

2024 클라우드 보안 가이드

GCP



2024 클라우드 보안 가이드 발간사

안녕하십니까?SK실더스입니다.

지난 몇년간 SK실더스의 취약점진단팀은 “클라우드 보안 가이드 - AWS, Azure, GCP” 3종을 매년 개선하여 발간했습니다.

현재 Cloud 환경으로 전환하고 쿠버네티스 서비스를 사용하여 구축하고 있는 기업의 사례가 많아지고 있습니다.

이러한 트렌드를 분석하고 변화에 대응하고자 올해도 “2024 클라우드 보안 가이드 - AWS, Azure, GCP” 3종의 개정판을 발간하게 되었습니다.

이번 가이드는 퍼블릭 클라우드 서비스의 안전한 사용을 위해 클라우드 구성 요소들의 보안정책 점검방법과 쿠버네티스 서비스에 대한 계정 관리, 가상 리소스 관리, 운영 등 3가지 영역을 새롭게 추가하여 사용자가 변화하는 트렌드에 적응하고 대응할 수 있도록 기준과 모범 사례를 제시 하였습니다.

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

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

감사합니다.

취약점진단팀 팀장
김 상 춘

목 차

I. 전체 목록	4
1. 체크리스트 항목	4
2. GCP 보안 가이드/ISMS 매칭 기준 항목	6
3. 위험도 구분	10
II. 세부항목 설정	11
1. 계정 관리	11
1.1 사용자 계정 관리	11
1.2 Cloud ID 사용자 정책 관리	18
1.3 Cloud ID 사용자 패스워드 정책 관리	25
1.4 Identity Platform 사용자 관리	28
1.5 API 활성화 및 사용 주기 관리	31
1.6 SSH 키 사용 관리	35
1.7 메타데이터 관리	39
1.8 SQL 계정 관리	43
1.9 MFA (Multi-Factor Authentication) 설정	46
1.10 GKE 사용자 관리	51
1.11 GKE 서비스 어카운트 관리	55
1.12 GKE 불필요한 익명 접근 관리	56
2. 권한 관리	58
2.1 인스턴스 서비스 정책 관리	58
2.2 네트워크 서비스 정책 관리	79
2.3 기타 서비스 정책 관리	98
3. 가상 리소스 관리	126
3.1 ID 및 API 액세스	126
3.2 VM 인스턴스 관리 및 보안	131
3.3 애플리케이션 방화벽	136
3.4 네트워크 방화벽 인/아웃바운드 ANY 설정 관리	139
3.5 네트워크 방화벽 인/아웃바운드 불필요 정책 관리	141
3.6 VPC 네트워크 서브넷 관리	143
3.7 VPC 네트워크 서브넷 비공개 구글 액세스 설정	148
3.8 공유 VPC 관리	151
3.9 VPN 연결 관리	158
3.10 Storage 버킷 ACL 관리	169
3.11 Storage 제어 관리	174
3.12 Storage 리소스 퍼블릭 Access 관리	178
3.13 GKE Pod 보안 정책 관리	182
4. 운영 관리	185

4.1 Compute Engine 디스크 암호화 설정.....	185
4.2 Compute Engine 이미지 암호화 설정.....	193
4.3 SQL 암호화 설정.....	201
4.4 Storage 암호화 설정.....	208
4.5 Storage 데이터 보존 정책 관리.....	214
4.6 SQL SSL 정책 관리.....	218
4.7 Load Balancing SSL 정책 관리.....	222
4.8 App Engine SSL 정책 관리.....	231
4.9 통신 구간 암호화 설정.....	239
4.10 감사 로그 기록 및 관리.....	240
4.11 감사 로그 면제 사용자 존재 여부.....	243
4.12 VPC 네트워크 흐름 로그 설정 관리.....	245
4.13 방화벽 로그 관리.....	247
4.14 로그 보관 설정.....	250
4.15 Google 계정 사용자 이상징후 알림 설정.....	254
4.16 Cloud ID 계정 사용자 이상징후 알림 설정.....	257
4.17 가상 리소스 이상징후 알림 설정.....	261
4.18 백업 사용 여부.....	265
4.19 보안 GKE 노드 설정.....	266
4.20 애플리케이션 레이어 보안 비밀 암호화 설정.....	268
4.21 워크로드 아이덴티티 설정.....	271
4.22 워크로드 취약점 스캔 설정.....	273
4.23 GKE Cluster 로깅 설정.....	277
4.24 GKE Cluster 모니터링 설정.....	280
ETC. 부록.....	283
가. 인증 및 접근 관리.....	283
나. 파드 보안.....	285
다. 네트워크 보안.....	286
라. 이미지 보안.....	287

I. 전체 목록

1. 체크리스트 항목

진단에 사용될 체크리스트는 국내/외 기술 자료를 바탕으로 작성되었습니다. GCP 보안가이드에서의 영역은 계정 관리(12개 항목), 권한 관리(3개 항목), 가상 리소스 관리(13개 항목), 운영 관리(24개 항목)으로 총 4개 영역에서 52개 항목으로 구성하였습니다.

[표] 1. GCP 보안 진단 체크리스트

영역	항목 코드	항목명	중요도
계정 관리	1.1	사용자 계정 관리	상
	1.2	Cloud ID 계정 정책 관리	중
	1.3	Cloud ID 계정 패스워드 정책 관리	중
	1.4	Identity Platform 사용자 관리	중
	1.5	API 활성화 및 사용 주기 관리	중
	1.6	SSH 키 사용 관리	상
	1.7	메타데이터 관리	상
	1.8	SQL 계정 관리	상
	1.9	MFA (Multi-Factor Authentication) 설정	중
	1.10	GKE 사용자 관리	상
	1.11	GKE 서비스 어카운트 관리	중
	1.12	GKE 불필요한 익명 접근 관리	상
권한 관리	2.1	인스턴스 서비스 정책 관리	상
	2.2	네트워크 서비스 정책 관리	상
	2.3	기타 서비스 정책 관리	상
가상 리소스 관리	3.1	ID 및 API 액세스	상
	3.2	VM 인스턴스 관리 및 보안	하
	3.3	애플리케이션 방화벽	중
	3.4	네트워크 방화벽 인/아웃바운드 ANY 설정 관리	상
	3.5	네트워크 방화벽 인/아웃바운드 불필요 정책 관리	상
	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	Storage 버킷 ACL 관리	중
	3.11	Storage 제어 관리	중
	3.12	Storage 리소스 퍼블릭 Access 관리	상
	3.13	GKE Pod 보안 정책 관리	상
운영 관리	4.1	Compute Engine 디스크 암호화 설정	중
	4.2	Compute Engine 이미지 암호화 설정	중

4.3	SQL 암호화 설정	중
4.4	Storage 암호화 설정	중
4.5	Storage 데이터 보안 관리	중
4.6	SQL SSL 정책 관리	상
4.7	Load Balancing SSL 정책 관리	상
4.8	App Engine SSL 정책 관리	상
4.9	통신 구간 암호화 설정	중
4.10	감사 로그 기록 및 관리	중
4.11	감사 로그 면제 사용자 존재 여부	중
4.12	VPC 네트워크 흐름 로그 설정 관리	중
4.13	방화벽 로그 관리	중
4.14	로그 보관 설정	중
4.15	Google 계정 사용자 이상징후 알림 설정	중
4.16	Cloud ID 계정 사용자 이상징후 알림 설정	하
4.17	가상 리소스 이상징후 알림 설정	중
4.18	백업 사용 여부	중
4.19	보안 GKE 노드 설정	중
4.20	애플리케이션 레이어 보안 비밀 암호화 설정	중
4.21	워크로드 아이덴티티 설정	중
4.22	워크로드 취약점 스캔 설정	중
4.23	GKE Cluster 로깅 설정	중
4.24	GKE Cluster 모니터링 설정	중

안녕을 지키는 기술

2. GCP 보안 가이드/ISMS 매칭 기준 항목

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

[표] 2. GCP 보안가이드와 ISMS 항목 매칭

영역	항목 코드	항목명	ISMS 기준항목
계정 관리	1.1	사용자 계정 관리	2.2.1 주요 직무자 지정 및 관리 2.2.5 퇴직 및 직무변경 관리 2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리
	1.2	Cloud ID 사용자 정책 관리	2.1.3 정보자산 관리 2.5.1 사용자 계정 관리 2.5.2 사용자 식별
	1.3	Cloud ID 사용자 패스워드 정책 관리	2.5.4 비밀번호 관리
	1.4	Identity Platform 사용자 관리	2.6.2 정보시스템 접근 2.6.6 원격접근 통제
	1.5	API 활성화 및 사용 주기 관리	2.5.4 비밀번호 관리 2.5.5 특수 계정 및 권한 관리 2.7.2 암호키 관리
	1.6	SSH 키 사용 관리	2.6.2 정보시스템 접근 2.6.6 원격접근 통제
	1.7	메타데이터 관리	2.1.3 정보자산 관리 2.7.2 암호키 관리
	1.8	SQL 계정 관리	2.5.4 비밀번호 관리 2.5.5 특수 계정 및 권한 관리
	1.9	MFA (Multi-Factor Authentication) 설정	2.5.3 사용자 인증 2.5.4 비밀번호 관리 2.6.2 정보시스템 접근 2.6.6 원격접근 통제
	1.10	GKE 사용자 관리	2.2.1 주요 직무자 지정 및 관리 2.2.5 퇴직 및 직무변경 관리 2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리
	1.11	GKE 서비스 어카운트 관리	2.5.1 사용자 계정 관리
	1.12	GKE 불필요한 익명 접근 관리	2.5.1 사용자 계정 관리

권한 관리	2.1	인스턴스 서비스 정책 관리	2.2.1 주요 직무자 지정 및 관리 2.2.2 직무 분리 2.2.5 퇴직 및 직무변경 관리 2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리 2.5.5 특수 계정 및 권한 관리 2.6.2 정보시스템 접근
	2.2	네트워크 서비스 정책 관리	2.2.1 주요 직무자 지정 및 관리 2.2.2 직무 분리 2.2.5 퇴직 및 직무변경 관리 2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리 2.5.5 특수 계정 및 권한 관리 2.6.2 정보시스템 접근
	2.3	기타 서비스 정책 관리	2.2.1 주요 직무자 지정 및 관리 2.2.2 직무 분리 2.2.5 퇴직 및 직무변경 관리 2.3.3 외부자 보안 이행 관리 2.5.1 사용자 계정 관리 2.5.5 특수 계정 및 권한 관리 2.6.2 정보시스템 접근 2.6.3 응용프로그램 접근 2.8.5 소스 프로그램 관리
가상 리소스 관리	3.1	ID 및 API 액세스	2.6.2 정보시스템 접근 2.6.7 인터넷 접속 통제 2.10.3 공개서버 보안
	3.2	VM 인스턴스 관리 및 보안	2.10.2 클라우드 보안
	3.3	애플리케이션 방화벽	2.6.1 네트워크 접근 2.6.6 원격접근 통제 2.6.7 인터넷 접속 통제
	3.4	네트워크 방화벽 인/아웃바운드 ANY 설정 관리	2.6.1 네트워크 접근 2.6.6 원격접근 통제 2.6.7 인터넷 접속 통제
	3.5	네트워크 방화벽 인/아웃바운드 불필요 정책 관리	2.6.1 네트워크 접근 2.6.6 원격접근 통제 2.6.7 인터넷 접속 통제
	3.6	VPC 네트워크 서브넷 관리	2.6.1 네트워크 접근 2.6.7 인터넷 접속 통제
	3.7	VPC 네트워크 서브넷 비공개 구글 액세스 설정	2.6.7 인터넷 접속 통제

	3.8	공유 VPC 관리	2.6.1 네트워크 접근
	3.9	VPN 연결 관리	2.6.1 네트워크 접근 2.6.7 인터넷 접속 통제
	3.10	Storage 버킷 ACL 관리	2.6.1 네트워크 접근 2.6.2 정보시스템 접근
	3.11	Storage 제어 관리	2.6.2 정보시스템 접근 2.6.6 원격접근 통제 2.6.7 인터넷 접속 통제 2.10.3 공개서버 보안
	3.12	Storage 리소스 퍼블릭 Access 관리	2.6.1 네트워크 접근 2.6.2 정보시스템 접근 2.6.6 원격접근 통제 2.6.7 인터넷 접속 통제 2.10.3 공개서버 보안
	3.13	GKE Pod 보안 정책 관리	2.6.3 응용프로그램 접근
운영 관리	4.1	Compute Engine 디스크 암호화 설정	2.7.1 암호정책 적용 2.7.2 암호키 관리
	4.2	Compute Engine 이미지 암호화 설정	2.7.1 암호정책 적용 2.7.2 암호키 관리
	4.3	SQL 암호화 설정	2.7.1 암호정책 적용 2.7.2 암호키 관리
	4.4	Storage 암호화 설정	2.7.1 암호정책 적용 2.7.2 암호키 관리
	4.5	Storage 데이터 보안 관리	2.6.4 데이터베이스 접근
	4.6	SQL SSL 정책 관리	2.7.1 암호정책 적용 2.10.5 정보전송 보안
	4.7	Load Balancing SSL 정책 관리	2.7.1 암호정책 적용 2.10.5 정보전송 보안
	4.8	App Engine SSL 정책 관리	2.7.1 암호정책 적용 2.10.5 정보전송 보안
	4.9	통신 구간 암호화 설정	2.7.1 암호정책 적용 2.10.5 정보전송 보안
	4.10	감사 로그 기록 및 관리	2.9.1 변경관리 2.9.2 성능 및 장애관리 2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검
	4.11	감사 로그 면제 사용자 존재 여부	2.5.6 접근권한 검토 2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검

	4.12	VPC 네트워크 흐름 로그 설정 관리	2.9.1 변경관리 2.9.2 성능 및 장애관리 2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검
	4.13	방화벽 로그 관리	2.9.1 변경관리 2.9.2 성능 및 장애관리 2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검
	4.14	로그 보관 설정	2.9.4 로그 및 접속기록 관리
	4.15	Google 계정 사용자 이상징후 알림 설정	2.11.3 이상행위 분석 및 모니터링
	4.16	Cloud ID 계정 사용자 이상징후 알림 설정	2.11.3 이상행위 분석 및 모니터링
	4.17	가상 리소스 이상징후 알림 설정	2.9.2 성능 및 장애관리 2.11.3 이상행위 분석 및 모니터링
	4.18	백업 사용 여부	2.9.2 성능 및 장애관리 2.9.3 백업 및 복구 관리 2.12.2 재해 복구 시험 및 개선
	4.19	보안 GKE 노드 설정	2.6.2 정보시스템 접근
	4.20	애플리케이션 레이어 보안 비밀 암호화 설정	2.7.1 암호정책 적용 2.7.2 암호키 관리
	4.21	워크로드 아이덴티티 설정	2.6.2 정보시스템 접근
	4.22	워크로드 취약점 스캔 설정	2.11.2 취약점 점검 및 조치
	4.23	GKE Cluster 로깅 설정	2.9.1 변경관리 2.9.2 성능 및 장애관리 2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검 2.11.3 이상행위 분석 및 모니터링
	4.24	GKE Cluster 모니터링 설정	2.9.2 성능 및 장애관리 2.11.3 이상행위 분석 및 모니터링

3. 위험도 구분

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

[표] 3. 위험도 구분

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



안녕을 지키는 기술

II. 세부항목 설정

1. 계정 관리

1.1 사용자 계정 관리

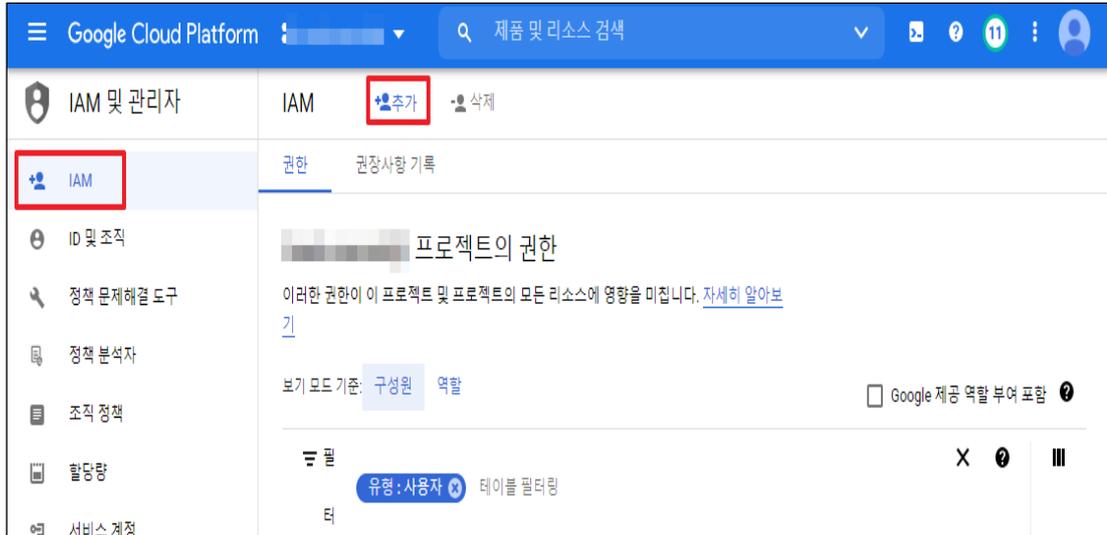
분류	계정 관리	중요도	상					
항목명	사용자 계정 관리							
항목 설명	<p>GCP(Google Cloud Platform)에서는 크게 구글 계정, 서비스 계정, Cloud ID의 3가지 형태의 계정을 사용하며 상세 내용은 다음과 같습니다.</p> <p>구글 계정은 구글의 온라인 서비스에 접근 인증과 허가를 제공하는 사용자 계정으로서 그중 GCP(Google Cloud Platform) 서비스 및 기타 구글 제품 이용이 가능합니다.</p> <p>서비스 계정은 개별 최종 사용자가 아닌 애플리케이션 또는 가상 머신에 속한 특별한 Google 계정입니다. 애플리케이션은 서비스 계정을 사용하여 서비스의 Google API를 호출하므로 사용자가 직접 관여하지 않습니다. 예를 들어, 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.</p> <p>Cloud ID는 Google에서 제공하는 IDaaS(Identity as a Service) 및 엔터프라이즈 모바일 관리(EMM) 제품으로 Google Workspace에서 사용이 가능하며 ID 서비스 및 엔드포인트 관리 기능을 제공합니다. 관리자는 Cloud ID를 사용하여 Google 관리 콘솔에서 사용자, 앱, 기기를 관리할 수 있으며, GCP(Google Cloud Platform) 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.</p>							
	<p>※ GCP 계정 유형</p> <table border="1"> <thead> <tr> <th>계정 유형</th> <th>상세내용</th> </tr> </thead> <tbody> <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> </tr> <tr> <td>사용자 관리 서비스 계정</td> <td>GCP 내에서 IAM 을 사용하여 자체적으로 생성할 수 있는 계정으로 생성 후 계정에 대한 IAM 역할을 부여하고, 서비스 계정으로 실행되도록 설정할 수 있습니다.</td> </tr> </tbody> </table>			계정 유형	상세내용	Google 관리 서비스 계정	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.	사용자 관리 서비스 계정
계정 유형	상세내용							
Google 관리 서비스 계정	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.							
사용자 관리 서비스 계정	GCP 내에서 IAM 을 사용하여 자체적으로 생성할 수 있는 계정으로 생성 후 계정에 대한 IAM 역할을 부여하고, 서비스 계정으로 실행되도록 설정할 수 있습니다.							

Cloud ID

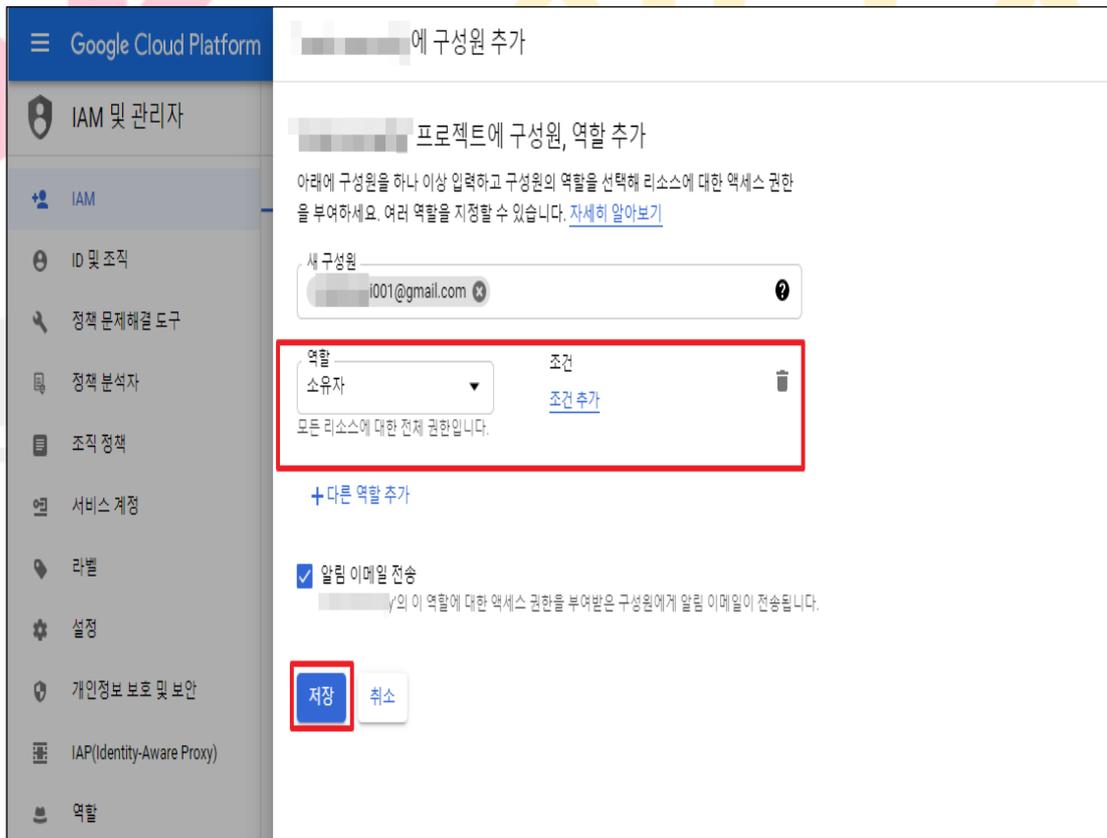
IDaaS(Identity as a Service) 및 엔터프라이즈 모바일 관리 서비스로 Google Workspace 에서 사용할 수 있는 독립형 ID 서비스 및 엔드포인트를 관리할 수 있는 서비스입니다.

가. IAM 내 사용자 추가

1) IAM 사용자 추가 버튼 클릭



2) Google 계정 사용자 추가 (역할 부여: 소유자)



설정
방법

3) 신규 사용자 추가 및 Google 계정에 최고 권한(소유자) 부여 확인

The screenshot shows the Google Cloud Platform IAM console. The left sidebar contains navigation options like 'IAM 및 관리자', 'IAM', 'ID 및 조직', etc. The main area is titled 'IAM' and shows '권한' (Permissions) for a project. A table lists roles assigned to users. One row is highlighted with a red box, showing a user with the role '소유자' (Owner) and a warning icon.

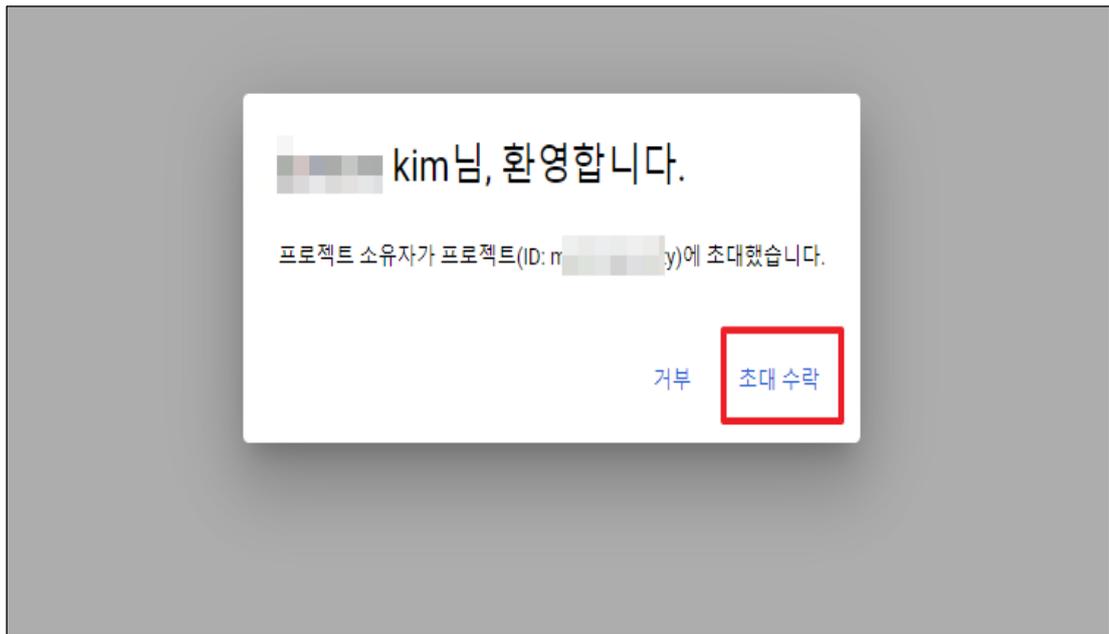
유형	구성원	이름	역할	분석된 권한 (조과/합계)
유형: 사용자			테이블 필터링	
□		001@gmail.com	소유자 ⚠	
□			Cloud SQL 관리자	32/
□			네트워크 관리 관리자	13/
			소유자	3409/36
□			Cloud SQL 관리자	8/
□			네트워크 관리 관리자	13/
			소유자	3366/36

4) Google 계정 사용자 최고 권한(소유자) 획득을 위한 이메일 인증

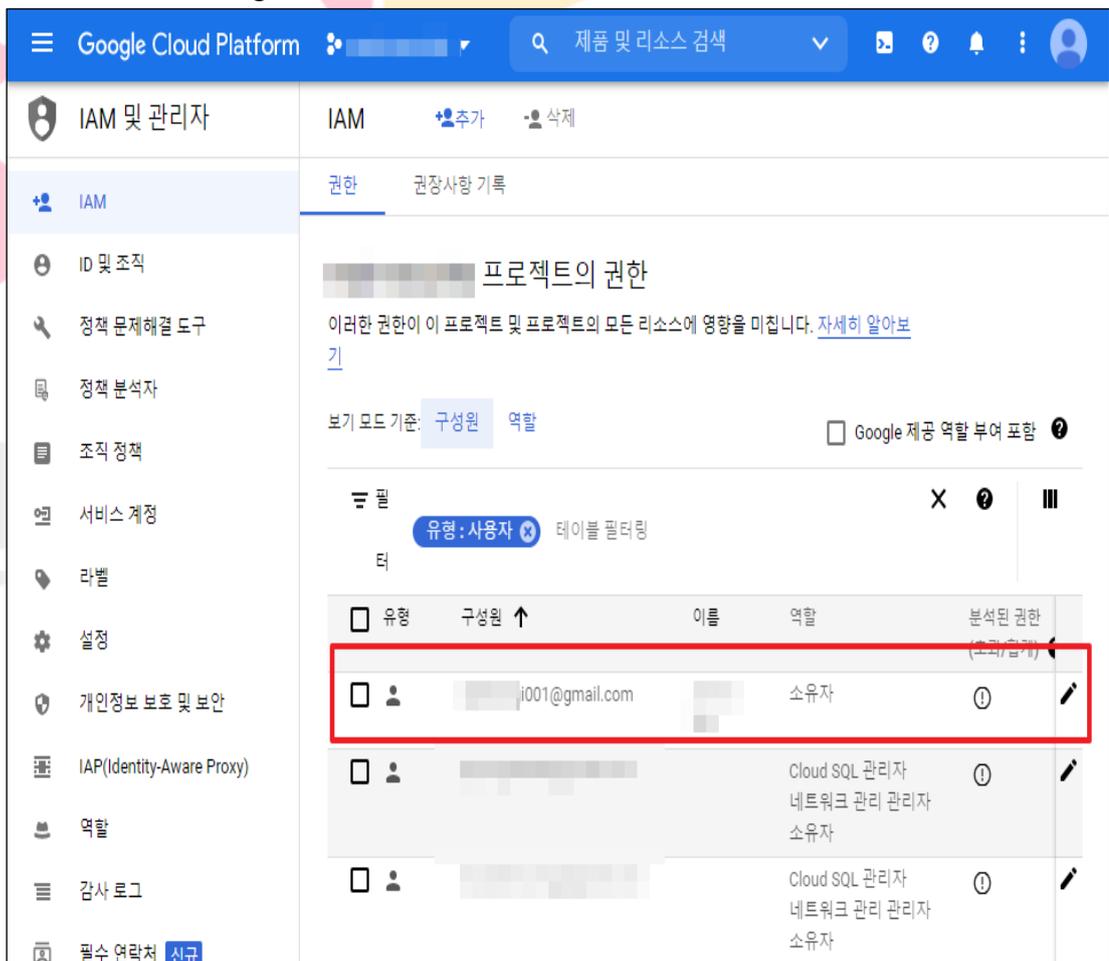
The screenshot shows a Gmail inbox with an email titled 'Google Developers Console 프로젝트 초대' (Google Developers Console Project Invitation). The email is from 'noreply-cloud@google.com' and is dated '오전 10:58 (0분 전)'. The body of the email contains an invitation link for a Google Cloud Platform project, which is highlighted with a red box.

https://console.cloud.google.com/invitation?nrriect=main0-security&account=01@gmail.com&memberEmail=j001@gmail.com

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



6) 추가된 신규 Google 계정 사용자 최종 권한 여부 확인



나. Cloud ID 설정 방법

1) GCP 콘솔에서 Cloud 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 jsmith입니다. 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 GCP(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 사용자만으로 제한할 수 있습니다.

GCP(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 GCP(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	<p>양호기준 : 관리자 권한을 보유한 다수 계정이 존재하지 않고 불필요한 계정이 존재하지 않을 경우</p> <p>취약기준 : 관리자 권한을 보유한 다수 계정과 불필요한 계정이 존재하는 경우</p>
비고	-



안녕을 지키는 기술

1.2 Cloud ID 사용자 정책 관리

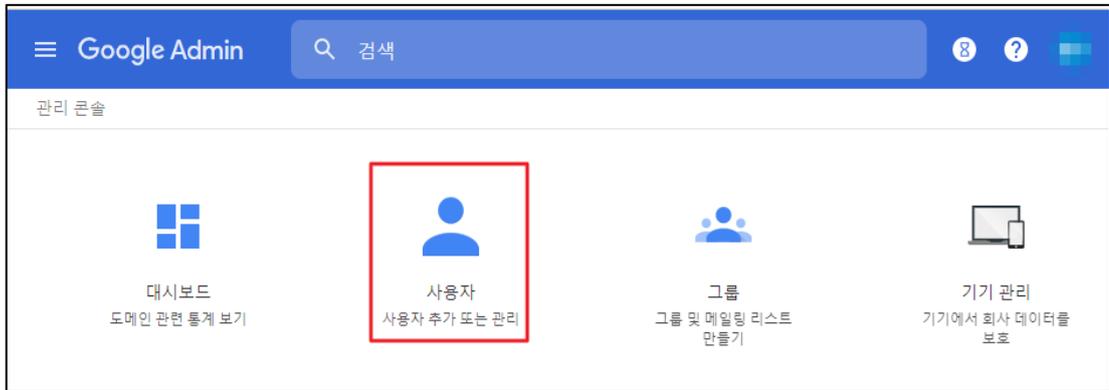
분류	계정 관리	중요도	중			
항목명	Cloud ID 사용자 정책 관리					
항목 설명	<p>Google Workspace를 통해 Cloud ID 사용자에게 관리(Admin) 콘솔에 대해 완전한 최고 사용자 액세스 권한을 부여하는 대신 제한된 작업만 수행하는 관리자 역할을 할당할 수 있으며 사용자에게 대한 직무 및 역할에 맞는 사용자 권한이 설정되어야 합니다. 또한, 권한 오남용이 발생하지 않도록 직무를 수행하는 임직원에게 대한 목록을 최신으로 관리해야 합니다.</p> <p>예를 들어 관리자가 A사용자에게 Gmail 설정 또는 헬프 데스크 작업 (예: 사용자 비밀번호 재설정)만 관리하도록 허용하길 원할 경우 기본으로 제공되는 관리자 역할을 할당하거나 직접 맞춤 역할 등을 활용해 서비스를 이용 해야합니다.</p>					
	<p>※ Google Workspace 사용자 기본 역할</p> <table border="1" data-bbox="304 862 1414 1827"> <thead> <tr> <th data-bbox="304 862 459 907">역할명</th> <th data-bbox="459 862 1414 907">상세내용</th> </tr> </thead> <tbody> <tr> <td data-bbox="304 907 459 1827">최고 관리자</td> <td data-bbox="459 907 1414 1827"> <p>관리 콘솔 및 Admin API의 모든 기능에 액세스할 수 있고 조직 계정을 모든 측면에서 관리할 수 있습니다.</p> <p>또한 최고 관리자는 모든 사용자의 캘린더 및 캘린더 일정 세부 정보에 대한 전체 액세스 권한을 보유하고 있습니다. 최고 관리자 권한을 부여 받은 사용자가 캘린더 권한을 사용할 수 있게 되려면 최대 24시간이 걸릴 수 있습니다.</p> <ul style="list-style-type: none"> - 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> </tbody> </table>			역할명	상세내용	최고 관리자
역할명	상세내용					
최고 관리자	<p>관리 콘솔 및 Admin API의 모든 기능에 액세스할 수 있고 조직 계정을 모든 측면에서 관리할 수 있습니다.</p> <p>또한 최고 관리자는 모든 사용자의 캘린더 및 캘린더 일정 세부 정보에 대한 전체 액세스 권한을 보유하고 있습니다. 최고 관리자 권한을 부여 받은 사용자가 캘린더 권한을 사용할 수 있게 되려면 최대 24시간이 걸릴 수 있습니다.</p> <ul style="list-style-type: none"> - 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 					

<p>그룹스 관리자</p>	<p>관리 콘솔에서 생성한 Google 그룹스에 대해 모든 권한을 보유하고 있습니다. 이 관리자는 관리 콘솔 및 Admin API 를 통해 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> - 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)
<p>사용자 관리 관리자</p>	<p>관리자가 아닌 사용자에게 모든 작업을 수행할 수 있습니다. 이 관리자는 관리 콘솔 및 Admin API 를 통해 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> - 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 <p>(* 관리자가 아닌 사용자에게만 해당됩니다. 이 관리자는 관리자 권한을 할당하거나 관리자 비밀번호를 재설정할 수 없으며 관리자 계정의 기타 설정도 변경할 수 없습니다. 최고 관리자만 작업 수행이 가능합니다.</p>
<p>헬프 데스크 관리자</p>	<p>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.</p> <p>사용자를 헬프 데스크 관리자 역할에 지정할 때 해당 사용자의 권한을 특정 조직 단위로 제한할 수 있습니다.</p>
<p>서비스 관리자</p>	<p>캘린더, 드라이브, 문서, 기타 서비스를 비롯하여 관리 콘솔에 추가된 특정 서비스 설정 및 기기를 관리할 수 있습니다. 이 관리자는 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> - 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)

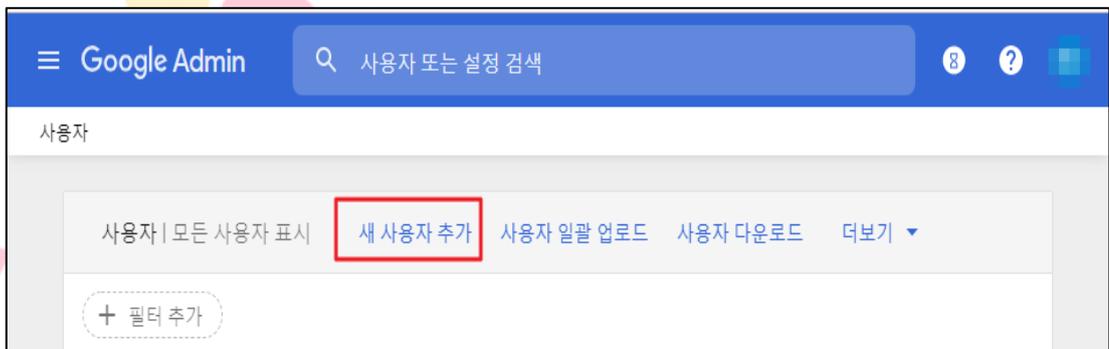
	<p>(*) 계정에 추가한 특정 제품(G Suite 서비스, 내 지도 프로 등), Marketplace 앱, 무료 Google 서비스(예: Google+ 및 Blogger)에만 적용됩니다. Google Vault, 클라우드 프린트 등 일부 제품 및 서비스에서는 서비스 관리자 역할을 지원하지 않습니다.</p>
<p>모바일 관리자</p>	<p>고급 휴대기기 관리를 통해 휴대기기를 관리할 수 있습니다. 이 관리자는 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> - 기기 프로비저닝 및 승인 - 앱 허용 - 기기 및 계정 차단 또는 초기화 - Android 기기 및 iOS 기기 정책 설정 - 도메인의 그룹 및 사용자 보기
<p>Google Voice 관리자</p>	<p>Voice 라이선스 할당을 제외한 모든 Google Voice 설정 및 프로비저닝을 관리할 수 있습니다. 이 관리자는 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> - 위치 추가 - 사용자에게 전화번호 할당 - 번호 이전 - 서비스 주소 변경 - 유선 전화 설정 - 자동 교환 설정
<p>리셀러 관리자</p>	<p>Google Workspace 공인 리셀러 및 Google Workspace 공인 유통업체와 협력하는 리셀러에게만 적용됩니다.</p>
<p>저장용량 관리자</p>	<p>관리 콘솔의 저장용량 페이지를 사용할 수 있습니다. 이 관리자는 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> - 조직의 저장용량 사용량 보기 - 가장 많은 저장용량을 사용 중인 사용자와 공유 드라이브 확인 - 저장용량 한도 설정 - 계정 보고서, 사용자 디렉터리, 공유 드라이브 목록 열기 <p>이 역할은 보고서 및 Drive 설정에 대한 전체 액세스 권한도 부여합니다.</p>

가. Cloud ID 사용자 역할 및 정보 작성

1) [Google Admin] > [관리콘솔] > [사용자]

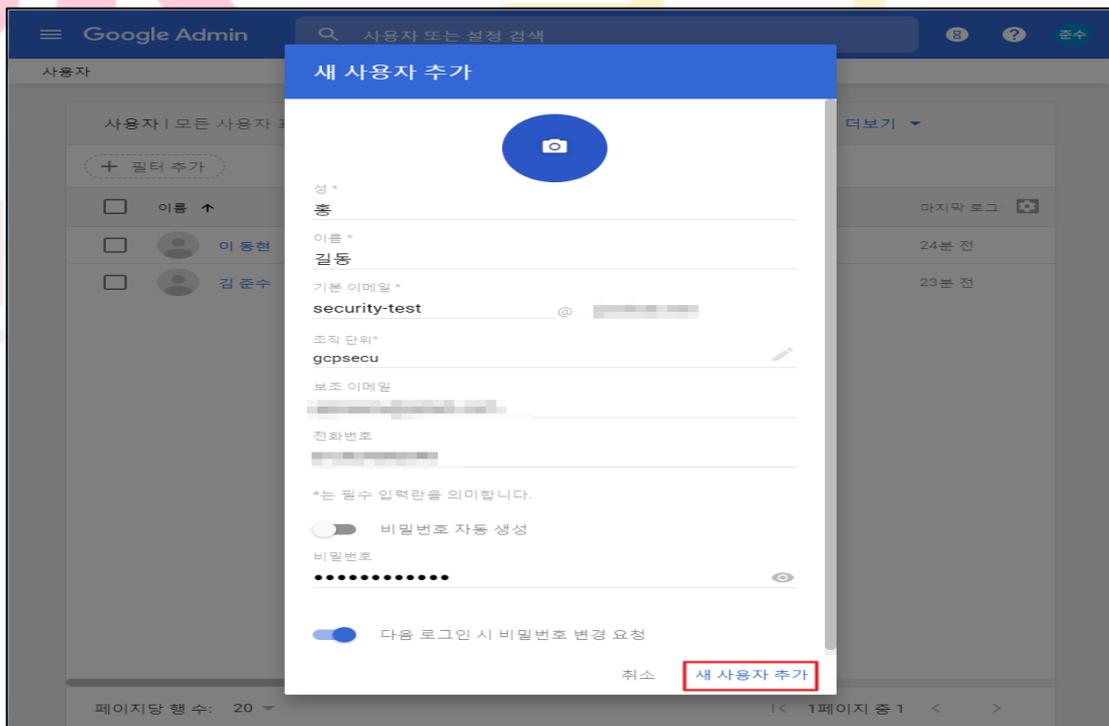


2) [사용자] > [새 사용자 추가]



설정
방법

3) 사용자 관련 정보 입력



4) 사용자 생성 및 추가 확인

Google Admin | 사용자 또는 설정 검색

사용자

사용자 | 모든 사용자 표시 | 새 사용자 추가 | 사용자 일괄 업로드 | 사용자 다운로드 | 더보기 ▾

+ 필터 추가

<input type="checkbox"/>	이름 ↑	이메일	상태	마지막 로그인
<input type="checkbox"/>	홍길동	security-test@... [redacted]	활성화(최근 추가됨)	로그인하지 않음
<input type="checkbox"/>	[redacted]	[redacted]	활성	28분 전
<input type="checkbox"/>	[redacted]	[redacted]	활성	27분 전

5) 관리자 역할 및 권한 지정

Google Admin | 사용자 또는 설정 검색

사용자 > 홍길동

홍길동
security-test@...
[redacted]

활성
마지막 로그인: 로그인하지 않음
생성된 날짜: 2019. 7. 16.

조직 단위
gcpsecu

비밀번호 재설정

사용자 이름 바꾸기

더보기

관리자 역할 및 권한

길동님에게 관리자 역할 및 권한이 없습니다.

역할 지정

앱

Google 앱	기타 클라우드 앱
사용 가능한 Google 서비스 51개 중 48개가 길동님에게 사용 설정되어 있습니다. 앱 사용/사용 중지	이 조직에 추가된 다른 클라우드 앱이 없습니다. 앱 검색 앱 사용/사용 중지

관리 기기

6) 역할 설정 후 저장

홍길동 > 관리자 역할 및 권한

홍길동
security-test@...
활성
마지막 로그인: 로그인하지 않음
생성된 날짜: 2019. 7. 16.

조직 단위
gcpsecu

- 비밀번호 재설정
- 사용자 이름 바꾸기
- 더보기

관리자 역할 및 권한

역할
길동님의 관리자 역할을 관리합니다. 기본 제공 역할을 할당하거나 특정한 권한이 부여된 맞춤 역할을 생성합니다.

역할 0개가 할당됨 [맞춤 역할 만들기](#)

역할 이름	역할 범위	할당 상태 ↑
최고 관리자 Google Apps Administrator Seed Role	모든 조직 단위	<input checked="" type="checkbox"/> 할당됨
헬프 데스크 관리자 Help Desk Administrator	-	<input type="checkbox"/> 할당되지 않음
서비스 관리자 Services Administrator	-	<input type="checkbox"/> 할당되지 않음
그룹스 관리자 Groups Administrator	-	<input type="checkbox"/> 할당되지 않음
사용자 관리 User Management Administrator	-	<input type="checkbox"/> 할당되지 않음

저장되지 않은 변경사항 1개 [취소](#) [저장](#)

홍길동 > 관리자 역할 및 권한

관리자

홍길동
security-test@...
활성
마지막 로그인: 로그인하지 않음
생성된 날짜: 2019. 7. 16.

조직 단위
gcpsecu

- 비밀번호 재설정
- 사용자 이름 바꾸기
- 더보기

관리자 역할 및 권한

역할
길동님의 관리자 역할을 관리합니다. 기본 제공 역할을 할당하거나 특정한 권한이 부여된 맞춤 역할을 생성합니다.

