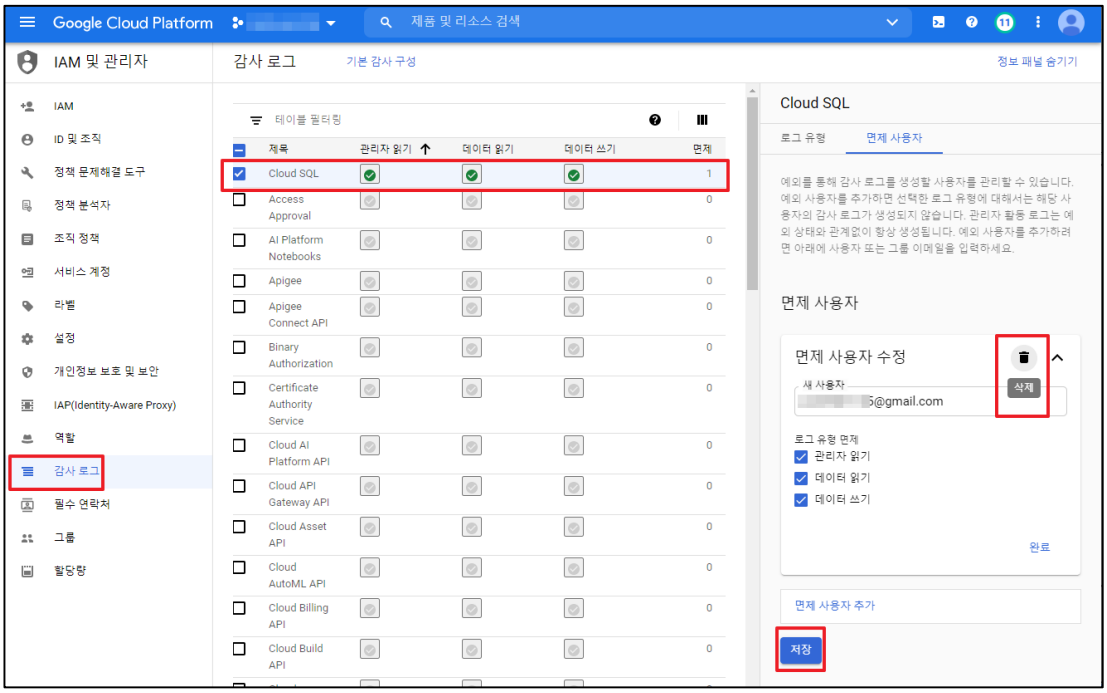
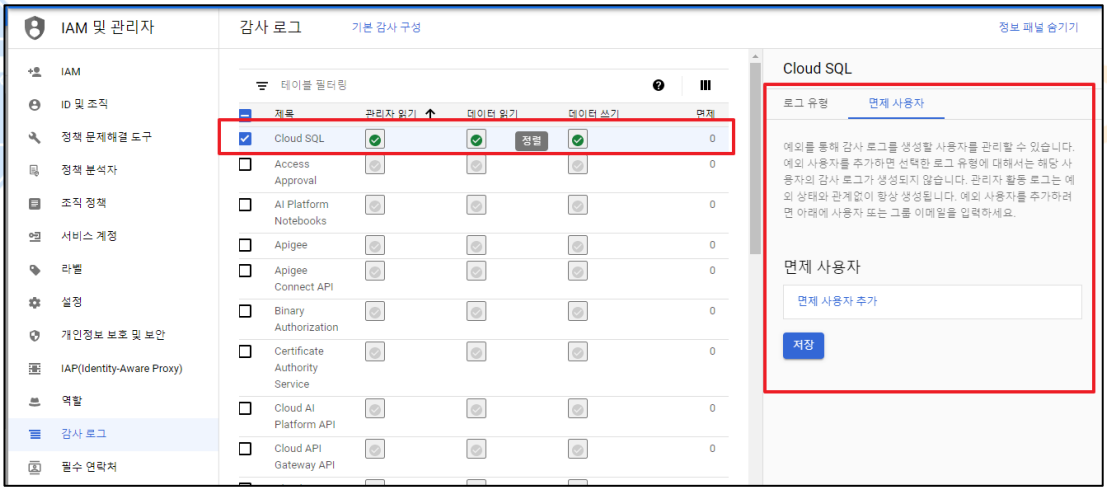
(*) 감사 로그 종류
<table>
<tr><th>구분</th><th>내용</th></tr>
<tr><td>관리자 활동 감사 로그</td><td>API 호출이나 리소스의 구성 또는 메타데이터를 수정하는 기타 관리 작업과 관련된 로그 항목 포함</td></tr>
<tr><td>시스템 이벤트 감사 로그</td><td>리소스의 구성 또는 메타데이터를 읽는 API 호출뿐만 아니라 사용자가 제공한 리소스 데이터를 생성, 수정 또는 읽는 사용자 주도 API 호출까지 포함</td></tr>
<tr><td>데이터 액세스 감사 로그</td><td>리소스 구성을 수정하는 Google Cloud 관리 작업의 로그 항목을 포함</td></tr>
<tr><td>정책 거부 감사 로그</td><td>보안 정책 위반으로 인해 Google Cloud 서비스가 사용자 또는 서비스 계정에 대한 액세스를 거부 시 생성</td></tr>
</table>
(*) 주요 리소스 별 감사 로그 기본 설정 현황
<table>
<tr><th>구분</th><th>GCE(Google Cloud Engine)</th><th>GCS(Google Cloud Storage)</th><th>Google Cloud SQL</th></tr>
<tr><td>관리자 활동 감사 로그</td><td>사용</td><td>사용</td><td>사용</td></tr>
<tr><td>시스템 이벤트 감사 로그</td><td>사용 중지</td><td>사용 중지</td><td>사용</td></tr>
<tr><td>데이터 액세스 감사 로그</td><td>사용</td><td>X</td><td>사용 중지</td></tr>
<tr><td>정책 거부 감사 로그</td><td>X</td><td>X</td><td>X</td></tr>
</table>
※ Cloud 감사 로그는 조직 구성원이 수행한 작업에 대한 로그를 제공하는 반면, 액세스 투명성 로그는 Google 직원이 수행한 작업에 대한 로그를 제공합니다. 또한, 중요 로그는</td></tr>
</table>

	보관기간을 설정해 사용하시기 바랍니다.
설정 방법	**가. 기본 감사로그 설정** 1) IAM 및 관리자 내 [감사로그] 페이지 접근 및 기본 감사 설정 확인  2) 기본 감사 구성 설정 후 저장  3) 로그탐색기 내 설정된 감사로그 확인

	
진단 기준	**양호기준** : Cloud 감사 로그가 설정되어 있을 경우 **취약기준** : Cloud 감사 로그가 설정되어 있지 않을 경우
비고	