역할 1개가 할당됨

역할 이름	역할 범위	할당 상태 ↑
최고 관리자 Google Apps Administrator Seed Role	모든 조직 단위	할당됨
헬프 데스크 관리자 Help Desk Administrator	-	할당되지 않음
서비스 관리자 Services Administrator	-	할당되지 않음
그룹스 관리자 Groups Administrator	-	할당되지 않음
사용자 관리 User Management Administrator	-	할당되지 않음

7) 사용자 정보 확인

The screenshot shows the Admin console interface. On the left is a navigation menu with options like '홈', '대시보드', '디렉터리', '사용자', '그룹', etc. The main content area shows the profile of a user named '홍길동' (Hong Gildong) with ID 'security-tes...'. The '사용자 정보' (User Information) section is highlighted with a red border and contains the following details:

- 사용자 세부정보**
- 연락처 정보**:
 - 이메일 (직장): security@sk.com
 - 전화 (직장): 010-1234-1234
 - 주소 (직장): 경기도 성남시
- 보조 이메일 주소(이메일 별칭)**: 보조 이메일, 보조 이메일 추가
- 직원 정보**:
 - 직원 ID: A1...
 - 직책: 선임
 - 직원 유형: 정규직
 - 관리자 이메일: security...
 - 부서: 취약점진단팀

진단
기준

양호기준

: Cloud ID 사용자 정보(연락처 및 직원 정보 등)가 설정되어 있을 경우

취약기준

: Cloud ID 사용자 정보(연락처 및 직원 정보 등)가 설정되어 있지 않을 경우

비고

-

안녕을 지키는 기술

1.3 Cloud ID 사용자 패스워드 정책 관리

분류	계정 관리	중요도	중
항목명	Cloud ID 사용자 패스워드 정책 관리		
항목 설명	<p>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.</p>		
	<p><패스워드 설정 기준></p> <p>1) 패스워드는 아래의 4가지 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성</p> <p>* 영문 대문자(26개), 영문 소문자(26개), 숫자(10개), 특수문자(32개)</p>		
	<p><패스워드는 비인가자에 의한 추측이 어렵도록 다음의 사항을 반영하여 설계해야 함></p> <p>1) Null 패스워드 사용 금지</p> <p>2) 문자 또는 숫자만으로 구성 금지</p> <p>3) 사용자 ID와 동일한 패스워드 금지</p> <p>4) 연속적인 문자 및 숫자 사용 금지</p> <p>5) 주기성 패스워드 사용 금지</p> <p>6) 전화번호, 생일, 계정명, hostname과 같이 추측하기 쉬운 패스워드 사용 금지</p>		
	<p>1) 패스워드 최소길이</p> <p>패스워드 추측 공격을 피하기 위하여 패스워드 최소 길이가 설정되어 있는지 점검함 패스워드 최소 길이가 설정되어 있지 않거나 짧게 설정되어 있을 경우 취약한 패스워드를 사용함으로써 인해 악의적인 사용자가 패스워드를 쉽게 유추 할 수 있음</p> <p>2) 패스워드 최대 사용기간</p> <p>패스워드가 임의의 경로를 통해 유출되었을 때, 임의로 접속한 사용자가 언제든지 다시 접속할 수 있는 환경을 방지하기 위해 패스워드 날짜 제한을 점검함</p> <p>3) 패스워드 최소 사용기간</p> <p>패스워드가 임의의 경로를 통해 유출되었을 때, 임의로 접속한 사용자가 언제든지 다시 접속할 수 있는 환경을 방지하기 위해 패스워드 날짜 제한을 점검함</p> <p>4) 이전 패스워드 기억</p> <p>이전에 사용하였던 패스워드를 기억하여 패스워드 변경 시 기존에 사용하였던 패스워드 재사용 금지</p> <p>- 패스워드 길이는 8자 이상 설정하는 것을 권고</p>		

- 패스워드 최대 사용 기간을 60일 이하로 설정할 것을 권고
- 패스워드 최소 사용 기간을 1일 이상으로 설정할 것을 권고

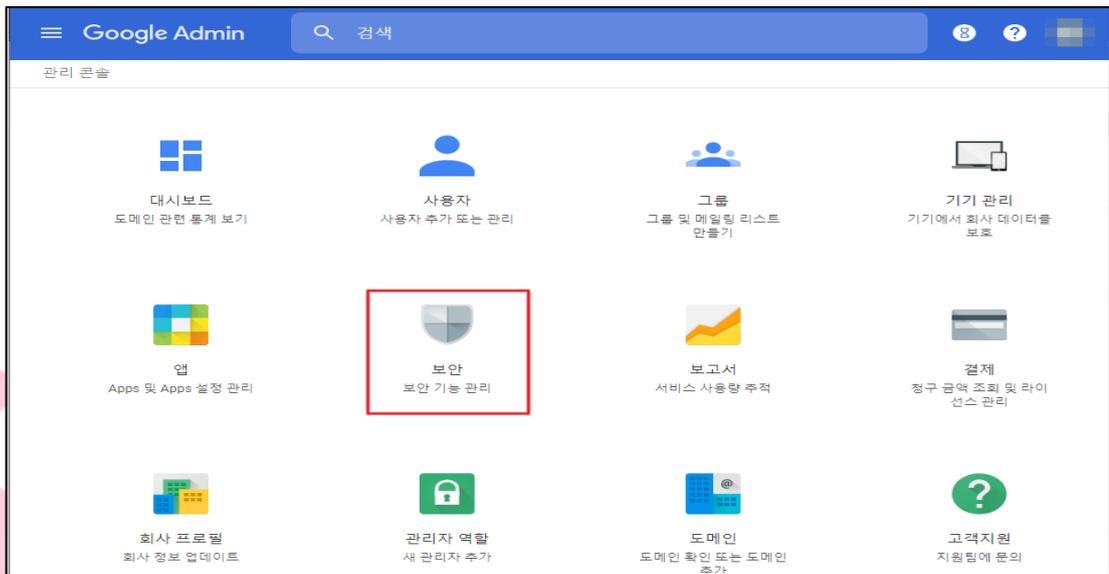
5) 암호 만료 활성화 및 재사용 제한

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

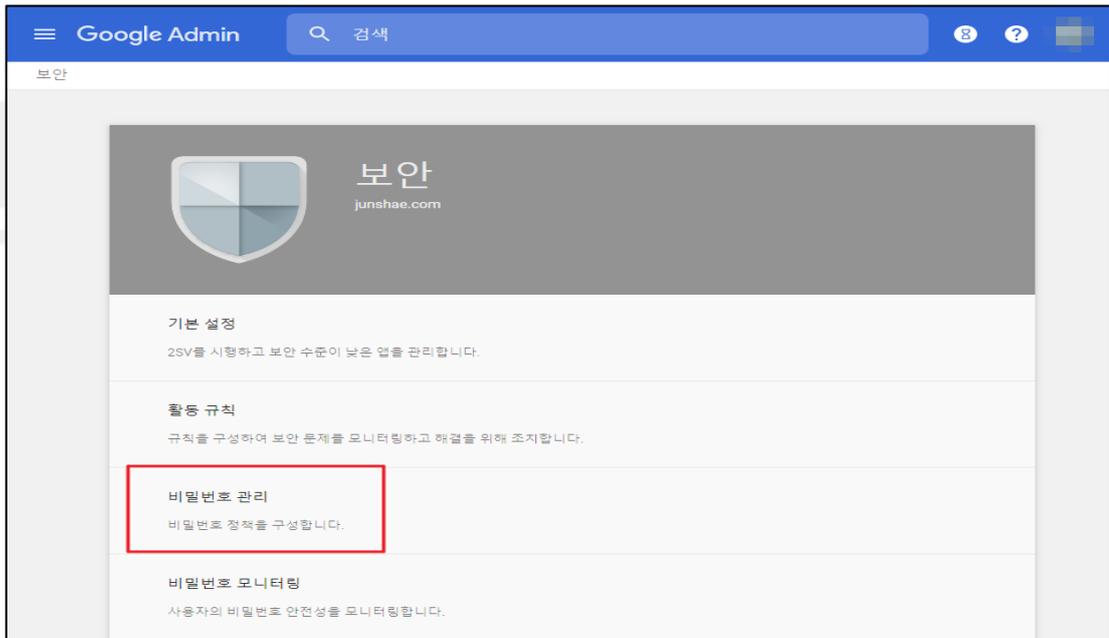
가. G Suite 계정의 패스워드 복잡도 및 만료 기간 설정

1) [관리 콘솔] > [보안]

- G Suite 계정 패스워드 정책 설정 시도



2) [비밀번호 관리]



설정
방법

3) 패스워드 강도 및 만료 기간 설정

보안 설정

조직 단위

조직 단위 검색

▼ [선택된 조직]

비밀번호 관리

비밀번호 관리
로컬 단위로 적용됨

조직에서 사용할 비밀번호 정책 구성

이러한 정책은 사용자가 타사 ID 공급업체로부터 인증된 상황과 같이 경우에 따라 적용되지 않습니다. 자세히 알아보기

강도
사용자는 강력한 암호를 사용해야 합니다. 자세히 알아보기

안전한 비밀번호 적용

비밀번호 길이
8~100자(영문 기준)여야 합니다.

최소 길이	-	최대 길이
8		100

비밀번호 안전성 및 길이 정책 시행
영향을 받는 사용자가 다음번에 비밀번호를 변경할 때 길이 및 안전성 요구사항에 관한 변경사항이 적용됩니다. 변경사항을 즉시 적용하려면 사용자가 다음번에 로그인할 때 시행되도록 설정하세요.

다음 로그인 시 비밀번호 정책 시행

재사용

비밀번호 재사용 허용

만료
비밀번호 재설정 빈도

60일 ▼

진단 기준

양호기준

: Cloud ID 계정의 패스워드 복잡성 기준 준수 및 암호 만료/재사용 제한 설정이 존재하는 경우

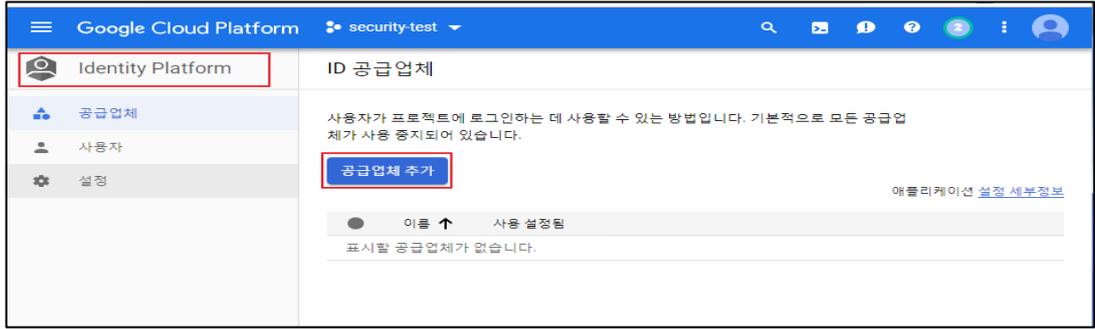
취약기준

: Cloud ID 계정의 패스워드 복잡성 기준 준수 및 암호 만료/재사용 제한 설정이 존재하지 않는 경우

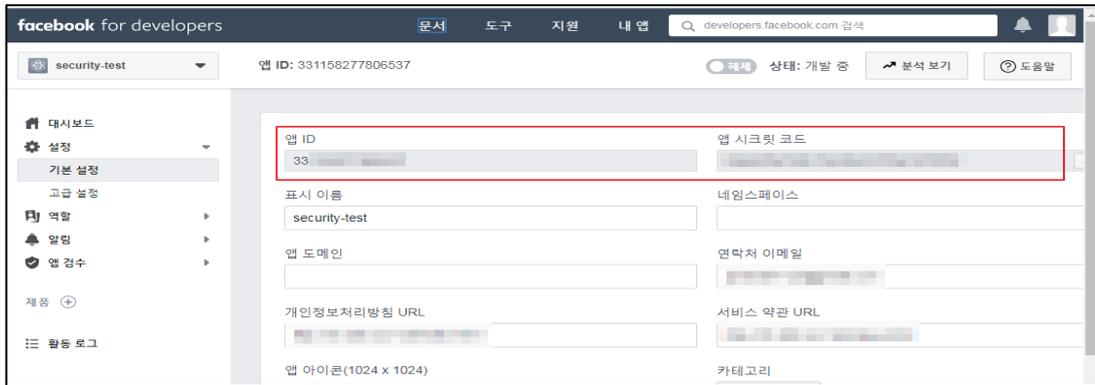
비고

1.4 Identity Platform 사용자 관리

분류	계정 관리	중요도	중												
항목명	Identity Platform 사용자 관리														
항목 설명	<p>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 GCP(Google Cloud Platform), 자체 백엔드 또는 다른 플랫폼에서 서비스를 작성하는 경우 안전하고 사용하기 쉬운 인증을 제공합니다.</p> <p>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 통합 ID 공급자를 사용하여 인증을 지원합니다.</p> <p>※ SDK를 사용한 인증</p> <table border="1"> <thead> <tr> <th>인증 구분</th> <th>상세 내용</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>※ 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 추가될 수 있는 옵션 기능으로 필수적으로 적용해야 하는 기능은 아닙니다.</p>			인증 구분	상세 내용	전자 메일 및 암호 기반 인증	전자 메일 주소와 암호로 사용자를 인증하는 방법입니다. SDK 는 전자 메일 주소와 암호를 사용하여 로그인하는 사용자를 만들고 관리하는 방법을 제공합니다.	페더레이션 ID 공급자 통합	타 플랫폼 ID 공급자와 통합하여 사용자를 인증하는 방법입니다. SDK 는 사용자가 Google, FaceBook, Twitter 및 GitHub 계정으로 로그인 할 수 있는 방법을 제공합니다.	전화 번호 인증	휴대 전화로 SMS 메시지를 보내 사용자를 인증합니다.	사용자 정의 인증 시스템 통합	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.	익명 인증	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.
	인증 구분	상세 내용													
전자 메일 및 암호 기반 인증	전자 메일 주소와 암호로 사용자를 인증하는 방법입니다. SDK 는 전자 메일 주소와 암호를 사용하여 로그인하는 사용자를 만들고 관리하는 방법을 제공합니다.														
페더레이션 ID 공급자 통합	타 플랫폼 ID 공급자와 통합하여 사용자를 인증하는 방법입니다. SDK 는 사용자가 Google, FaceBook, Twitter 및 GitHub 계정으로 로그인 할 수 있는 방법을 제공합니다.														
전화 번호 인증	휴대 전화로 SMS 메시지를 보내 사용자를 인증합니다.														
사용자 정의 인증 시스템 통합	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.														
익명 인증	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.														
설정 방법	<p>가. Identity Platform 설정 방법 (페더레이션 ID 공급자 통합)</p> <p>1) [Tool] > [Identity Platform] > [공급업체] > [공급업체 추가]</p>														



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

: 공급업체 설정 중 '익명(Anonymous)' 인증이 존재하지 않을 경우

취약기준

: 공급업체 설정 중 '익명(Anonymous)' 인증이 존재하는 경우

비고

SK shieldus

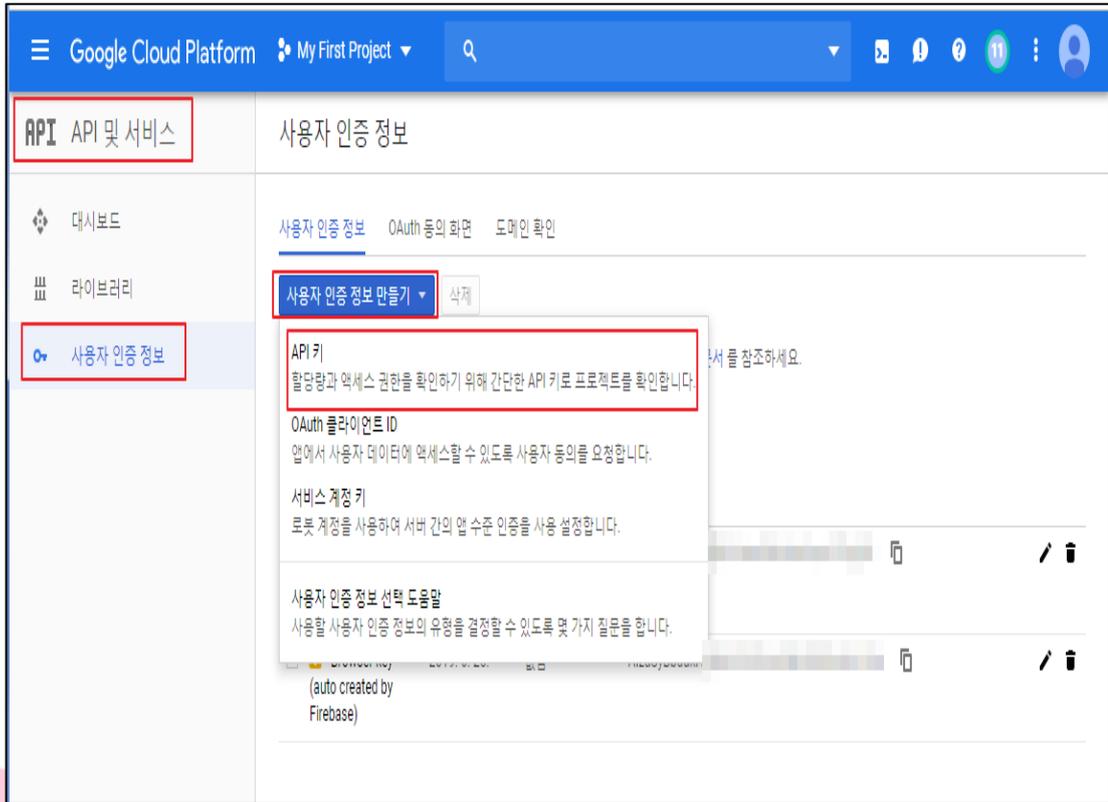
안녕을 지키는 기술

1.5 API 활성화 및 사용 주기 관리

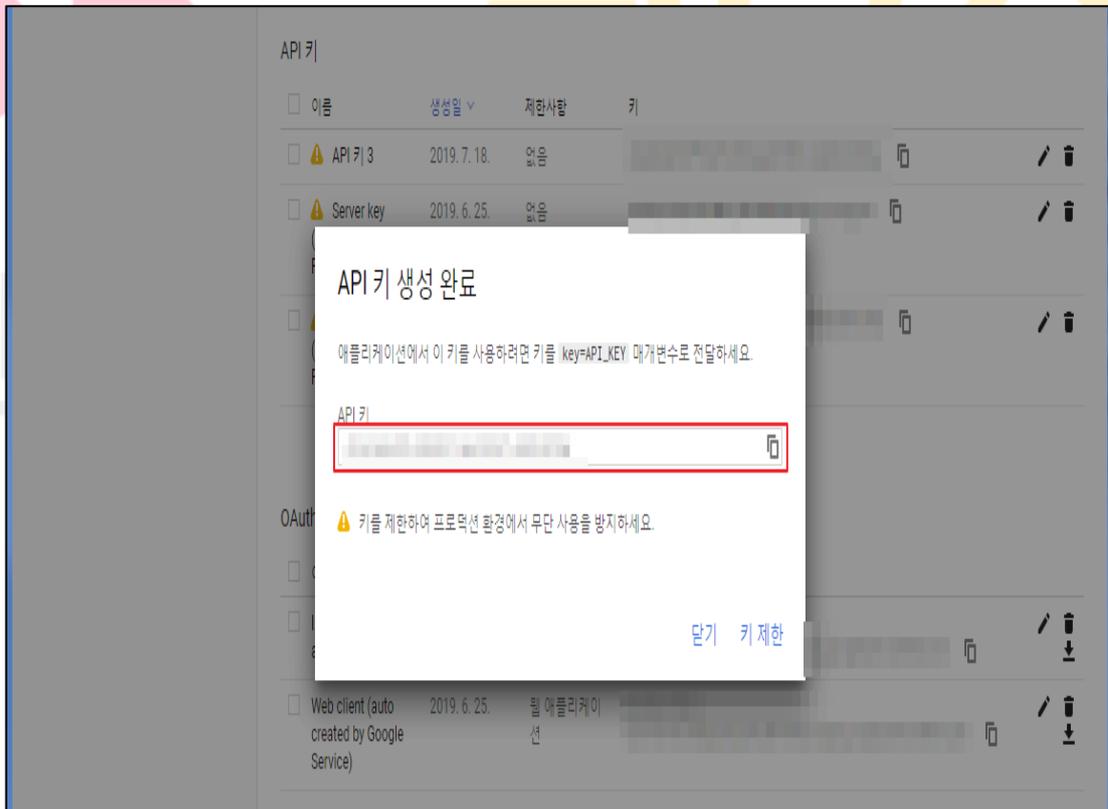
분류	계정 관리	중요도	중																		
항목명	API 활성화 및 사용 주기 관리																				
항목 설명	<p>Google Cloud API는 GCP(Google Cloud Platform)의 핵심으로서 저장소 액세스부터 머신러닝 기반 이미지 분석 및 Cloud Platform 애플리케이션에 이르기까지 모든 기능을 손쉽게 추가할 수 있도록 지원합니다. 이처럼 Google Cloud API 키 인증은 서비스 제공자가 발급해준 키를 통해 인증을 하는 방식으로 API 키가 노출되면 전체 보안이 침해당할 수 있으므로 API 키는 안전하게 관리되어야 합니다.</p> <p>일반적으로 클라이언트가 API 키에 액세스할 수 있으므로 API 키를 쉽게 도난당할 수 있습니다. API 키를 도난당하면 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.</p> <p>※ Cloud API 키 속성</p> <table border="1"> <thead> <tr> <th>구분</th> <th>속성</th> <th>내용</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>※ 모든 제한사항에 대해 '없음 또는 제한 안 함' 설정은 '테스트 목적' 등과 같은 서비스 특성을 고려해 사용하시기 바랍니다.</p>			구분	속성	내용	키	HTTP 리퍼러	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.	IP 주소	API 키 액세스를 특정 IP 주소로 제한을 가능하게 해줍니다.	Android 앱	Android 애플리케이션의 경우에는 Android 앱을 사용합니다. 이 옵션을 사용하려면 패키지 이름과 SHA-1 서명 인증서 디지털 지문을 추가해야 합니다.	iOS 앱	iOS 애플리케이션의 경우, iOS 앱을 사용합니다. 이 옵션을 사용하려면 API 호출을 특정 iOS 번들로 제한하도록 iOS 번들 식별자를 최소한 하나 이상 추가해야 합니다.	웹사이트	URL 경로 지정	URL 경로 설정을 통해 API 키의 적용 범위 지정이 가능합니다.	API 키	API 키 지정	API 제한사항은 API 키를 사용해서 호출할 수 있는 API 를 지정합니다. 프로덕션 애플리케이션에서 사용되는 모든 API 키는 API 제한사항을 사용해야 합니다.
	구분	속성	내용																		
키	HTTP 리퍼러	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.																			
	IP 주소	API 키 액세스를 특정 IP 주소로 제한을 가능하게 해줍니다.																			
	Android 앱	Android 애플리케이션의 경우에는 Android 앱을 사용합니다. 이 옵션을 사용하려면 패키지 이름과 SHA-1 서명 인증서 디지털 지문을 추가해야 합니다.																			
	iOS 앱	iOS 애플리케이션의 경우, iOS 앱을 사용합니다. 이 옵션을 사용하려면 API 호출을 특정 iOS 번들로 제한하도록 iOS 번들 식별자를 최소한 하나 이상 추가해야 합니다.																			
웹사이트	URL 경로 지정	URL 경로 설정을 통해 API 키의 적용 범위 지정이 가능합니다.																			
API 키	API 키 지정	API 제한사항은 API 키를 사용해서 호출할 수 있는 API 를 지정합니다. 프로덕션 애플리케이션에서 사용되는 모든 API 키는 API 제한사항을 사용해야 합니다.																			
설정	가. API 키 생성																				

방법

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



2) API 키 생성 완료



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

Google Cloud Platform My First Project

API 키 제한 및 이름 변경

이름* security test

키 제한사항

이 키는 제한되지 않습니다. 제한사항을 통해 승인되지 않은 사용 및 할당량 도종을 방지할 수 있습니다. [자세히 알아보기](#)

애플리케이션 제한사항

애플리케이션 제한사항은 API 키를 사용할 수 있는 웹사이트, IP 주소 또는 애플리케이션을 제어합니다. 키별로 애플리케이션 제한사항 1개를 설정할 수 있습니다.

없음

HTTP 리퍼러(웹사이트)

IP 주소(웹 서버, 크론 작업 등)

Android 앱

iOS 앱

웹사이트 제한사항

키 사용량 요청을 지정된 웹사이트로 제한합니다.

비워 두면 API 키가 모든 웹사이트의 요청을 수락합니다.

항목 추가

API 제한사항

API 제한사항은 이 키를 호출할 수 있는 사용 설정된 API를 지정합니다.

키 제한 안함

이 키는 모든 API를 호출할 수 있습니다.

키 제한

API 4개

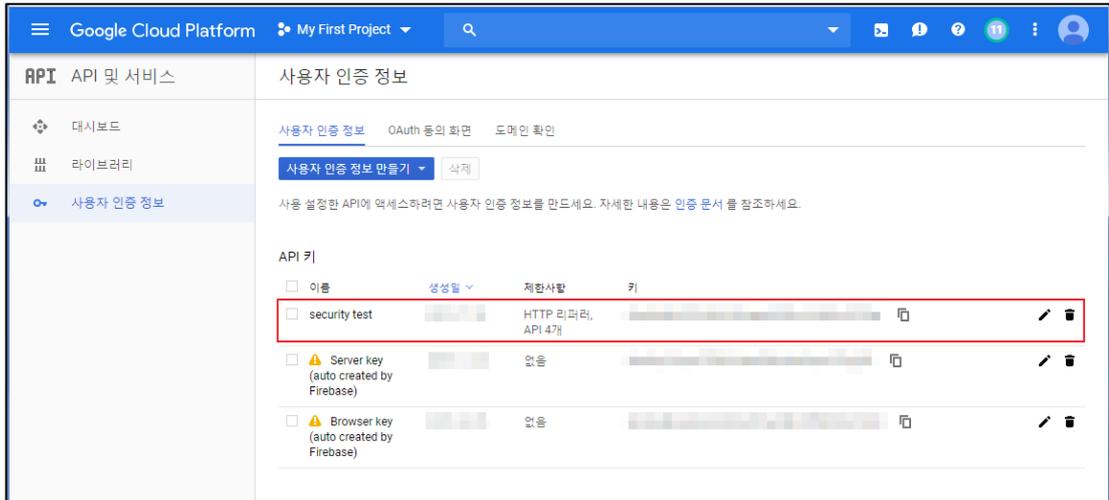
선택한 API:

- App Engine Admin API
- BigQuery API
- Stackdriver Logging API
- Stackdriver Monitoring API

참고: 설정이 적용되는 데 최대 5분이 걸릴 수 있습니다.

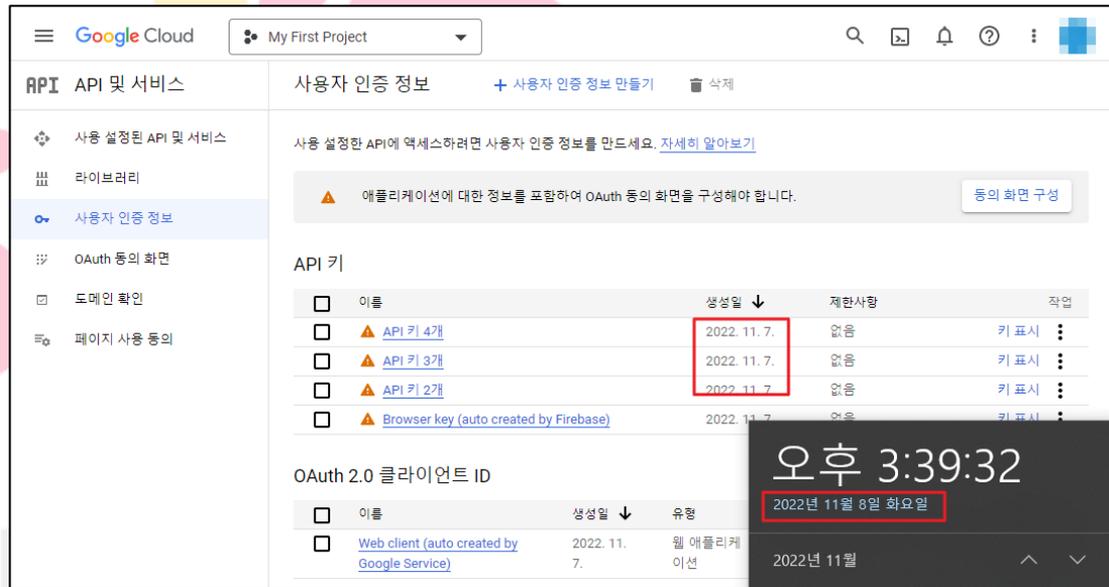
저장 취소

4) API 키 제한 설정 완료



나. API 키 주기 확인

1) [API 및 서비스] > [사용자 인증 정보] > [API 키] > 키 생성일 확인



양호기준

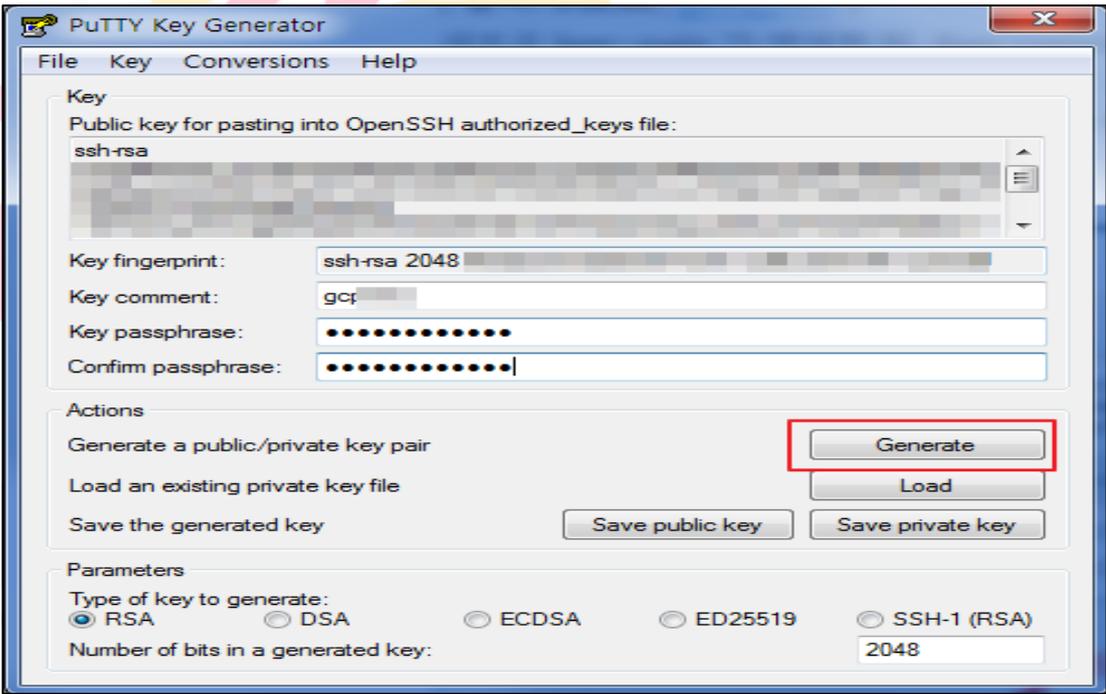
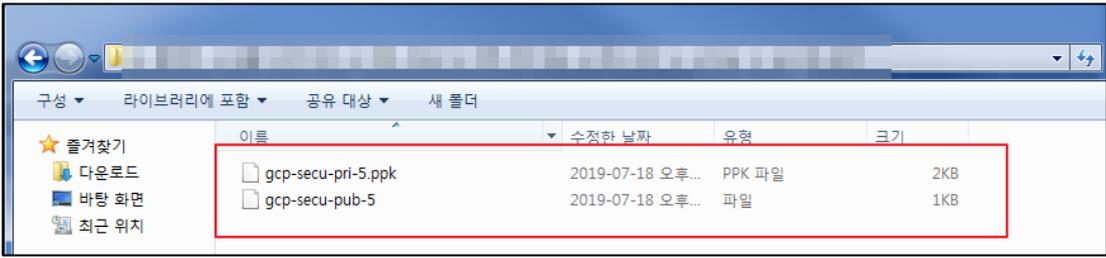
: API 키를 사용하게 될 경우 사용 주기가 60일 이내일 경우

취약기준

: API 키를 사용하게 될 경우 사용 주기가 60일 초과일 경우

비고

1.6 SSH 키 사용 관리

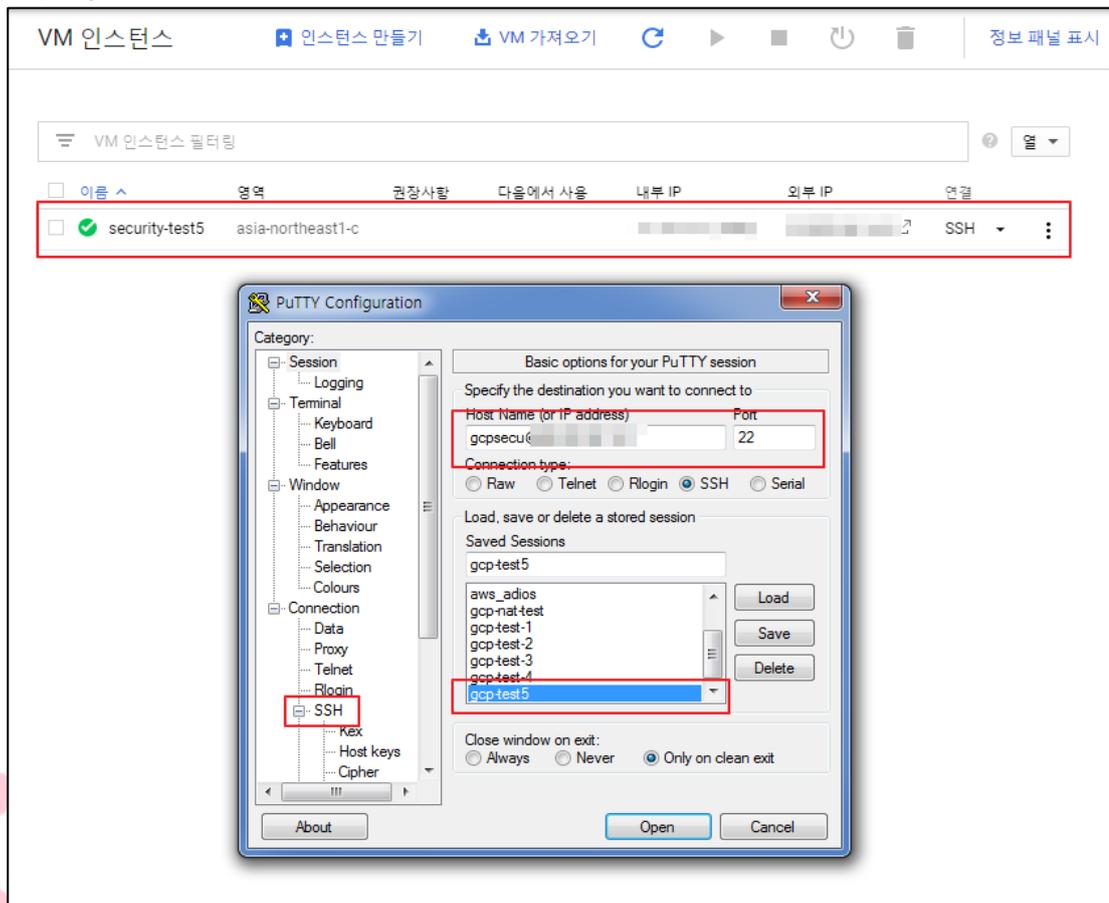
분류	계정 관리	중요도	상
항목명	SSH 키 사용 관리		
항목 설명	<p>Linux VM 인스턴스를 연결하려면 고유 한 개인 SSH 키 파일과 일치하는 공용 SSH 키 파일로 구성된 고유 한 SSH 키가 필요합니다. SSH 키는 Compute Engine 도구를 사용하여 연결할 때마다 생성되고 관리됩니다. 그러나 타사 도구와 연결하려면 다음 옵션 중 하나를 사용하여 공개 SSH 키를 인스턴스에 제공해야 합니다.</p> <p>퍼블릭/프라이빗 Cloud Compute 에 안전한 보안 접속을 하기 위해서는 필수로 설정 적용이 필요한 기능으로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

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

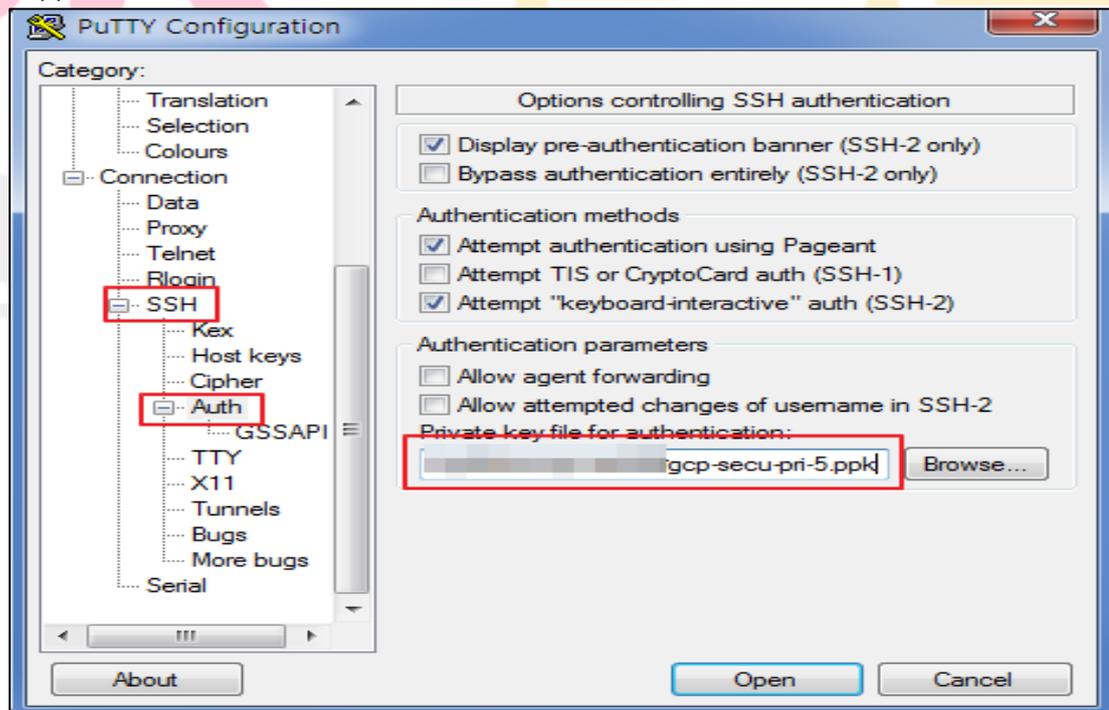
Google Cloud Platform console interface showing the 'SSH 키' (SSH Key) management page. The '메타데이터' (Metadata) section is active, and the 'SSH 키' menu item is highlighted. The page displays a list of SSH keys, with the 'gcpsecu' key selected. The public key content is visible in a text area. A red box highlights the '+ 항목 추가' (Add item) button at the bottom of the list.

Google Cloud Platform console interface showing the 'SSH 키' (SSH Key) management page. The '메타데이터' (Metadata) section is active, and the 'SSH 키' menu item is highlighted. The page displays a list of SSH keys, with the 'gcpsecu' key selected. The public key content is visible in a text area. A red box highlights the '+ 항목 추가' (Add item) button at the bottom of the list.

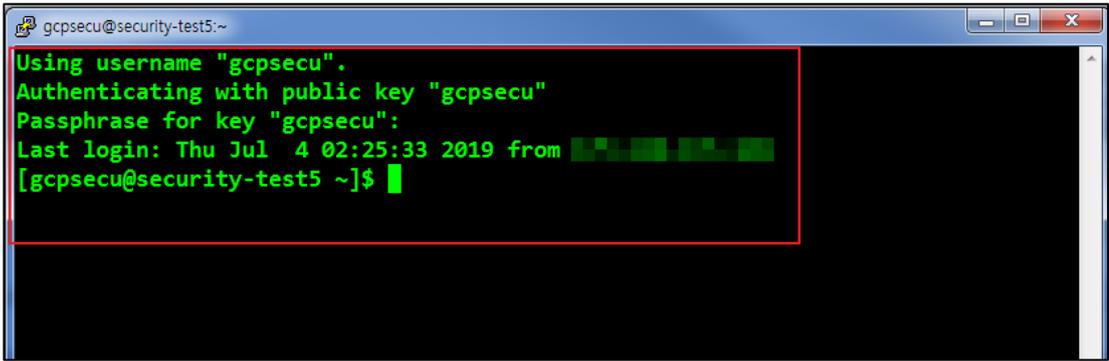
4) putty 내 SSH 접근을 위한 '계정명@hostname(IP)' 및 SSH 키 등록



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



6) SSH 키를 통한 Linux VM Instance 접근 성공 확인



```
gcpsecu@security-test5:~  
Using username "gcpsecu".  
Authenticating with public key "gcpsecu"  
Passphrase for key "gcpsecu":  
Last login: Thu Jul 4 02:25:33 2019 from [REDACTED]  
[gcpsecu@security-test5 ~]$
```

양호기준

: SSH 키를 통해 VM 인스턴스에 접근이 가능할 경우

취약기준

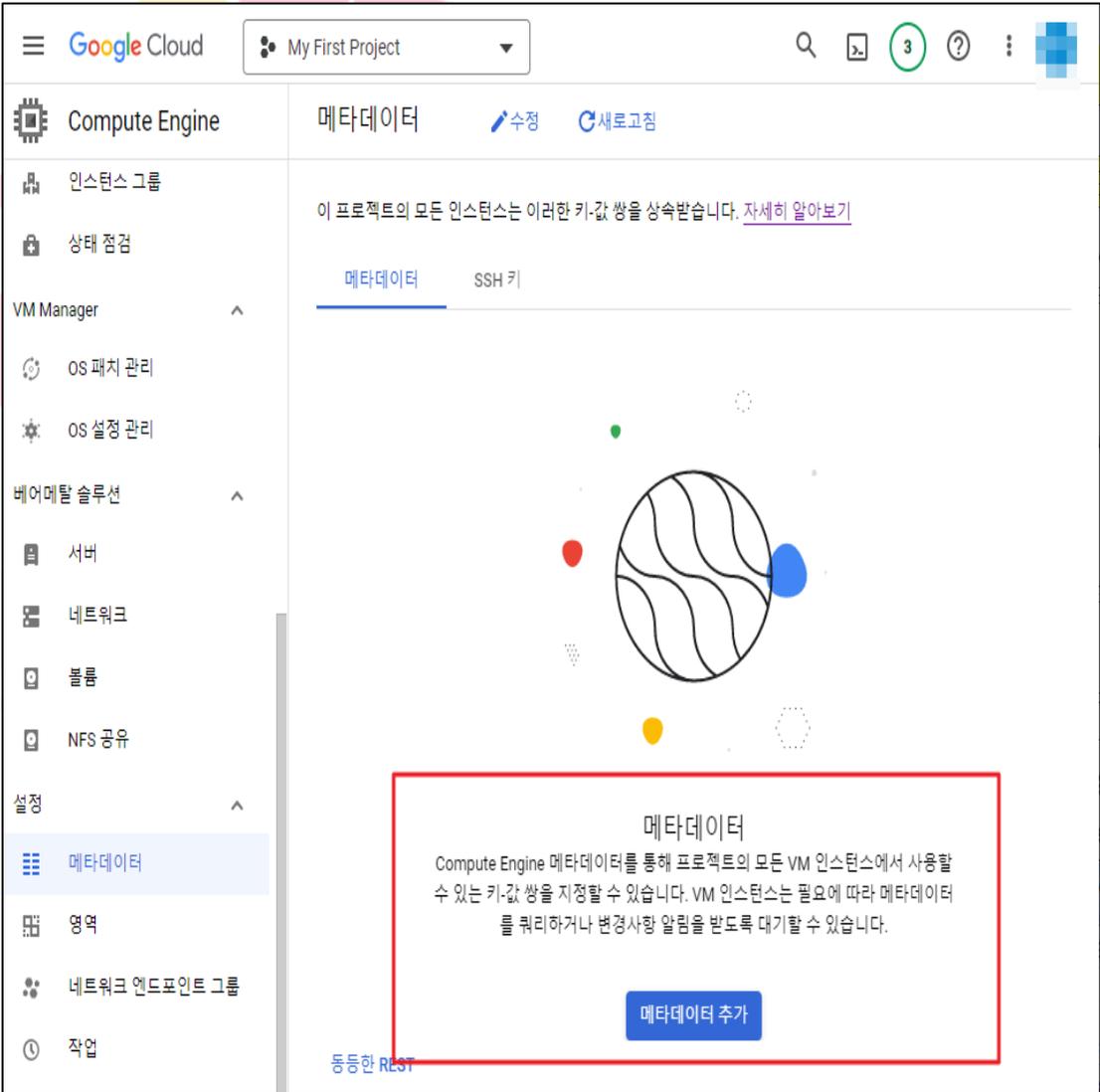
: SSH 키를 통하지 않고 일반 패스워드를 통해 VM 인스턴스에 접근이 가능할 경우

비고



안녕을 지키는 기술

1.7 메타데이터 관리

분류	계정 관리	중요도	상
항목명	메타데이터 관리		
항목 설명	<p>가상 머신(VM) 인스턴스는 메타데이터 서버에 메타데이터를 저장합니다. VM 은 추가 승인 없이 메타데이터 서버 API 에 자동으로 액세스할 수 있습니다. 메타데이터는 key:value 쌍으로 저장이 되며 메타데이터 서버에서 정보를 가져올 수 있습니다.</p> <p>메타데이터 URL 을 쿼리할 수 있는 모든 프로세스에서 메타데이터 서버의 모든 값에 액세스할 수 있으며 서버에 쓰는 모든 커스텀 메타데이터 값이 포함됩니다. 이때 메타데이터 서버에 민감 또는 주요한 값을 쓰거나 타사 프로세스를 실행할 때 보안상 문제가 될 가능성이 높아 주의해 사용해야 합니다.</p>		
설정 방법	<p>가. 메타데이터 생성 및 VM Instance 적용/확인</p> <p>1) 커스텀 메타데이터 추가</p>  <p>The screenshot shows the Google Cloud console interface for 'My First Project'. The left sidebar is expanded to 'Compute Engine' > 'Metadata'. The main content area shows a 'Metadata' tab with a 'Add Metadata' button highlighted in a red box. The dialog box text reads: '메타데이터. Compute Engine 메타데이터를 통해 프로젝트의 모든 VM 인스턴스에서 사용할 수 있는 키-값 쌍을 지정할 수 있습니다. VM 인스턴스는 필요에 따라 메타데이터를 쿼리하거나 변경사항 알림을 받도록 대기할 수 있습니다.' Below the text is a blue button labeled '메타데이터 추가'.</p>		

2) [메타데이터] > [메타데이터] 내 Key:Value 값 입력 후 저장

Google Cloud My First Project

Compute Engine 메타데이터 수정 새로고침

이 프로젝트의 모든 인스턴스는 이러한 키-값 쌍을 상속받습니다. [자세히 알아보기](#)

메타데이터 SSH 키

메타데이터

키 1 *	값 1
startup-script	<pre>#!/bin/bash apt-get update apt-get install -y apache2 cat <<EOF /usr/bin/htpasswd /etc/passwd <html><body><h1>Hello World</h1> <p>metadata test</p> </body></html> EOF</pre>

저장 취소

3) 등록된 메타데이터 확인

Google Cloud My First Project

Compute Engine 메타데이터 수정 새로고침

이 프로젝트의 모든 인스턴스는 이러한 키-값 쌍을 상속받습니다. [자세히 알아보기](#)

메타데이터 SSH 키

키 ↑	값
startup-script	#!/bin/bash

동등한 REST

메타데이터 저장 성공 X

4) 등록된 메타데이터 확인을 위한 VM 인스턴스 중지 및 시작

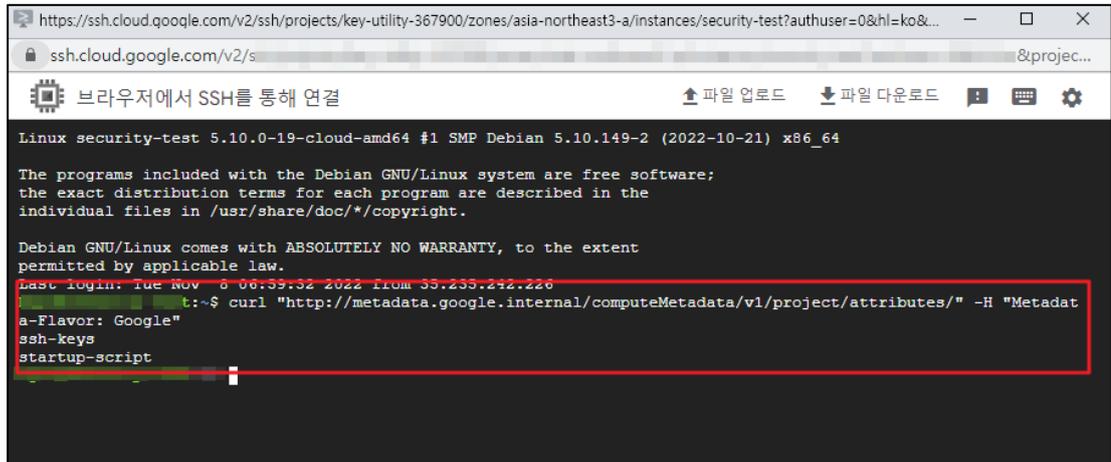
The screenshot shows the Google Cloud Compute Engine console. On the left, the 'VM 인스턴스' (VM Instances) menu is selected. The main area displays a list of VM instances. One instance is highlighted with a red box. A context menu is open over this instance, with '시작/재개' (Start/Restart) and '중지' (Stop) options highlighted in red. The instance details on the right show 'security-test' with tabs for 'PERMISSIONS', 'LABELS', and 'MONITORING'.

5) 메타데이터 값 적용 확인

The screenshot shows the Google Cloud Compute Engine console with the '외부 IP' (External IP) field highlighted in red. Below the console, a browser window shows the output of a terminal session. The terminal displays 'Hello World' and 'metadata test', confirming that the metadata has been applied. The browser's address bar shows the URL 'https://console.cloud.google.com/compute/project=key-unity-307/900' and the IP address '34.64.210.249' is visible in the address bar.

나. 기본 메타데이터 값 호출

1) SSH 키를 통한 Linux VM Instance 접근 성공 확인



```
Linux security-test 5.10.0-19-cloud-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Nov  8 06:59:32 2022 from 35.235.242.226
t:~$ curl "http://metadata.google.internal/computeMetadata/v1/project/attributes/" -H "Metadat
a-Flavor: Google"
ssh-keys
startup-script
```

양호기준

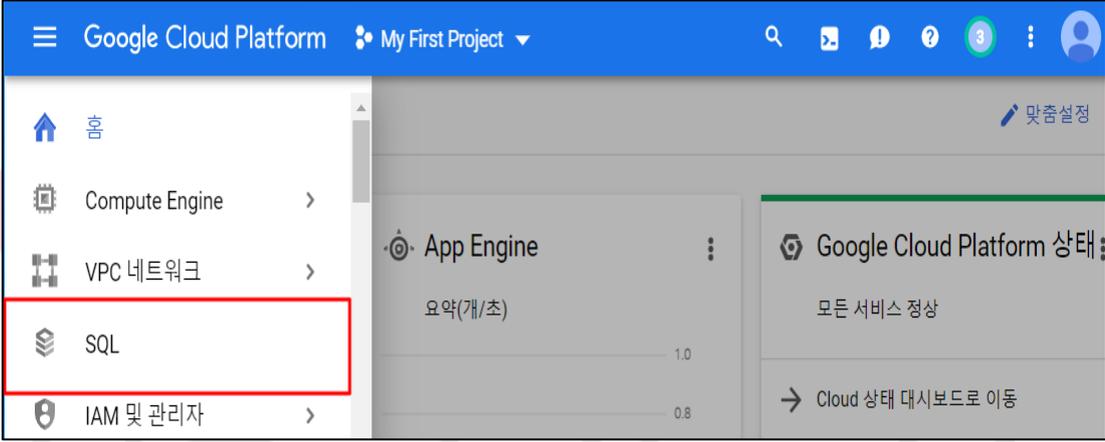
: SSH 접근 후 메타데이터 접근 시 주요정보가 출력되거나 확인되고 있지 않을 경우

취약기준

: SSH 접근 후 메타데이터 접근 시 주요정보가 출력되거나 확인되고 있을 경우

비고

1.8 SQL 계정 관리

분류	계정 관리	중요도	상
항목명	SQL 계정 관리		
항목 설명	<p>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.</p> <p>SQL DB의 루트 비밀번호가 없으면 누구나 전체 관리 권한으로 이 인스턴스에 연결할 수 있습니다. 승인된 사용자에게만 권한이 부여되도록 루트 비밀번호를 설정해야 합니다.</p> <p>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.</p>		
설정 방법	<p>가. Cloud SQL 루트 패스워드 설정</p> <p>1) [메인] > [SQL]</p>  <p>2) Cloud SQL 인스턴스 생성</p> 		

3) 데이터베이스 엔진 선택

The screenshot shows the Google Cloud SQL console interface. At the top, it says 'Google Cloud' and 'My First Project'. Below that, there's a navigation bar with 'SQL' and '인스턴스 만들기'. The main content area is titled '데이터베이스 엔진 선택'. There are three cards representing different database engines: MySQL (version 8.0, 5.7, 5.6), PostgreSQL (version 14, 13, 12, 11, 10, 9.6), and SQL Server (version 2019, 2017). Each card has a '선택' (Select) button. A red box highlights the MySQL and PostgreSQL options. Below the cards, there is a link: 'Cloud SQL 데이터베이스 엔진에 대한 추가 컨텍스트가 필요하신가요? 자세히 알아보기'.

4) 비밀번호 정책 설정 및 루트 비밀번호 생성

The screenshot shows the 'MySQL 인스턴스 만들기' (Create MySQL Instance) page. The '인스턴스 정보' (Instance Info) section has a text input for '인스턴스 ID *' with the value 'sql-test'. Below it, there's a note: '소문자, 숫자, 하이픈을 사용하세요. 영문자로 시작해야 합니다.' The '비밀번호 *' (Password) section has a masked password field and a '생성' (Generate) button. Below that, there's a note: '루트 사용자의 비밀번호를 설정하세요. 자세히 알아보기'. There are three checkboxes: '비밀번호 없음' (unchecked), '대문자, 소문자, 숫자, 영숫자가 아닌 문자를 포함해야 합니다.' (checked), '사용자 이름을 포함해서는 안 됩니다.' (checked), and '10자(영문 기준) 이상이어야 합니다.' (checked). The '비밀번호 정책' (Password Policy) section explains that using password policy requires authenticating all local users with the password. The '인스턴스 수준 비밀번호 정책' (Instance-level password policy) section explains that these requirements apply to all local users. There are two checked checkboxes: '최소 길이 설정' (Minimum length) and '복잡성 요구' (Complexity requirements). The '최소 길이 설정' section has a text input for '최소 글자 수' (Minimum length) with the value '10' and a range of '1~30'. The '복잡성 요구' section has a note: '비밀번호에 대문자, 소문자, 숫자, 기호를 포함해야 합니다.' The '비밀번호 재사용 제한' (Password reuse prevention) section has a checked checkbox and a note: '비밀번호를 최소 횟수 이상 변경해야 재사용할 수 있습니다.' Below it, there's a text input for '최소 비밀번호 변경 횟수' (Minimum password change count) with the value '3' and a range of '1~5'. On the right side, there's a '요약' (Summary) section with a list of configuration options: 리전, DB 버전, vCPU, 메모리, 저장용량, 네트워크 처리량(MB/초), 디스크 처리량(MB/초), IOPS, 연결, 백업, 가용성, and point-in-time recovery.

여러 영역(고가용성)
선택한 리전 내의 다른 영역으로 자동으로 장애 조치가 적용됩니다. 프로덕션 인스턴스에 권장되며 비용이 증가합니다.

▼ 영역 지정

인스턴스 맞춤설정
나중에 인스턴스 구성을 맞춤설정할 수도 있습니다.

▼ 구성 옵션 표시

인스턴스 만들기 취소

5) 인스턴스 생성 완료

Google Cloud My First Project

SQL 인스턴스 + 인스턴스 만들기 데이터 마이그레이션 정보 패널

필터 속성 이름 또는 값 입력

<input type="checkbox"/>	인스턴스 ID	↑	유형	공개 IP 주소	비공개 IP 주소	인스턴스 연결 이름	고가용성	위치
<input checked="" type="checkbox"/>	sql-test		MySQL 5.7	34.64.210.103		my-first-proje...	추가	asia-northeast3

6) 패스워드가 설정된 루트 계정 확인

Google Cloud My First Project

SQL 사용자

기본 인스턴스

- 개요
- 쿼리 통계 **신규**
- 연결
- 사용자**
- 데이터베이스
- 백업
- 복제본
- 작업

모든 인스턴스 > sql-test

sql-test
MySQL 5.7

사용자 계정을 통해 사용자와 애플리케이션이 인스턴스에 연결할 수 있습니다. [Learn more](#)

+ 사용자 계정 추가

<input type="radio"/>	사용자 이름	↑	호스트 이름	인증	비밀번호 상태	
<input checked="" type="radio"/>	root		%(모든 호스트)	기본 제공	해당 사항 없음	⋮

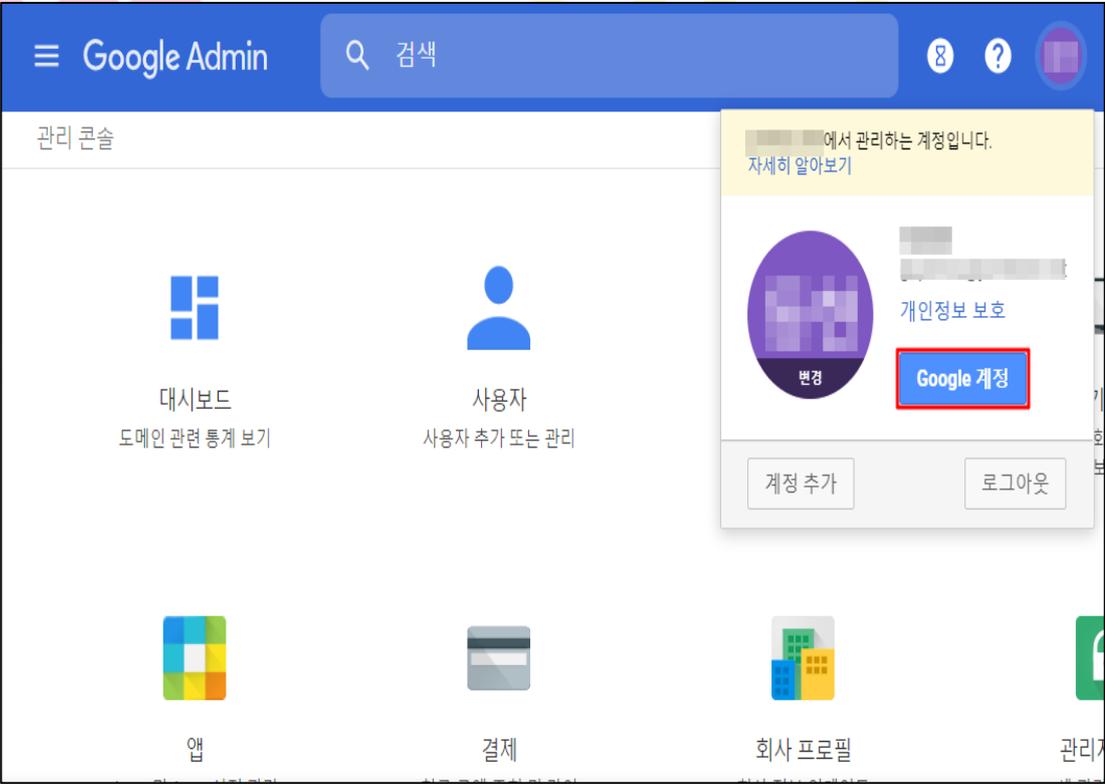
진단 기준

양호기준
: 패스워드 활성화 및 복잡도 설정이 존재하는 경우

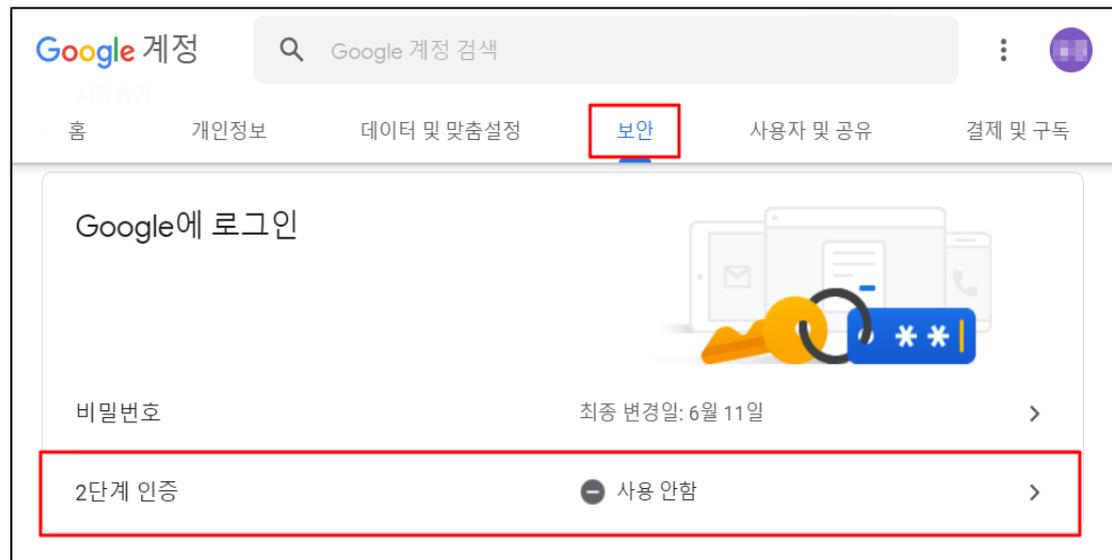
취약기준
: 패스워드 비활성 및 복잡도 설정이 존재하지 않는 경우

비고

1.9 MFA (Multi-Factor Authentication) 설정

분류	계정 관리	중요도	중												
항목명	MFA (Multi-Factor Authentication) 설정														
항목 설명	<p>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 키 뿐만 아니라 GCP가 지원하는 추가 인증을 요청 함으로써 보안을 강화하며 2-Factor-Authentication(MFA)는 다음의 형태로 사용자 인증을 할 수 있습니다.</p> <p>(*) 사용 가능한 2단계 인증(2-Factor-Authentication, MFA) 방식</p> <table border="1" data-bbox="280 629 903 913"> <thead> <tr> <th>No</th> <th>인증 수단</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Google 메시지</td> </tr> <tr> <td>2</td> <td>보안 키</td> </tr> <tr> <td>3</td> <td>Google OTP 또는 기타 인증 코드 생성기</td> </tr> <tr> <td>4</td> <td>SMS 또는 전화로 인증 코드 받기</td> </tr> <tr> <td>5</td> <td>백업 코드</td> </tr> </tbody> </table> <p>(*) 2단계 인증(2-Factor-Authentication, MFA) 설정은 각 사용자별 각자 맞는 방식으로 추가 설정해야 합니다.</p>			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
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														
설정 방법	<p>가. 관리자 2-factor 설정</p> <p>1) [메인] > [Google 계정]</p> 														

2) [보안] > [2단계 인증]



Google 계정

Google 계정 검색

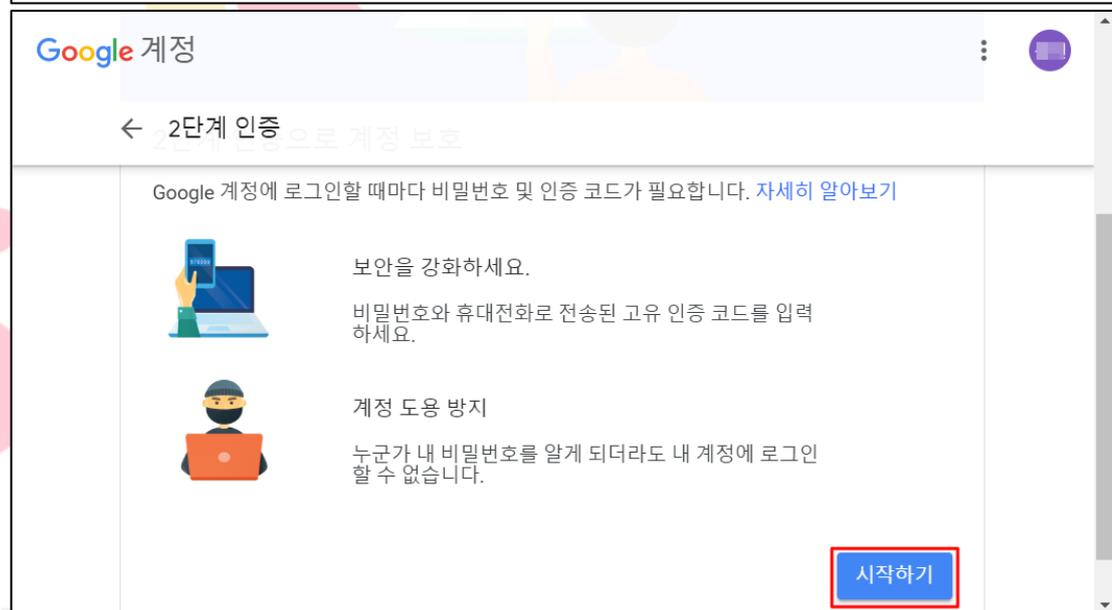
시작하기

홈 개인정보 데이터 및 맞춤설정 **보안** 사용자 및 공유 결제 및 구독

Google에 로그인

비밀번호 최종 변경일: 6월 11일 >

2단계 인증 사용 안함 >



Google 계정

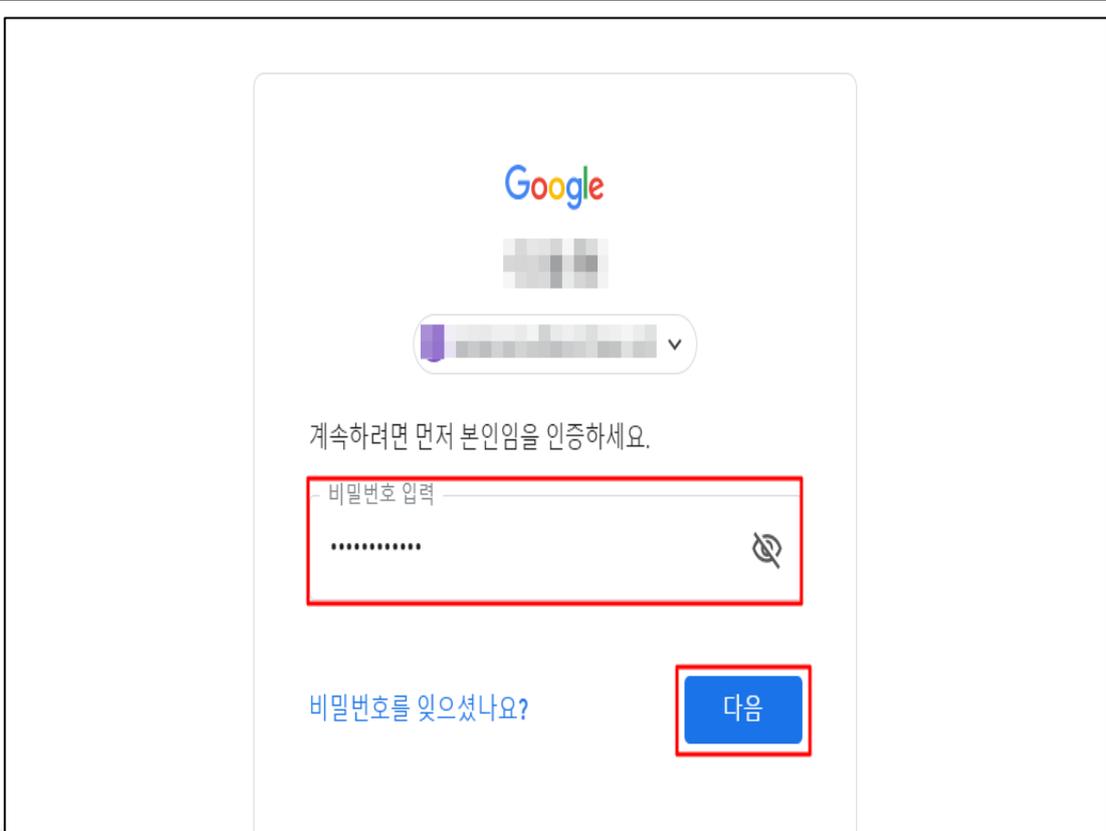
← 2단계 인증으로 계정 보호

Google 계정에 로그인할 때마다 비밀번호 및 인증 코드가 필요합니다. [자세히 알아보기](#)

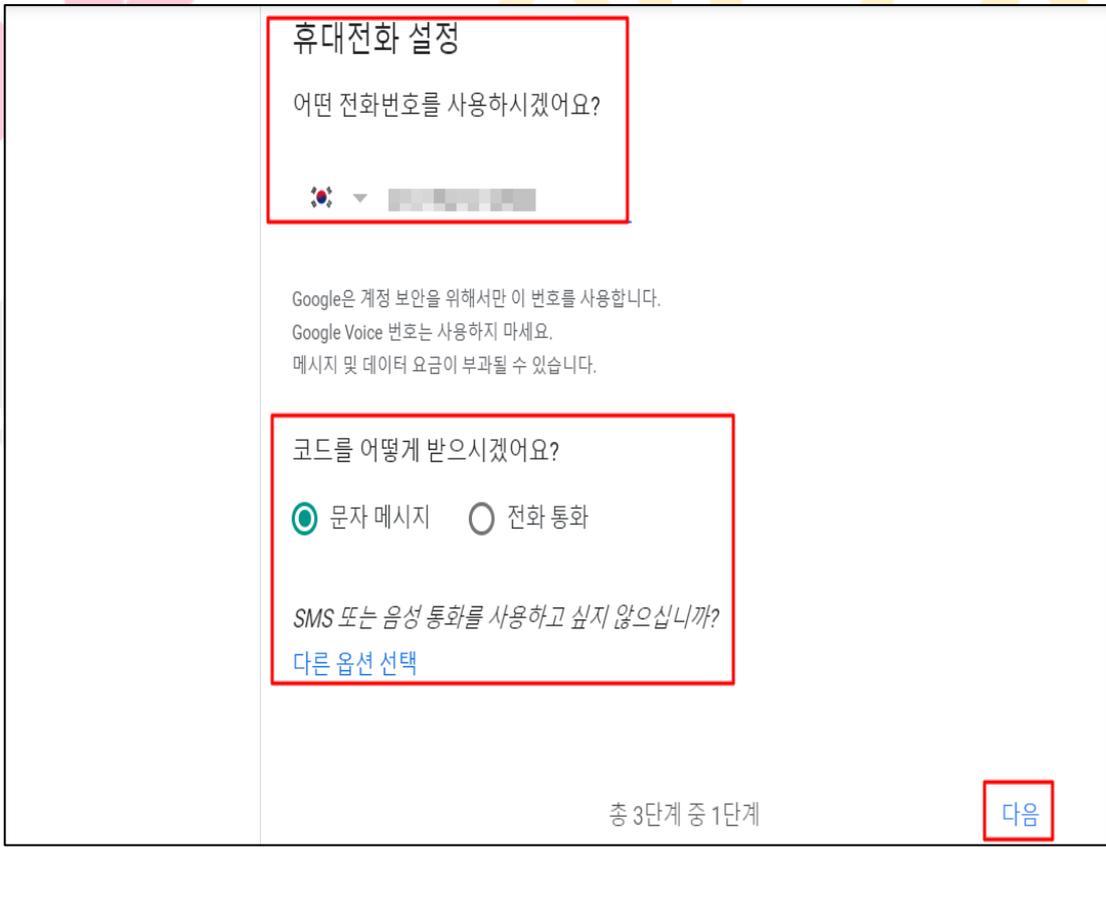
 보안을 강화하세요.
비밀번호와 휴대전화로 전송된 고유 인증 코드를 입력하세요.

 계정 도용 방지
누군가 내 비밀번호를 알게 되더라도 내 계정에 로그인할 수 없습니다.

시작하기



3) [휴대전화 설정]



4) [인증번호 확인]



작동 여부 확인

Google에서 인증 코드가 포함된 SMS를 방금 [redacted] 번으로 전송했습니다.

코드 입력

478428

받지 못하셨나요? [재전송](#)

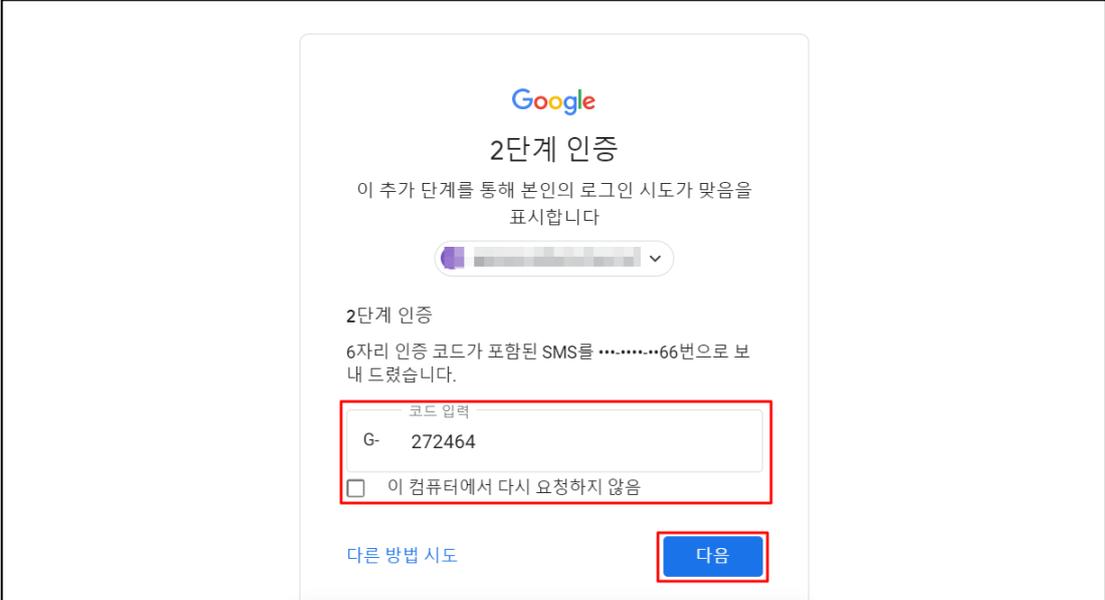
[뒤로](#) 총 3단계 중 2단계 [다음](#)



완료되었습니다. 2단계 인증을 사용하도록 설정하시겠습니까?

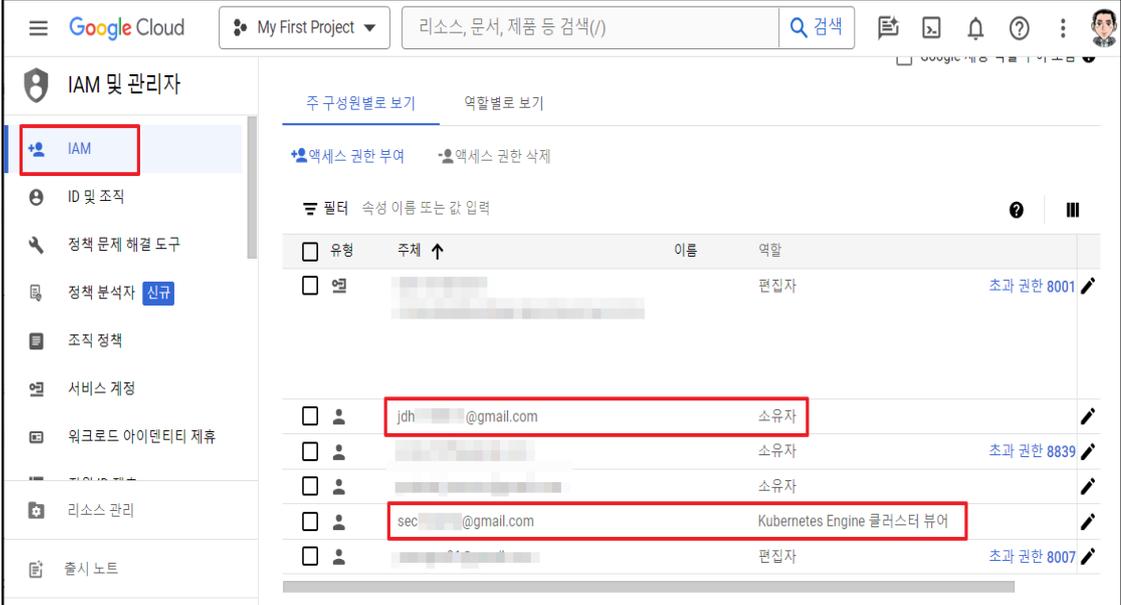
이제 작동 방식에 대해 알아보았으니 Google 계정([redacted])에 2단계 인증을 사용하도록 설정하시겠습니까?

총 3단계 중 3단계 [사용](#)

	
진단 기준	<p>양호기준 : Cloud ID 모든 사용자 계정에 MFA가 활성화되어 있을 경우</p> <p>취약기준 : Cloud ID 모든 사용자 계정에 MFA가 비활성화되어 있을 경우</p>
비고	MFA 인증을 사용하지 않고 SSO 인증을 통해서 로그인할 경우 양호로 처리될 수 있음

안녕을 지키는 기술

1.10 GKE 사용자 관리

분류	계정 관리	중요도	상									
항목명	GKE 사용자 관리											
항목 설명	<p>기본적으로 GCP 계정은 리소스에 대한 접근을 허용하는 최소한의 사용자 수와 권한으로 관리되어야 합니다.</p> <p>GCP에서는 IAM 사용자에게 GKE Cluster에 대한 액세스 권한을 부여해야 하는 경우 Kubernetes RBAC 설정을 통해 Cluster 내 객체에 세분화된 권한을 부여할 수 있습니다.</p>											
	<p>(*) RBAC 역할 및 바인딩 유형(참고)</p> <table border="1" data-bbox="276 645 1428 1025"> <thead> <tr> <th>구분</th> <th>내용</th> </tr> </thead> <tbody> <tr> <td>Role</td> <td>단일 네임스페이스로 제한되는 권한 집합</td> </tr> <tr> <td>ClusterRole</td> <td>모든 네임스페이스 또는 전체 Cluster에 적용할 수 있는 권한 집합</td> </tr> <tr> <td>RoleBinding</td> <td>특정 네임스페이스 내에서 사용자 또는 그룹에 Role 또는 ClusterRole을 바인딩</td> </tr> <tr> <td>ClusterRoleBinding</td> <td>Cluster에서 모든 네임스페이스의 사용자 또는 그룹에 ClusterRole을 바인딩</td> </tr> </tbody> </table>			구분	내용	Role	단일 네임스페이스로 제한되는 권한 집합	ClusterRole	모든 네임스페이스 또는 전체 Cluster에 적용할 수 있는 권한 집합	RoleBinding	특정 네임스페이스 내에서 사용자 또는 그룹에 Role 또는 ClusterRole을 바인딩	ClusterRoleBinding
구분	내용											
Role	단일 네임스페이스로 제한되는 권한 집합											
ClusterRole	모든 네임스페이스 또는 전체 Cluster에 적용할 수 있는 권한 집합											
RoleBinding	특정 네임스페이스 내에서 사용자 또는 그룹에 Role 또는 ClusterRole을 바인딩											
ClusterRoleBinding	Cluster에서 모든 네임스페이스의 사용자 또는 그룹에 ClusterRole을 바인딩											
설정 방법	<p>※ RBAC은 Cluster 및 네임스페이스 수준에서 접근 제어를 하는 반면 IAM은 프로젝트 수준에서 작동하기 때문에 계정별 접근 범위를 지정하고 업무 수행에 필요한 최소 권한만 부여하여 사용해야 합니다.</p>											
	<p>가. IAM 사용자 접근 권한 확인</p> <p>1) IAM 사용자 역할 확인</p> 											

2) 권한 부여된 계정(jdh*****)으로 GKE 리소스 접근 시도

```
Google Cloud My First Project 소유자  
CLOUD SHELL  
터미널 (ethereal-audio-413401) X +  
jdh @cloudshell:~ (ethereal-audio-413401) $ gcloud info | grep Account  
Account: [jdh @gmail.com]  
jdh @cloudshell:~ (ethereal-audio-413401) $ kubectl get pods  
NAME READY STATUS RESTARTS AGE  
nginx-1-64b86779d8-55sk8 1/1 Running 0 2d4h  
nginx-1-64b86779d8-r9qgt 1/1 Running 0 2d4h  
nginx-1-64b86779d8-t96fs 1/1 Running 0 2d4h  
jdh @cloudshell:~ (ethereal-audio-413401) $
```

3) 권한 미부여된 계정(sec*****)으로 GKE 리소스 접근 시도

```
Google Cloud My First Project 클러스터 뷰어  
CLOUD SHELL  
터미널 (ethereal-audio-413401) X + 편집기 열기  
sec @cloudshell:~ (ethereal-audio-413401) $ gcloud info | grep Account  
Account: [sec @gmail.com]  
sec @cloudshell:~ (ethereal-audio-413401) $ kubectl get pods  
Error from server (Forbidden): pods is forbidden: User "sec @gmail.com" cannot list resource "pods" in API group "" in the namespace "default": requires one of ["container.pods.list"] permission(s).  
sec @cloudshell:~ (ethereal-audio-413401) $
```

나. GKE ClusterRole/ClusterRoleBinding 생성 및 등록

1) ClusterRole 파일 생성 (pods 관련 권한 추가)

```
Google Cloud My First Project  
CLOUD SHELL  
터미널 (ethereal-audio-413401) X +  
apiVersion: rbac.authorization.k8s.io/v1  
kind: ClusterRole  
metadata:  
  name: cluster-pod-reader  
rules:  
- apiGroups:  
  - ""  
  resources:  
  - pods  
  verbs:  
  - get  
  - list  
  - watch  
~  
~  
"pod-clusterrole.yaml" 13L, 181B
```

2) ClusterRole 파일 적용

```
Google Cloud My First Project
CLOUD SHELL
터미널 (ethereal-audio-413401) X +
jdh@cloudshell:~ (ethereal-audio-413401) $ kubectl apply -f pod-clusterrole.yaml
clusterrole.rbac.authorization.k8s.io/cluster-pod-reader created
jdh@cloudshell:~ (ethereal-audio-413401) $
```

3) ClusterRole 생성 확인

```
Google Cloud My First Project
CLOUD SHELL
터미널 (ethereal-audio-413401) X +
jdh@cloudshell:~ (ethereal-audio-413401) $ kubectl get clusterrole
NAME                                CREATED AT
admin                                2024-02-06T01:20:20Z
ca-cr-actor                          2024-02-06T01:20:48Z
cloud-provider                        2024-02-06T01:21:27Z
cluster-admin                        2024-02-06T01:20:19Z
cluster-autoscaler                   2024-02-06T01:20:46Z
cluster-pod-reader                   2024-02-22T05:03:45Z
edit                                  2024-02-06T01:20:20Z
external-metrics-reader              2024-02-06T01:21:23Z
fluentbit-gke-pod-label-reader       2024-02-06T01:20:50Z
```

4) ClusterRoleBinding 생성 및 사용자 추가

```
Google Cloud My First Project
CLOUD SHELL
터미널 (ethereal-audio-413401) X +
jdh@cloudshell:~ (ethereal-audio-413401) $ kubectl create clusterrolebinding pod-rolebinding --clusterrole=cluster-pod-reader --user=sec.@gmail.com
clusterrolebinding.rbac.authorization.k8s.io/pod-rolebinding created
jdh@cloudshell:~ (ethereal-audio-413401) $
```

5) ClusterRoleBinding 생성 확인

```
Google Cloud My First Project
CLOUD SHELL
터미널 (ethereal-audio-413401) X +
jdh@cloudshell:~ (ethereal-audio-413401) $ kubectl get clusterrolebinding
NAME                ROLE                                AGE
ca-cr               ClusterRole/ca-cr-actor            16d
cluster-admin       ClusterRole/cluster-admin          16d
cluster-autoscaler  ClusterRole/cluster-autoscaler    16d
cluster-autoscaler-updateinfo  ClusterRole/read-updateinfo       16d
event-exporter-rb   ClusterRole/view                   16d
pod-rolebinding     ClusterRole/cluster-pod-reader     6m42s
snapshot-controller-role  ClusterRole/snapshot-controller-runner 16d
system:basic-user   ClusterRole/system:basic-user      16d
```

6) ClusterRoleBinding 정보 확인

```

cloudshell:~ (ethereal-audio-413401) $ kubectl describe clusterrolebinding pod-rolebinding
Name:         pod-rolebinding
Labels:       <none>
Annotations:  <none>
Role:
  Kind: ClusterRole
  Name: cluster-pod-reader
Subjects:
  Kind  Name                               Namespace
  ----  ---                               -
  User  sec.*****@gmail.com
  
```

다. GKE RBAC 적용 유무 확인

1) 권한 부여된 계정(sec*****@gmail.com)으로 GKE 리소스(pods 및 그 외 리소스) 접근 시도

```

cloudshell:~ (ethereal-audio-413401) $ kubectl get pods
NAME                                READY   STATUS    RESTARTS   AGE
nginx-1-64b86779d8-55sk8            1/1    Running   0           2d4h
nginx-1-64b86779d8-r9ggt            1/1    Running   0           2d4h
nginx-1-64b86779d8-t96fs            1/1    Running   0           2d4h
cloudshell:~ (ethereal-audio-413401) $ kubectl get role --all-namespaces
Error from server (Forbidden): roles.rbac.authorization.k8s.io is forbidden: User "sec.*****@gmail.com" cannot list resource "roles" in API group "rbac.authorization.k8s.io" at the cluster scope: requires one of ["container.roles.list"] permission(s).
cloudshell:~ (ethereal-audio-413401) $
  
```

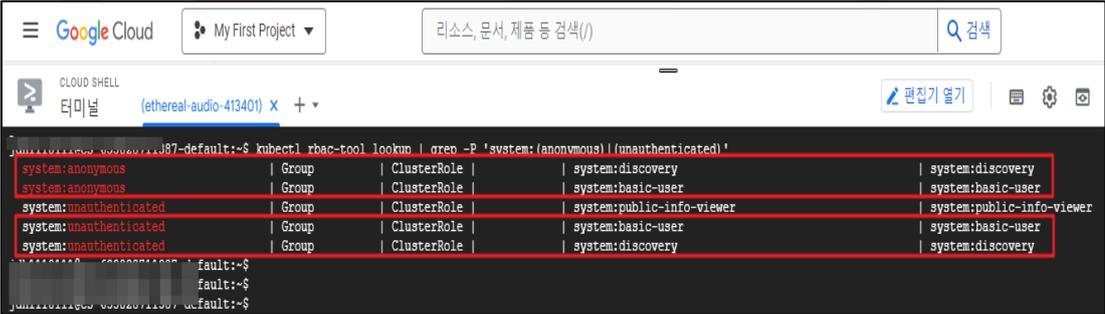
진단 기준	<p>양호기준</p> <p>: GKE 리소스 접근을 위한 RBAC 설정이 인가된 사용자만 설정되어 있는 경우</p>
	<p>취약기준</p> <p>: GKE 리소스 접근을 위한 RBAC 설정이 인가된 사용자만 설정되어 있지 않은 경우</p>