4.2 감사 로그 면제 사용자 존재 여부

분류	감사/추적	중요도	중
항목명	감사 로그 면제 사용자 존재 여부		
항목 설명	Cloud 감사 로그 내 면제 사용자 설정을 통해 감사 로그를 생성할 사용자를 제어할 수 있습니다. 면제 사용자를 추가하면 선택한 로그 유형에서 해당 사용자의 감사 로그가 생성되지 않으나, 관리자 활동 로그의 경우 면제 사용자 설정 여부와 관계없이 항상 생성됩니다. 면제 사용자는 [액세스] - [감사 로그] 내 Google Cloud 서비스 클릭 - [면제 사용자] 메뉴에서 추가/삭제 할 수 있으며, 불필요한 면제 사용자가 존재하지 않도록 주기적 확인이 필요합니다.		
설정 방법	**가. 감사로그 내 면제 사용자 확인** 1) 감사로그 면제 사용자가 존재하는 서비스 확인  2) 면제 사용자 확인  **나. 면제 사용자 삭제**		

	1) 면제 사용자 삭제  2) 면제 사용자 삭제 확인 
진단 기준	**양호기준** : 감사로그 내 면제 사용자가 존재하지 않는 경우 **취약기준** : 감사로그 내 면제 사용자가 존재하는 경우
비고	

4.3 Google 계정 사용자 이상징후 알림 설정

분류	감사/추적	중요도	중
항목명	Google 계정 사용자 이상징후 알림 설정		

항목 설명

Cloud Monitoring은 Google Cloud, Amazon Web Services(AWS), 호스팅된 업타임 프로브, 애플리케이션 계측에서 측정항목, 이벤트, 메타데이터를 수집합니다. BindPlane 서비스를 사용하여 150개 이상의 공통 애플리케이션 구성요소, 온프레미스 시스템, 하이브리드 클라우드 시스템에서 이 데이터를 수집할 수도 있습니다. Google Cloud의 작업 제품군은 이러한 데이터를 수집하고 대시보드, 차트, 알림을 통해 유용한 정보를 제공합니다. BindPlane은 추가 비용 없이 Google Cloud 프로젝트에 포함되어 있습니다.

안전한 Google 계정 사용을 위해 Cloud Monitoring 서비스 내 알림 정책 설정을 통해 Google 계정 사용자의 이상징후 확인이 가능합니다.

Cloud Console의 [모니터링] - [알림] - [CREATE POLICY] 메뉴를 통해 알림 정책 설정이 가능하며, 아래와 같이 기본적으로 정의되어 있는 정책을 이용하여 사용자 이상징후 여부를 확인할 수 있습니다. 또한 사용자가 정의한 로그 기반 측정항목을 이용하여 임의의 알림 정책 설정도 가능합니다.

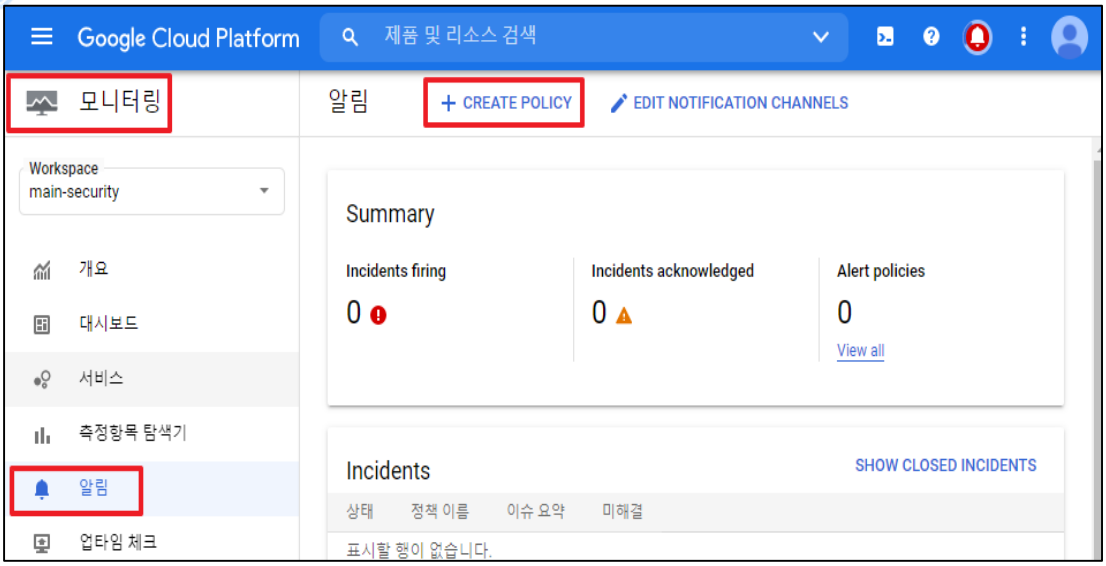
(*) Google 계정 사용자 이상징후 확인을 위한 기본 정의 알림 정책 (참고)

구분	측정항목
IAM	service_account/authn_events_count service_account/key/authn_events_count