비고

1.11 GKE 서비스 어카운트 관리

분류	계정 관리	중요도	중
항목명	GKE 서비스 어카운트 관리		
항목 설명	<p>서비스 어카운트는 파드에 쿠버네티스 RBAC 역할을 할당할 수 있는 특수한 유형의 개체이며 Cluster 내의 각 네임스페이스에 기본 서비스 어카운트가 자동으로 생성됩니다. 특정 서비스 어카운트를 참조하지 않고 네임스페이스에 파드를 배포하면, 해당 네임스페이스의 파드에 자동으로 할당되고 서비스 어카운트의(JWT) 토큰은 특정 경로의 볼륨으로 파드에 마운트됩니다. 애플리케이션이 Kubernetes API를 호출할 필요가 없는 경우 애플리케이션의 PodSpec에서 automountServiceAccountToken 속성을 false로 설정하거나 각 네임스페이스의 기본 서비스 어카운트를 패치하여 더 이상 파드에 자동으로 마운트되지 않도록 해야 합니다.</p>		
설정 방법	<p>가. 서비스 어카운트 토큰 자동 마운트 비활성화</p> <p>1) 서비스 어카운트 토큰 자동 마운트 비활성화 여부 확인</p> <pre data-bbox="309 853 1414 1099"> @cloudshell:~ (ethereal-audio-413401) \$ kubectl get serviceaccount default -o yaml apiVersion: v1 automountServiceAccountToken: true kind: ServiceAccount metadata: creationTimestamp: "2024-02-06T01:20:29Z" name: default namespace: default resourceVersion: "9906217" uid: 048801a5-050f-49ce-baa4-c8477584e14f @cloudshell:~ (ethereal-audio-413401) \$ </pre> <p>2) 서비스 어카운트 토큰 자동 마운트 비활성화 (false) 설정 및 확인</p> <pre data-bbox="309 1200 1414 1424"> @cloudshell:~ (ethereal-audio-413401) \$ kubectl patch serviceaccount default -p '{"automountServiceAccountToken": false}' serviceaccount/default patched @cloudshell:~ (ethereal-audio-413401) \$ kubectl get serviceaccount default -o yaml apiVersion: v1 automountServiceAccountToken: false kind: ServiceAccount metadata: creationTimestamp: "2024-02-06T01:20:29Z" name: default namespace: default resourceVersion: "9912438" uid: 048801a5-050f-49ce-baa4-c8477584e14f @cloudshell:~ (ethereal-audio-413401) \$ </pre>		
진단 기준	<p>양호기준 : 네임스페이스 또는 서비스 어카운트 설정 내 automountServiceAccountToken 값이 False로 설정된 경우</p> <p>취약기준 : 네임스페이스 또는 서비스 어카운트 설정 내 automountServiceAccountToken 값이 True로 설정된 경우</p>		
비고			

1.12 GKE 불필요한 익명 접근 관리

분류	계정 관리	중요도	상
항목명	GKE 불필요한 익명 접근 관리		
<p>항목 설명</p>	<p>클라우드 환경 내에서는 모든 API 및 리소스 작업 시에 대해 익명 사용자의 접근을 비활성화하여 이용해야 합니다. 쿠버네티스는 기본 제공 사용자 "system:anonymous"s 에 대한 RoleBinding 또는 ClusterRoleBinding을 생성하여 익명 액세스 권한을 부여할 수 있습니다. kubectl rbac-tool 또는 rbac-lookup 도구를 사용하여 "system:anonymous" 사용자가 Cluster에 대해 갖는 권한을 조회 할 수 있으며 "system:public-info-viewer" 권한 외의 ClusterRole 또는 모든 역할은 "system:anonymous" 또는 "system:unauthenticated" 그룹에 바인딩되지 않도록 해야합니다.</p> <p>※ 특정 API에서 익명 액세스를 활성화해야 하는 경우 익명 사용자가 특정 API만 액세스할 수 있도록 하고 인증 없이 해당 API를 노출해도 Cluster가 취약해지지 않도록 해야 하며 정보보안팀 확인 또는 담당자 승인을 득한 후 사용하시기 권고 드립니다.</p> <p>※ cluster-admin 액세스 구성 오류를 악용하는 대규모 멀웨어 공격으로부터 Cluster를 보호하기 위해 버전 1.28 이상이 실행되는 GKE Cluster는 cluster-admin ClusterRole을 system:anonymous 사용자 또는 system:unauthenticated 또는 system:authenticated 그룹에 바인딩하는 것을 허용하지 않습니다.</p>		
<p>설정 방법</p>	<p>가. GKE 내 불필요한 익명 접근 삭제</p> <p>1) kubectl 명령을 통한 불필요 익명 사용자 조회 (system:anonymous unauthenticated)</p> <pre>kubectl rbac-tool lookup grep -P 'system:(anonymous) (unauthenticated)'</pre>  <p>2) 불필요 익명 접근 Cluster 연결 정책 삭제 (system:discovery 및 system:basic-user)</p>		

```
# Please edit the object below. Lines beginning with a '#' will be ignored,
# and an empty file will abort the edit. If an error occurs while saving this file will be
# reopened with the relevant failures.
#
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  annotations:
    rbac.authorization.kubernetes.io/autoupdate: "true"
  creationTimestamp: "2024-02-06T01:20:21Z"
  labels:
    kubernetes.io/bootstrapping: rbac-defaults
    name: system:discovery
  resourceVersion: "133"
  uid: 839c2d42-d1b6-4615-a1da-a11cd66b2c89
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: system:discovery
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:unauthenticated
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:anonymous
```

```
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:authenticated
```

```
# Please edit the object below. Lines beginning with a '#' will be ignored,
# and an empty file will abort the edit. If an error occurs while saving this file will be
# reopened with the relevant failures.
#
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  annotations:
    rbac.authorization.kubernetes.io/autoupdate: "true"
  creationTimestamp: "2024-02-06T01:20:21Z"
  labels:
    kubernetes.io/bootstrapping: rbac-defaults
    name: system:basic-user
  resourceVersion: "133"
  uid: 62c56fc5-c5ff-488d-bcb4-bcba5bb5e021
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: system:basic-user
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:unauthenticated
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:anonymous
```

```
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:authenticated
```

3) 불필요 익명 접근 정책 삭제 결과 확인

```
CLOUD SHELL
터미널 (ethereal-audio-413401) x +
kubectl -n kube-system get clusterrolebinding | grep -P 'system:(anonymous|unauthenticated)'
system:unauthenticated | Group | ClusterRole | system:public-info-viewer
system:anonymous | Group | ClusterRole | system:public-info-viewer
```

진단 기준	양호기준 : ClusterRole 에 system:anonymous unauthenticated 그룹이 바인딩 되어있지 않는 경우
	취약기준 : ClusterRole 에 system:anonymous unauthenticated 그룹이 바인딩 되어 있는 경우
비고	※ Cluster 내 "system:public-info-viewer" ClusterRole 정책은 진단 기준 제외

2. 권한 관리

2.1 인스턴스 서비스 정책 관리

분류	권한 관리	중요도	상														
항목명	인스턴스 서비스 정책 관리																
항목 설명	<p>GCP(Google Cloud Platform)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 인스턴스 서비스 별 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.</p> <p>※ 인스턴스 서비스 구분</p> <table border="1"> <thead> <tr> <th>서비스 구분</th> <th>서비스 상세</th> </tr> </thead> <tbody> <tr> <td>Compute Engine</td> <td>Compute Engine 인스턴스에서는 Google에서 제공하는 Linux 및 Windows Server용 공개 이미지뿐만 아니라 사용자가 만들거나 기존 시스템에서 가져올 수 있는 비공개 커스텀 이미지를 실행할 수 있습니다.</td> </tr> <tr> <td>Cloud SQL</td> <td>Cloud SQL은 로컬 MySQL, PostgreSQL, SQL Server 데이터베이스의 클라우드 기반으로 제공되는 서비스로 Cloud SQL 인스턴스는 호스트 Google Cloud 서버에서 실행되는 가상 머신(VM)으로 구동할 수 있습니다.</td> </tr> <tr> <td>Cloud Storage</td> <td>Cloud Storage는 Google Cloud에 객체를 저장하는 서비스입니다. 객체는 모든 형식의 파일로 구성된 변경할 수 없는 데이터 조각입니다. 객체를 버킷이라는 컨테이너에 저장합니다. 모든 버킷은 프로젝트와 연결되며 프로젝트를 조직 아래에서 그룹화할 수 있습니다. Google Cloud의 각 프로젝트, 버킷, 객체는 Compute Engine 인스턴스와 같은 Google Cloud의 리소스입니다.</td> </tr> <tr> <td>MemoryStore</td> <td>Memorystore for Memcached는 Google Cloud의 확장성이 뛰어난 완전 관리형 Memcached 서비스와 Memorystore for Redis는 Redis 인메모리 데이터 저장소를 통해 완전 관리형 서비스를 제공하여 밀리초 이하로 데이터에 액세스할 수 있는 애플리케이션 캐시를 빌드할 수 있는 서비스로 나뉘어집니다.</td> </tr> <tr> <td>FileStore</td> <td>Filestore 인스턴스는 Compute Engine 가상 머신(VM) 인스턴스 또는 Google Kubernetes Engine Cluster에서 실행되는 애플리케이션에서 사용할 수 있는 Google Cloud의 완전 관리형 NFS 파일 서버입니다.</td> </tr> <tr> <td>Cloud Bigtable</td> <td>Cloud Bigtable은 Google의 완전 관리형 NoSQL 빅데이터 데이터베이스 서비스입니다. Google 검색, 애널리틱스, 지도, Gmail 등 Google의 수많은 핵심 서비스를 운영하는 데이터베이스입니다.</td> </tr> </tbody> </table>			서비스 구분	서비스 상세	Compute Engine	Compute Engine 인스턴스에서는 Google에서 제공하는 Linux 및 Windows Server용 공개 이미지뿐만 아니라 사용자가 만들거나 기존 시스템에서 가져올 수 있는 비공개 커스텀 이미지를 실행할 수 있습니다.	Cloud SQL	Cloud SQL은 로컬 MySQL, PostgreSQL, SQL Server 데이터베이스의 클라우드 기반으로 제공되는 서비스로 Cloud SQL 인스턴스는 호스트 Google Cloud 서버에서 실행되는 가상 머신(VM)으로 구동할 수 있습니다.	Cloud Storage	Cloud Storage는 Google Cloud에 객체를 저장하는 서비스입니다. 객체는 모든 형식의 파일로 구성된 변경할 수 없는 데이터 조각입니다. 객체를 버킷이라는 컨테이너에 저장합니다. 모든 버킷은 프로젝트와 연결되며 프로젝트를 조직 아래에서 그룹화할 수 있습니다. Google Cloud의 각 프로젝트, 버킷, 객체는 Compute Engine 인스턴스와 같은 Google Cloud의 리소스입니다.	MemoryStore	Memorystore for Memcached는 Google Cloud의 확장성이 뛰어난 완전 관리형 Memcached 서비스와 Memorystore for Redis는 Redis 인메모리 데이터 저장소를 통해 완전 관리형 서비스를 제공하여 밀리초 이하로 데이터에 액세스할 수 있는 애플리케이션 캐시를 빌드할 수 있는 서비스로 나뉘어집니다.	FileStore	Filestore 인스턴스는 Compute Engine 가상 머신(VM) 인스턴스 또는 Google Kubernetes Engine Cluster에서 실행되는 애플리케이션에서 사용할 수 있는 Google Cloud의 완전 관리형 NFS 파일 서버입니다.	Cloud Bigtable	Cloud Bigtable은 Google의 완전 관리형 NoSQL 빅데이터 데이터베이스 서비스입니다. Google 검색, 애널리틱스, 지도, Gmail 등 Google의 수많은 핵심 서비스를 운영하는 데이터베이스입니다.
	서비스 구분	서비스 상세															
	Compute Engine	Compute Engine 인스턴스에서는 Google에서 제공하는 Linux 및 Windows Server용 공개 이미지뿐만 아니라 사용자가 만들거나 기존 시스템에서 가져올 수 있는 비공개 커스텀 이미지를 실행할 수 있습니다.															
	Cloud SQL	Cloud SQL은 로컬 MySQL, PostgreSQL, SQL Server 데이터베이스의 클라우드 기반으로 제공되는 서비스로 Cloud SQL 인스턴스는 호스트 Google Cloud 서버에서 실행되는 가상 머신(VM)으로 구동할 수 있습니다.															
	Cloud Storage	Cloud Storage는 Google Cloud에 객체를 저장하는 서비스입니다. 객체는 모든 형식의 파일로 구성된 변경할 수 없는 데이터 조각입니다. 객체를 버킷이라는 컨테이너에 저장합니다. 모든 버킷은 프로젝트와 연결되며 프로젝트를 조직 아래에서 그룹화할 수 있습니다. Google Cloud의 각 프로젝트, 버킷, 객체는 Compute Engine 인스턴스와 같은 Google Cloud의 리소스입니다.															
	MemoryStore	Memorystore for Memcached는 Google Cloud의 확장성이 뛰어난 완전 관리형 Memcached 서비스와 Memorystore for Redis는 Redis 인메모리 데이터 저장소를 통해 완전 관리형 서비스를 제공하여 밀리초 이하로 데이터에 액세스할 수 있는 애플리케이션 캐시를 빌드할 수 있는 서비스로 나뉘어집니다.															
	FileStore	Filestore 인스턴스는 Compute Engine 가상 머신(VM) 인스턴스 또는 Google Kubernetes Engine Cluster에서 실행되는 애플리케이션에서 사용할 수 있는 Google Cloud의 완전 관리형 NFS 파일 서버입니다.															
	Cloud Bigtable	Cloud Bigtable은 Google의 완전 관리형 NoSQL 빅데이터 데이터베이스 서비스입니다. Google 검색, 애널리틱스, 지도, Gmail 등 Google의 수많은 핵심 서비스를 운영하는 데이터베이스입니다.															

Cloud Datastore	Datastore 모드의 Firestore는 자동 확장, 고성능, 간편한 애플리케이션 개발을 위해 설계된 NoSQL 문서 데이터베이스입니다.
-----------------	--

※ IAM 역할

IAM 역할 구분	역할 이름	상세설명
기본 역할	뷰어	상태에 영향을 주지 않는 읽기 전용 작업에 대한 권한이 부여됩니다. 예) 기존 리소스 또는 데이터의 조회(수정 제외)가 해당됨
	편집자	모든 뷰어 권한에 더해 기존 리소스 변경과 같이 상태를 변경하는 작업에 대한 권한까지 포함됩니다.
	소유자	모든 편집자 권한 및 다음 작업에 대한 권한이 포함됩니다. - 프로젝트 및 프로젝트 내의 모든 리소스에 대한 역할 및 관리 - 프로젝트에 대한 결제 설정
프로젝트 역할	서비스 계정 행위자	해당 역할은 지원이 중단되었기 때문에 서비스 계정으로 작업을 실행하려면 서비스 계정 사용자 역할을 사용해야 합니다. 서비스 계정 행위자로서 동일한 권한을 효과적으로 제공하려면 서비스 계정 토큰 생성자 권한도 부여해야 합니다.
	브라우저	폴더, 조직, Cloud IAM 을 포함한 프로젝트의 계층구조를 탐색할 수 있는 읽기 액세스입니다. 해당 역할에는 프로젝트의 리소스를 볼 수 있는 권한이 제공되지 않습니다.
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 Datastore	가져오기 및 내보내기를 관리할 수 있는 전체 액세스 권한을 제공합니다.

Cloud Datastore 역할	가져오기 내보내기 관리자	
	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.
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 덮어쓰기 할 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 관리자	객체와 버킷에 대한 전체 제어 권한을 부여합니다.
	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.

Compute Engine 역할	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 계정으로 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 계정으로 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 서브 넷을 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	<p>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.</p> <p>예를 들어, 방화벽과 SSL 인증서를 관리하는 보안 팀과 나머지 네트워킹 리소스를 관리하는 네트워킹팀이 회사에 있는 경우, 네트워킹팀의 그룹에 networkAdmin 역할을 부여하면 됩니다.</p>
Compute 보안 관리자	<p>방화벽 규칙과 SSL 인증서를 생성, 수정, 삭제할 권한이 있습니다.</p> <p>예를 들어, 방화벽과 SSL 인증서를 관리하는 보안 팀과 나머지 네트워킹 리소스를 관리하는 네트워킹팀이 회사에 있는 경우, 보안 팀의 그룹에 securityAdmin 역할을 부여하면 됩니다.</p>
컴퓨팅 이미지 사용자	<p>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.</p>
Compute Storage 관리자	<p>디스크, 이미지, 스냅샷을 생성, 수정, 삭제할 권한이 있습니다.</p> <p>예를 들어, 회사에 이미지 관리 담당자가 있지만 이들에게 프로젝트에 대한 편집자 역할은 주고 싶지 않은 경우, 이들의 계정에 storageAdmin 역할을 부여하면 됩니다.</p>
공유 VPC 관리자	<p>공유 VPC 호스트 프로젝트를 관리할 권한이 있습니다. 구체적으로 프로젝트를 호스팅하고 공유 VPC 서비스 프로젝트를 호스트 프로젝트 네트워크에 연결할 수 있는 권한입니다.</p> <p>조직 관리자만이 이 역할을 조직에 부여할 수 있습니다.</p>
Compute 관리자	<p>모든 Compute Engine 리소스를 관리할 수 있는 전체 권한입니다. 사용자가 서비스 계정으로 실행하도록 구성된 가상 머신 인스턴스를 관리하는 경우에는 roles/iam.serviceAccountUser 역할도 부여해야 합니다.</p>
Compute 뷰어	<p>Compute Engine 리소스를 가져와 나열할 수 있지만 리소스에 저장된 데이터를 읽을 수는 없는 읽기 전용 액세스 권한입니다.</p>

		예를 들어, 이 역할을 부여받은 계정은 모든 디스크를 프로젝트에 목록화할 수 있지만 해당 디스크의 데이터는 전혀 읽을 수 없습니다.
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.

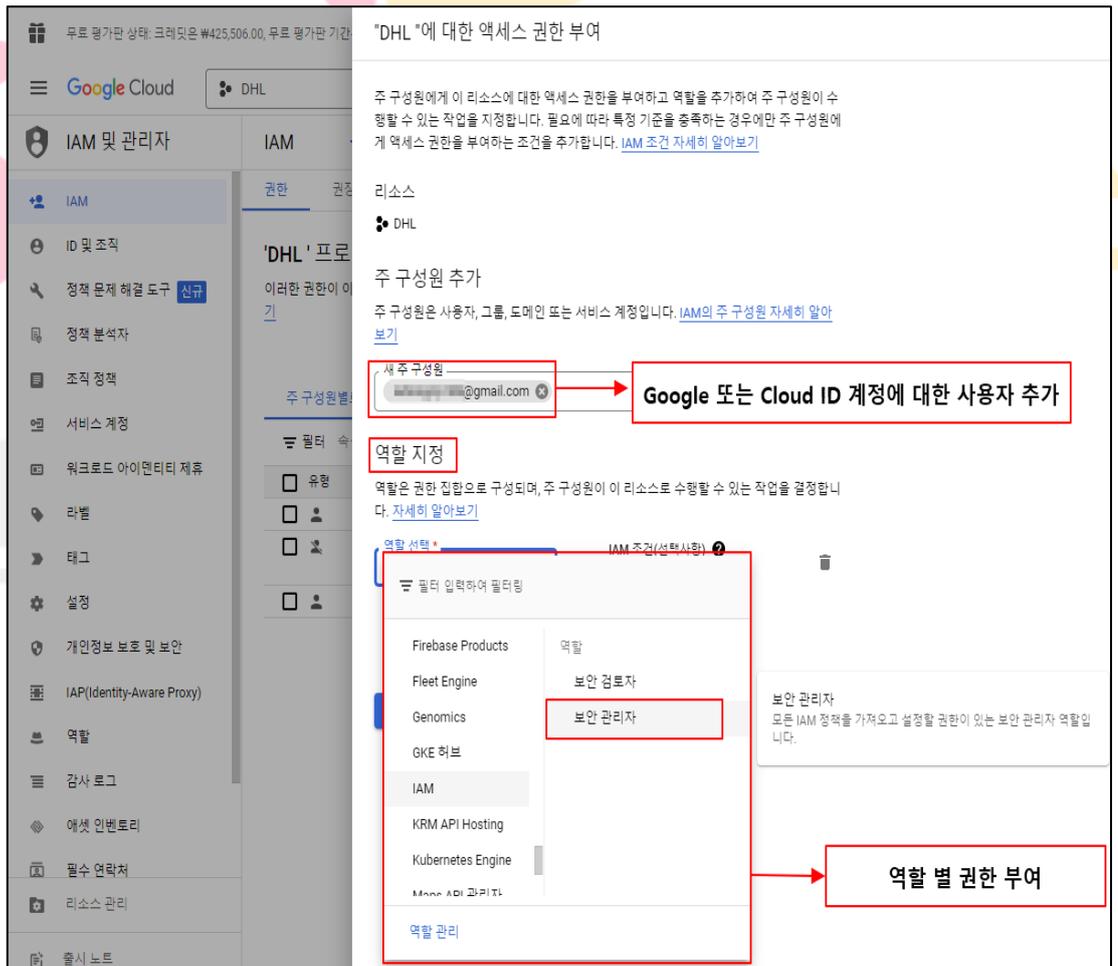
※ Google Cloud에서 제공되는 역할별 정책이 아닌 고객 커스텀 정책을 통한 IAM 권한
관리가 이루어질 경우 고객 커스텀 정책 내 권한에 대해서는 별도 담당자 확인이
필요합니다.

설정
방법

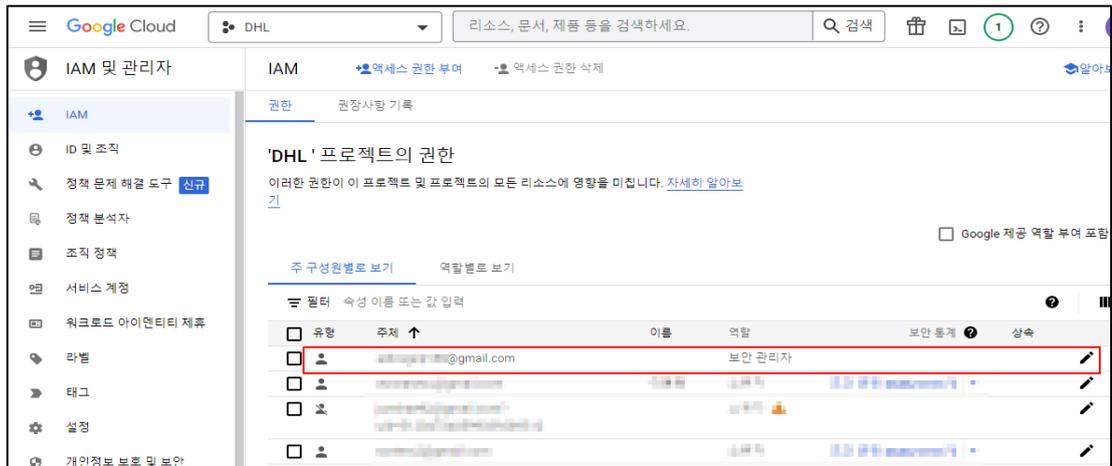
가. Google Cloud 에서 사전 정의된 역할로의 IAM 사용자 계정 생성
1) [IAM 및 관리자] > [IAM] > [추가]



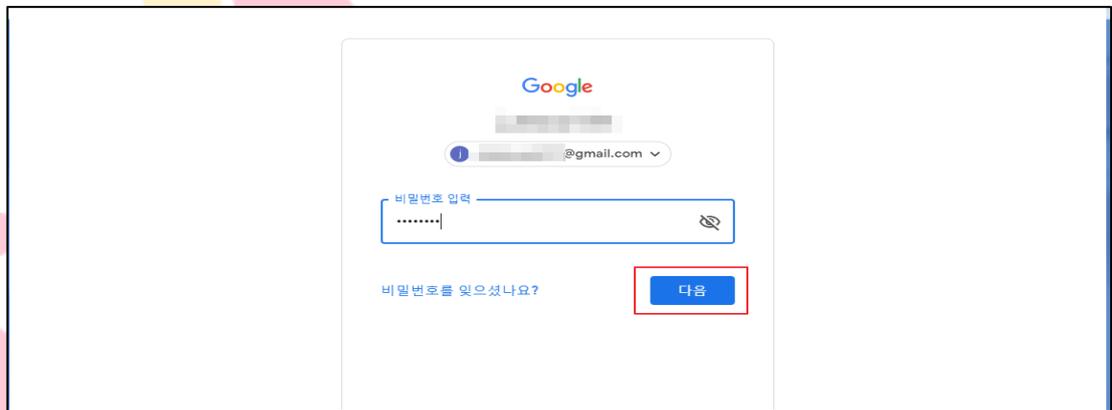
2) 권한을 부여하고자 하는 사용자(Google 또는 Cloud ID 계정) 추가 및 역할별 권한 부여



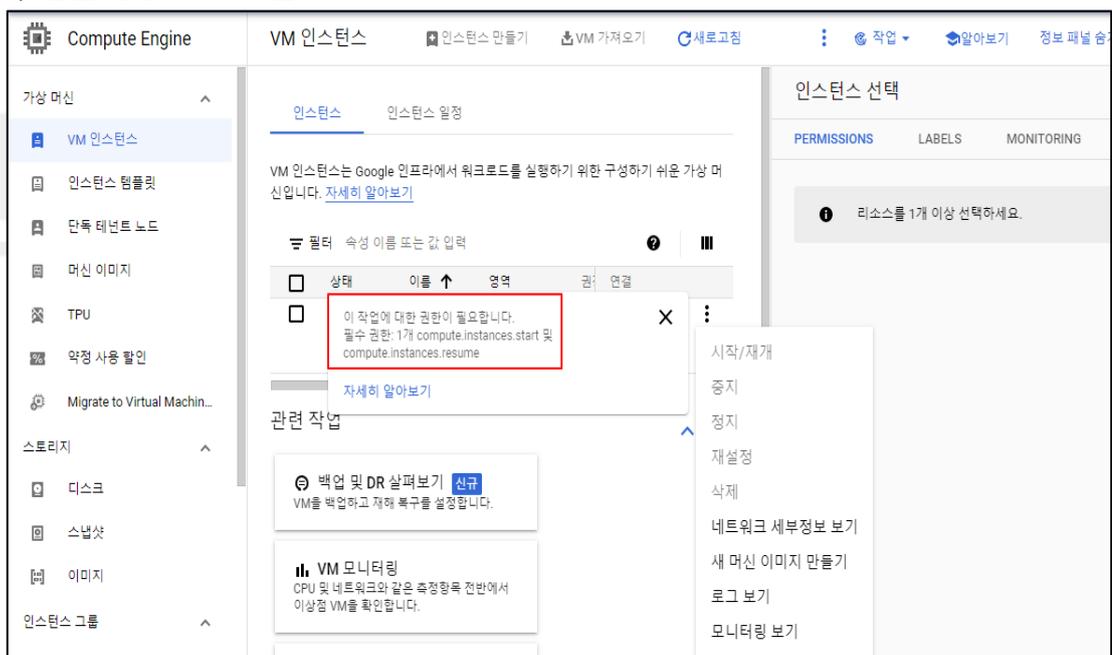
3) 사용자 추가 확인



4) 권한을 부여한 사용자로 Google Cloud Console 로그인 시도



5) 권한 정상 부여 확인

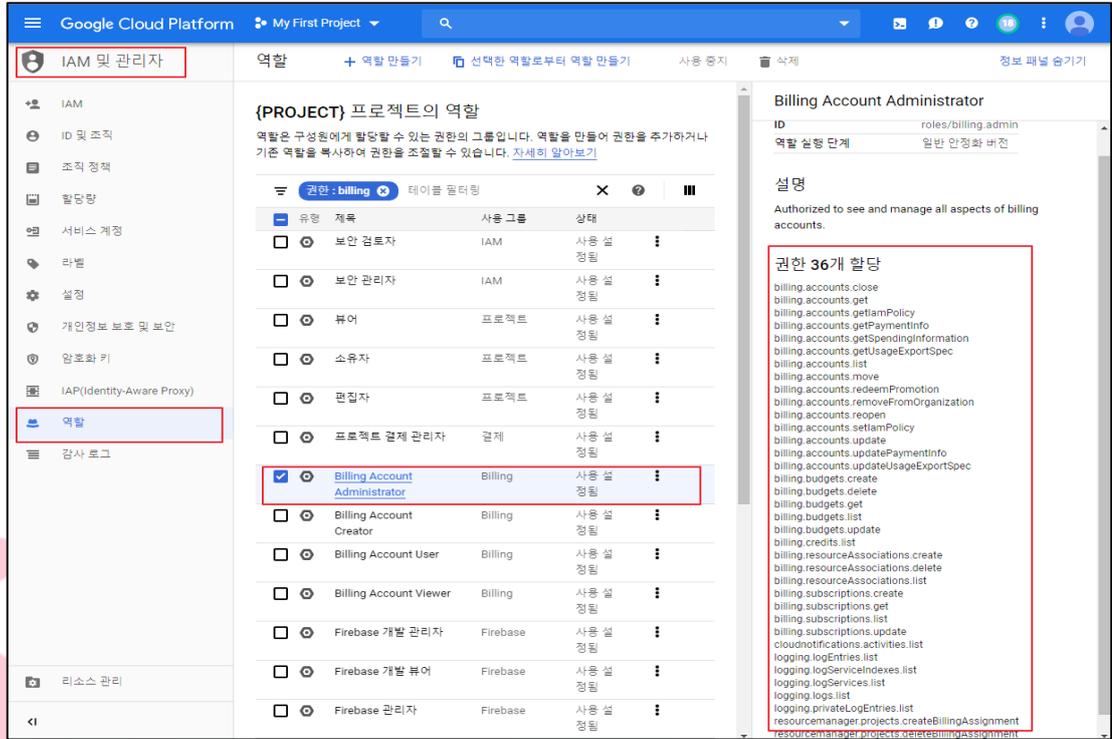


예제 1. 계정 사용 권한이 서비스 역할에 맞게 정의되어 있을 경우

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

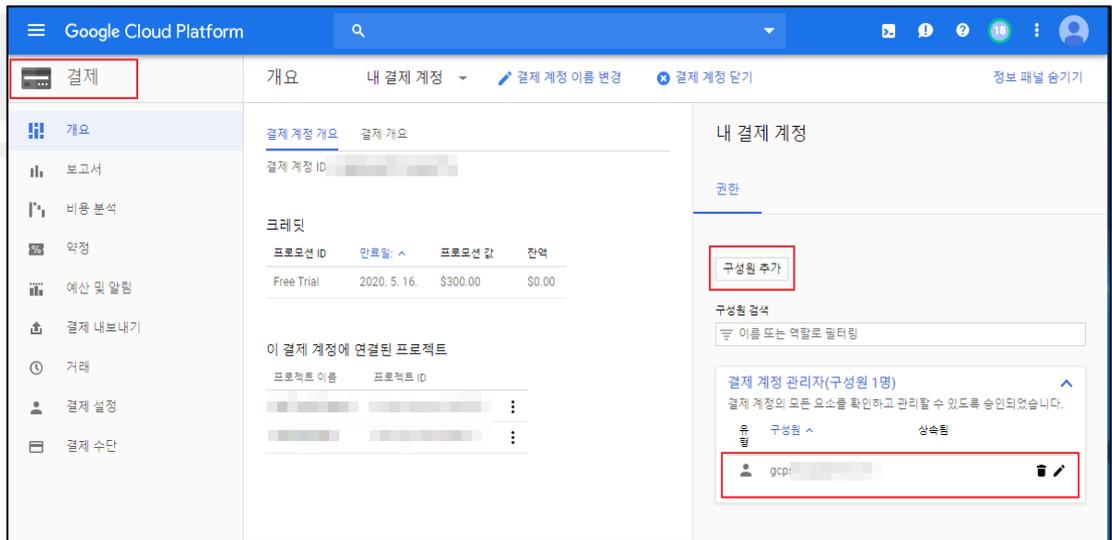
1) [IAM 및 관리자] > [역할]

- '비용 및 재무 관리자' 에게 필요한 역할 및 권한 확인

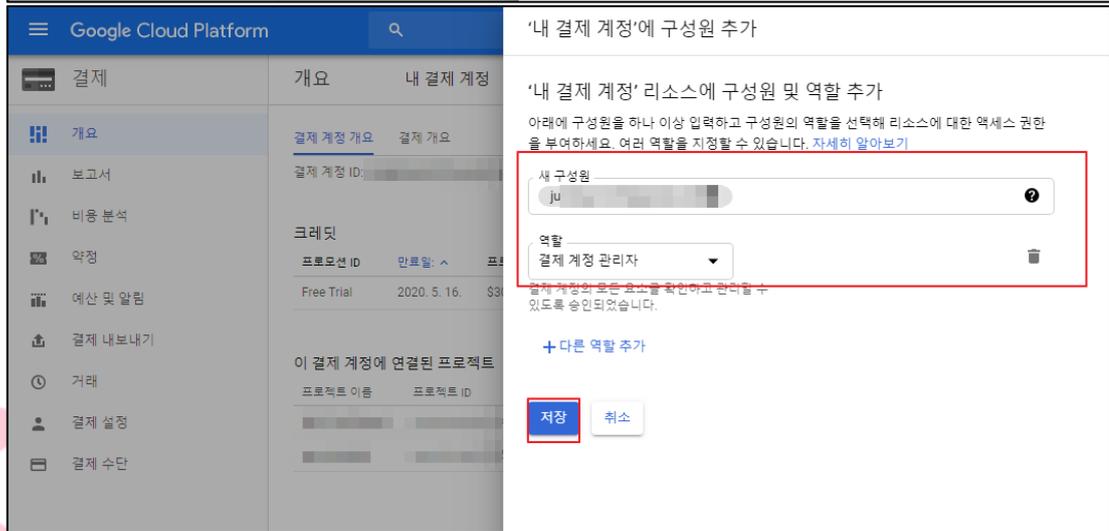
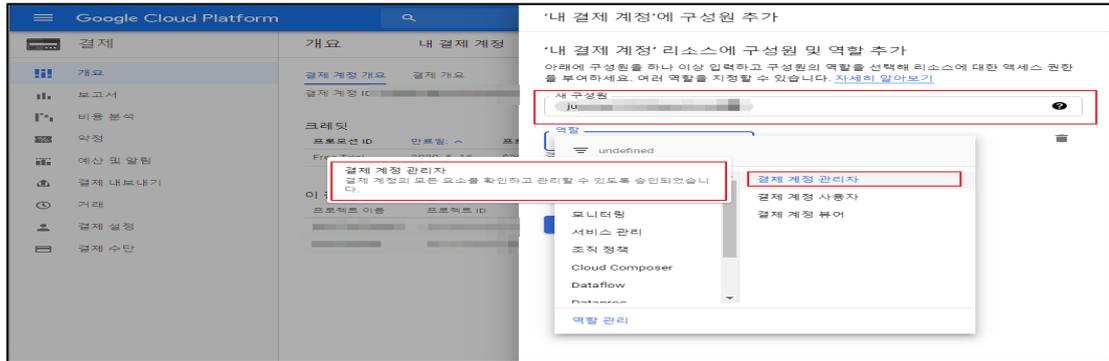


2) [결제] > [구성원 추가]

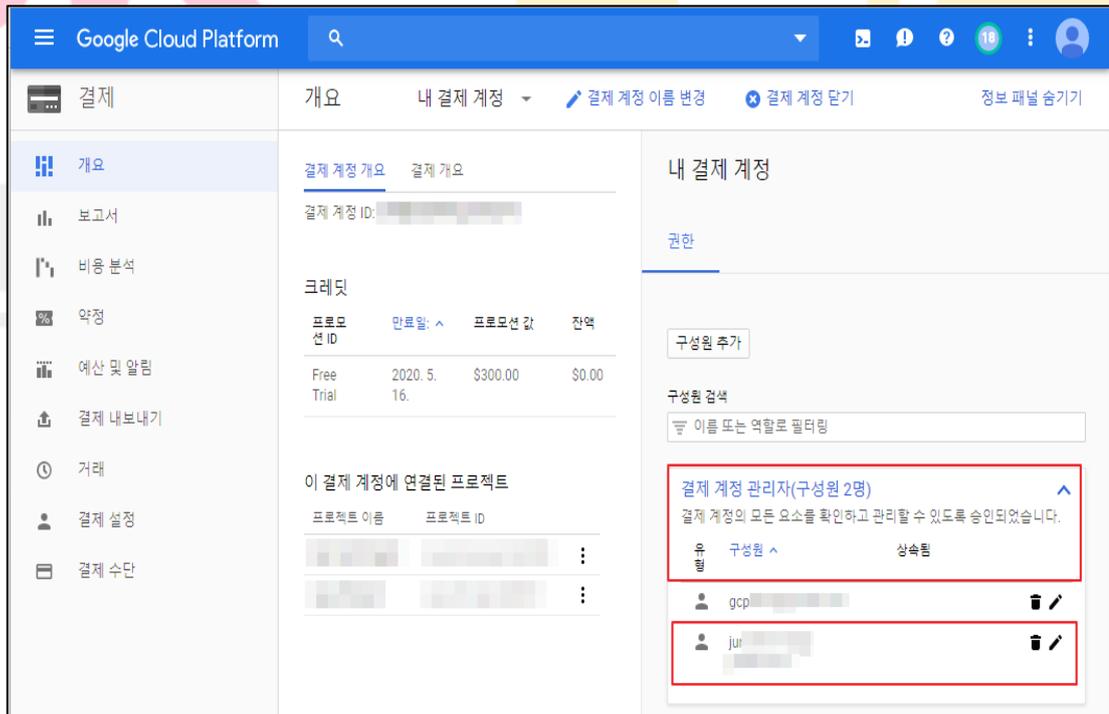
- '비용 및 재무 관리자' 역할 부여를 위한 사용자 추가
- 그림 내 '결제 계정 관리자'의 경우 최고 관리자에 한해서만 권한이 부여되어 있음



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

Google Cloud Platform My First Project

IAM 및 관리자 IAM + 추가 - 삭제

'My First Project' 프로젝트의 권한

이러한 권한이 이 프로젝트 및 프로젝트의 모든 리소스에 영향을 미칩니다. [자세히 알아보기](#)

보기 모드 기준: 구성원 역할

유형: 사용자 테이블 필터링

유형	구성원 ↑	이름	역할	상속
<input type="checkbox"/>	사용자	[Redacted]	탐색자 소스 저장소 리더	
<input type="checkbox"/>	사용자	[Redacted]	소유자	
<input type="checkbox"/>	사용자	[Redacted]	프로젝트 결제 관리자	

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

Google Cloud Platform 'My First Project'에 구성원 추가

'My First Project' 프로젝트에 구성원, 역할 추가

아래에 구성원을 하나 이상 입력하고 구성원의 역할을 선택해 리소스에 대한 액세스 권한을 부여하세요. 여러 역할을 지정할 수 있습니다. [자세히 알아보기](#)

새 구성원: ju... ?

역할: 탐색자
GCP 리소스를 탐색할 수 있는 액세스 권한입니다.

역할: 모니터링 뷰어
모든 모니터링 데이터 및 구성에 대한 정보를 가져오고 나열할 수 있는 읽기 전용 액세스 권한입니다.

+ 다른 역할 추가

저장 취소

7) 추가로 설정한 '비용 및 재무 관리자'의 역할 확인

The screenshot shows the Google Cloud Platform IAM interface. The left sidebar lists various IAM-related options, with 'IAM' selected. The main content area is titled 'IAM' and shows the role assignment for 'My First Project'. A table lists the assigned roles, with the role '비용 및 재무 관리자' (Cost and Billing Manager) highlighted in red. The role is assigned to a user with the email 'ju...' and the role '비용 및 재무 관리자' (Cost and Billing Manager).

유형	구성원	이름	역할	상속
<input type="checkbox"/>	<input type="checkbox"/>		탐색자 소스 저장소 리더	
<input type="checkbox"/>	<input type="checkbox"/>		소유자	
<input type="checkbox"/>	<input type="checkbox"/>		프로젝트 결제 관리자	
<input type="checkbox"/>	<input type="checkbox"/>	ju	탐색자 모니터링 뷰어	

8) 역할 할당 후 '비용 및 재무 관리자' 계정으로 로그인 시도

The screenshot shows the Google login page. The email address 'ju...' is entered in the search bar. Below the search bar, there is a password input field labeled '비밀번호 입력' (Enter password). A blue button labeled '다음' (Next) is visible. A red box highlights the text '비용 및 재무 관리자' (Cost and Billing Manager) below the login form.

"비용 및 재무 관리자" 계정으로 로그인 시도

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

이 프로젝트의 인스턴스를 볼 수 있는 권한이 없습니다.

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

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

보고서 내 결제 계정 인쇄 필터 표시

종류	금액	변화
(총 비용)	US\$108.11	↑ -1,081,200%
(예상 총 비용)	US\$153.45	↑ -1,534,600%

역할 및 권한을 할당받은 서비스(EX 결제)에 대해 서비스 접근 및 이용 가능 확인

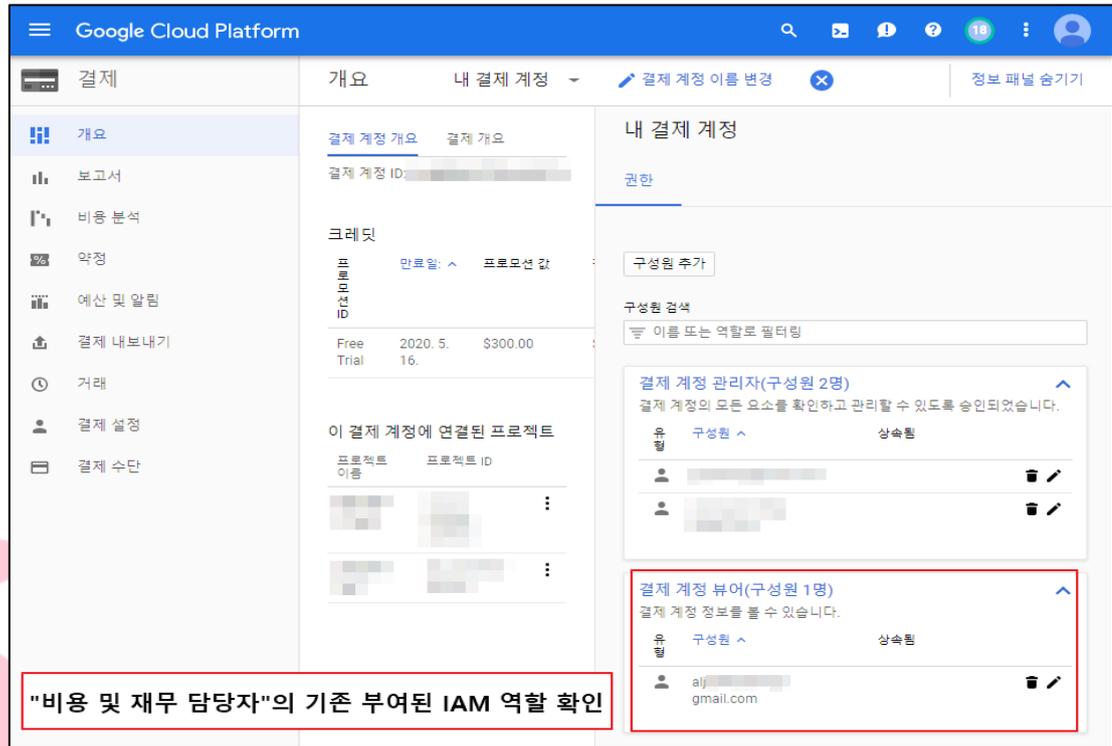
비용 추세

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]

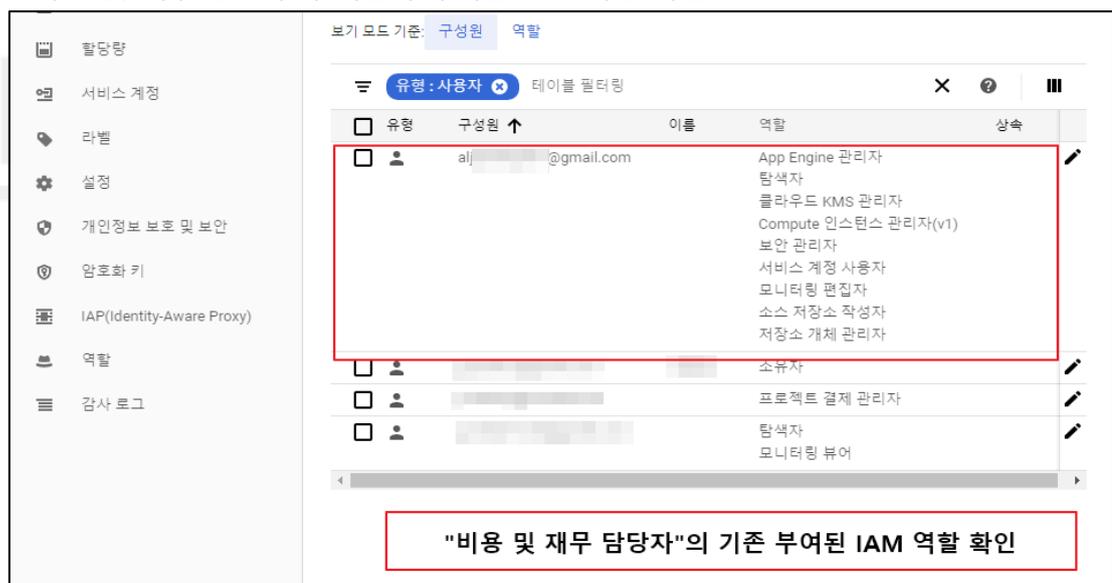
- '비용 및 재무 담당자' 계정 및 사용자 역할 권한 확인



"비용 및 재무 담당자"의 기존 부여된 IAM 역할 확인

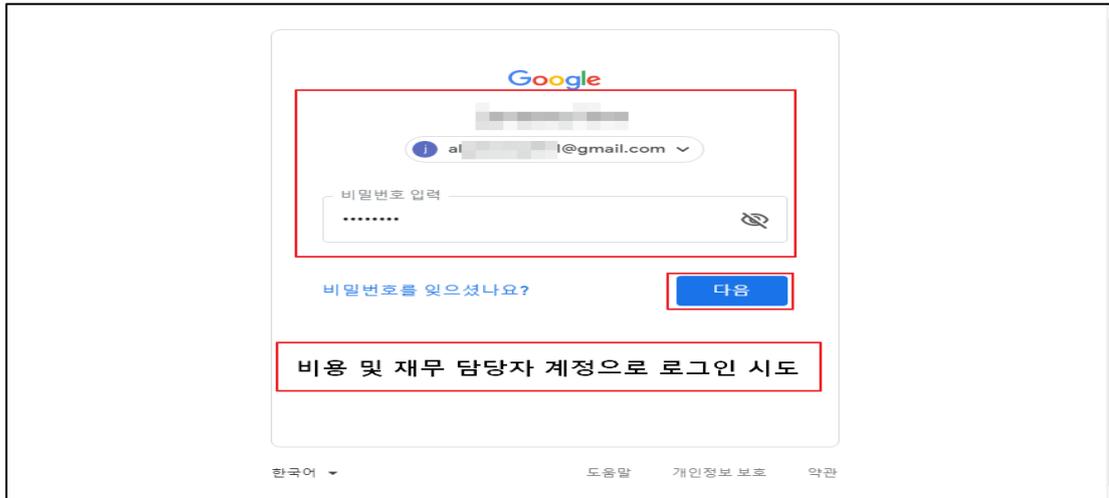
2) [IAM 및 관리자] > [IAM]

- '비용 및 재무 담당자'의 기존에 부여된 IAM 역할 확인



"비용 및 재무 담당자"의 기존 부여된 IAM 역할 확인

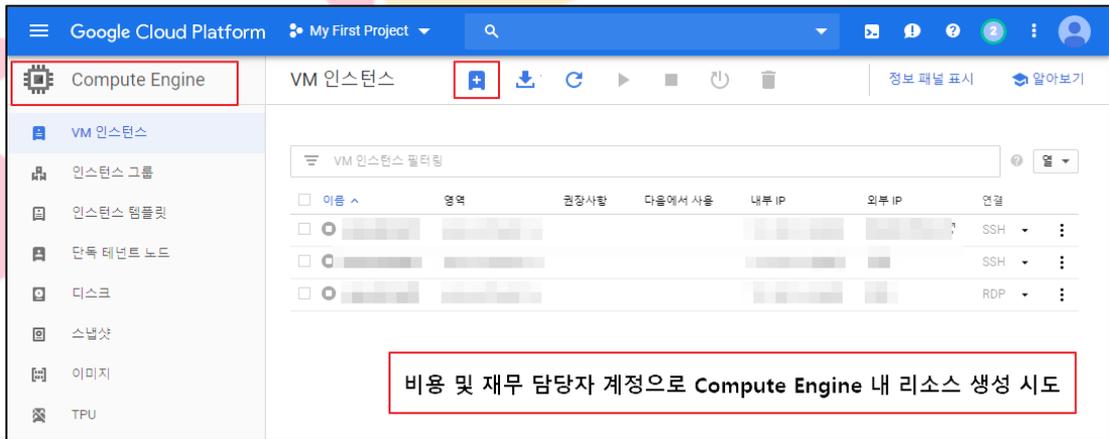
3) '비용 및 재무 담당자' 계정으로 로그인 시도



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)



Google Cloud Platform My First Project

← 인스턴스 만들기

VM 인스턴스를 만들려면 옵션 중 하나를 선택하세요.

- 새 VM 인스턴스**
VM 인스턴스 하나를 처음부터 만듭니다.
- 템플릿에서 VM 인스턴스 만들기**
기존 템플릿에서 VM 인스턴스 하나를 만듭니다.
- Marketplace**
VM 인스턴스에 바로 사용할 수 있는 솔루션을 배포합니다.

이름 ?
instance-1

리전 ? us-central1(아이오와) **영역** ? us-central1-a

머신 구성

머신 계열
일반 용도
일반적인 작업 부하에 적합한 머신 유형이며 가격 및 유연성을 위해 최적화되었습니다.

세대
1
Skylake CPU 플랫폼 또는 이전 버전의 플랫폼에서 제공

머신 유형
n1-standard-1(vCPU 1개, 3.75GB 메모리)

	vCPU	메모리
	1	3.75GB

∨ CPU 플랫폼 및 GPU

컨테이너 ?
 이 VM 인스턴스에 컨테이너 이미지를 배포합니다. 자세히 알아보기

부팅 디스크 ?
 새로운 10GB 표준 영구 디스크 이미지
Debian GNU/Linux 9 (stretch) [변경]

ID 및 API 액세스 ?

서비스 계정 ?
Compute Engine default service account

액세스 범위 ?
 기본 액세스 허용
 모든 Cloud API에 대한 전체 액세스 허용
 각 API에 액세스 설정

방화벽 ?
태그 및 방화벽 규칙을 추가하여 인터넷에서 특정 네트워크 트래픽을 허용합니다.
 HTTP 트래픽 허용
 HTTPS 트래픽 허용

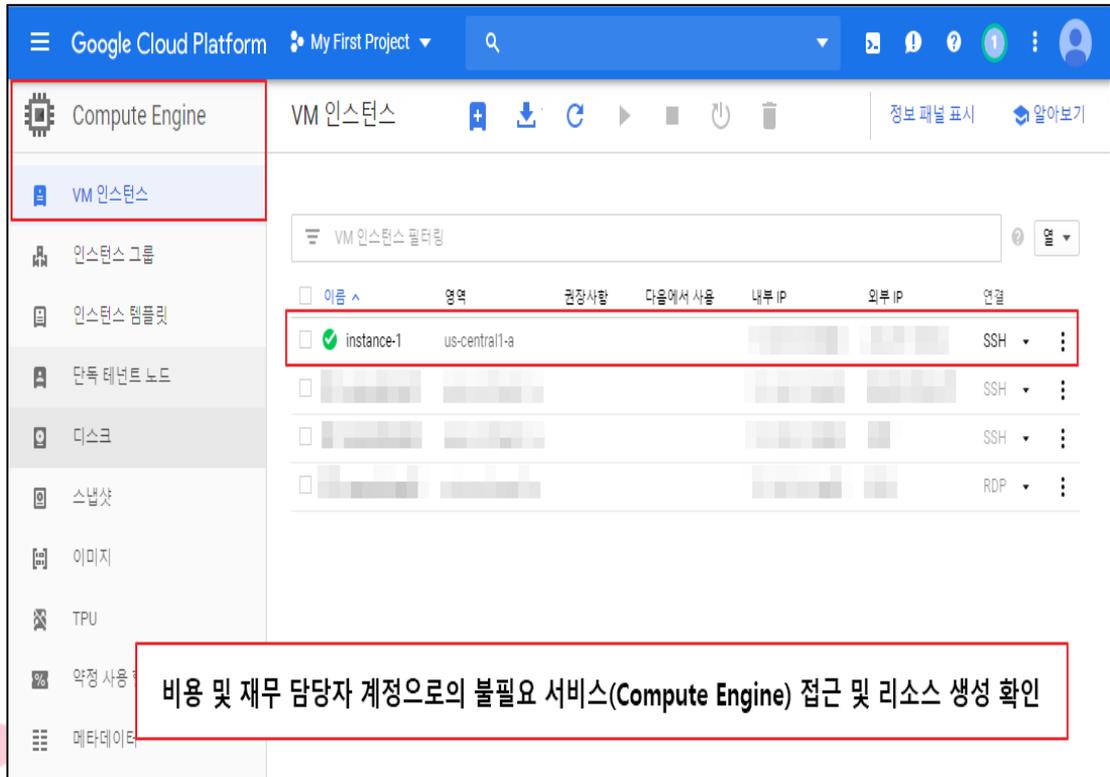
∨ 관리, 보안, 디스크, 네트워킹, 단독 임대

이 인스턴스의 요금이 청구됩니다. [Compute Engine 가격 책정](#)

만들기 취소

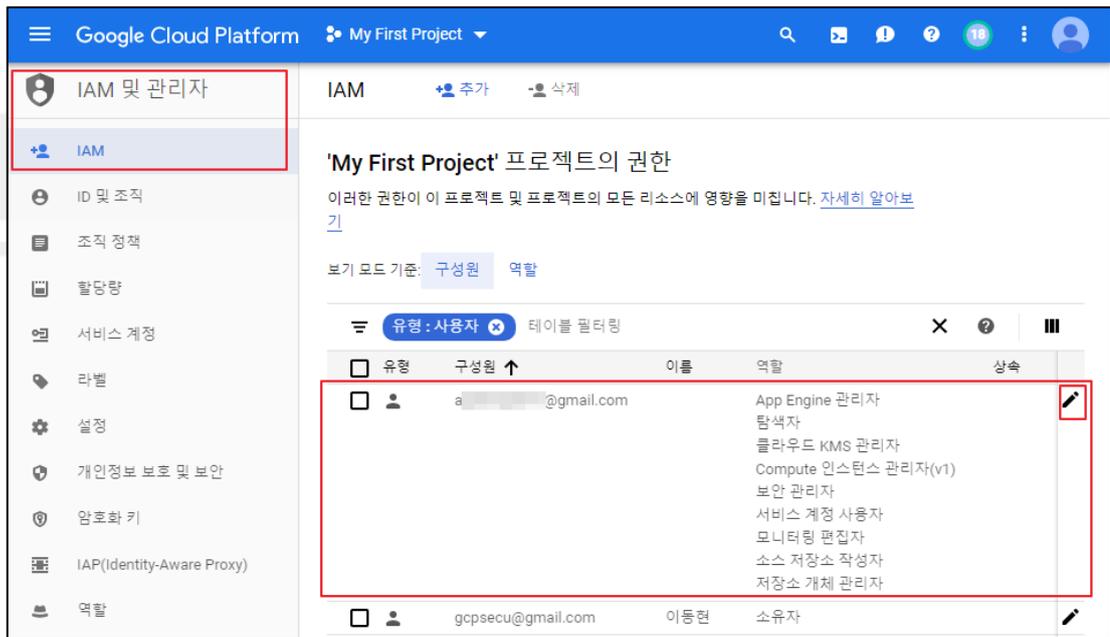
동등한 REST 또는 명령줄

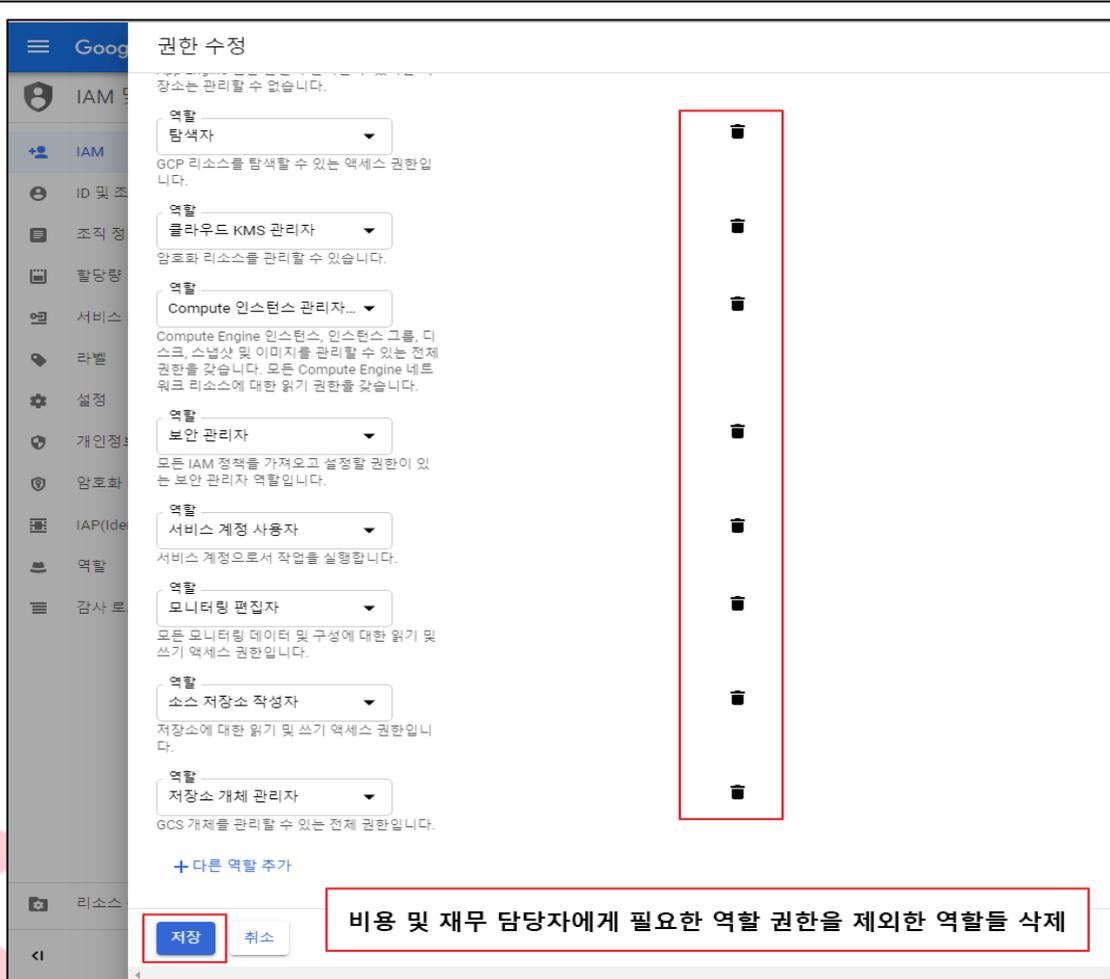
5) 담당 역할(비용 및 재무 담당자) 외 Google Cloud 내 서비스 이용 시도 ②
 - 임의의 VM 인스턴스(instance-1) 생성 완료



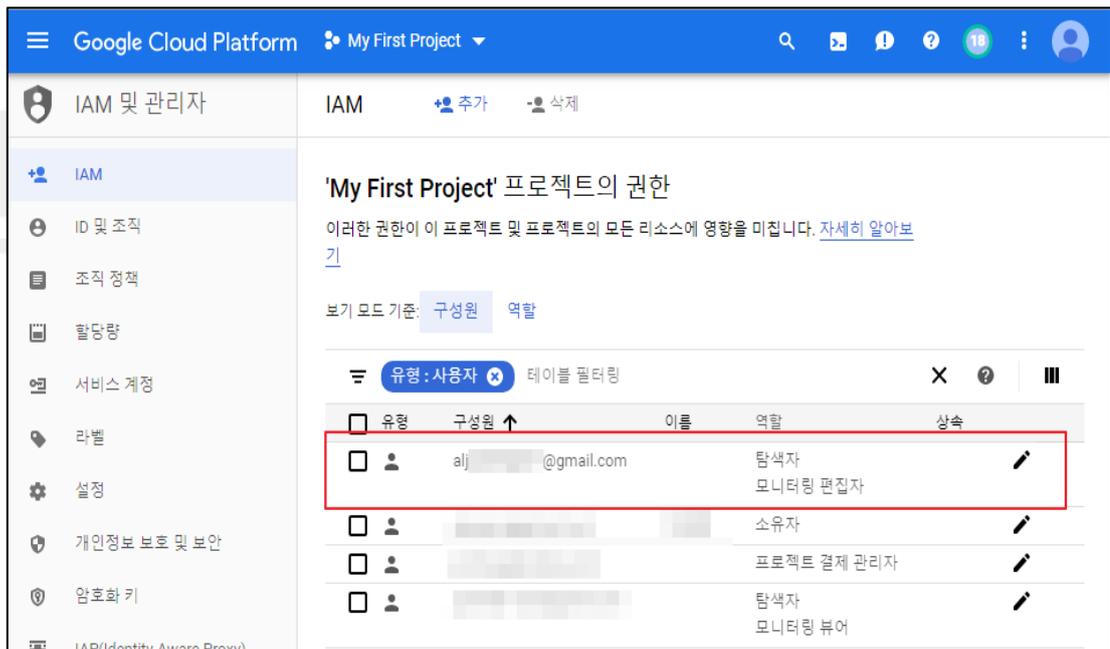
6) [IAM 및 관리자] > [IAM] > [사용자 계정 역할 권한 수정]

- '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)

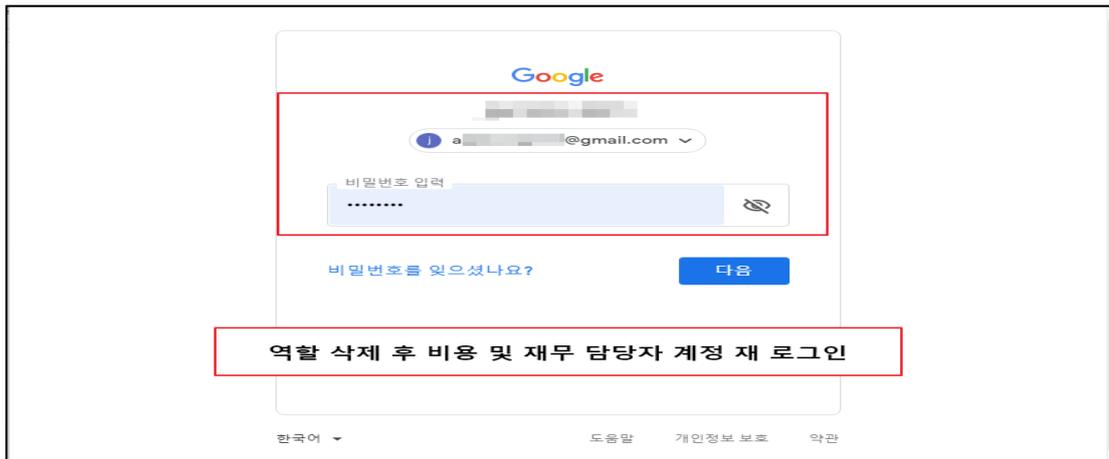




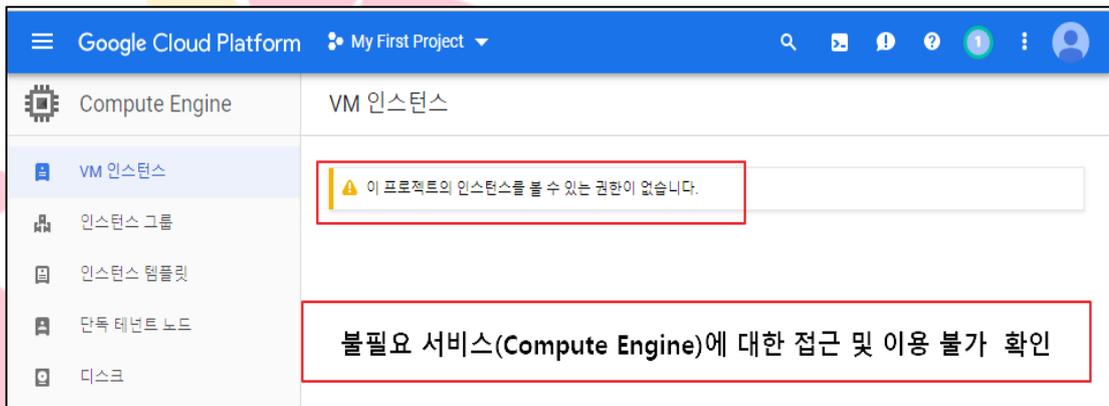
7) '비용 및 재무 담당자' 테스트 계정 내 담당 서비스(비용 및 재무 관리)에 필요한 최소 권한만 할당됨을 확인



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



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.

진단 기준

양호기준
: 인스턴스 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있을 경우

취약기준
: 인스턴스 서비스 IAM 사용 권한이 각각 서비스 역할에 맞지 설정되어 있지 않을 경우

비고

2.2 네트워크 서비스 정책 관리

분류	권한 관리	중요도	상																		
항목명	네트워크 서비스 정책 관리																				
항목 설명	<p>GCP(Google Cloud Platform)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 네트워크 서비스 별 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.</p> <p>※ 네트워크 서비스 구분</p> <table border="1"> <thead> <tr> <th>서비스 구분</th> <th>서비스 상세</th> </tr> </thead> <tbody> <tr> <td>VPC 네트워크</td> <td>Google Cloud Virtual 프라이빗 Cloud(VPC)는 Compute Engine 가상 머신(VM) 인스턴스, Google Kubernetes Engine(GKE) 컨테이너, App Engine 가변형 환경에 네트워킹 기능을 제공합니다. VPC는 클라우드 기반 서비스에 대해 확장 가능하고 유연한 전역 네트워킹을 제공하는 서비스입니다.</td> </tr> <tr> <td>Cloud Load Balancing</td> <td>부하 분산기는 애플리케이션의 여러 인스턴스에 사용자 트래픽을 분산합니다. 부하 분산은 부하를 분산시켜 애플리케이션에 성능 문제가 발생할 위험을 줄여주는 서비스입니다.</td> </tr> <tr> <td>Cloud DNS</td> <td>DNS는 IP 주소 및 기타 데이터를 저장하고 이름별로 조회할 수 있는 계층형 분산 데이터베이스입니다. Cloud DNS를 사용하면 자체 DNS 서버와 소프트웨어 관리 부담 없이 DNS에 영역 및 레코드를 게시할 수 있는 서비스입니다.</td> </tr> <tr> <td>Cloud CDN</td> <td>Cloud CDN은 전역 외부 HTTP(S) 부하 분산기 또는 전역 외부 HTTP(S) 부하 분산기(기본)를 통해 사용자에게 콘텐츠를 제공하는 서비스입니다.</td> </tr> <tr> <td>Cloud NAT</td> <td>Cloud NAT는 Google Cloud용 완전 관리형 소프트웨어 정의 네트워크 주소 변환 지원을 제공하는 서비스입니다.</td> </tr> <tr> <td>VPN</td> <td>Cloud VPN은 IPsec VPN 터널을 통해 피어 네트워크를 Google 네트워크로 안전하게 확장할 수 있는 서비스입니다.</td> </tr> <tr> <td>Cloud Router</td> <td>Cloud Router를 사용하면 경계 게이트웨이 프로토콜(BGP)을 통해 Virtual 프라이빗 Cloud(VPC) 네트워크와 피어 네트워크 간에 경로를 동적으로 교환할 수 있는 서비스입니다.</td> </tr> <tr> <td>방화벽</td> <td>VPC 방화벽 규칙을 사용하면 지정한 구성을 기준으로 가상 머신(VM) 인스턴스 간의 연결을 허용하거나 거부할 수 있는 서비스입니다.</td> </tr> </tbody> </table> <p>※ IAM 역할</p>			서비스 구분	서비스 상세	VPC 네트워크	Google Cloud Virtual 프라이빗 Cloud(VPC)는 Compute Engine 가상 머신(VM) 인스턴스, Google Kubernetes Engine(GKE) 컨테이너, App Engine 가변형 환경에 네트워킹 기능을 제공합니다. VPC는 클라우드 기반 서비스에 대해 확장 가능하고 유연한 전역 네트워킹을 제공하는 서비스입니다.	Cloud Load Balancing	부하 분산기는 애플리케이션의 여러 인스턴스에 사용자 트래픽을 분산합니다. 부하 분산은 부하를 분산시켜 애플리케이션에 성능 문제가 발생할 위험을 줄여주는 서비스입니다.	Cloud DNS	DNS는 IP 주소 및 기타 데이터를 저장하고 이름별로 조회할 수 있는 계층형 분산 데이터베이스입니다. Cloud DNS를 사용하면 자체 DNS 서버와 소프트웨어 관리 부담 없이 DNS에 영역 및 레코드를 게시할 수 있는 서비스입니다.	Cloud CDN	Cloud CDN은 전역 외부 HTTP(S) 부하 분산기 또는 전역 외부 HTTP(S) 부하 분산기(기본)를 통해 사용자에게 콘텐츠를 제공하는 서비스입니다.	Cloud NAT	Cloud NAT는 Google Cloud용 완전 관리형 소프트웨어 정의 네트워크 주소 변환 지원을 제공하는 서비스입니다.	VPN	Cloud VPN은 IPsec VPN 터널을 통해 피어 네트워크를 Google 네트워크로 안전하게 확장할 수 있는 서비스입니다.	Cloud Router	Cloud Router를 사용하면 경계 게이트웨이 프로토콜(BGP)을 통해 Virtual 프라이빗 Cloud(VPC) 네트워크와 피어 네트워크 간에 경로를 동적으로 교환할 수 있는 서비스입니다.	방화벽	VPC 방화벽 규칙을 사용하면 지정한 구성을 기준으로 가상 머신(VM) 인스턴스 간의 연결을 허용하거나 거부할 수 있는 서비스입니다.
	서비스 구분	서비스 상세																			
	VPC 네트워크	Google Cloud Virtual 프라이빗 Cloud(VPC)는 Compute Engine 가상 머신(VM) 인스턴스, Google Kubernetes Engine(GKE) 컨테이너, App Engine 가변형 환경에 네트워킹 기능을 제공합니다. VPC는 클라우드 기반 서비스에 대해 확장 가능하고 유연한 전역 네트워킹을 제공하는 서비스입니다.																			
	Cloud Load Balancing	부하 분산기는 애플리케이션의 여러 인스턴스에 사용자 트래픽을 분산합니다. 부하 분산은 부하를 분산시켜 애플리케이션에 성능 문제가 발생할 위험을 줄여주는 서비스입니다.																			
	Cloud DNS	DNS는 IP 주소 및 기타 데이터를 저장하고 이름별로 조회할 수 있는 계층형 분산 데이터베이스입니다. Cloud DNS를 사용하면 자체 DNS 서버와 소프트웨어 관리 부담 없이 DNS에 영역 및 레코드를 게시할 수 있는 서비스입니다.																			
	Cloud CDN	Cloud CDN은 전역 외부 HTTP(S) 부하 분산기 또는 전역 외부 HTTP(S) 부하 분산기(기본)를 통해 사용자에게 콘텐츠를 제공하는 서비스입니다.																			
	Cloud NAT	Cloud NAT는 Google Cloud용 완전 관리형 소프트웨어 정의 네트워크 주소 변환 지원을 제공하는 서비스입니다.																			
	VPN	Cloud VPN은 IPsec VPN 터널을 통해 피어 네트워크를 Google 네트워크로 안전하게 확장할 수 있는 서비스입니다.																			
	Cloud Router	Cloud Router를 사용하면 경계 게이트웨이 프로토콜(BGP)을 통해 Virtual 프라이빗 Cloud(VPC) 네트워크와 피어 네트워크 간에 경로를 동적으로 교환할 수 있는 서비스입니다.																			
	방화벽	VPC 방화벽 규칙을 사용하면 지정한 구성을 기준으로 가상 머신(VM) 인스턴스 간의 연결을 허용하거나 거부할 수 있는 서비스입니다.																			

IAM 역할 구분	역할 이름	상세설명
기본 역할	뷰어	상태에 영향을 주지 않는 읽기 전용 작업에 대한 권한이 부여됩니다. 예) 기존 리소스 또는 데이터의 조회(수정 제외)가 해당됨
	편집자	모든 뷰어 권한에 더해 기존 리소스 변경과 같이 상태를 변경하는 작업에 대한 권한까지 포함됩니다.
	소유자	모든 편집자 권한 및 다음 작업에 대한 권한이 포함됩니다. - 프로젝트 및 프로젝트 내의 모든 리소스에 대한 역할 및 관리 - 프로젝트에 대한 결제 설정
프로젝트 역할	서비스 계정 행위자	해당 역할은 지원이 중단되었기 때문에 서비스 계정으로써 작업을 실행하려면 서비스 계정 사용자 역할을 사용해야 합니다. 서비스 계정 행위자로서 동일한 권한을 효과적으로 제공하려면 서비스 계정 토큰 생성자 권한도 부여해야 합니다.
	브라우저	폴더, 조직, Cloud IAM 을 포함한 프로젝트의 계층구조를 탐색할 수 있는 읽기 액세스입니다. 해당 역할에는 프로젝트의 리소스를 볼 수 있는 권한이 제공되지 않습니다.
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.
Compute Engine 역할	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.
	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 뷰어	Compute Engine 리소스를 가져와 나열할 수 있지만 리소스에 저장된 데이터를 읽을 수는 없는 읽기 전용 액세스 권한입니다. 예를 들어, 이 역할을 부여받은 계정은 모든 디스크를 프로젝트에 목록화할 수 있지만 해당 디스크의 데이터는 전혀 읽을 수 없습니다.
네트워크 관리	관리자	네트워크 관리 리소스에 대한 전체 액세스 권한입니다.
	뷰어	네트워크 관리 리소스에 대한 읽기 전용 액세스 권한입니다.
네트워크 관리자		베어메탈 솔루션 네트워크 리소스의 관리자입니다.
서비스 네트워킹 서비스 에이전트		서비스 개발자에게 필요한 네트워크 피어링 설정과 같은 네트워크 구성을 관리할 권한을 부여합니다.
서비스 디렉터리 네트워크 연결자		서비스 디렉터리 엔드포인트에 VPC 네트워크를 연결할 수 있는 액세스 권한을 부여합니다.
Cloud Workstation 네트워크 관리자		워크스테이션 Cluster 를 공유 VPC 네트워크에 연결할 수 있는 권한을 부여합니다.

※ 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			N/A

관리자 및 담당자

※ 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(Google 또는 Cloud ID 계정) 추가 및 역할별 권한 부여

"DHL"에 대한 액세스 권한 부여

주 구성원에게 이 리소스에 대한 액세스 권한을 부여하고 역할을 추가하여 주 구성원이 수행할 수 있는 작업을 지정합니다. 필요에 따라 특정 기준을 충족하는 경우에만 주 구성원에게 액세스 권한을 부여하는 조건을 추가합니다. [IAM 조건 자세히 알아보기](#)

리소스

- DHL

주 구성원 추가

주 구성원은 사용자, 그룹, 도메인 또는 서비스 계정입니다. [IAM의 주 구성원 자세히 알아보기](#)

새 주 구성원

Google 또는 Cloud ID 계정에 대한 사용자 추가

역할 지정

역할은 권한 집합으로 구성되며, 주 구성원이 이 리소스로 수행할 수 있는 작업을 결정합니다. [자세히 알아보기](#)

역할 선택

IAM 조건(선택사항)

역할

- 네트워크 관리 관리자
- 네트워크 관리 뷰어**

네트워크 관리 뷰어

네트워크 관리 리소스에 대한 읽기 전용 액세스 권한입니다.

역할 별 권한 부여

3) 사용자 추가 확인

리소스, 문서, 제품 등을 검색하세요. 🔍 검색

IAM 및 관리자 IAM 액세스 권한 부여 액세스 권한 삭제

권한 권한사항 기록

'DHL' 프로젝트의 권한

이러한 권한이 이 프로젝트 및 프로젝트의 모든 리소스에 영향을 미칩니다. [자세히 알아보기](#)

Google 제공 역할 부여 포함

주 구성원별로 보기 역할별로 보기

필터 속성 이름 또는 값 입력

<input type="checkbox"/>	유형	주제 ↑	이름	역할	보안 통계	상속
<input type="checkbox"/>	사용자		...@gmail.com	네트워크 관리 뷰어		✎
<input type="checkbox"/>	그룹			✎
<input type="checkbox"/>	서비스 계정			✎
<input type="checkbox"/>	서비스 계정			✎

4) 권한을 부여한 사용자로 Google Cloud Console 로그인 시도



5) 권한 정상 부여 확인

이름 ↑	리전	서브넷	MTU	모드	내부 IP 범위	외부 IP 범위	보조 IPv4 범위	게이트웨이	방화벽 규칙
▼ default		36	1460	자동	없음				4
	us-central1	default			10.128.0.0/20	없음	없음	10.128.0.1	
	eu-west-1	default			10.132.0.0/20	없음	없음	10.132.0.1	
	us-west1	default			10.138.0.0/20	없음	없음	10.138.0.1	

예제 1. 계정 사용 권한이 서비스 역할에 맞게 정의되어 있을 경우

- 사내 Google Cloud 이용 요금에 대한 원활한 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

The screenshot shows the Google Cloud IAM console for 'My First Project'. The 'Roles' page is selected, and the 'Billing Account Administrator' role is highlighted. The role's permissions are listed as follows:

권한	테이블 필터링
billing.accounts.close	
billing.accounts.get	
billing.accounts.getIamPolicy	
billing.accounts.getPaymentInfo	
billing.accounts.getSpendingInformation	
billing.accounts.getUsageExportSpec	
billing.accounts.list	
billing.accounts.move	
billing.accounts.redeemPromotion	
billing.accounts.removeFromOrganization	
billing.accounts.reopen	
billing.accounts.setIamPolicy	
billing.accounts.update	
billing.accounts.updatePaymentInfo	
billing.accounts.updateUsageExportSpec	
billing.budgets.create	
billing.budgets.delete	
billing.budgets.get	
billing.budgets.list	
billing.budgets.update	
billing.credits.list	
billing.resourceAssociations.create	
billing.resourceAssociations.delete	
billing.resourceAssociations.list	
billing.subscriptions.create	
billing.subscriptions.get	
billing.subscriptions.list	
billing.subscriptions.update	
cloudnotifications.activities.list	
logging.logEntries.list	
logging.logServiceIndexes.list	
logging.logServices.list	
logging.logs.list	
logging.privateLogEntries.list	
resourceManager.projects.createBillingAssignment	
resourceManager.projects.deleteBillingAssignment	

2) [결제] > [구성원 추가]

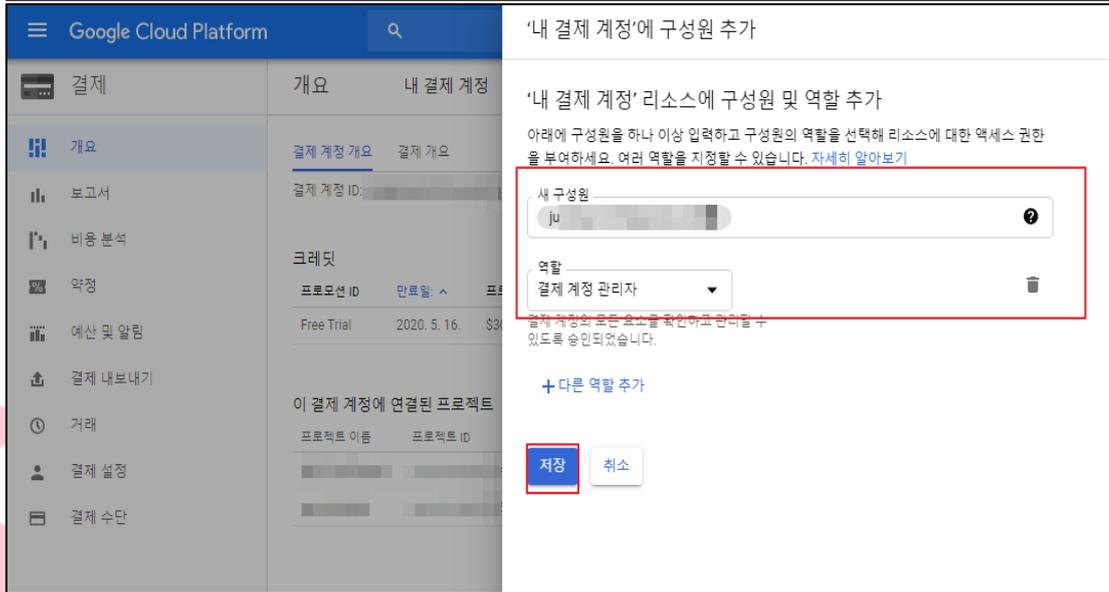
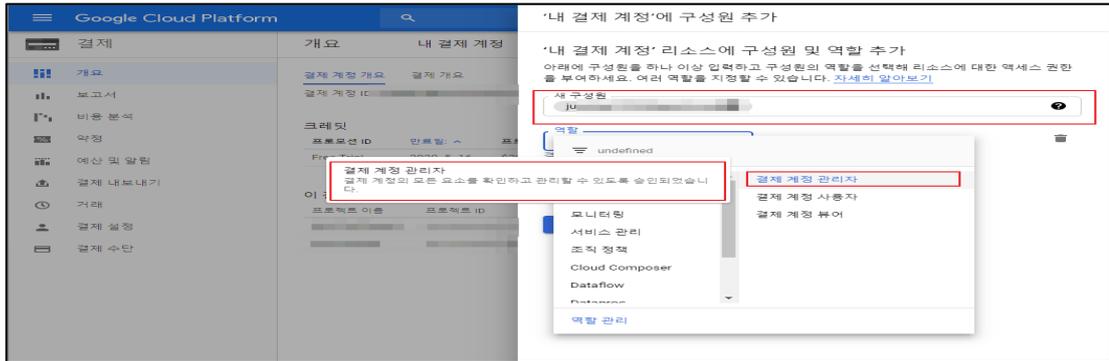
- '비용 및 재무 관리자' 역할 부여를 위한 사용자 추가

- 그림 내 '결제 계정 관리자'의 경우 최고 관리자에 한해서만 권한이 부여되어 있음

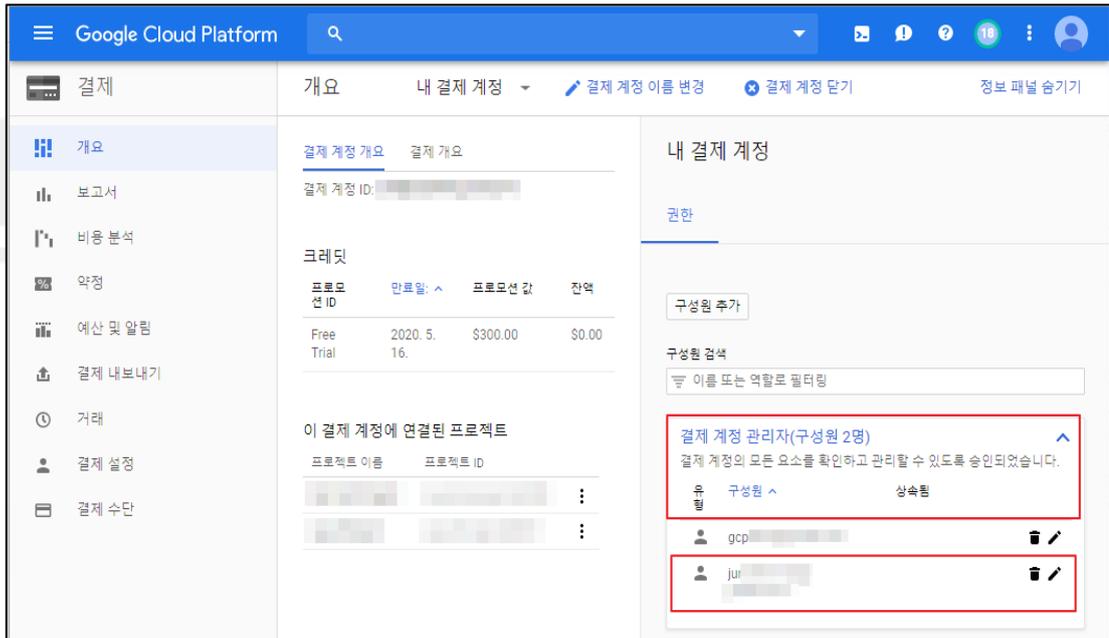
The screenshot shows the Google Cloud Billing console for '내 결제 계정'. The '구성원 추가' (Add Member) button is highlighted. Below it, the '결제 계정 관리자(구성원 1명)' (Billing Account Administrator (1 member)) section is visible, showing a list of members with their roles and inheritance status.

이름 또는 역할로 필터링
결제 계정 관리자(구성원 1명)
결제 계정의 모든 요소를 확인하고 관리할 수 있도록 승인되었습니다.
유형: 구성원 상속됨
gcp: [이름] [역할]

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

The screenshot shows the Google Cloud Platform IAM interface for 'My First Project'. The 'IAM 및 관리자' menu is open, and the 'IAM' sub-menu is selected. The '추가' (Add) button is highlighted. Below, the '구성원' (Members) section shows a table of roles:

유형	구성원	이름	역할	상속
<input type="checkbox"/>			탐색자 소스 저장소 리더	
<input type="checkbox"/>			소유자	
<input type="checkbox"/>			프로젝트 결제 관리자	

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

The screenshot shows the 'Add Member' dialog in Google Cloud Platform IAM for 'My First Project'. The '새 구성원' (New Member) field contains 'ju...'. Two roles are selected and highlighted with red boxes:

- 탐색자 (Viewer):** GCP 리소스를 탐색할 수 있는 액세스 권한입니다.
- 모니터링 뷰어 (Monitoring Viewer):** 모든 모니터링 데이터 및 구성에 대한 정보를 가져오고 나열할 수 있는 읽기 전용 액세스 권한입니다.

Buttons for '저장' (Save) and '취소' (Cancel) are visible at the bottom.

7) 추가로 설정한 '비용 및 재무 관리자'의 역할 확인

The screenshot shows the Google Cloud Platform IAM console for 'My First Project'. The left sidebar lists various IAM management options, with 'IAM' selected. The main content area displays the role assignment for 'My First Project'. A table lists the assigned roles, with the role '비용 및 재무 관리자' (Cost and Finance Manager) highlighted in a red box. The role is assigned to a user with the email 'ju...' and the role '비용 및 재무 관리자' (Cost and Finance Manager) is listed as the role assigned to the user.

유형	구성원	이름	역할	상속
<input type="checkbox"/>			탐색자 소스 저장소 리더	
<input type="checkbox"/>			소유자	
<input type="checkbox"/>			프로젝트 결제 관리자	
<input type="checkbox"/>		ju	탐색자 모니터링 뷰어	

8) 역할 할당 후 '비용 및 재무 관리자' 계정으로 로그인 시도

The screenshot shows the Google login page. The email field is filled with 'ju...' and the password field is empty. The '다음' (Next) button is highlighted in a red box. Below the login form, a red box contains the text: "비용 및 재무 관리자" 계정으로 로그인 시도. At the bottom of the page, there are links for '한국어', '도움말', '개인정보 보호', and '약관'.

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

The screenshot shows the Google Cloud Platform interface for the 'Compute Engine' service. The left sidebar contains a navigation menu with 'VM 인스턴스' (VM Instances) highlighted. The main content area displays a warning message: '이 프로젝트의 인스턴스를 볼 수 있는 권한이 없습니다.' (You do not have permission to view instances in this project). A red box highlights this message. Another red box at the bottom of the screenshot contains the text: '역할 및 권한을 할당 받지 못한 서비스(EX Compute Engine)에 대해 서비스 접근 불가 확인'.