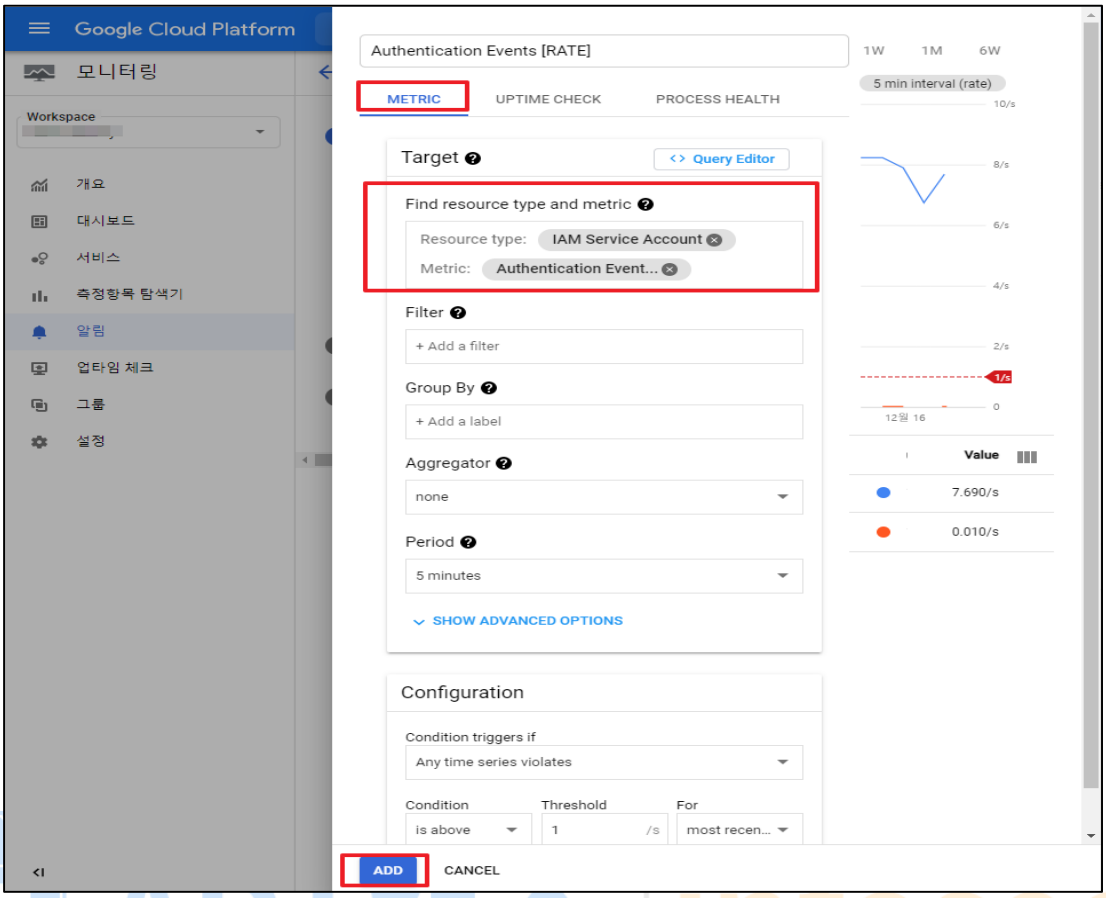
설정 방법

가. Google 계정 사용자 이상징후 경보 설정 방법

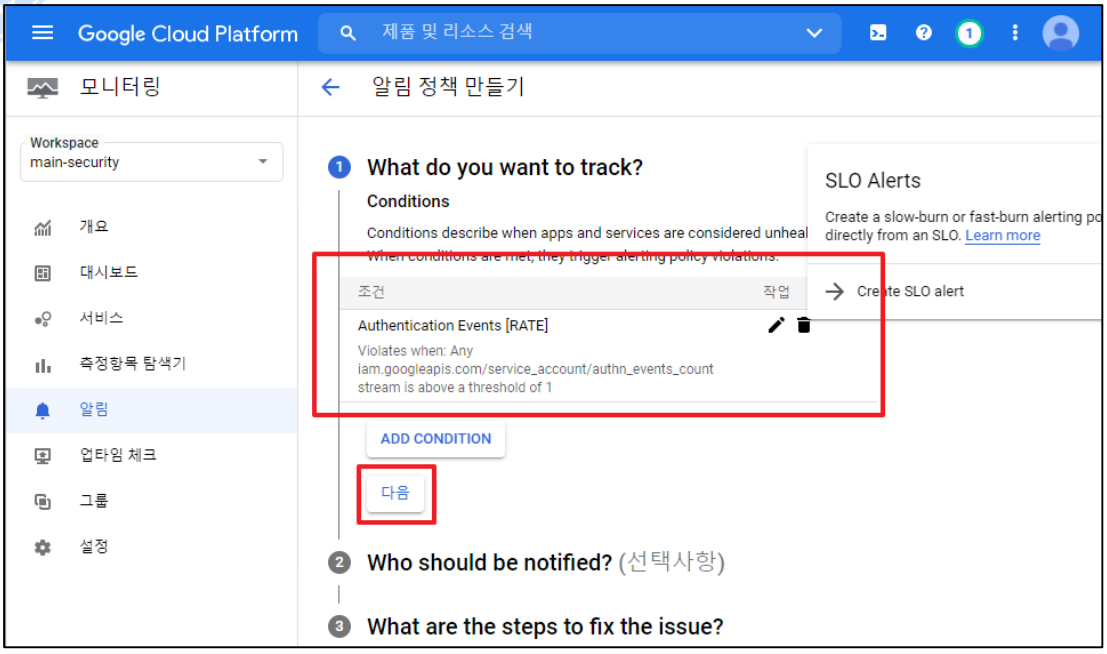
1) 모니터링 내 [알림] 페이지 접근 및 정책 생성 클릭



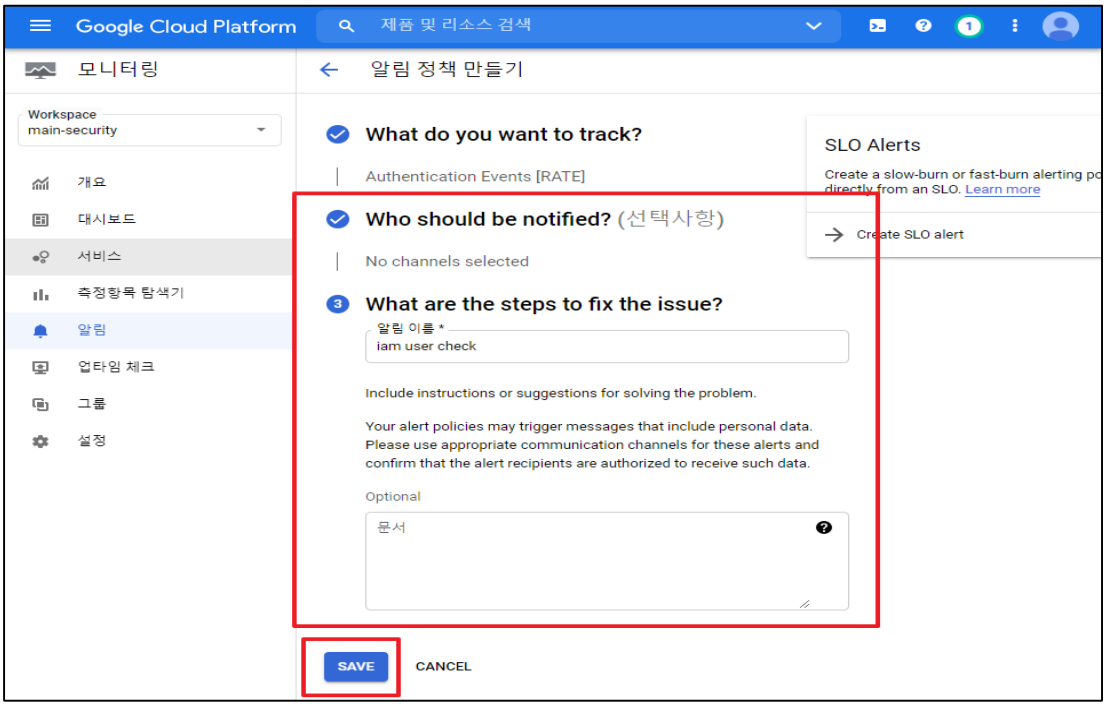
2) METRIC 설정 및 기타 세부 Condition 설정



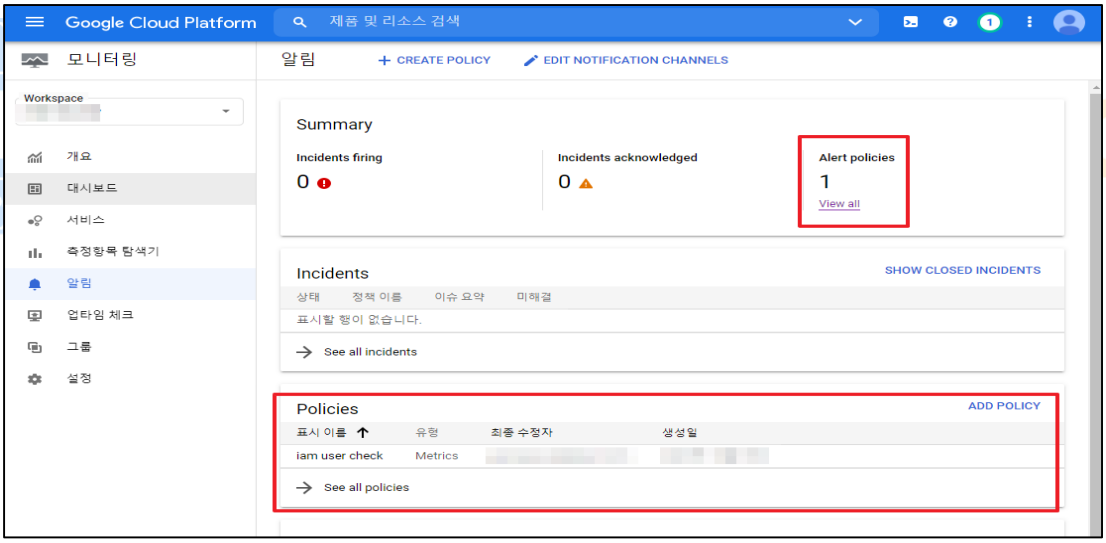
3) Policy 저장 확인 및 추가옵션 설정을 위한 [다음] 버튼 클릭