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

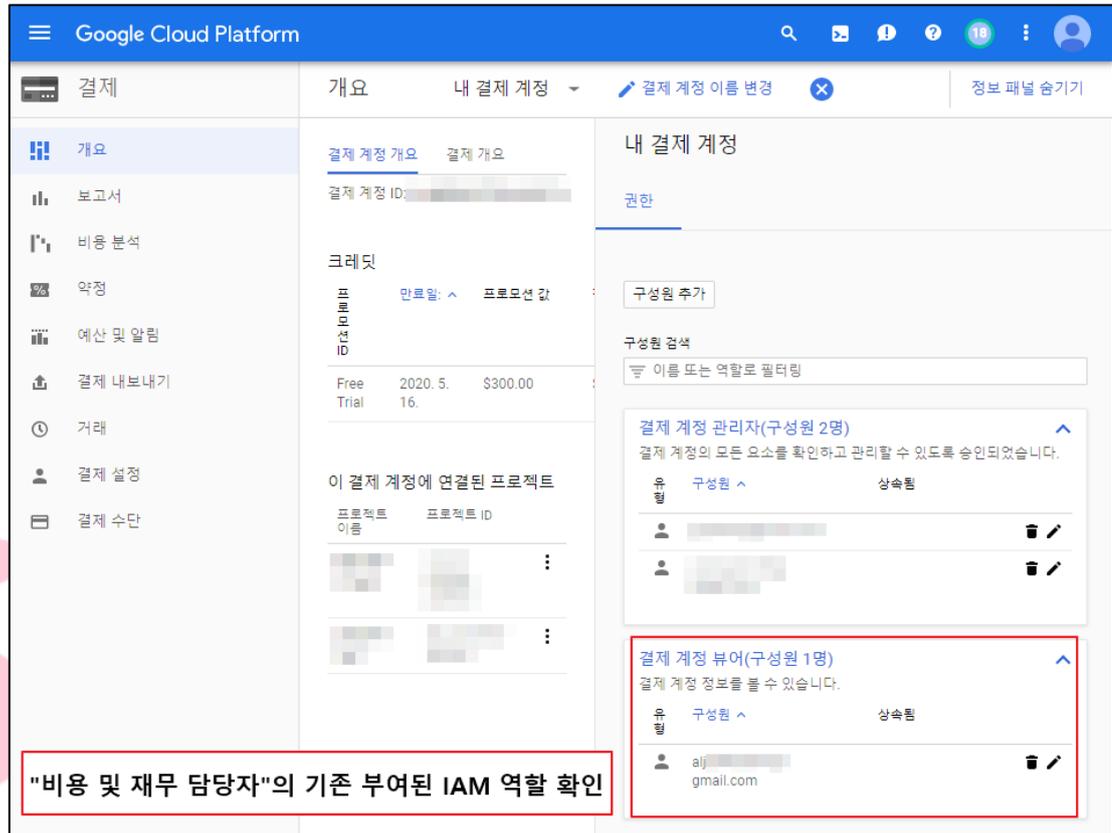
The screenshot shows the Google Cloud Platform 'Billing' console. The left sidebar lists navigation options like '결제' (Billing), '개요' (Overview), '보고서' (Reports), '비용 분석' (Cost Analysis), '약정' (Commitments), '거래' (Transactions), '결제 설정' (Billing Settings), and '결제 수단' (Payment Methods). The main content area displays a '보고서' (Reports) section with two cost summary cards. The first card shows a total cost of US\$108.11 with a change of -1,081,200% and includes a note 'includes -US\$43.35 in credits'. The second card shows a total cost of US\$153.45 with a change of -1,534,600% and includes a note '크레딧의 -US\$69.47 포함'. Below these cards is a line graph showing cost trends over time, with a legend for '비용 추세' (Cost Trend). A red box highlights the cost summary cards and the graph, with text inside: '역할 및 권한을 할당받은 서비스(EX 결제)에 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]

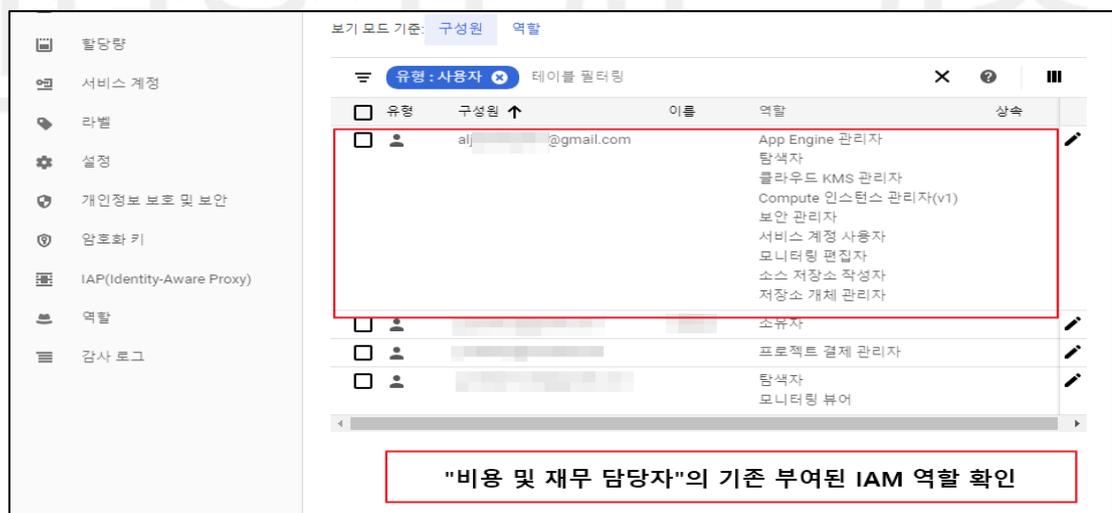
- '비용 및 재무 담당자' 계정 및 사용자 역할 권한 확인



"비용 및 재무 담당자"의 기존 부여된 IAM 역할 확인

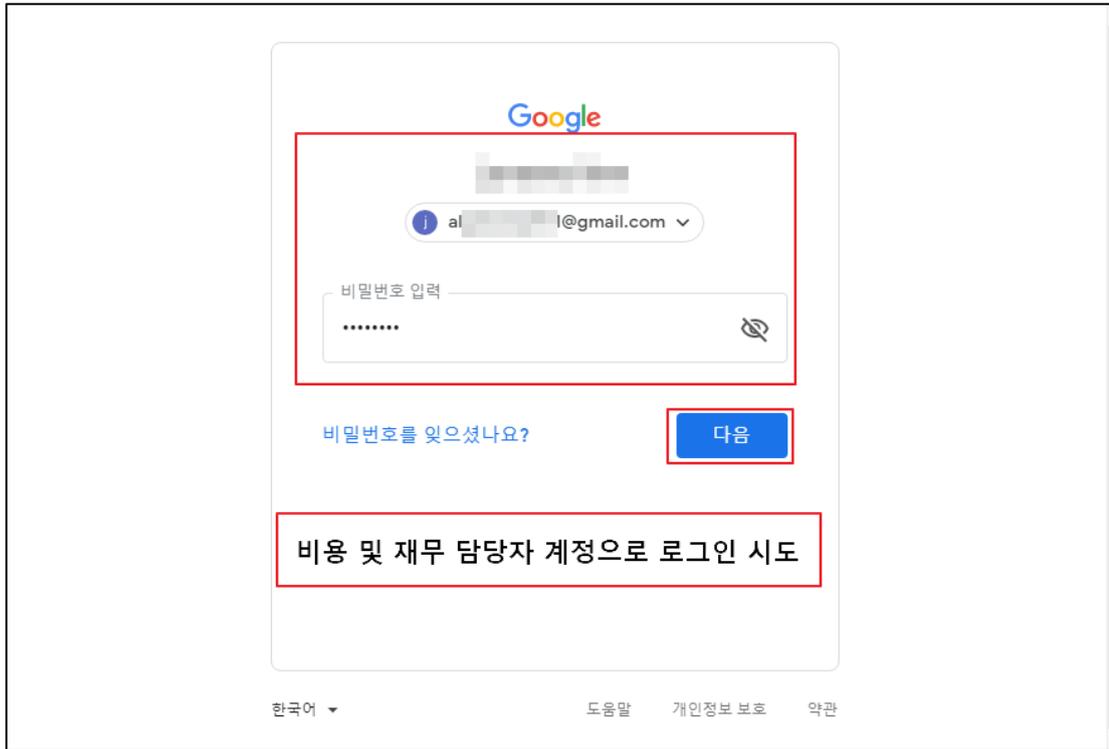
2) [IAM 및 관리자] > [IAM]

- '비용 및 재무 담당자'의 기존에 부여된 IAM 역할 확인



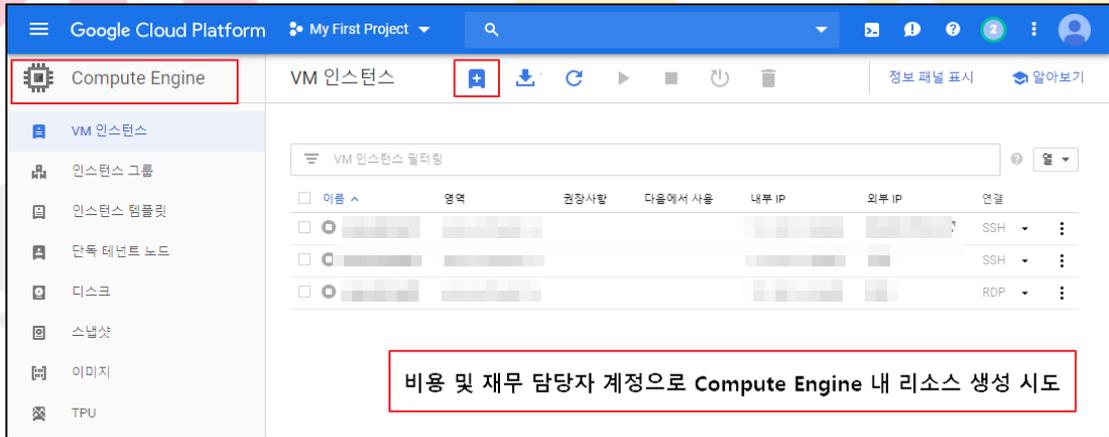
"비용 및 재무 담당자"의 기존 부여된 IAM 역할 확인

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)



Google Cloud Platform My First Project

← 인스턴스 만들기

VM 인스턴스를 만들려면 옵션 중 하나를 선택하세요.

- 새 VM 인스턴스**
VM 인스턴스 하나를 처음부터 만듭니다.
- 템플릿에서 VM 인스턴스 만들기**
기존 템플릿에서 VM 인스턴스 하나를 만듭니다.
- Marketplace**
VM 인스턴스에 바로 사용할 수 있는 솔루션을 배포합니다.

이름 ?
instance-1

리전 ?
us-central1(아이오와) **영역** ?
us-central1-a

머신 구성

머신 계열
일반 용도
일반적인 작업 부하에 적합한 머신 유형이며 가격 및 유연성을 위해 최적화되었습니다.

세대
1
Skylake CPU 플랫폼 또는 이전 버전의 플랫폼에서 제공

머신 유형
n1-standard-1(vCPU 1개, 3.75GB 메모리)

vCPU	메모리
1	3.75GB

∨ CPU 플랫폼 및 GPU

컨테이너 ?
 이 VM 인스턴스에 컨테이너 이미지를 배포합니다. 자세히 알아보기

부팅 디스크 ?
새로운 10GB 표준 영구 디스크 이미지
Debian GNU/Linux 9 (stretch) **변경**

ID 및 API 액세스 ?

서비스 계정 ?
Compute Engine default service account

액세스 범위 ?

- 기본 액세스 허용
- 모든 Cloud API에 대한 전체 액세스 허용
- 각 API에 액세스 설정

방화벽 ?
태그 및 방화벽 규칙을 추가하여 인터넷에서 특정 네트워크 트래픽을 허용합니다.

- HTTP 트래픽 허용
- HTTPS 트래픽 허용

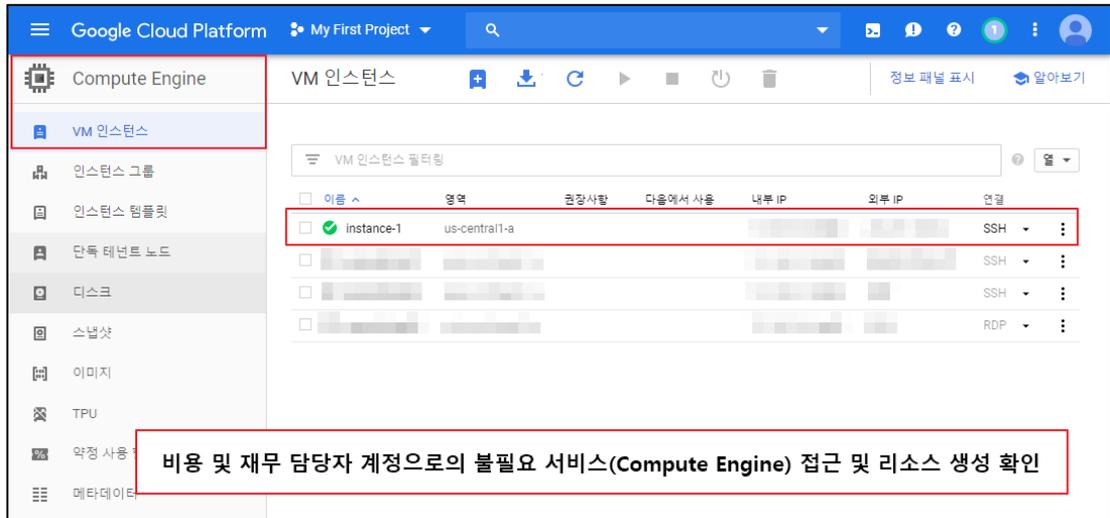
∨ 관리, 보안, 디스크, 네트워킹, 단독 임대

이 인스턴스의 요금이 청구됩니다. [Compute Engine 가격 책정](#)

만들기 취소

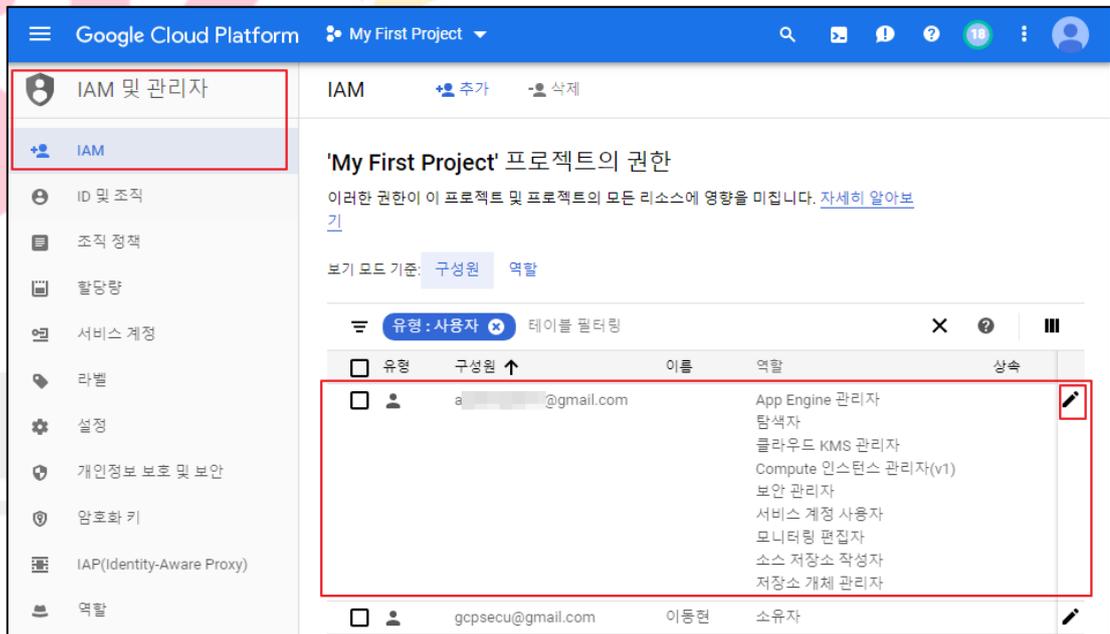
동등한 REST 또는 명령줄

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)



권한 수정

권한은 관리할 수 없습니다.

역할: **탐색자**
 Google 리소스를 탐색할 수 있는 액세스 권한입니다.

역할: **클라우드 KMS 관리자**
 암호화 리소스를 관리할 수 있습니다.

역할: **Compute 인스턴스 관리자...**
 Compute Engine 인스턴스, 인스턴스 그룹, 디스크, 스냅샷 및 이미지를 관리할 수 있는 전제 권한을 갖습니다. 모든 Compute Engine 네트워크 리소스에 대한 읽기 권한을 갖습니다.

역할: **보안 관리자**
 모든 IAM 정책을 가져오고 설정할 권한이 있는 보안 관리자 역할입니다.

역할: **서비스 계정 사용자**
 서비스 계정으로서 작업을 실행합니다.

역할: **모니터링 편집자**
 모든 모니터링 데이터 및 구성에 대한 읽기 및 쓰기 액세스 권한입니다.

역할: **소스 저장소 작성자**
 저장소에 대한 읽기 및 쓰기 액세스 권한입니다.

역할: **저장소 개체 관리자**
 GCS 개체를 관리할 수 있는 전제 권한입니다.

[+ 다른 역할 추가](#)

저장 **취소**

비용 및 재무 담당자에게 필요한 역할 권한을 제외한 역할들 삭제

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

Google Cloud Platform My First Project

IAM 및 관리자 IAM **추가** **삭제**

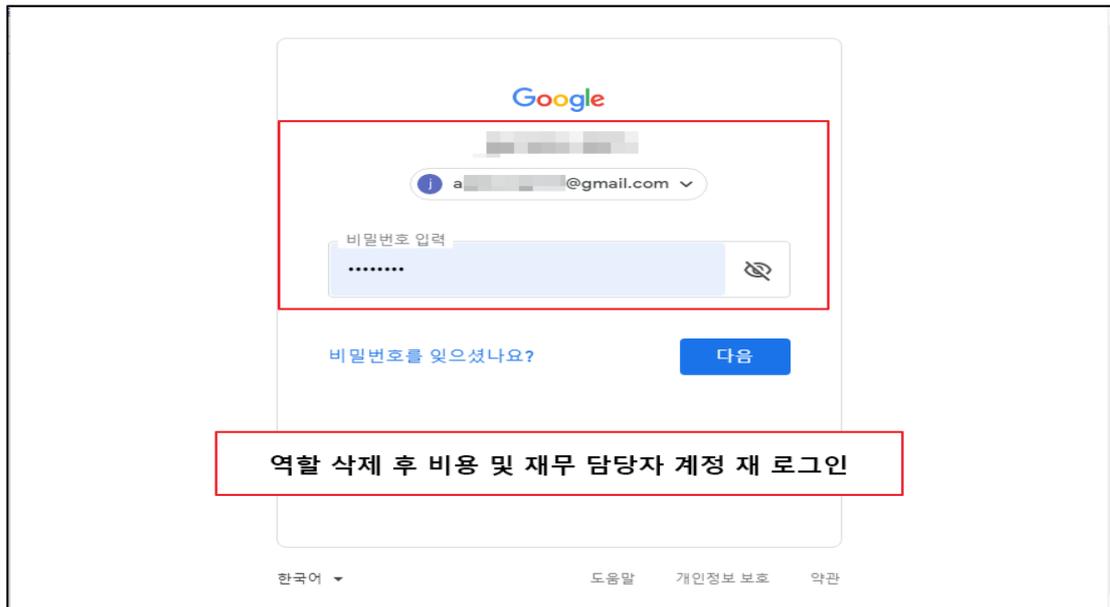
'My First Project' 프로젝트의 권한
 이러한 권한이 이 프로젝트 및 프로젝트의 모든 리소스에 영향을 미칩니다. [자세히 알아보기](#)

보기 모드 기준: **구성원** **역할**

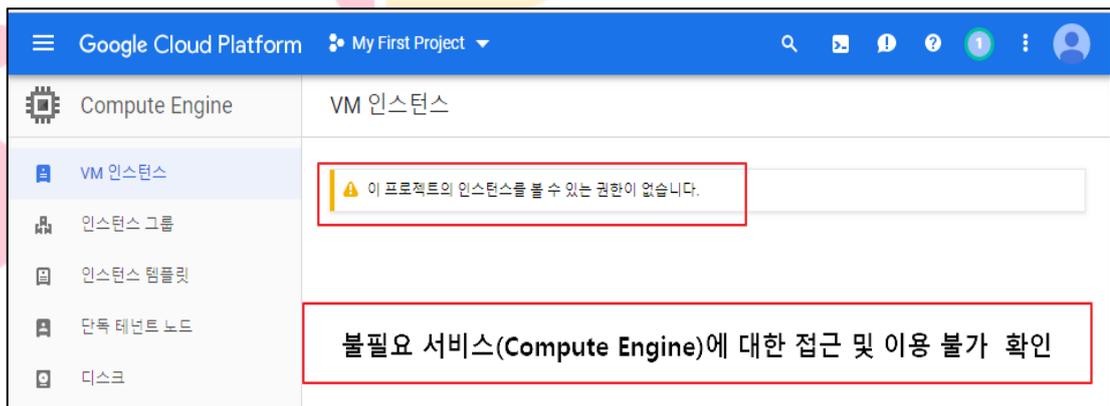
유형: 사용자 x 테이블 필터링

<input type="checkbox"/>	유형	구성원 ↑	이름	역할	상속
<input type="checkbox"/>	사용자	alj	@gmail.com	탐색자 모니터링 편집자	
<input type="checkbox"/>	사용자			소유자	
<input type="checkbox"/>	사용자			프로젝트 결제 관리자	
<input type="checkbox"/>	사용자			탐색자 모니터링 뷰어	

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



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.

진단 기준	<p>양호기준 : 네트워크 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있을 경우</p> <p>취약기준 : 네트워크 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있지 않을 경우</p>
비고	

2.3 기타 서비스 정책 관리

분류	권한 관리	중요도	상																						
항목명	기타 서비스 정책 관리																								
항목 설명	<p>(GCP(Google Cloud Platform)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 기타 서비스 별 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.</p> <p>※ 네트워크 서비스 구분</p> <table border="1"> <thead> <tr> <th>서비스 구분</th> <th>서비스 상세</th> </tr> </thead> <tbody> <tr> <td>App Engine</td> <td>App Engine은 확장 가능한 웹 애플리케이션을 개발하고 호스팅하기 위한 완전 관리형 서버리스 플랫폼 서비스입니다.</td> </tr> <tr> <td>Cloud Billing</td> <td>Cloud Billing 서비스는 사용중인 서비스 및 리소스 사용량에 따른 결제 금액을 확인할 수 있는 서비스입니다. Cloud Billing 계정 또는 프로젝트 수준에서 액세스 권한을 설정하면 여러 사용자 또는 역할의 보기 권한을 다양한 수준에서 제어할 수 있습니다.</td> </tr> <tr> <td>Cloud Dataflow</td> <td>Dataflow는 다양한 데이터 처리 패턴을 실행하는 관리형 서비스로 일괄 및 스트리밍 데이터 처리 파이프라인을 배포할 수 있습니다.</td> </tr> <tr> <td>Cloud Dataproc</td> <td>Dataproc은 일괄 처리, 쿼리, 스트리밍, 머신러닝에 오픈소스 데이터 도구를 사용할 수 있는 관리형 Apache Spark 및 Apache Hadoop 서비스입니다.</td> </tr> <tr> <td>Dialogflow</td> <td>Dialogflow는 대화식 사용자 인터페이스를 모바일 앱, 웹 애플리케이션, 기기, 봇, 대화형 음성 응답 시스템 등에 쉽게 설계하고 통합할 수 있는 자연어 이해 플랫폼 서비스입니다.</td> </tr> <tr> <td>Cloud Key Management Service</td> <td>Cloud Key Management Service를 사용하면 하나의 중앙 집중식 클라우드 서비스에서 암호화 키를 만들고 가져오고 관리할 수 있으며 암호화 작업을 수행할 수 있는 서비스입니다.</td> </tr> <tr> <td>Cloud Pub/Sub</td> <td>Pub/Sub는 독립적인 애플리케이션이 서로 메시지를 주고받게 해주는 완전 관리형 실시간 메시징 서비스입니다.</td> </tr> <tr> <td>Deployment Manager</td> <td>Google Cloud Deployment Manager는 Google Cloud 리소스 만들기 및 관리를 자동화하는 인프라 배포 서비스입니다.</td> </tr> <tr> <td>Cloud IAM</td> <td>Identity and Access Management(IAM)를 사용하면 Google Cloud 리소스에 대한 권한을 만들고 관리할 수 있습니다. IAM은 Google Cloud 서비스의 액세스 제어를 단일 시스템으로 통합하고 일관성 있는 작업 집합을 제공하는 서비스입니다.</td> </tr> <tr> <td>Resource Manager</td> <td>Google Cloud는 조직, 프로젝트와 같이 다른 Google Cloud 리소스를 그룹화하고 계층별로 구성할 수 있는 컨테이너 리소스를 제공합니다. 이러한 계층별 조직을 사용하면 액세스 제어 및 구성 설정과 같은</td> </tr> </tbody> </table>			서비스 구분	서비스 상세	App Engine	App Engine은 확장 가능한 웹 애플리케이션을 개발하고 호스팅하기 위한 완전 관리형 서버리스 플랫폼 서비스입니다.	Cloud Billing	Cloud Billing 서비스는 사용중인 서비스 및 리소스 사용량에 따른 결제 금액을 확인할 수 있는 서비스입니다. Cloud Billing 계정 또는 프로젝트 수준에서 액세스 권한을 설정하면 여러 사용자 또는 역할의 보기 권한을 다양한 수준에서 제어할 수 있습니다.	Cloud Dataflow	Dataflow는 다양한 데이터 처리 패턴을 실행하는 관리형 서비스로 일괄 및 스트리밍 데이터 처리 파이프라인을 배포할 수 있습니다.	Cloud Dataproc	Dataproc은 일괄 처리, 쿼리, 스트리밍, 머신러닝에 오픈소스 데이터 도구를 사용할 수 있는 관리형 Apache Spark 및 Apache Hadoop 서비스입니다.	Dialogflow	Dialogflow는 대화식 사용자 인터페이스를 모바일 앱, 웹 애플리케이션, 기기, 봇, 대화형 음성 응답 시스템 등에 쉽게 설계하고 통합할 수 있는 자연어 이해 플랫폼 서비스입니다.	Cloud Key Management Service	Cloud Key Management Service를 사용하면 하나의 중앙 집중식 클라우드 서비스에서 암호화 키를 만들고 가져오고 관리할 수 있으며 암호화 작업을 수행할 수 있는 서비스입니다.	Cloud Pub/Sub	Pub/Sub는 독립적인 애플리케이션이 서로 메시지를 주고받게 해주는 완전 관리형 실시간 메시징 서비스입니다.	Deployment Manager	Google Cloud Deployment Manager는 Google Cloud 리소스 만들기 및 관리를 자동화하는 인프라 배포 서비스입니다.	Cloud IAM	Identity and Access Management(IAM)를 사용하면 Google Cloud 리소스에 대한 권한을 만들고 관리할 수 있습니다. IAM은 Google Cloud 서비스의 액세스 제어를 단일 시스템으로 통합하고 일관성 있는 작업 집합을 제공하는 서비스입니다.	Resource Manager	Google Cloud는 조직, 프로젝트와 같이 다른 Google Cloud 리소스를 그룹화하고 계층별로 구성할 수 있는 컨테이너 리소스를 제공합니다. 이러한 계층별 조직을 사용하면 액세스 제어 및 구성 설정과 같은
	서비스 구분	서비스 상세																							
	App Engine	App Engine은 확장 가능한 웹 애플리케이션을 개발하고 호스팅하기 위한 완전 관리형 서버리스 플랫폼 서비스입니다.																							
	Cloud Billing	Cloud Billing 서비스는 사용중인 서비스 및 리소스 사용량에 따른 결제 금액을 확인할 수 있는 서비스입니다. Cloud Billing 계정 또는 프로젝트 수준에서 액세스 권한을 설정하면 여러 사용자 또는 역할의 보기 권한을 다양한 수준에서 제어할 수 있습니다.																							
	Cloud Dataflow	Dataflow는 다양한 데이터 처리 패턴을 실행하는 관리형 서비스로 일괄 및 스트리밍 데이터 처리 파이프라인을 배포할 수 있습니다.																							
	Cloud Dataproc	Dataproc은 일괄 처리, 쿼리, 스트리밍, 머신러닝에 오픈소스 데이터 도구를 사용할 수 있는 관리형 Apache Spark 및 Apache Hadoop 서비스입니다.																							
	Dialogflow	Dialogflow는 대화식 사용자 인터페이스를 모바일 앱, 웹 애플리케이션, 기기, 봇, 대화형 음성 응답 시스템 등에 쉽게 설계하고 통합할 수 있는 자연어 이해 플랫폼 서비스입니다.																							
	Cloud Key Management Service	Cloud Key Management Service를 사용하면 하나의 중앙 집중식 클라우드 서비스에서 암호화 키를 만들고 가져오고 관리할 수 있으며 암호화 작업을 수행할 수 있는 서비스입니다.																							
	Cloud Pub/Sub	Pub/Sub는 독립적인 애플리케이션이 서로 메시지를 주고받게 해주는 완전 관리형 실시간 메시징 서비스입니다.																							
	Deployment Manager	Google Cloud Deployment Manager는 Google Cloud 리소스 만들기 및 관리를 자동화하는 인프라 배포 서비스입니다.																							
Cloud IAM	Identity and Access Management(IAM)를 사용하면 Google Cloud 리소스에 대한 권한을 만들고 관리할 수 있습니다. IAM은 Google Cloud 서비스의 액세스 제어를 단일 시스템으로 통합하고 일관성 있는 작업 집합을 제공하는 서비스입니다.																								
Resource Manager	Google Cloud는 조직, 프로젝트와 같이 다른 Google Cloud 리소스를 그룹화하고 계층별로 구성할 수 있는 컨테이너 리소스를 제공합니다. 이러한 계층별 조직을 사용하면 액세스 제어 및 구성 설정과 같은																								

	리소스의 일반 측면을 관리할 수 있습니다. Resource Manager API를 사용하면 이러한 컨테이너 리소스를 프로그래매틱 방식으로 관리할 수 있습니다.
Cloud Source Repositoies	Cloud Source Repositories는 Google Cloud에서 호스팅되는 모든 기능을 갖춘 비공개 Git 저장소입니다.

※ IAM 역할

IAM 역할 구분	역할 이름	상세설명
기본 역할	뷰어	상태에 영향을 주지 않는 읽기 전용 작업에 대한 권한이 부여됩니다. 예) 기존 리소스 또는 데이터의 조회(수정 제외)가 해당됨
	편집자	모든 뷰어 권한에 더해 기존 리소스 변경과 같이 상태를 변경하는 작업에 대한 권한까지 포함됩니다.
	소유자	모든 편집자 권한 및 다음 작업에 대한 권한이 포함됩니다. - 프로젝트 및 프로젝트 내의 모든 리소스에 대한 역할 및 관리 - 프로젝트에 대한 결제 설정
프로젝트 역할	서비스 계정 행위자	해당 역할은 지원이 중단되었기 때문에 서비스 계정으로 작업을 실행하려면 서비스 계정 사용자 역할을 사용해야 합니다. 서비스 계정 행위자로서 동일한 권한을 효과적으로 제공하려면 서비스 계정 토큰 생성자 권한도 부여해야 합니다.
	브라우저	폴더, 조직, Cloud IAM 을 포함한 프로젝트의 계층구조를 탐색할 수 있는 읽기 액세스입니다. 해당 역할에는 프로젝트의 리소스를 볼 수 있는 권한이 제공되지 않습니다.
App Engine 역할	App Engine 관리자	모든 애플리케이션 구성 및 설정에 대한 읽기/쓰기/수정 액세스입니다.
	App Engine 서비스 관리자	모든 애플리케이션 구성과 설정에 대한 읽기 전용 액세스입니다. 모듈 수준 및 버전 수준 설정에 대한 쓰기 액세스를 가지고 있으며 새로운 버전은 배포할 수 없습니다.
	App Engine 배포자	모든 애플리케이션 구성과 설정에 대한 읽기 전용 액세스입니다. 새로운 버전 생성만 가능한 쓰기 액세스로 트래픽을 수신하지 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 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 Dataproc 역할	Cloud Dataproc 편집기	머신 유형, 네트워크, 프로젝트 및 영역 등 Cloud Dataproc 관리에 필수적인 리소스를 보는 데 필요한 권한을 제공합니다.
	Cloud Dataproc 뷰어	Cloud Dataproc 리소스에 대한 읽기 전용 액세스를 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 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.
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 관리자	폴더에 대한 Cloud IAM 정책을 관리할 수 있는 권한을 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 대상을 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.

※ 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

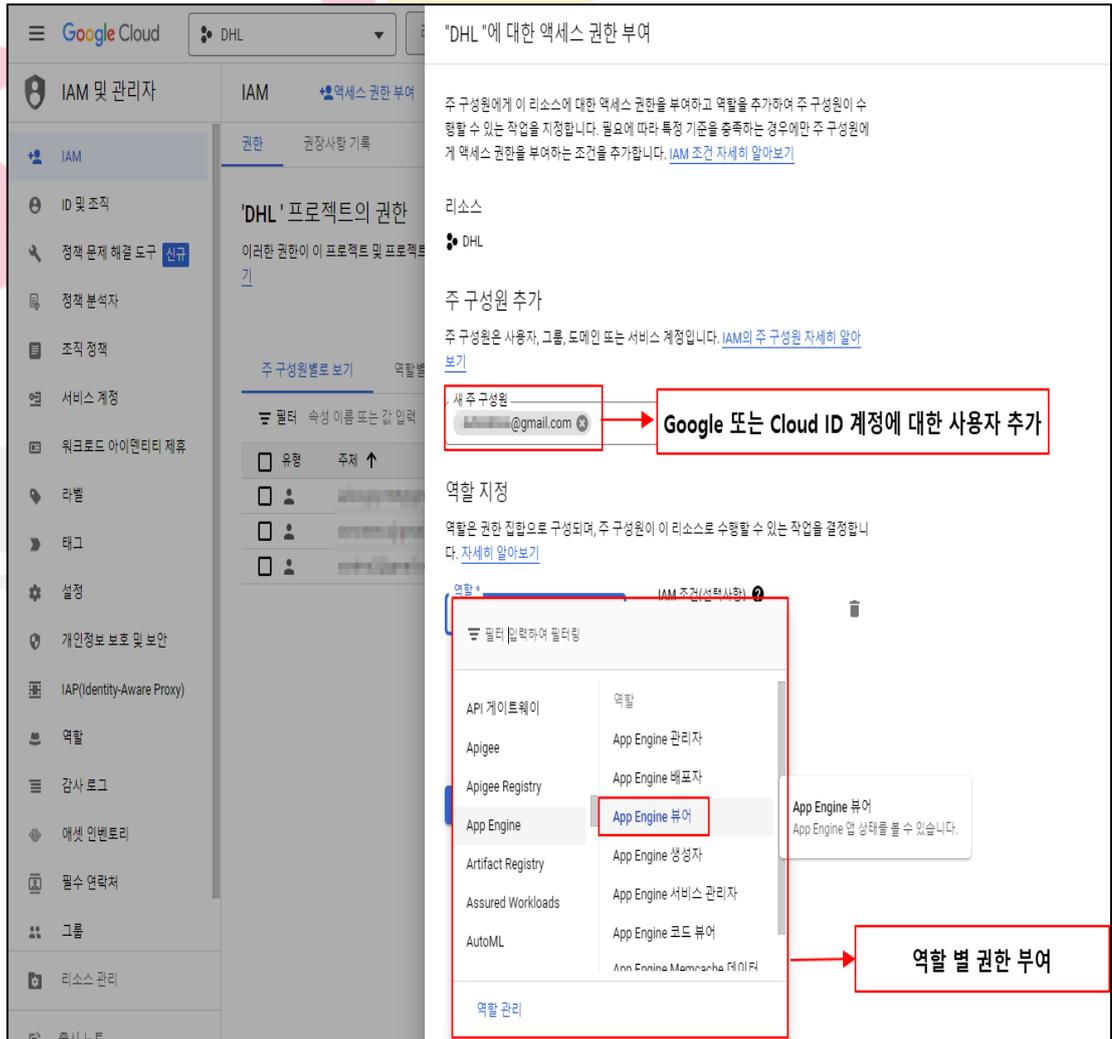
관리가 이루어질 경우 고객 커스텀 정책 내 권한에 대해서는 별도 담당자 확인이 필요합니다.

가. Google Cloud 에서 사전 정의된 역할로의 IAM 사용자 계정 생성

1) [IAM 및 관리자] > [IAM] > [추가]



2) 권한을 부여하고자 하는 사용자(Google 또는 Cloud ID 계정) 추가 및 역할별 권한 부여



설정
방법

3) 사용자 추가 확인

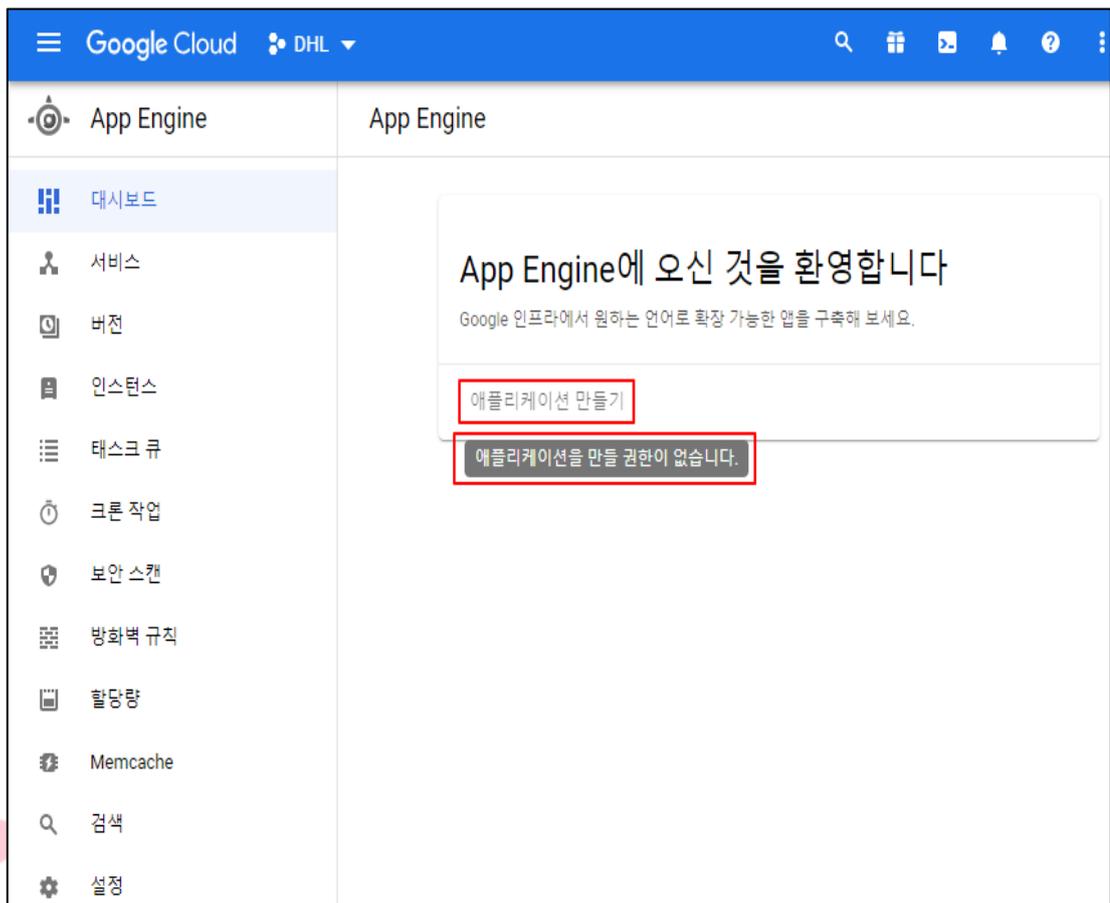
The screenshot shows the Google Cloud IAM console for a project named 'DHL'. The left sidebar contains navigation options like 'IAM 및 관리자', 'ID 및 조직', '정책 문제 해결 도구', etc. The main content area is titled 'DHL' 프로젝트의 권한' and includes a table of users and their roles. The first row in the table is highlighted with a red box.

유형	주제	이름	역할	보안 통계	상속
<input type="checkbox"/>	사용자	admin@gmail.com	App Engine 뷰어		<input type="checkbox"/>
<input type="checkbox"/>	서비스 계정	admin@project.com	서비스 계정		<input type="checkbox"/>
<input type="checkbox"/>	서비스 계정	admin@project.com	서비스 계정		<input type="checkbox"/>
<input type="checkbox"/>	서비스 계정	admin@project.com	서비스 계정		<input type="checkbox"/>

4) 권한을 부여한 사용자로 Google Cloud Console 로그인 시도

The screenshot shows the Google login page. The user's email address is entered in the top field. The password field is labeled '비밀번호 입력' and contains several dots. A blue '다음' (Next) button is highlighted with a red box.