4) 추가 선택 옵션 정의 및 Policy 정책 저장



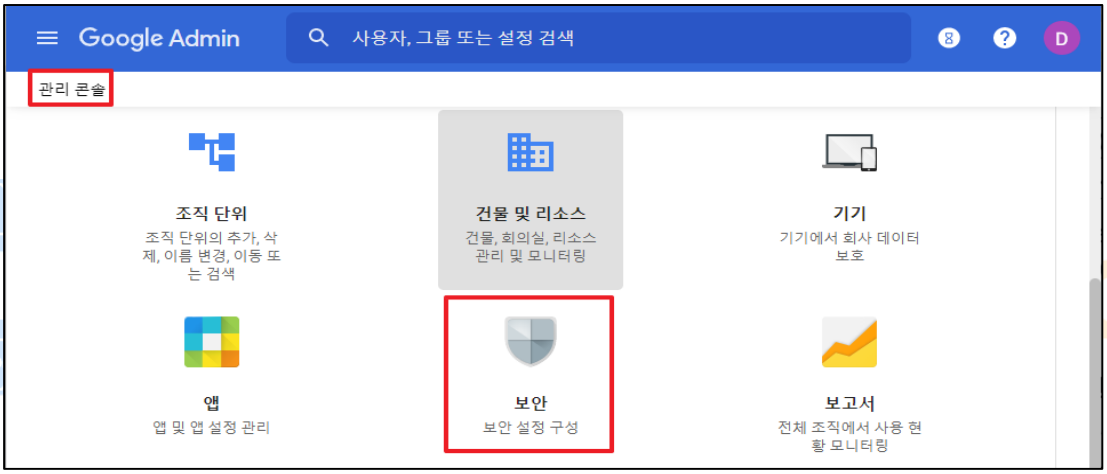
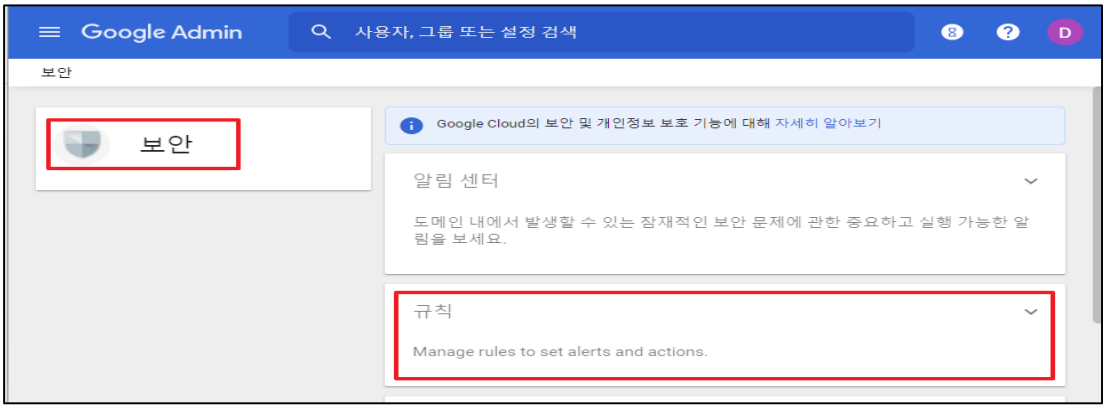
5) 설정한 Policy 정책 확인

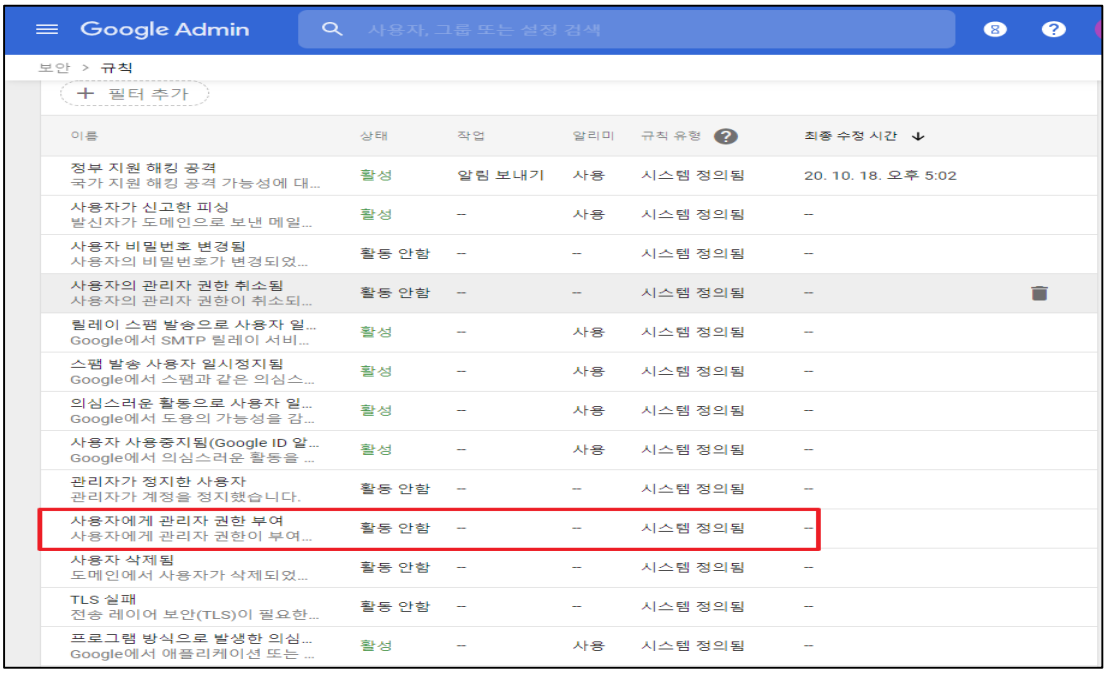


진단 기준	**양호기준** : Google 계정 사용자 이상징후에 대한 알림 설정이 되어 있을 경우 **취약기준** : Google 계정 사용자 이상징후에 대한 알림 설정이 되어있지 않을 경우
비고	