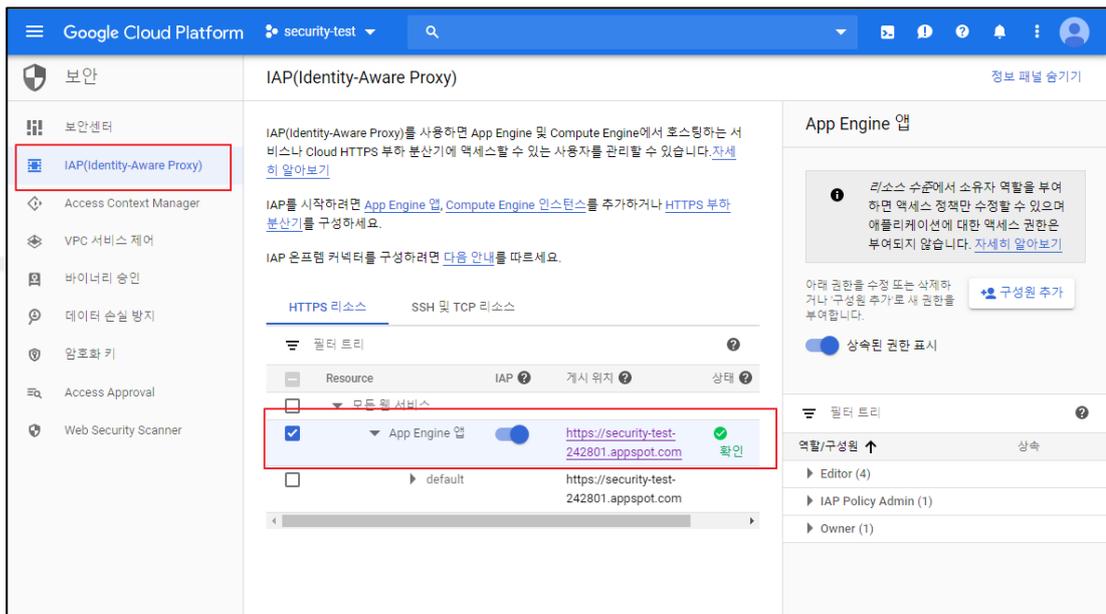
5) 권한 정상 부여 확인



나. Cloud IAP (Identity-Aware Proxy) 사용 설정

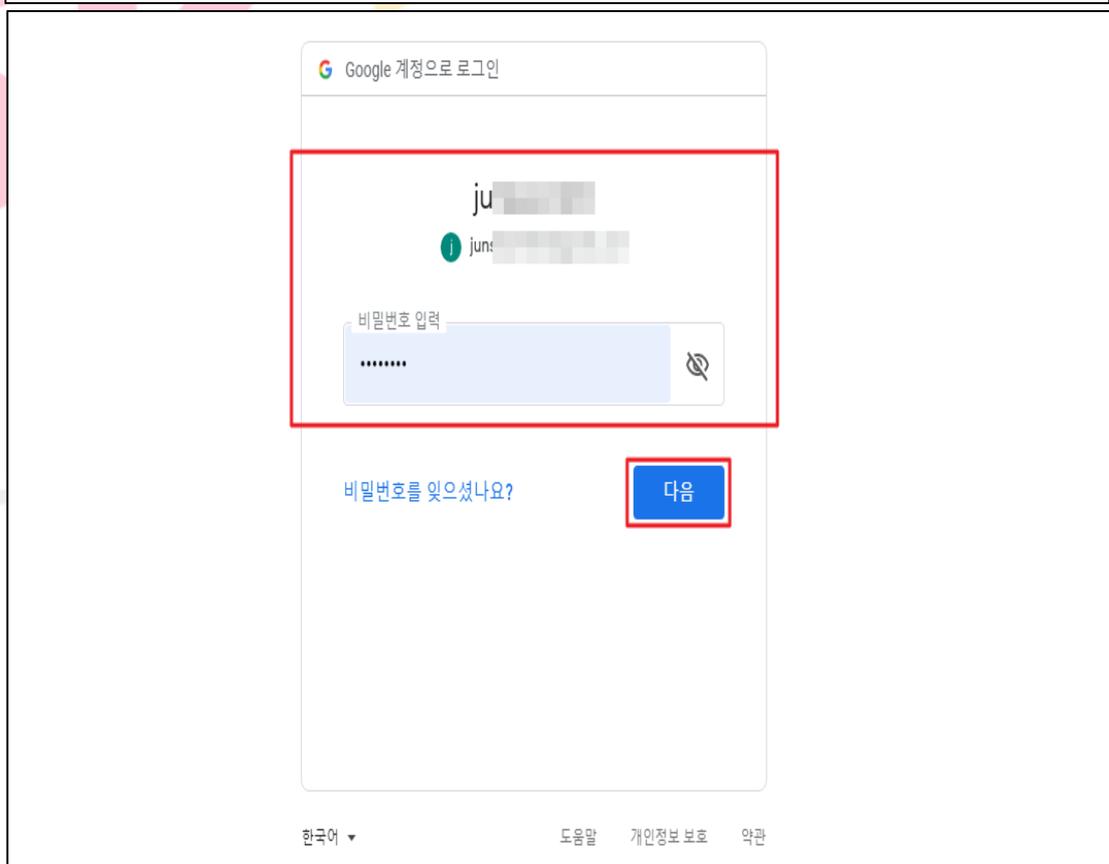
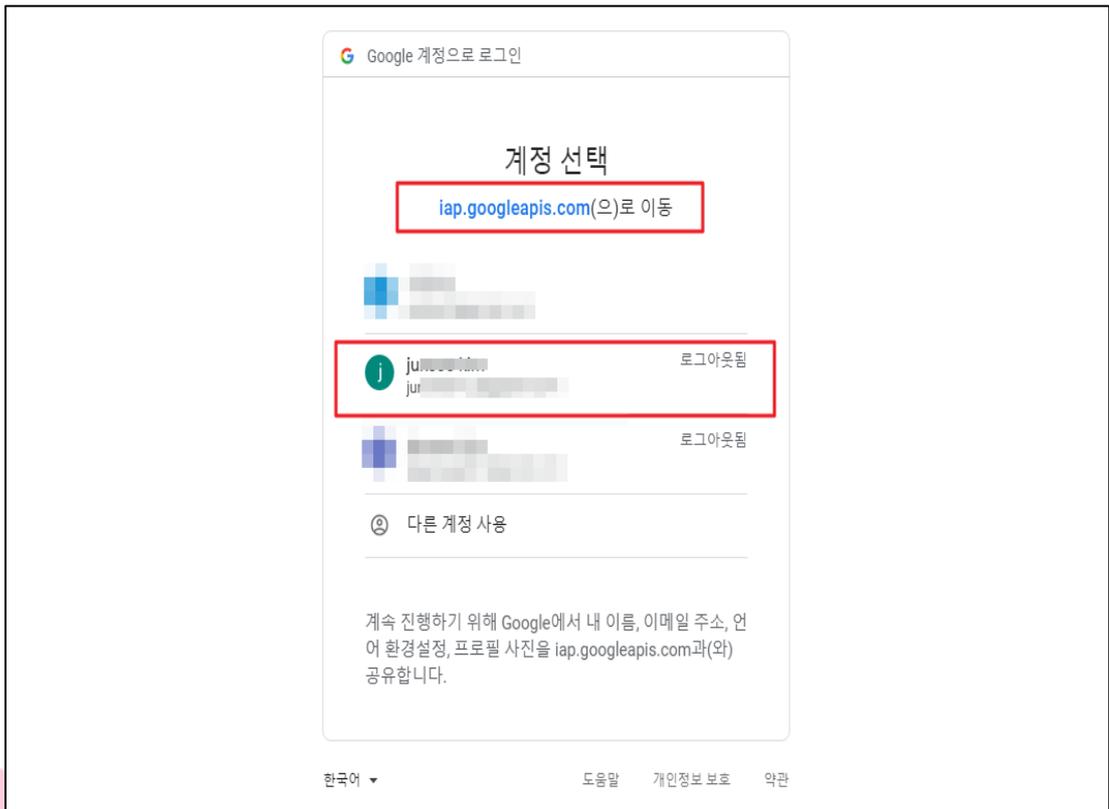
1) [보안] > [IAP(Identity-Aware Proxy)]

- 추가하려는 사용자의 권한 확인을 위한 웹 서비스 접근 시도

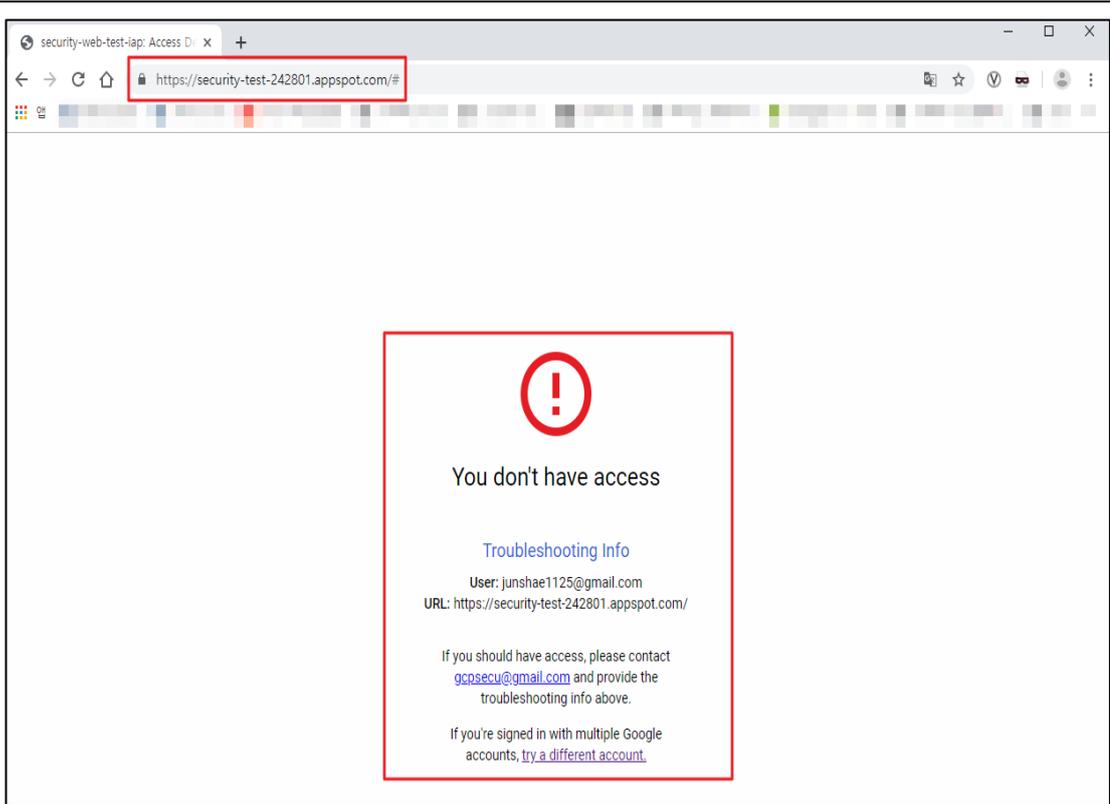


2) [Google 계정 로그인]

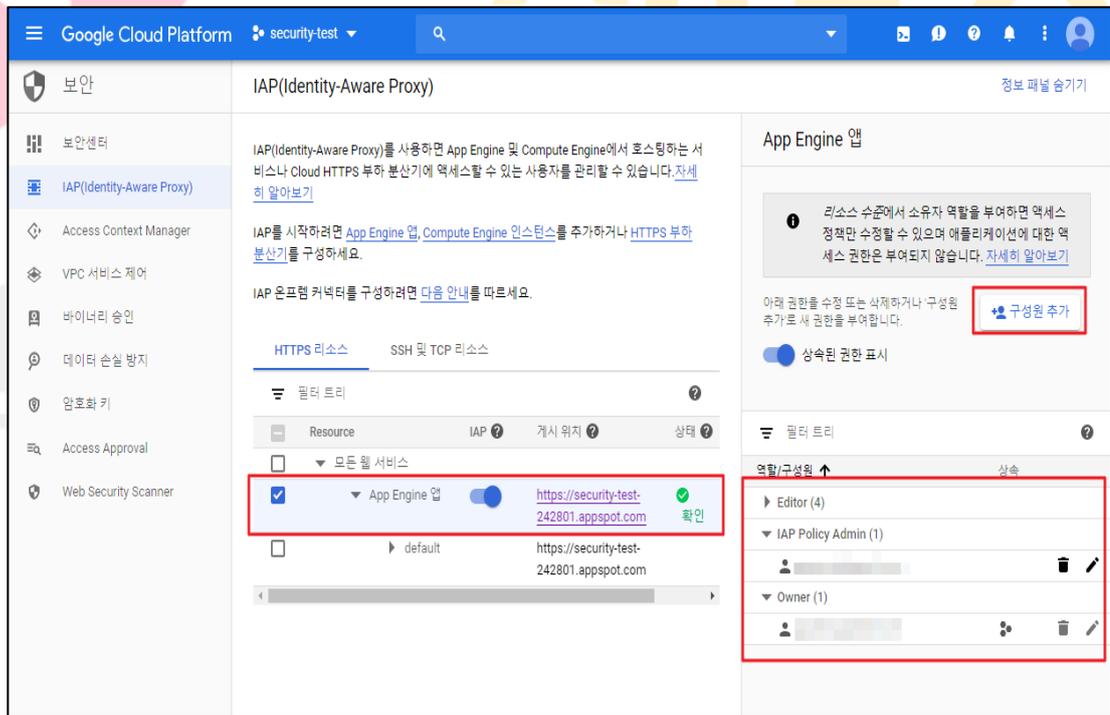
- IAP가 적용된 서비스 접근 시도 시 사용자 계정 확인



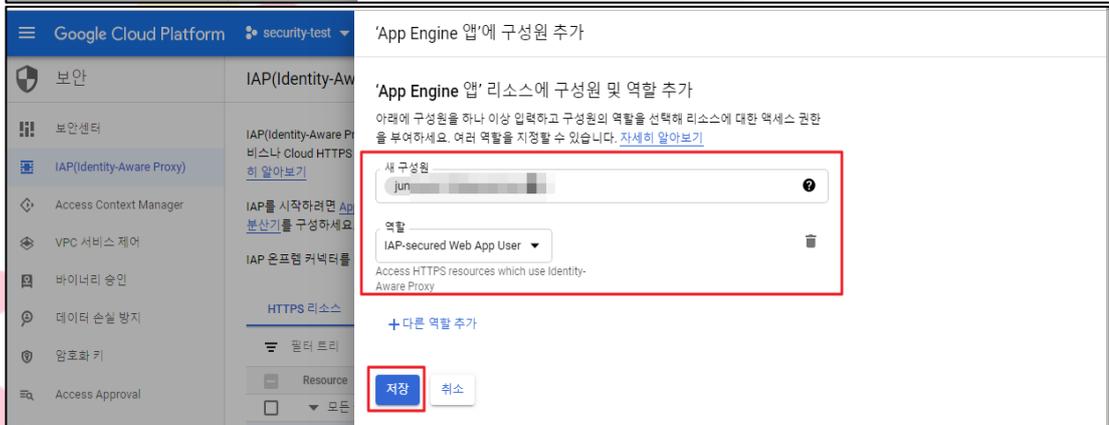
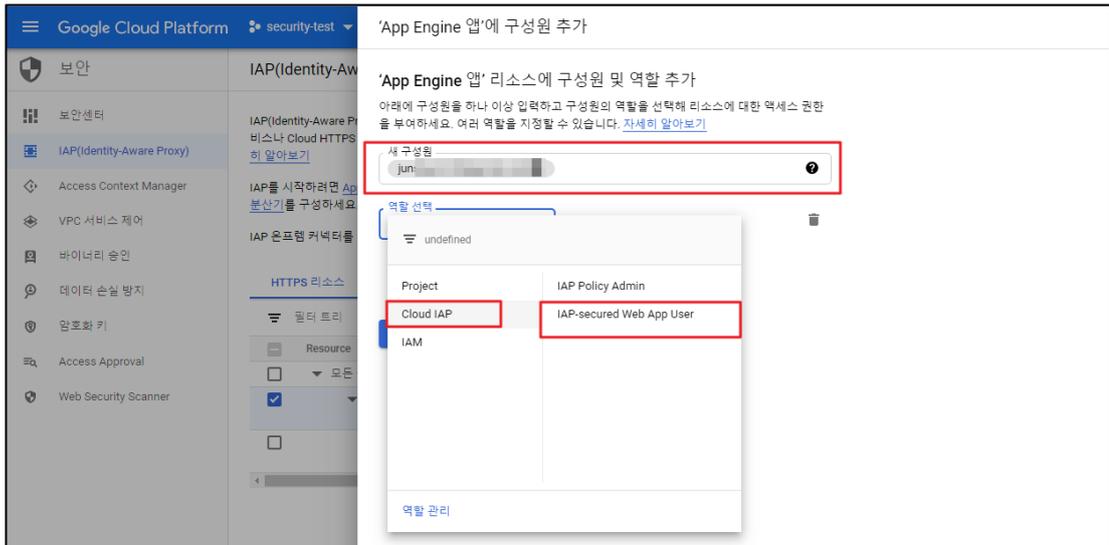
3) 로그인 사용자 웹 서비스에 대한 접근 권한 부재 확인



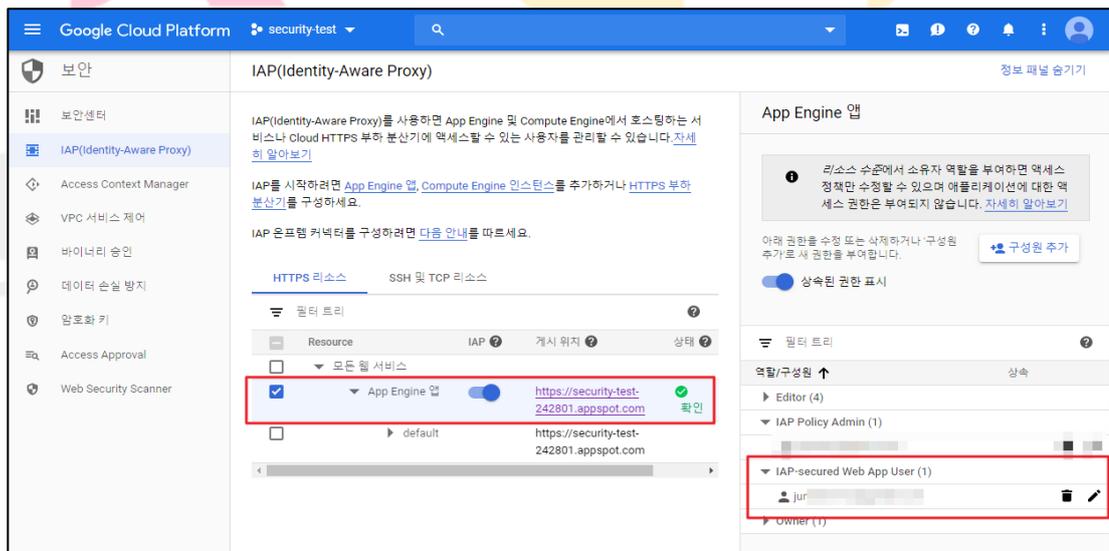
4) [보안] > [IAP(Identity-Aware Proxy)] > [리소스 선택] > [구성원 추가]
 - 이용하고자 하는 웹 서비스(리소스) 내 사용자 역할 및 구성원 정보 확인



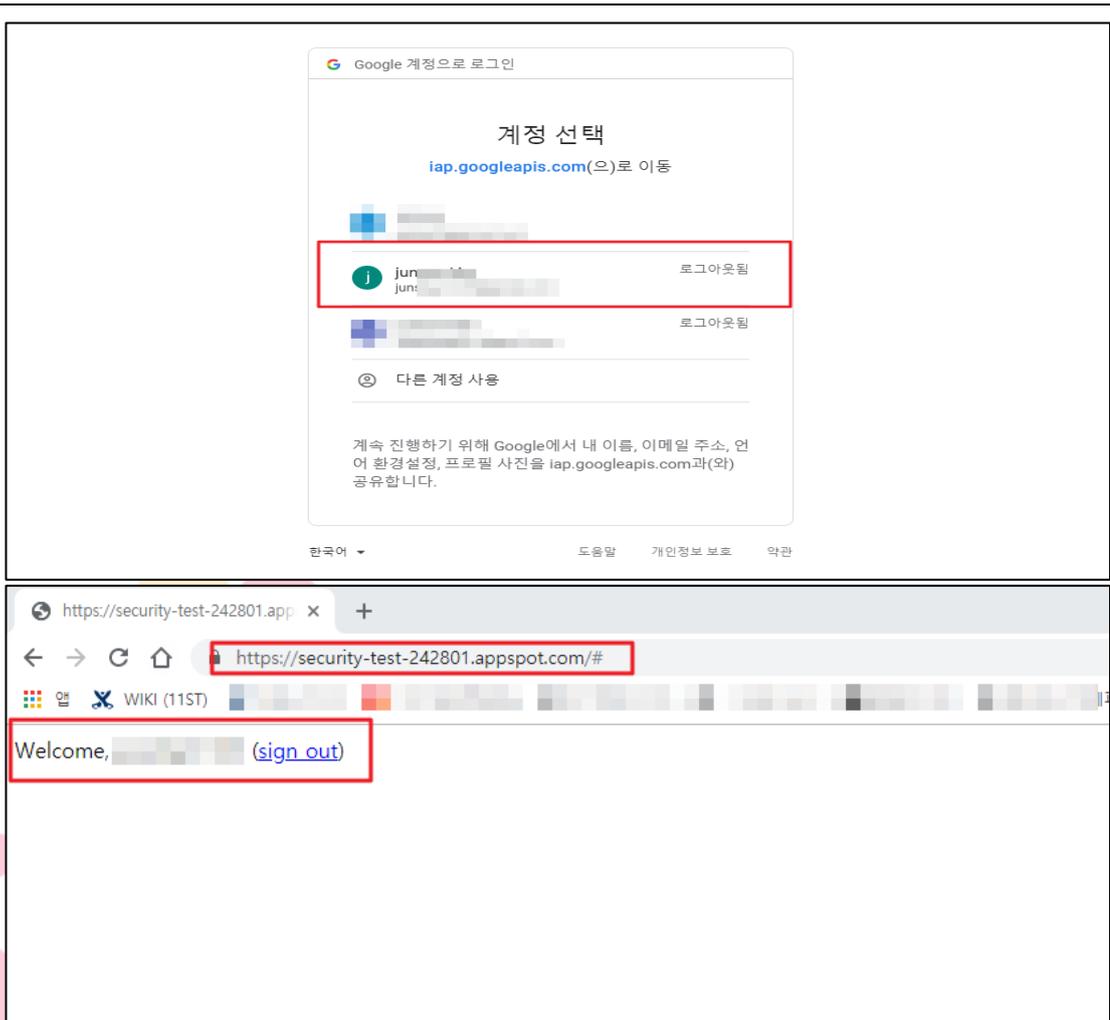
5) 새 구성원 검색 및 역할 할당



6) 추가된 사용자 계정/역할 확인 및 웹 서비스 재 접근 시도



7) 추가된 사용자 서비스 정상 접근 확인



예제 1. 계정 사용 권한이 서비스 역할에 맞게 정의되어 있을 경우

- 사내 Google Cloud 이용 요금에 대한 원활한 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

The screenshot shows the Google Cloud IAM role configuration page for the 'Billing Account Administrator' role. The role is selected in the list, and its permissions are displayed on the right. A red box highlights the list of 36 permissions.

권한 36개 할당

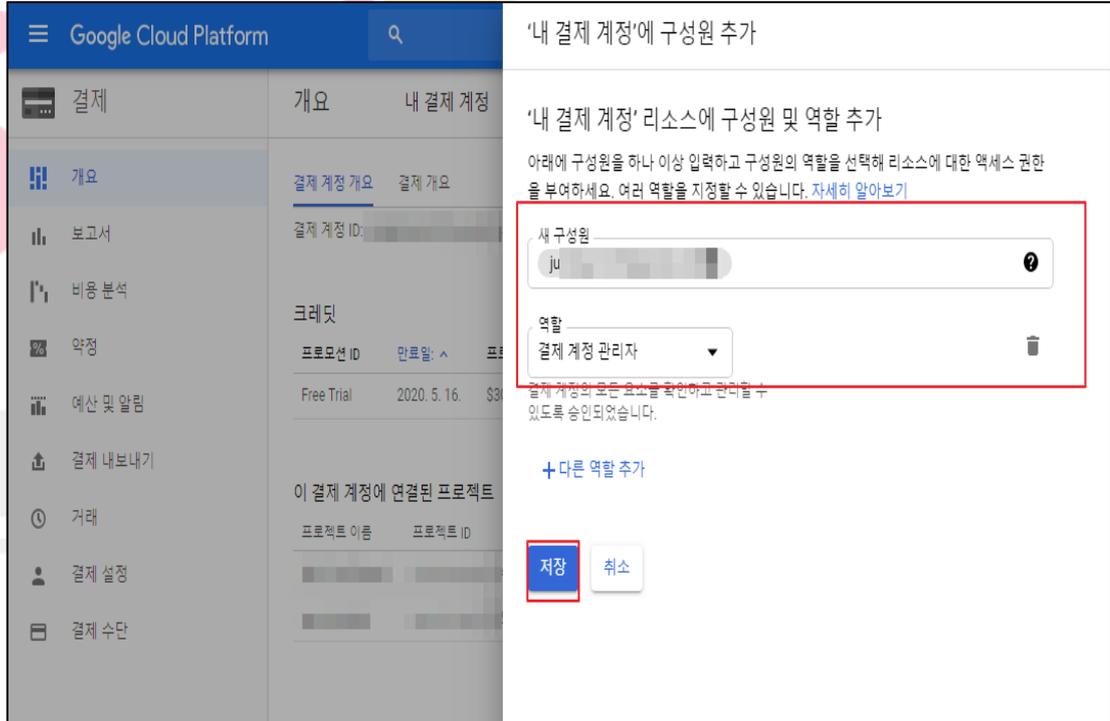
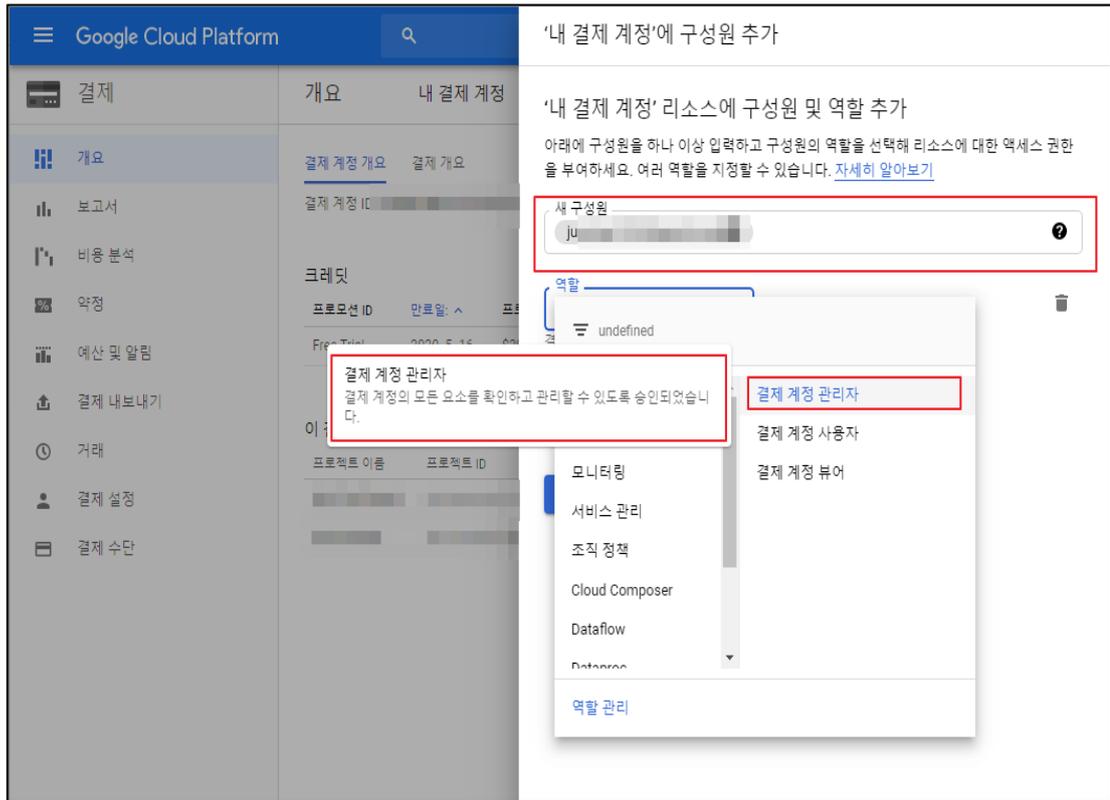
- billing.accounts.close
- billing.accounts.get
- billing.accounts.getIamPolicy
- billing.accounts.getPaymentInfo
- billing.accounts.getSpendingInformation
- billing.accounts.getUsageExportSpec
- billing.accounts.list
- billing.accounts.move
- billing.accounts.redeemPromotion
- billing.accounts.removeFromOrganization
- billing.accounts.reopen
- billing.accounts.setIamPolicy
- billing.accounts.update
- billing.accounts.updatePaymentInfo
- billing.accounts.updateUsageExportSpec
- billing.budgets.create
- billing.budgets.delete
- billing.budgets.get
- billing.budgets.list
- billing.budgets.update
- billing.credits.list
- billing.resourceAssociations.create
- billing.resourceAssociations.delete
- billing.resourceAssociations.list
- billing.subscriptions.create
- billing.subscriptions.get
- billing.subscriptions.list
- billing.subscriptions.update
- cloudnotifications.activities.list
- logging.logEntries.list
- logging.logServiceIndexes.list
- logging.logServices.list
- logging.logs.list
- logging.privateLogEntries.list
- resourcemanager.projects.createBillingAssignment
- resourcemanager.projects.deleteBillingAssignment

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

The screenshot shows the Google Cloud Billing page for a specific account. The '결제' (Billing) tab is selected. The '내 결제 계정' (My Billing Account) section shows account details. The '구성원 추가' (Add Member) button is highlighted with a red box. Below it, the '결제 계정 관리자(구성원 1명)' (Billing Account Administrator (1 member)) section shows the current administrator's details.

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

The screenshot shows the Google Cloud Platform Billing page. The left sidebar contains navigation options: 결제 (Billing), 개요 (Overview), 보고서 (Reports), 비용 분석 (Cost Analysis), 약정 (Agreements), 예산 및 알림 (Budgets and Alerts), 결제 내보내기 (Export Billing), 거래 (Transactions), 결제 설정 (Billing Settings), and 결제 수단 (Payment Methods). The main content area is divided into three sections: '결제 계정 개요' (Billing Account Overview) showing account ID and credit details; '내 결제 계정' (My Billing Account) with a '권한' (Permissions) sub-section; and '이 결제 계정에 연결된 프로젝트' (Projects connected to this billing account) with a table of project names and IDs. The '권한' section shows a list of users, with two users highlighted in red boxes: '결제 계정 관리자(구성원 2명)' (Billing Account Administrator (2 members)) and 'jur'. Below the screenshot, the text reads: '5) [IAM 및 관리자] > [IAM] > [추가] - '결제 계정 관리자' 권한 외 '비용 및 재무 관리자'에게 필요한 추가 역할 부여'.

5) [IAM 및 관리자] > [IAM] > [추가]
 - '결제 계정 관리자' 권한 외 '비용 및 재무 관리자'에게 필요한 추가 역할 부여

안녕을 지키는 기술

The screenshot shows the Google Cloud Platform IAM interface. The top navigation bar includes 'Google Cloud Platform', 'My First Project', and a search icon. The left sidebar contains 'IAM 및 관리자' (IAM and Admin) and 'IAM' (highlighted with a red box). Below the sidebar are various IAM management options like 'ID 및 조직', '조직 정책', '할당량', '서비스 계정', '라벨', '설정', '개인정보 보호 및 보안', and '암호화 키'. The main content area is titled 'IAM' and includes '+ 추가' (Add) and '- 삭제' (Remove) buttons. The main heading is 'My First Project' 프로젝트의 권한 (Permissions for 'My First Project' project). A sub-heading explains that these permissions affect all resources in the project and provides a link to '자세히 알아보기' (Learn more). Below this, there's a filter for '유형: 사용자' (Type: User) and a table of roles. The table has columns for '유형' (Type), '구성원' (Member), '이름' (Name), '역할' (Role), and '상속' (Inheritance). Three roles are listed: '탐색자' (Viewer), '소스 저장소 리더' (Source Storage Leader), and '소유자' (Owner). The '역할' column for the first two roles is highlighted with a red box.

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

The screenshot shows the 'My First Project'에 구성원 추가 (Add member to 'My First Project') page. The left sidebar is the same as in the previous screenshot. The main heading is 'My First Project' 프로젝트에 구성원, 역할 추가 (Add member, role to 'My First Project' project). A sub-heading explains that one or more members can be added and roles can be selected to grant access to resources. Below this, there's a form to add a new member. The '새 구성원' (New member) field contains 'ju' and is highlighted with a red box. Below the member field, there are two role selection dropdowns. The first dropdown is set to '탐색자' (Viewer) and is highlighted with a red box. The second dropdown is set to '모니터링 뷰어' (Monitoring Viewer) and is also highlighted with a red box. Below the role selection, there are two buttons: '저장' (Save) and '취소' (Cancel). The '저장' button is highlighted with a red box.

7) 추가로 설정한 '비용 및 재무 관리자'의 역할 확인

Google Cloud Platform My First Project

IAM 및 관리자 IAM 추가 삭제

'My First Project' 프로젝트의 권한

이러한 권한이 이 프로젝트 및 프로젝트의 모든 리소스에 영향을 미칩니다. [자세히 알아보기](#)

보기 모드 기준: **구성원** 역할

유형: 사용자 테이블 필터링

유형	구성원 ↑	이름	역할	상속
사용자	[redacted]	[redacted]	탐색자 소스 저장소 리더	✎
사용자	[redacted]	[redacted]	소유자	✎
사용자	[redacted]	[redacted]	프로젝트 결제 관리자	✎
사용자	ju	[redacted]	탐색자 모니터링 뷰어	✎

8) 역할 할당 후 '비용 및 재무 관리자' 계정으로 로그인 시도

Google

ju

ju

비밀번호 입력

비밀번호를 잊으셨나요? **다음**

"비용 및 재무 관리자" 계정으로 로그인 시도

한국어 도움말 개인정보 보호 약관

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

Google Cloud Platform My First Project

Compute Engine VM 인스턴스

이 프로젝트의 인스턴스를 볼 수 있는 권한이 없습니다.

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

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

Google Cloud Platform

결제 보고서 내 결제 계정 인쇄 필터 표시

US\$108.11 (총 비용) ↑ -1,081,200% includes -US\$43.35 in credits

US\$153.45 (예상 총 비용) ↑ -1,534,600% 크레딧의 -US\$69.47 포함

역할 및 권한을 할당받은 서비스(EX 결제)에 대해 서비스 접근 및 이용 가능 확인

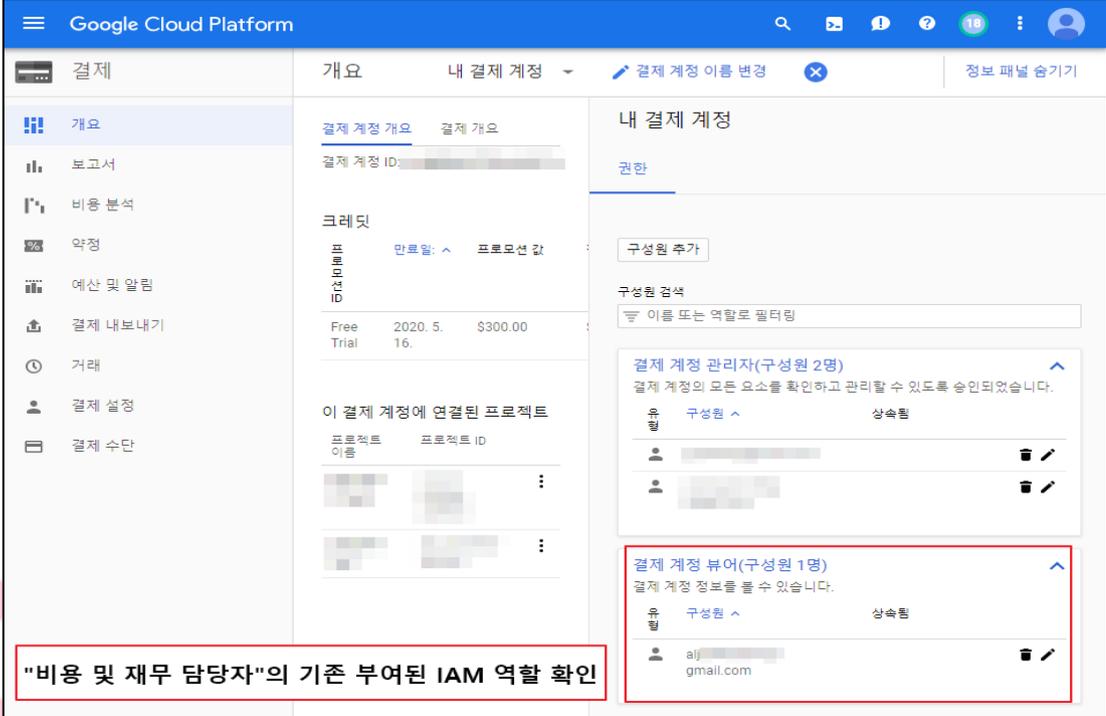
비용 추세

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]

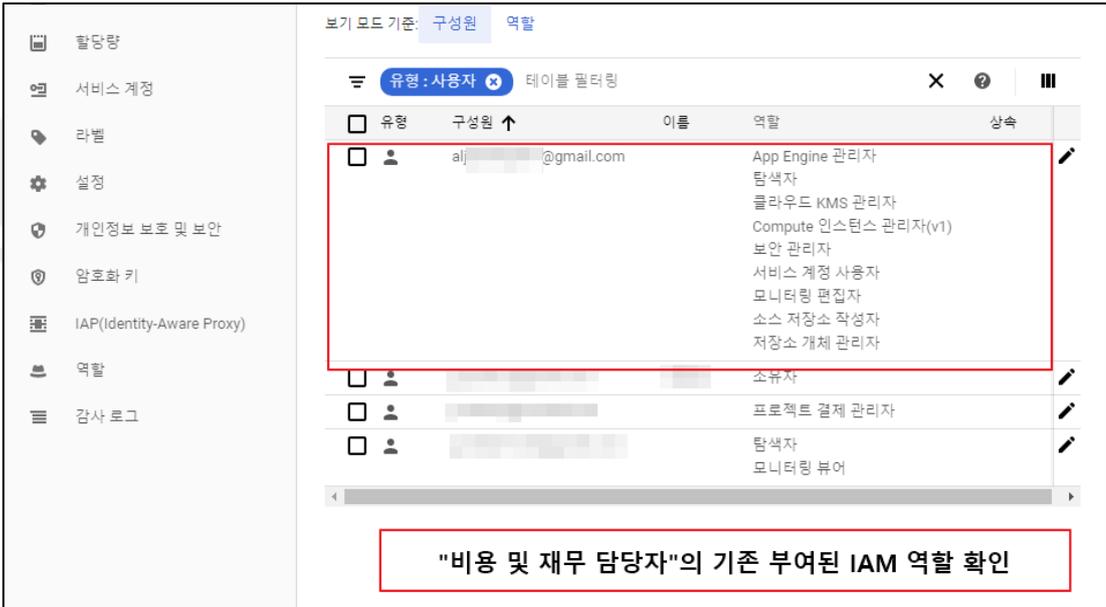
- '비용 및 재무 담당자' 계정 및 사용자 역할 권한 확인



"비용 및 재무 담당자"의 기존 부여된 IAM 역할 확인

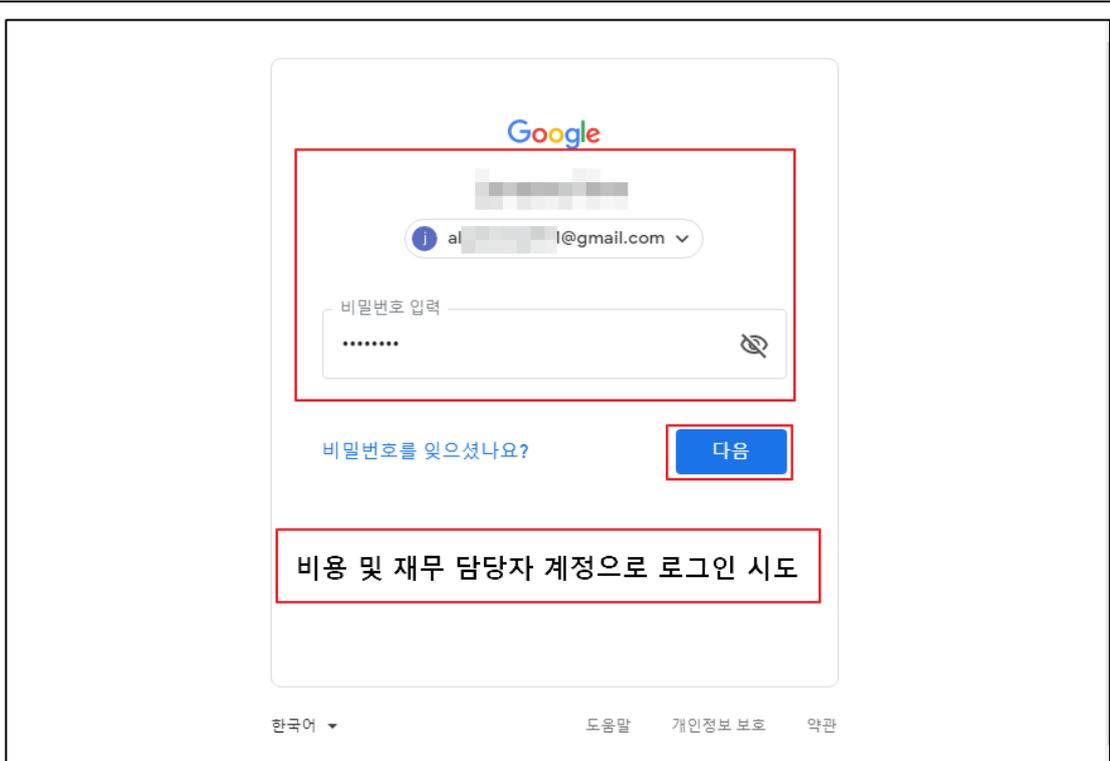
2) [IAM 및 관리자] > [IAM]

- '비용 및 재무 담당자'의 기존에 부여된 IAM 역할 확인



"비용 및 재무 담당자"의 기존 부여된 IAM 역할 확인

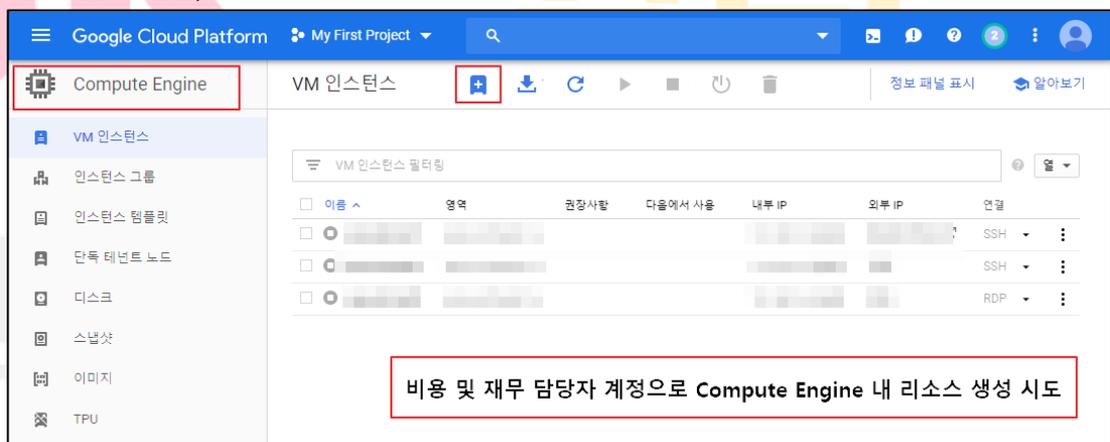
3) '비용 및 재무 담당자' 계정으로 로그인 시도



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)



Google Cloud Platform My First Project

← 인스턴스 만들기

VM 인스턴스를 만들려면 옵션 중 하나를 선택하세요.

- 새 VM 인스턴스**
VM 인스턴스 하나를 처음부터 만듭니다.
- 템플릿에서 VM 인스턴스 만들기**
기존 템플릿에서 VM 인스턴스 하나를 만듭니다.
- Marketplace**
VM 인스턴스에 바로 사용할 수 있는 솔루션을 배포합니다.

이름 ?
instance-1

리전 ? us-central1(아이오와) **영역** ? us-central1-a

머신 구성

머신 계열
일반 용도
일반적인 작업 부하에 적합한 머신 유형이며 가격 및 유연성을 위해 최적화되었습니다.

세대
1
Skylake CPU 플랫폼 또는 이전 버전의 플랫폼에서 제공

머신 유형
n1-standard-1(vCPU 1개, 3.75GB 메모리)

vCPU	메모리
1	3.75GB

∨ CPU 플랫폼 및 GPU

컨테이너 ?
 이 VM 인스턴스에 컨테이너 이미지를 배포합니다. 자세히 알아보기

부팅 디스크 ?
새로운 10GB 표준 영구 디스크 이미지
Debian GNU/Linux 9 (stretch) 변경

ID 및 API 액세스 ?

서비스 계정 ?
Compute Engine default service account

액세스 범위 ?

- 기본 액세스 허용
- 모든 Cloud API에 대한 전체 액세스 허용
- 각 API에 액세스 설정

방화벽 ?
타그 및 방화벽 규칙을 추가하여 인터넷에서 특정 네트워크 트래픽을 허용합니다.