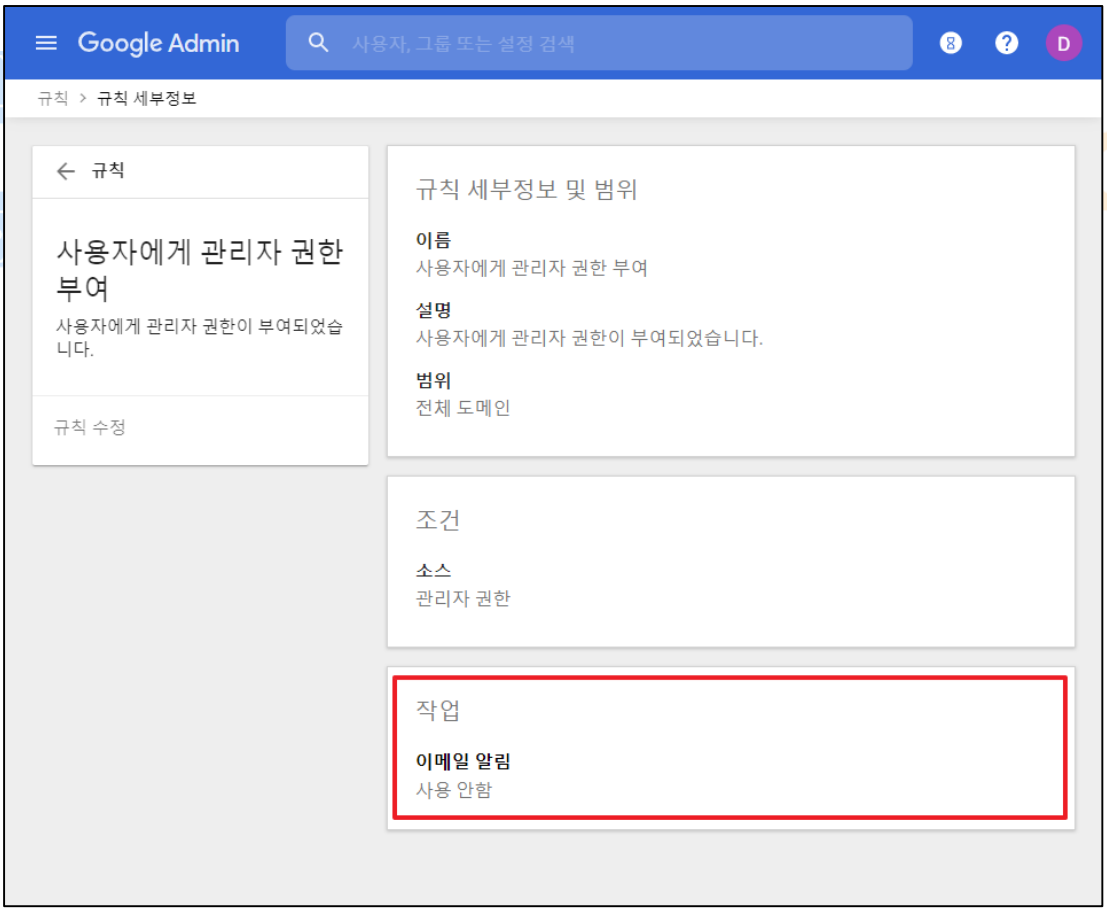
4.4 Cloud ID 계정 사용자 이상징후 알림 설정

분류	감사/추적	**중요도**	하
항목명	Cloud ID 계정 사용자 이상징후 알림 설정		

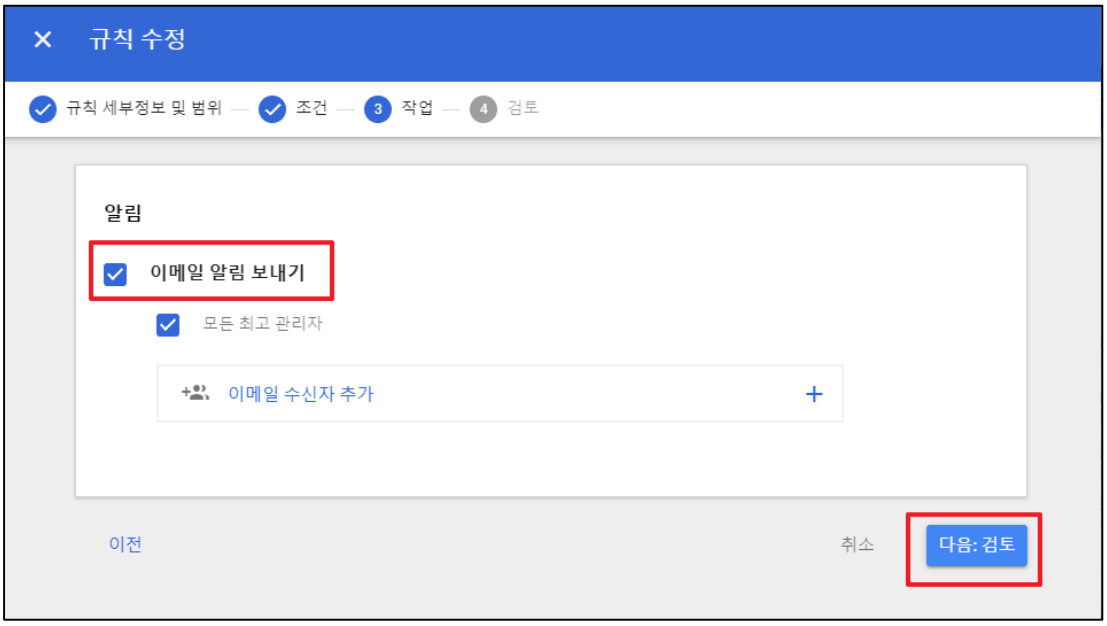
항목 설명	안전한 Cloud ID 계정 사용을 위해서는 관리 콘솔(https://admin.google.com) 내 사용자 이상징후 알림 설정은 관리자 관리 콘솔(https://admin.google.com)의 [보안] - [보안규칙] 메뉴에서 확인 및 설정이 가능하며, 아래와 같은 이상징후는 필수로 알림 설정을 해주어야 합니다. **(*) 알림이 필요한 이상징후** - 비밀번호 유출 - 사용중지된 사용자 활성화됨 - 의심스러운 로그인 - 사용자에게 관리자 권한 부여 - 사용자 사용중지됨(Google ID 알림)
설정 방법	**가. Cloud ID 사용자 이상징후 경보 설정 방법** 1) 관리콘솔 (admin.google.com) 내 [보안] 페이지 클릭  2) 보안 페이지 내 [규칙] 클릭  3) 설정하고자하는 알림 클릭 (ex_ "사용자에게 관리자 권한 부여")



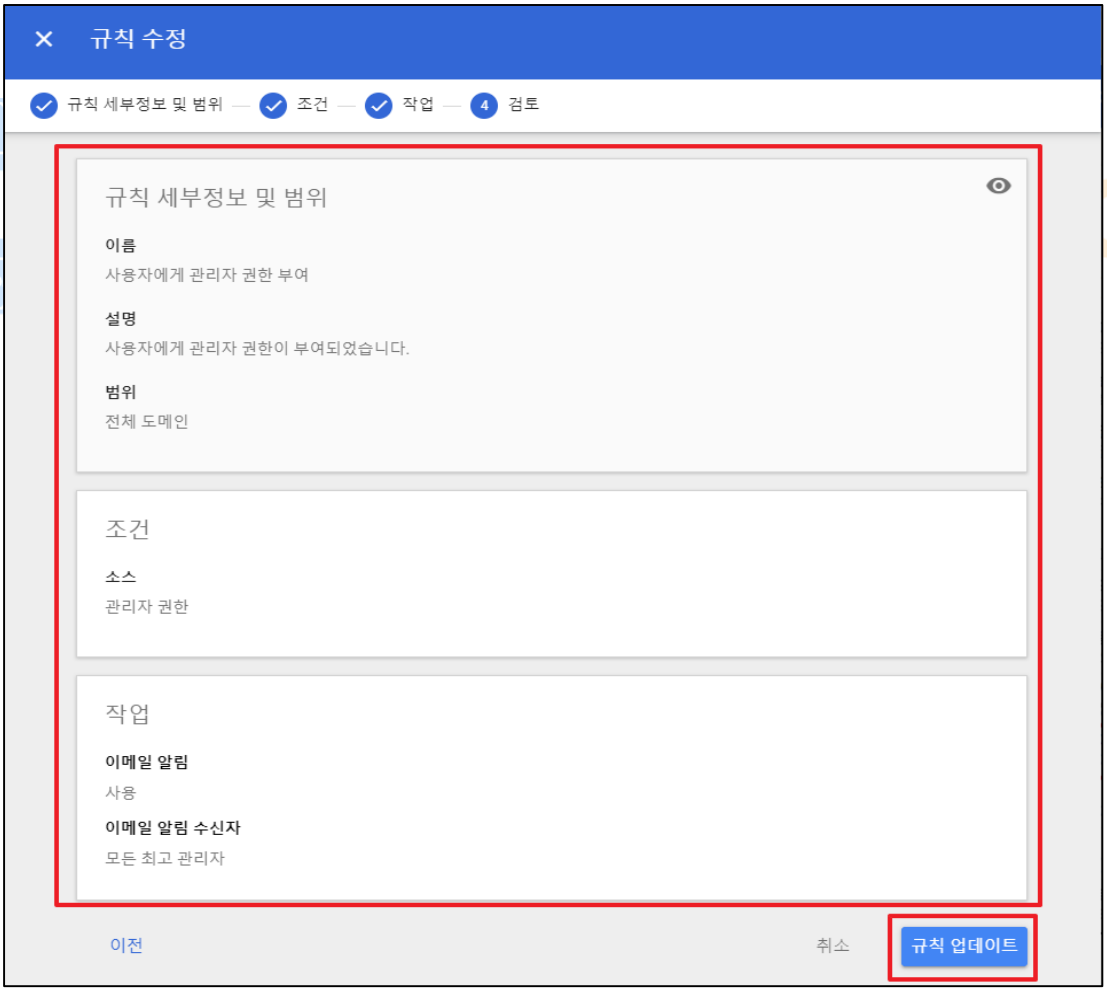
4) [작업] 필드 내 이메일 알림 클릭



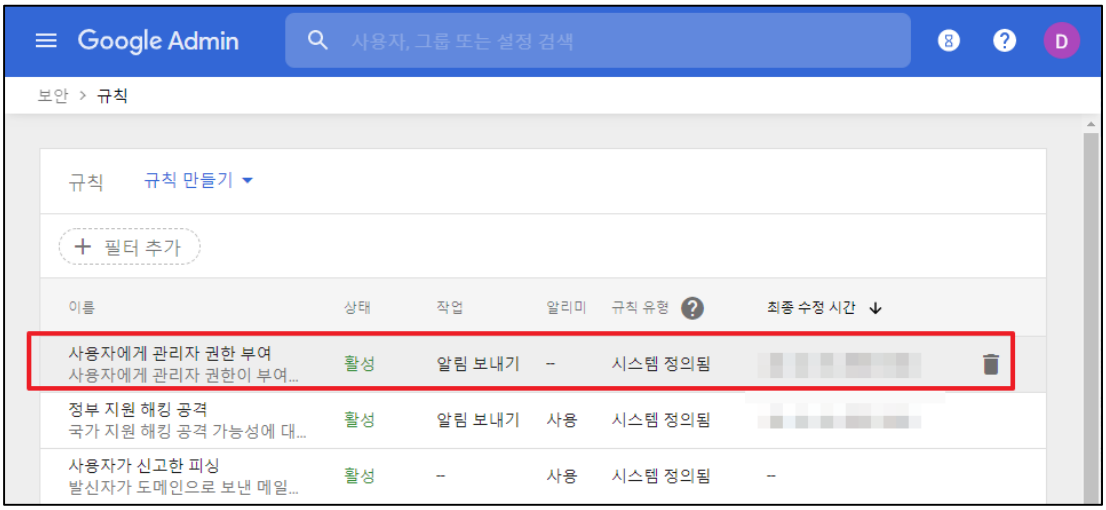
5) "이메일 알림 보내기" 체크 및 이메일 수신자 설정



6) 설정한 알림 규칙 확인 후 최종 업데이트



7) 설정한 알림 규칙 확인

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>진단
기준</td><td>양호기준
: Google 계정 사용자 이상징후에 대한 알림 설정이 되어 있을 경우

취약기준
: Google 계정 사용자 이상징후에 대한 알림 설정이 되어있지 않을 경우</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

4.5 가상 리소스 이상징후 알림 설정

<table>
<tr><td>분류</td><td>감사/추적</td><td>중요도</td><td>중</td></tr>
<tr><td>항목명</td><td colspan="3">가상 리소스 이상징후 알림 설정</td></tr>
<tr><td>항목
설명</td><td colspan="3">
Cloud Monitoring은 Google Cloud, Amazon Web Services(AWS), 호스팅된 업타임 프로브, 애플리케이션 계측에서 측정항목, 이벤트, 메타데이터를 수집합니다. BindPlane 서비스를 사용하여 150개 이상의 공통 애플리케이션 구성요소, 온프레미스 시스템, 하이브리드 클라우드 시스템에서 이 데이터를 수집할 수도 있습니다. Google Cloud의 작업 제품군은 이러한 데이터를 수집하고 대시보드, 차트, 알림을 통해 유용한 정보를 제공합니다. BindPlane은 추가 비용 없이 Google Cloud 프로젝트에 포함되어 있습니다.

안전한 Google 계정 사용을 위해 Cloud Monitoring 서비스 내 알림 정책 설정을 통해 이용중인 Cloud 가상리소스(Compute, Cloud SQL, Storage, Networking)에 대한 이상징후 확인이 가능합니다.

Cloud Console의 [모니터링] - [알림] - [CREATE POLICY] 메뉴를 통해 알림 정책 설정이 가능하며, 아래와 같이 기본적으로 정의되어 있는 정책을 이용하여 GCP 리소스 이상징후 여부를 확인할 수 있습니다. 또한 사용자가 정의한 로그 기반 측정항목을 이용하여 임의의 알림 정책 설정도 가능합니다.

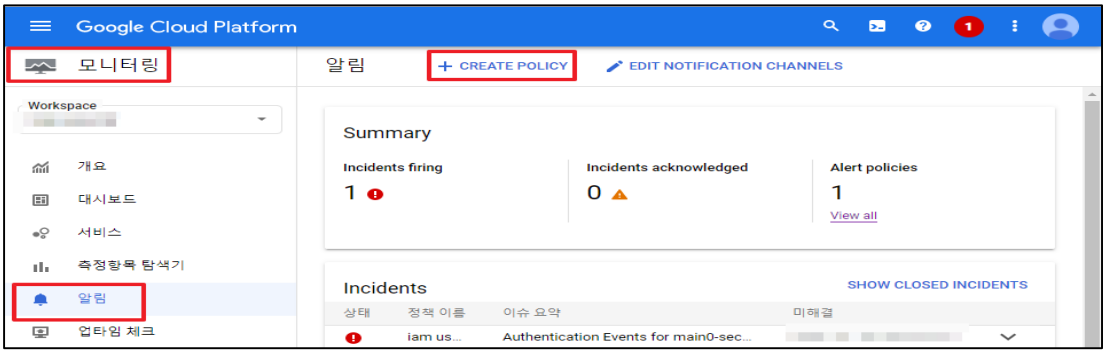
(*) GCP 리소스 이상징후 확인을 위한 기본 정의 알림 정책 (참고)
<table>
<tr><th>구분</th><th>측정항목</th></tr>
<tr><td>Compute</td><td>instance/cpu/utilization (CPU 사용률)
instance/memory/balloon/ram_used (메모리 사용률)
instance/integrity/late_boot_validation_status (부팅 무결성 검증)
guest/system/uptime (가동 시간)
... 등</td></tr>
<tr><td>Cloud SQL</td><td>database/cpu/utilization (CPU 사용률)
database/disk/utilization (디스크 사용률)
database/instance_state (인스턴스 상태)
database/memory/utilization (메모리 사용률)
... 등</td></tr>
<tr><td>Storage</td><td>network/received_bytes_count (수신 바이트)
network/sent_bytes_count (전송 바이트)
authz/object_specific_acl_mutation_count (ACL 변경 사항)
... 등</td></tr>
<tr><td>Networking</td><td>interconnect_attachment/ingress_bytes_count (GCP에서 온 프레미스 호스트로 전송된 바이트 수)
vm_flow/rtt (TCP 연결을 통해 측정된 RTT 분포)
vpn_tunnel/egress_bytes_count, vpn_tunnel/ingress_bytes_count (VPN</td></tr>
</table>
</td></tr>
</table>

	터널을 통해 GCP에서 송·수신된 바이트 수) … 등

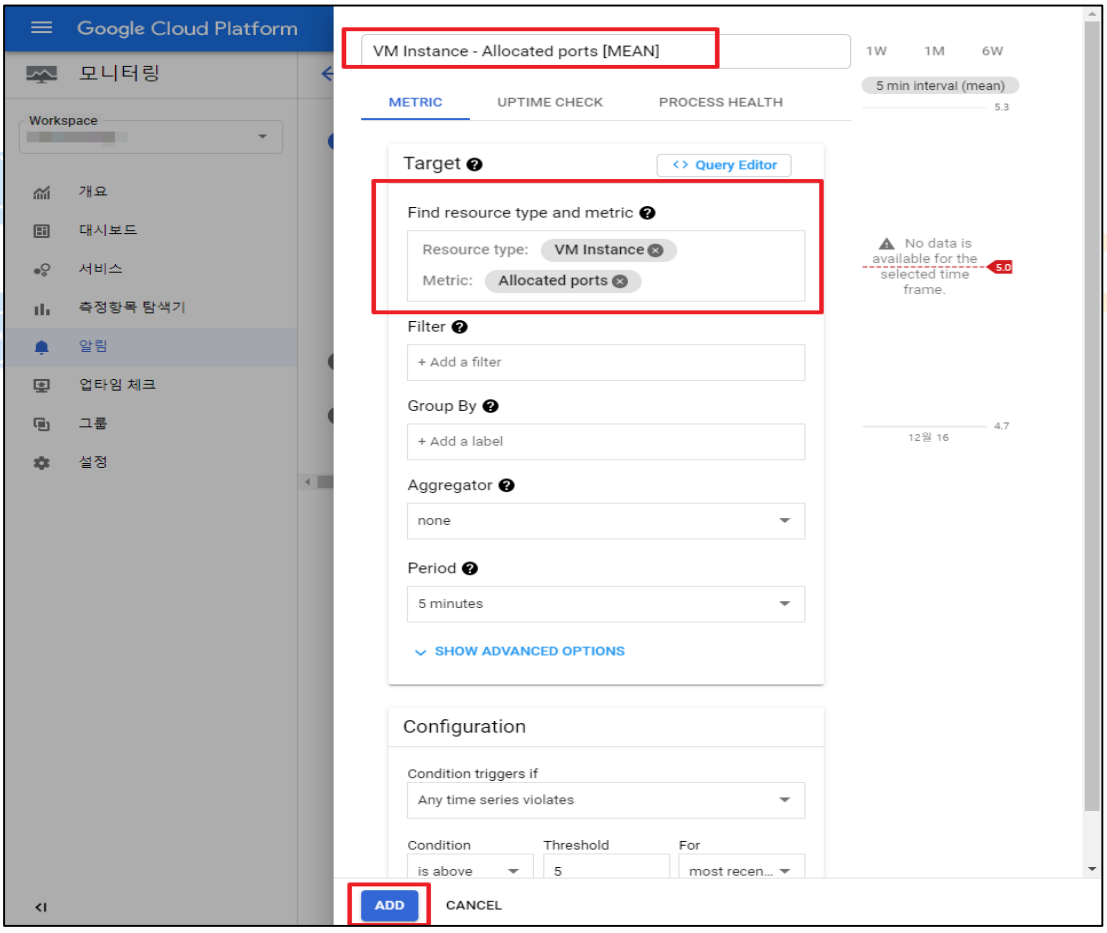
설정 방법

가. 가상 리소스 이상징후 경보 설정 방법

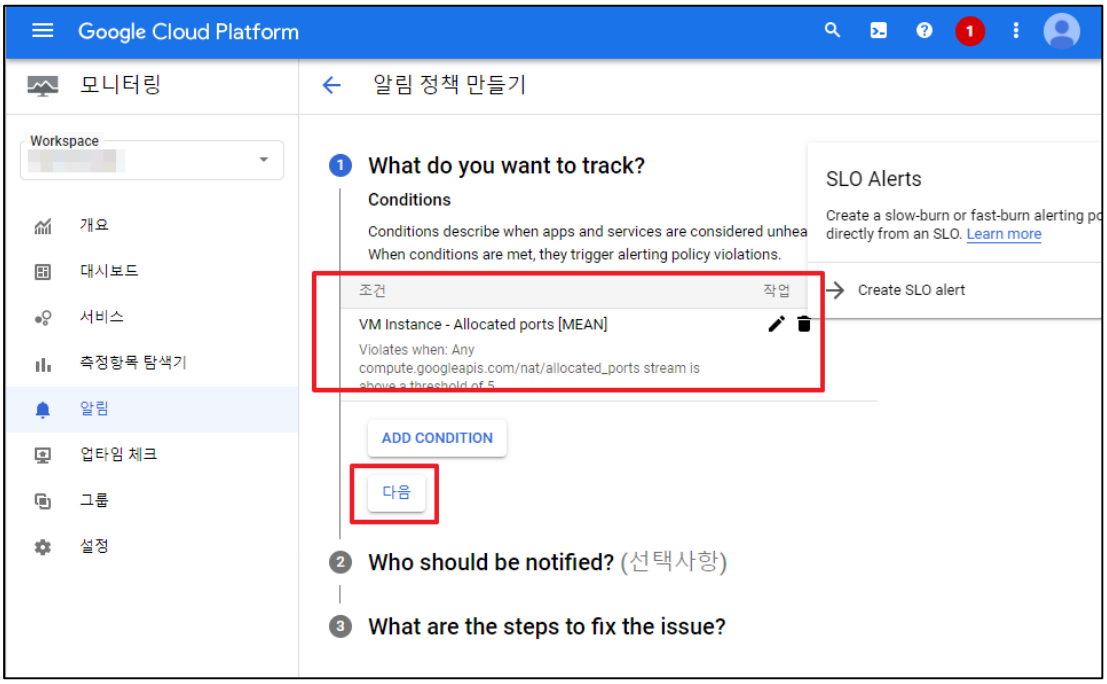
1) 모니터링 내 [알림] 페이지 접근 및 정책 생성 클릭



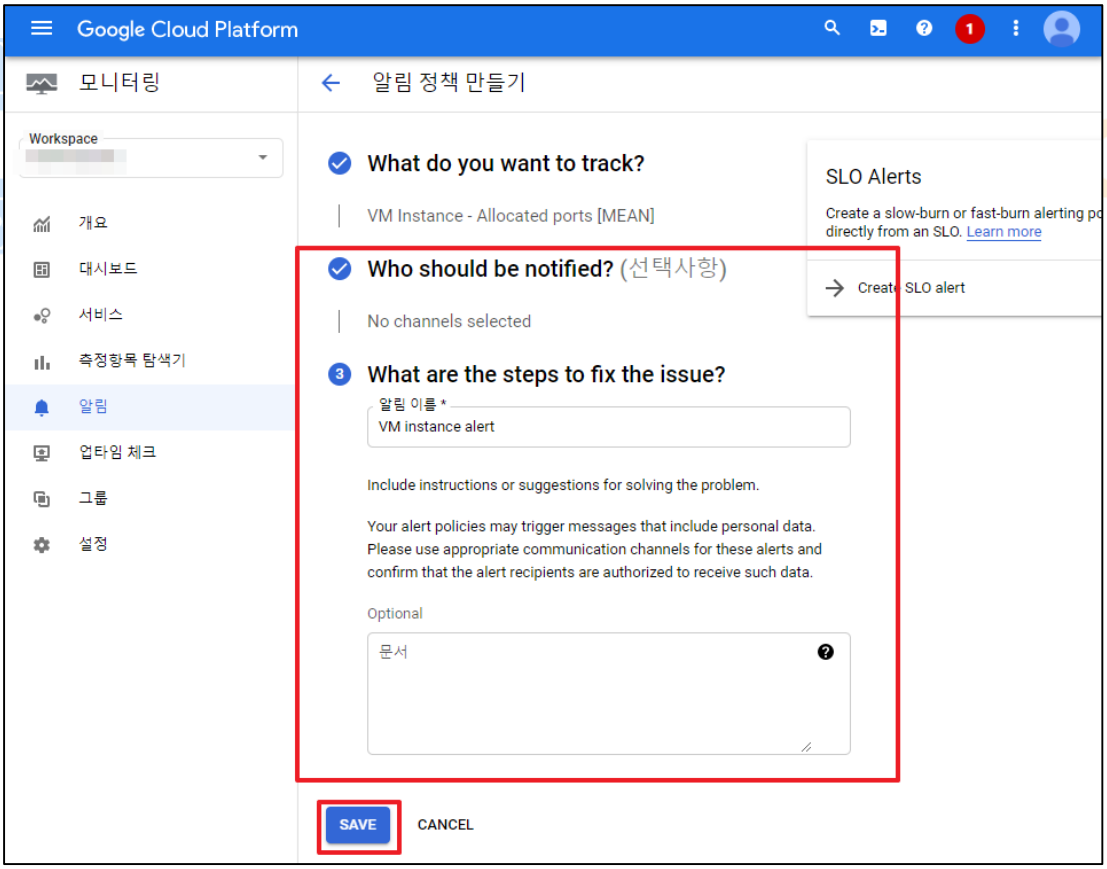
2) METRIC 설정 및 기타 세부 Condition 설정



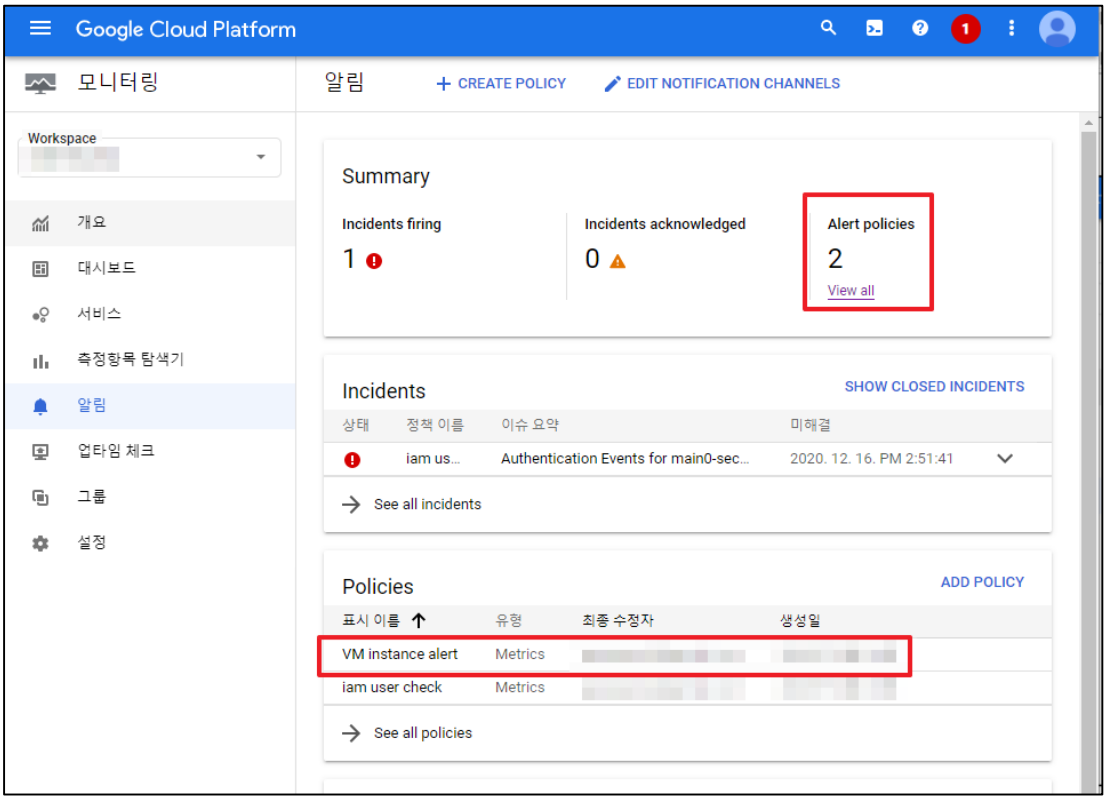
3) Policy 저장 확인 및 추가옵션 설정을 위한 [다음] 버튼 클릭



4) 추가 선택 옵션 정의 및 Policy 정책 저장



5) 설정한 Policy 정책 확인

	
진단 기준	**양호기준** : 사용중인 GCP 리소스에 대한 경보가 설정되어 있을 경우 **취약기준** : 사용중인 GCP 리소스에 대한 경보가 설정되어 있지 않을 경우
비고	

2021 클라우드 보안 가이드 -GCP

ADT캡스 | infosec

경기도 성남시 분당구 판교로 227번길 23

발행인 : ADT캡스 취약점진단팀