- HTTP 트래픽 허용
- HTTPS 트래픽 허용

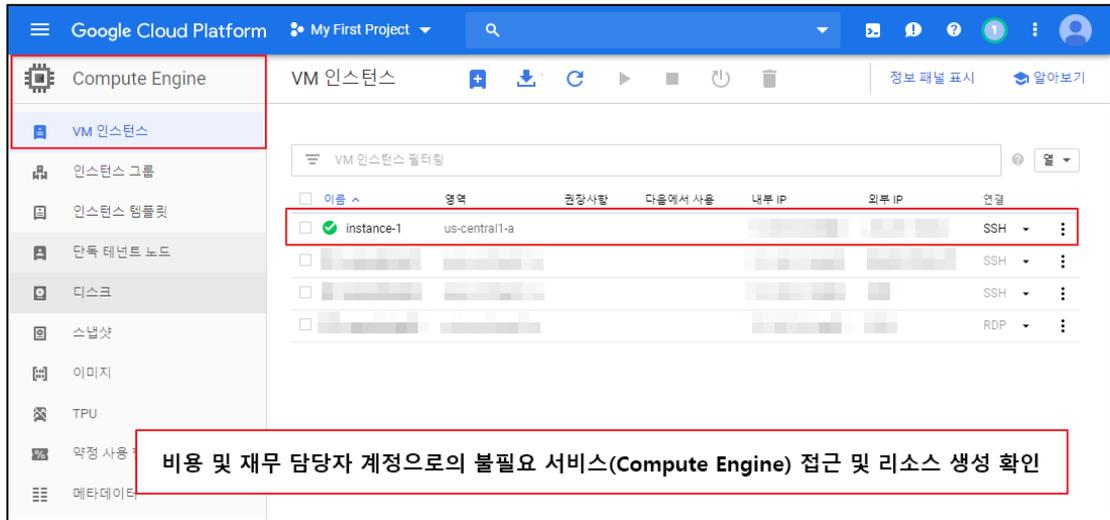
∨ 관리, 보안, 디스크, 네트워킹, 단독 임대

이 인스턴스의 요금이 청구됩니다. [Compute Engine 가격 책정](#)

만들기 취소

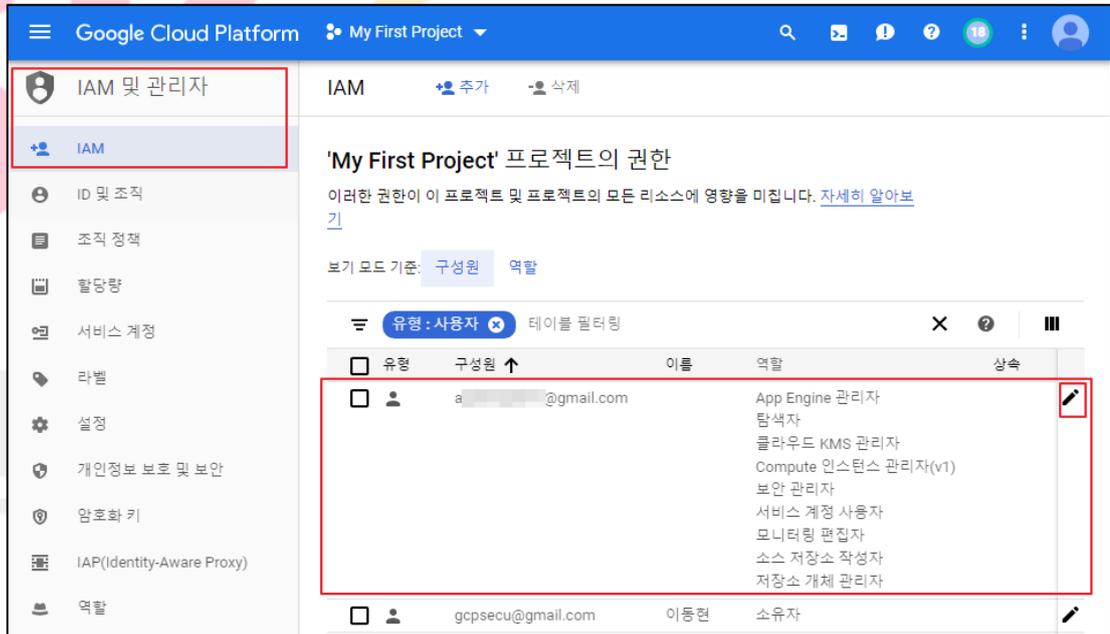
등등한 REST 또는 명령줄

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)



권한 수정

역할: **탐색자**
 GCP 리소스를 탐색할 수 있는 액세스 권한입니다.

역할: **클라우드 KMS 관리자**
 암호화 리소스를 관리할 수 있습니다.

역할: **Compute 인스턴스 관리자...**
 Compute Engine 인스턴스, 인스턴스 그룹, 디스크, 스냅샷 및 이미지를 관리할 수 있는 전체 권한을 갖습니다. 모든 Compute Engine 네트워크 리소스에 대한 읽기 권한을 갖습니다.

역할: **보안 관리자**
 모든 IAM 정책을 가져오고 설정할 권한이 있는 보안 관리자 역할입니다.

역할: **서비스 계정 사용자**
 서비스 계정으로서 작업을 실행합니다.

역할: **모니터링 편집자**
 모든 모니터링 데이터 및 구성에 대한 읽기 및 쓰기 액세스 권한입니다.

역할: **소스 저장소 작성자**
 저장소에 대한 읽기 및 쓰기 액세스 권한입니다.

역할: **저장소 개체 관리자**
 GCS 개체를 관리할 수 있는 전체 권한입니다.

+ 다른 역할 추가

저장 취소

비용 및 재무 담당자에게 필요한 역할 권한을 제외한 역할들 삭제

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

Google Cloud Platform My First Project

IAM 및 관리자 IAM

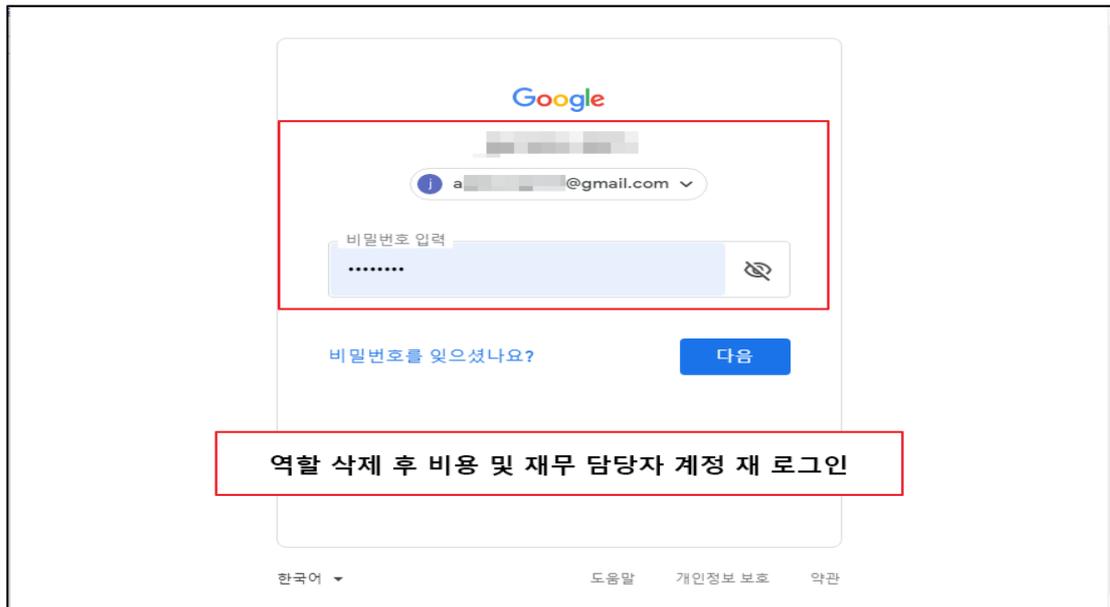
'My First Project' 프로젝트의 권한

이러한 권한이 이 프로젝트 및 프로젝트의 모든 리소스에 영향을 미칩니다. [자세히 알아보기](#)

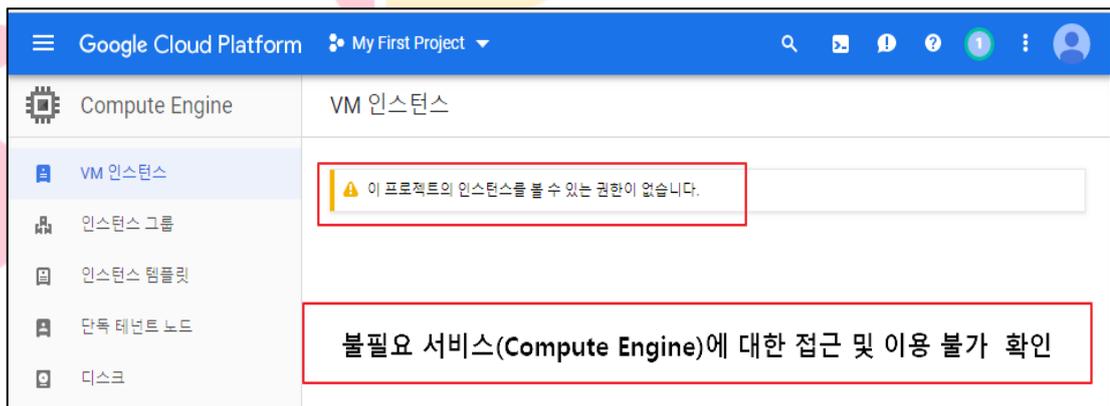
보기 모드 기준: 구성원 역할

유형	구성원	이름	역할	상속
<input type="checkbox"/>	사용자	alj...@gmail.com	탐색자 모니터링 편집자	
<input type="checkbox"/>	사용자	...	소유자	
<input type="checkbox"/>	사용자	...	프로젝트 결제 관리자	
<input type="checkbox"/>	사용자	...	탐색자 모니터링 뷰어	

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



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.

<p>진단 기준</p>	<p>양호기준 : 기타 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있을 경우</p> <p>취약기준 : 기타 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있지 않을 경우</p>
<p>비고</p>	

3. 가상 리소스 관리

3.1 ID 및 API 액세스

분류	가상 리소스 관리	중요도	상																								
항목명	ID 및 API 액세스																										
항목 설명	<p>VM에서 실행되는 애플리케이션은 서비스 계정을 사용하여 Google Cloud API를 호출합니다. 사용할 서비스 계정과 허용할 API 액세스 수준을 선택할 수 있다.</p> <p>※ 액세스 설정 Google Cloud API 리스트</p> <table border="1"> <thead> <tr> <th>구분</th> <th>상세내용</th> </tr> </thead> <tbody> <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>GCP(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, Cluster, 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> </tbody> </table>			구분	상세내용	사용자 정보	임대 단위 생성 및 관리 기능을 포함하여 관리형 서비스 제작자가 서비스 소비자와의 관계를 관리할 수 있도록 지원하는 유틸리티를 제공합니다.	서비스 관리	관리형 서비스 게시 및 서비스 구성 관리 메소드를 제공합니다.	서비스 제어	액세스 제어, 로깅 및 모니터링 서비스와의 통합 등, 관리형 서비스에 대한 제어부 기능을 제공합니다.	작업 대기열	GCP(Google Cloud Platform) 프로젝트에서 API 를 나열, 활성화, 비활성화하는 메소드를 제공합니다.	저장소	대량의 불변 데이터 객체를 저장하고 가져옵니다.	클라우드 소스 저장소	외부 데이터 소스의 데이터를 Google Cloud Storage 버킷에 전송하거나, Google Cloud Storage 버킷 사이에서 데이터를 전송합니다.	BigQuery	데이터 생성, 관리, 공유, 쿼리 기능을 제공합니다.	Bigtable 관리자	Cloud Bigtable 인스턴스, Cluster, 테이블을 관리합니다.	Bigtable 데이터	테라바이트, 페타바이트 단위의 스키마 없는 데이터를 저장하는 NoSQL 빅데이터 솔루션에 액세스합니다.	Cloud 게시/구독	애플리케이션 사이에서 안정적인 다대다 비동기 메시징 기능을 제공합니다.	Cloud Datastore	스키마 없는 NoSQL 문서 데이터베이스에 액세스하여 애플리케이션을 위한 강력하고 확장성이 뛰어난 완전 관리형 저장소를 제공합니다.
	구분	상세내용																									
	사용자 정보	임대 단위 생성 및 관리 기능을 포함하여 관리형 서비스 제작자가 서비스 소비자와의 관계를 관리할 수 있도록 지원하는 유틸리티를 제공합니다.																									
	서비스 관리	관리형 서비스 게시 및 서비스 구성 관리 메소드를 제공합니다.																									
	서비스 제어	액세스 제어, 로깅 및 모니터링 서비스와의 통합 등, 관리형 서비스에 대한 제어부 기능을 제공합니다.																									
	작업 대기열	GCP(Google Cloud Platform) 프로젝트에서 API 를 나열, 활성화, 비활성화하는 메소드를 제공합니다.																									
	저장소	대량의 불변 데이터 객체를 저장하고 가져옵니다.																									
	클라우드 소스 저장소	외부 데이터 소스의 데이터를 Google Cloud Storage 버킷에 전송하거나, Google Cloud Storage 버킷 사이에서 데이터를 전송합니다.																									
	BigQuery	데이터 생성, 관리, 공유, 쿼리 기능을 제공합니다.																									
	Bigtable 관리자	Cloud Bigtable 인스턴스, Cluster, 테이블을 관리합니다.																									
	Bigtable 데이터	테라바이트, 페타바이트 단위의 스키마 없는 데이터를 저장하는 NoSQL 빅데이터 솔루션에 액세스합니다.																									
	Cloud 게시/구독	애플리케이션 사이에서 안정적인 다대다 비동기 메시징 기능을 제공합니다.																									
Cloud Datastore	스키마 없는 NoSQL 문서 데이터베이스에 액세스하여 애플리케이션을 위한 강력하고 확장성이 뛰어난 완전 관리형 저장소를 제공합니다.																										

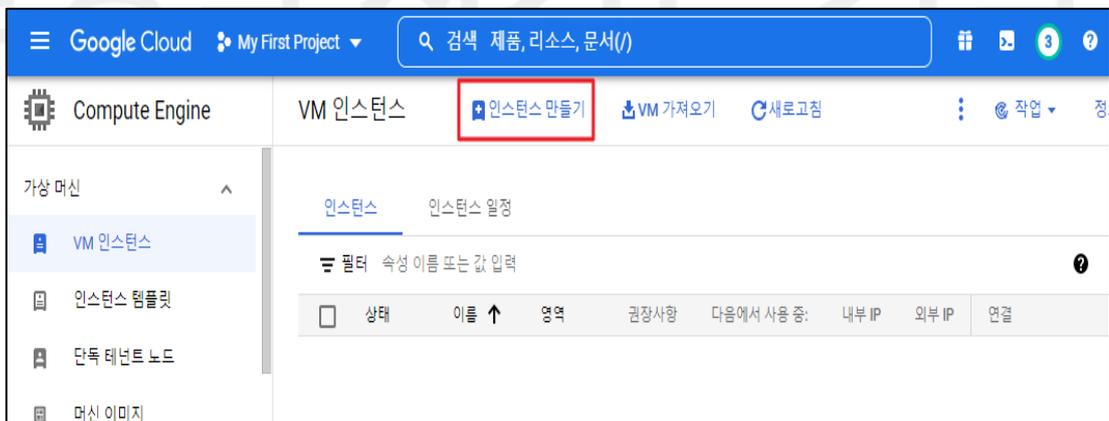
Cloud Debugger	실행 중인 애플리케이션을 중단하거나 지연시키지 않고, 애플리케이션의 호출 스택과 변수를 조사합니다.
Cloud SQL	완전 관리형 MySQL 데이터베이스를 제공하는 Cloud SQL 인스턴스를 생성하고 구성합니다.
Compute Engine	GCP(Google Cloud Platfor)에서 가상 머신을 생성하고 실행합니다.
Stackdriver 추적	Stackdriver Trace 에 추적 데이터를 보내고 가져옵니다. App Engine 애플리케이션은 기본값으로 데이터를 생성하므로, 별도의 작업 없이 이용할 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.

가. ID 및 API 액세스 설정

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



2) 인스턴스 만들기



설정
방법

3) VM 인스턴스 옵션 및 정보 입력

VM 인스턴스를 만들려면 옵션 중 하나를 선택하세요.

- 새 VM 인스턴스**
VM 인스턴스 하나를 처음부터 만듭니다.
- 템플릿에서 VM 인스턴스 만들기
기존 템플릿에서 VM 인스턴스 하나를 만듭니다.
- Marketplace
VM 인스턴스에 바로 사용할 수 있는 솔루션을 배포합니다.

이름: instance-1

리전: us-central1 (아이오와) 영역: us-central1-a

머신 구성

머신 계열: 일반 용도 메모리 최적화
일반적인 작업 부하에 적합한 머신 유형이며 가격 및 유연성을 위해 최적화되었습니다.

세대: 1
Skylake CPU 플랫폼 또는 이전 버전의 플랫폼에서 제공

머신 유형: n1-standard-1 (vCPU 1개, 3.75GB 메모리)

	vCPU	메모리
	1	3.75GB

4) '기본 액세스 허용' 액세스 범위 설정

Debian GNU/Linux 9 (stretch) 변경

ID 및 API 액세스

서비스 계정: Compute Engine default service account

액세스 범위

- 기본 액세스 허용
- 모든 Cloud API에 대한 전체 액세스 허용
- 각 API에 액세스 설정

방화벽

태그 및 방화벽 규칙을 추가하여 인터넷에서 특정 네트워크 트래픽을 허용합니다.

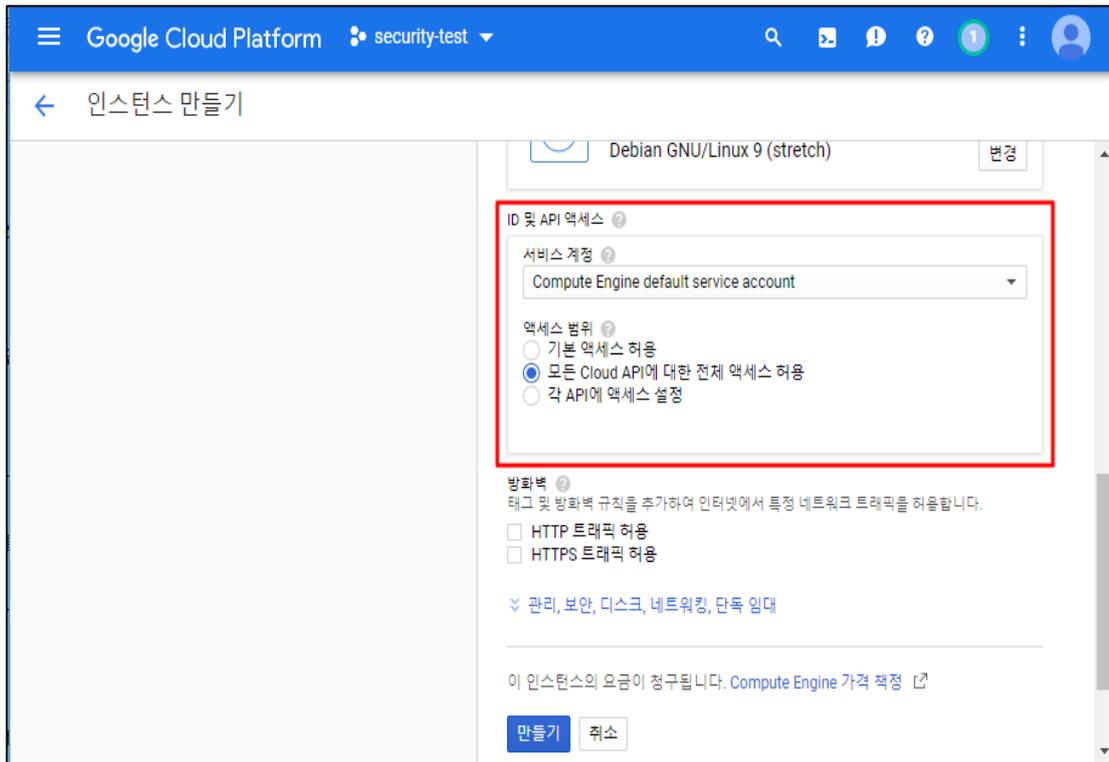
- HTTP 트래픽 허용
- HTTPS 트래픽 허용

관리, 보안, 디스크, 네트워킹, 단독 임대

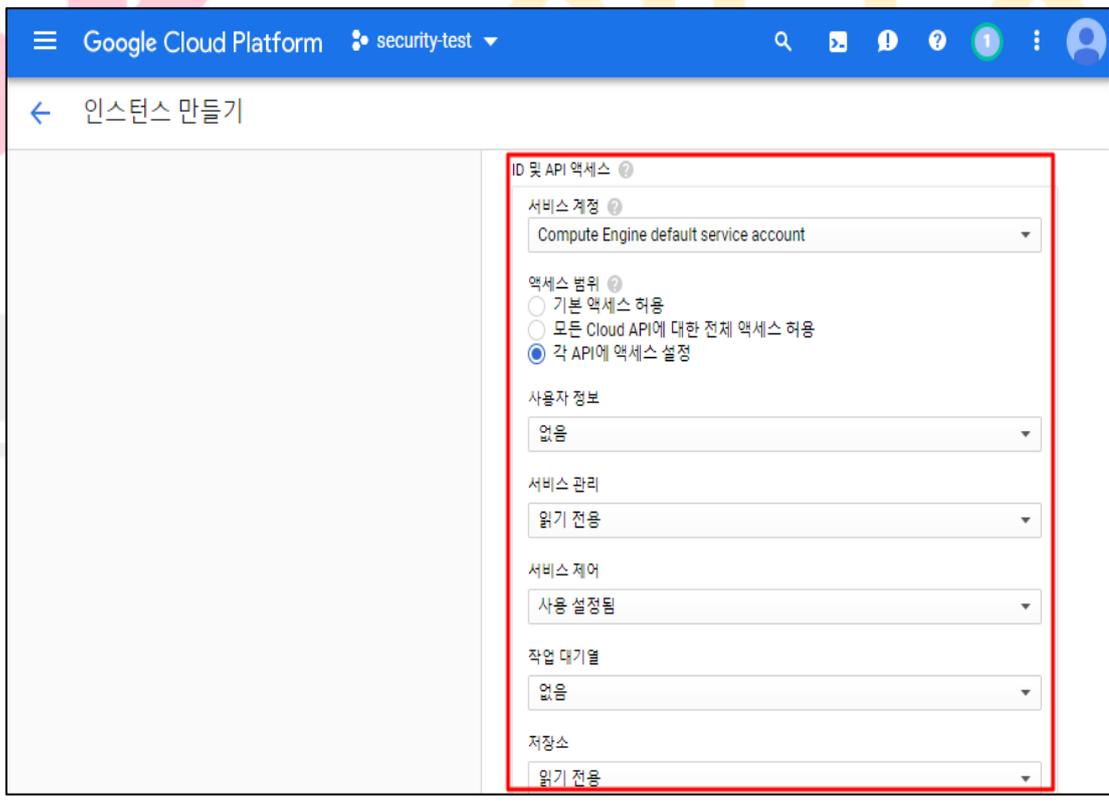
이 인스턴스의 요금이 청구됩니다. [Compute Engine 가격 책정](#)

만들기 취소

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



6) '각 API 에 액세스 설정' 액세스 범위 설정



	클라우드 소스 저장소 <input type="text" value="없음"/> BigQuery <input type="text" value="없음"/> Bigtable 관리자 <input type="text" value="없음"/> Bigtable 데이터 <input type="text" value="없음"/> Cloud 계서/구독 <input type="text" value="없음"/> Cloud Datastore <input type="text" value="없음"/> Cloud Debugger <input type="text" value="없음"/>
	Cloud SQL <input type="text" value="없음"/> Compute Engine <input type="text" value="없음"/> Stackdriver 추적 <input type="text" value="쓰기 전용"/> Stackdriver Logging API <input type="text" value="쓰기 전용"/> Stackdriver Monitoring API <input type="text" value="쓰기 전용"/>

7) 인스턴스 생성 완료

VM 인스턴스	VM 인스턴스	VM 인스턴스	VM 인스턴스	VM 인스턴스
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]
<input checked="" type="checkbox"/>	instance-1	us-central1-a	[blurred]	(nic0)
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]

진단
기준

양호기준

: 서비스 역할에 맞게 API 액세스 설정이 되어 있는 경우

취약기준

: 서비스 역할에 맞게 API 액세스 설정이 되어 있지 않은 경우

비고

3.2 VM 인스턴스 관리 및 보안

분류	가상 리소스 관리	중요도	하								
항목명	VM 인스턴스 관리 및 보안										
항목 설명	<p>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 삭제 보호(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.</p> <p>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.</p> <p>※ VM 인스턴스 보안 설정</p>										
	<table border="1"> <thead> <tr> <th>제목</th> <th>설명</th> </tr> </thead> <tbody> <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> </tbody> </table>			제목	설명	보안 부팅 설정	안전한 부팅에서는 모든 부팅 구성요소의 디지털 서명을 확인하고 서명 확인에 실패할 경우 부팅 프로세스를 중단하여 시스템에서 인증된 소프트웨어만 실행하도록 보장합니다.	vTPM 설정	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.	무결성 모니터링 사용 설정	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.
	제목	설명									
	보안 부팅 설정	안전한 부팅에서는 모든 부팅 구성요소의 디지털 서명을 확인하고 서명 확인에 실패할 경우 부팅 프로세스를 중단하여 시스템에서 인증된 소프트웨어만 실행하도록 보장합니다.									
vTPM 설정	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.										
무결성 모니터링 사용 설정	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.										
<p>※ 무결성 모니터링은 신중한 부팅에서 수집하는 데이터를 기반으로 하기 때문에 vTPM을 사용 중지하면 무결성 모니터링도 사용 중지됩니다.</p>											

가. VM 인스턴스 보안 설정

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



2) 인스턴스 만들기



3) VM 인스턴스 옵션 및 정보 입력



4) 부팅 디스크 변경

Google Cloud My First Project

인스턴스 만들기

VM 인스턴스를 만들려면 옵션 중 하나를 선택하세요.

- 새 VM 인스턴스**
VM 인스턴스 하나를 처음부터 만듭니다.
- 템플릿에서 VM 인스턴스 만들기
기존 템플릿에서 VM 인스턴스 하나를 만듭니다.
- 머신 이미지에서 VM 인스턴스 만들기
기존 머신 이미지에서 VM 인스턴스 하나를 만듭니다.
- Marketplace
VM 인스턴스에 바로 사용할 수 있는 솔루션을 배포합니다.

컨테이너
이 VM 인스턴스에 컨테이너 이미지 배포

DEPLOY CONTAINER

부팅 디스크

이름 instance-1
 유형 새로운 균형 있는 영구 디스크
 크기 10GB
 라이선스 유형 무료
 이미지 Debian GNU/Linux 11 (bullseye)

변경

5) VM 이미지 설정

Google Cloud My First Project

인스턴스 만들기

VM 인스턴스를 만들려면 옵션 중 하나를 선택하세요.

- 새 VM 인스턴스**
VM 인스턴스 하나를 처음부터 만듭니다.
- 템플릿에서 VM 인스턴스 만들기
기존 템플릿에서 VM 인스턴스 하나를 만듭니다.
- 머신 이미지에서 VM 인스턴스 만들기
기존 머신 이미지에서 VM 인스턴스 하나를 만듭니다.
- Marketplace
VM 인스턴스에 바로 사용할 수 있는 솔루션을 배포합니다.

부팅 디스크

이 이미지나 스냅샷을 선택하여 부팅 디스크를 만들거나 기존 디스크를 연결하세요. 원하는 내용을 찾을 수 없으신가요? 수백 개의 VM 솔루션을 살펴보세요. [Marketplace](#)

공개 이미지 커스텀 이미지 스냅샷 보관처리 스냅샷 기존 디스크

운영체제 Rocky Linux
 버전 * Rocky Linux 8
 x86_64, x86_64 built on 20221102
 부팅 디스크 유형 * 균형 있는 영구 디스크

디스크 유형 비교

크기(GB) * 20

고급 구성 표시

선택 취소

6) [관리] > [삭제 보호 사용 설정]

Google Cloud My First Project

인스턴스 만들기

VM 인스턴스를 만들려면 옵션 중 하나를 선택하세요.

- 새 VM 인스턴스**
VM 인스턴스 하나를 처음부터 만듭니다.
- 템플릿에서 VM 인스턴스 만들기
기존 템플릿에서 VM 인스턴스 하나를 만듭니다.
- 머신 이미지에서 VM 인스턴스 만들기
기존 머신 이미지에서 VM 인스턴스 하나를 만듭니다.
- Marketplace
VM 인스턴스에 바로 사용할 수 있는 솔루션을 배포합니다.

관리
설명, 삭제 보호, 예약, 자동화, 가용성 정책

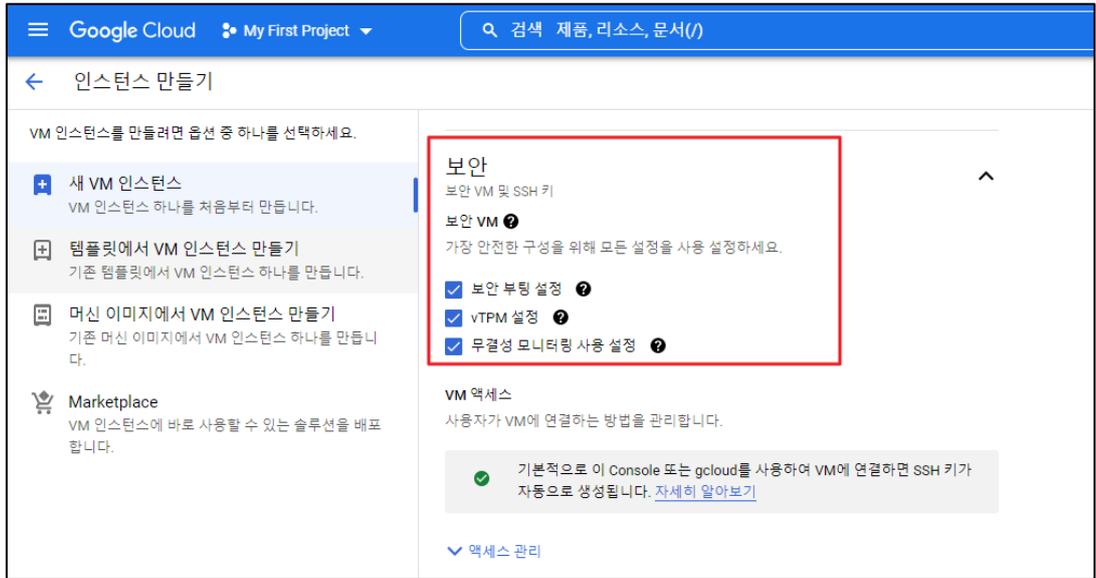
설명

삭제 보호

삭제 보호 사용 설정

예약
애플리케이션 정책
생성된 예약 자동 사용

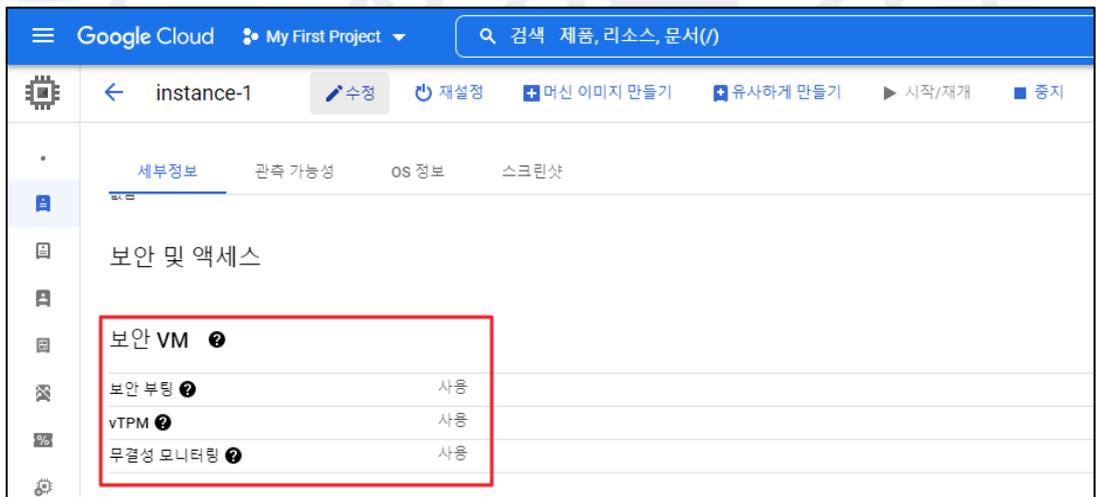
7) [보안] > [보안 VM] > [보안 부팅 설정], [vTPM 설정], [무결성 모니터링 사용 설정]



8) 인스턴스 생성 완료



9) 설정된 보안 VM 옵션 확인

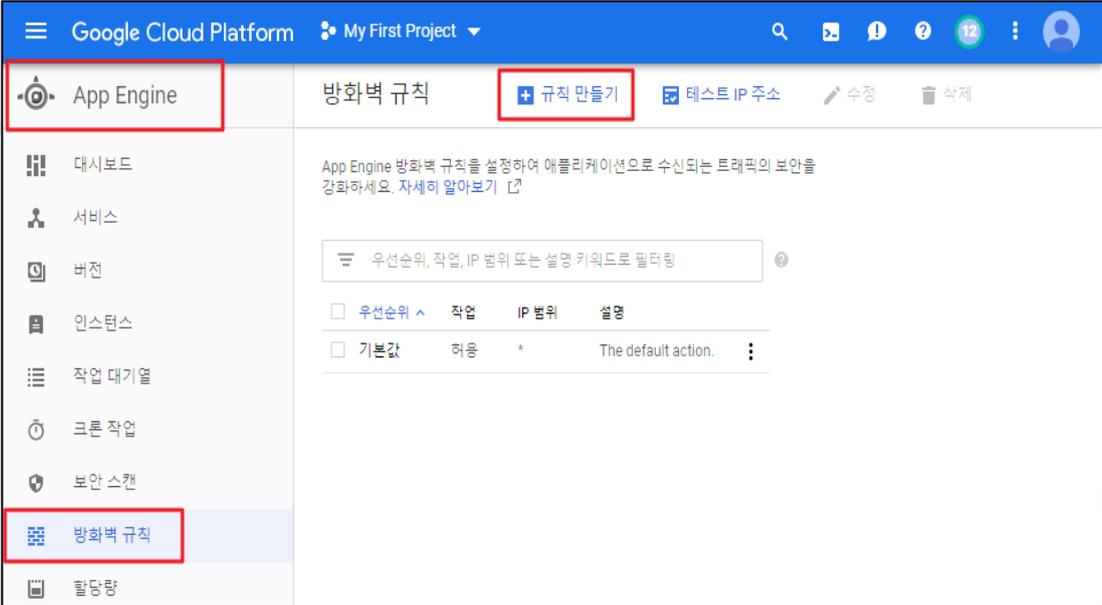


진단 기준	<p>양호기준 : 인스턴스 보안 부팅 설정을 사용하고 있을 경우</p> <p>취약기준 : 인스턴스 보안 부팅 설정을 사용하고 있지 않을 경우</p>
비고	

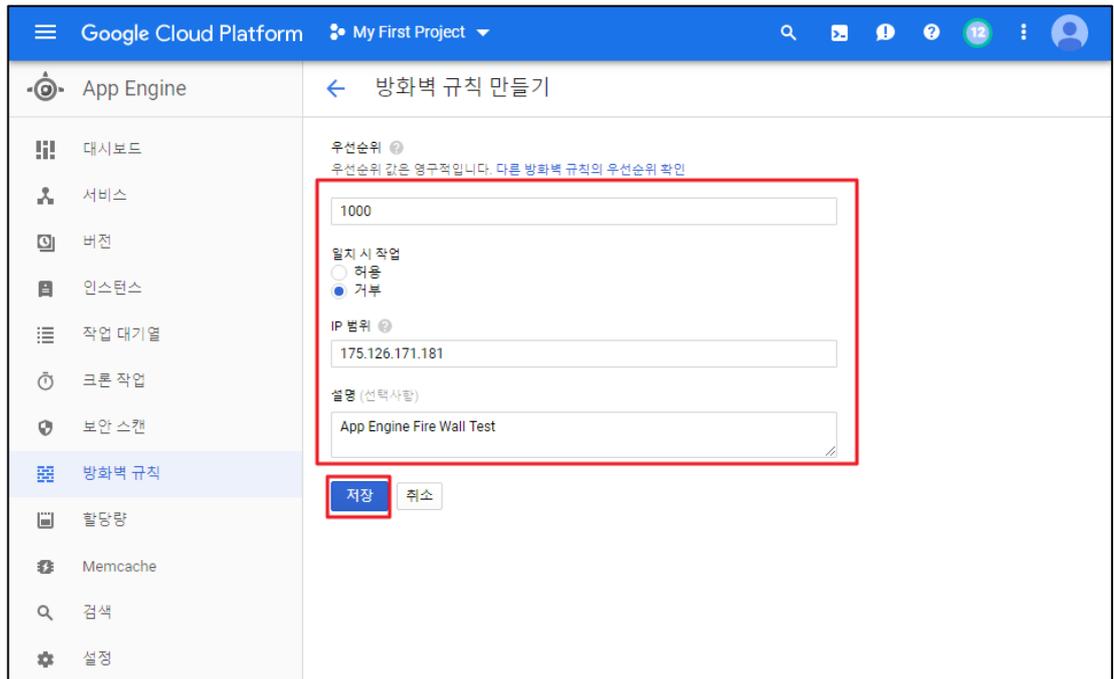


안녕을 지키는 기술

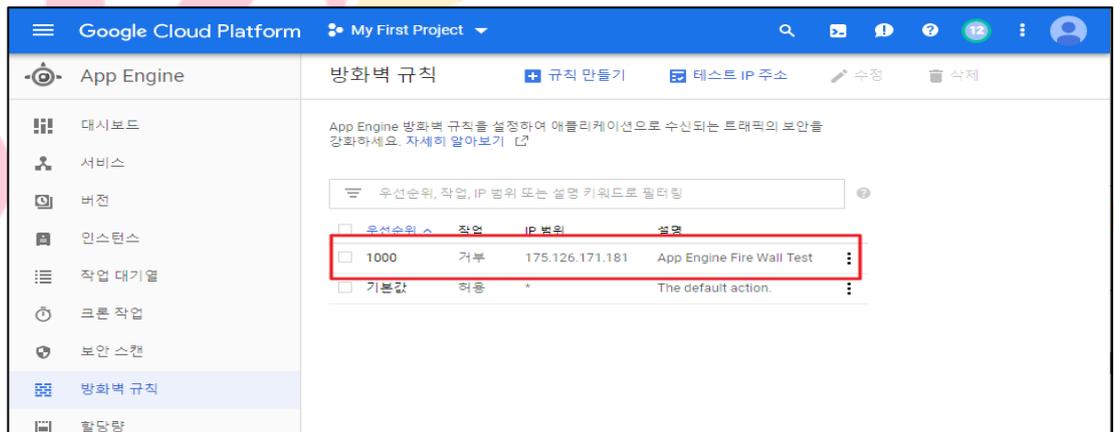
3.3 애플리케이션 방화벽

분류	가상 리소스 관리	중요도	중
항목명 항목 설명	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>		
설정 방법	<p>가. App Engine 방화벽 내 규칙 생성</p> <p>1) [App Engine] > [방화벽 규칙] > [규칙 만들기]</p> <p>- App Engine 서비스 내 방화벽 규칙 생성 시도</p> 		

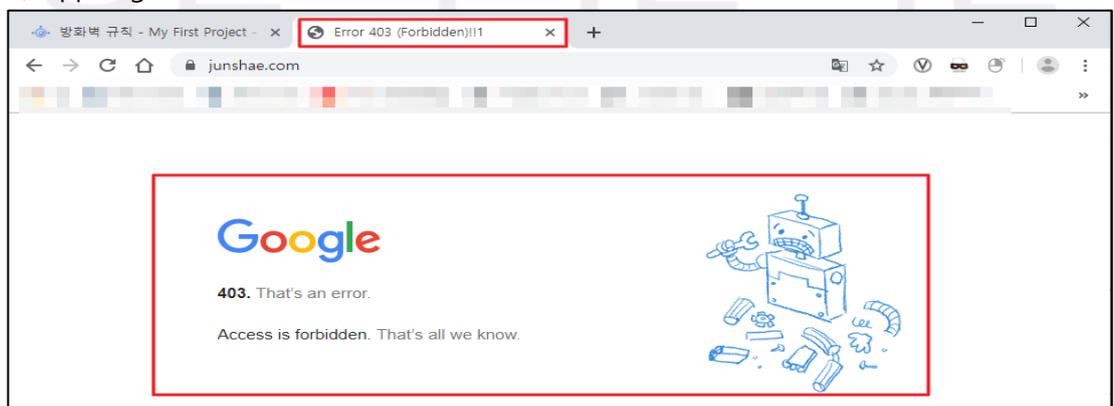
2) 적용하고자 하는 서비스에 대해 방화벽 규칙 설정



3) 방화벽 규칙 생성 확인



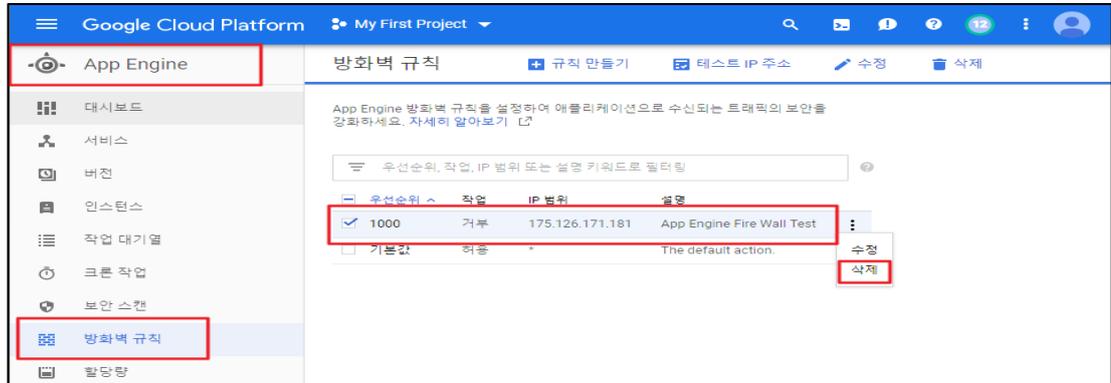
4) App Engine 방화벽 규칙 적용 확인



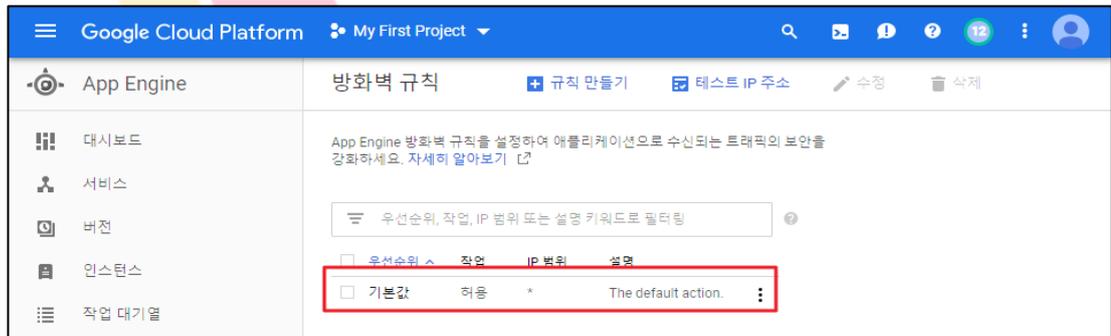
나. App Engine 방화벽 내 규칙 삭제

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

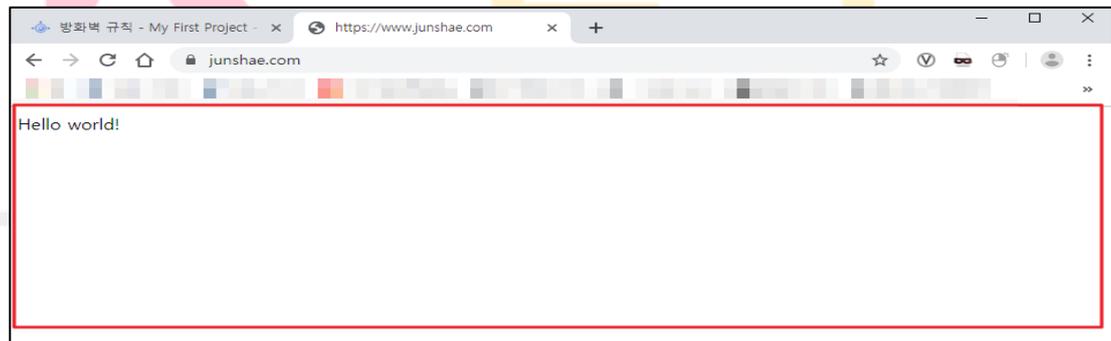
- 방화벽 규칙 삭제 시도



2) 방화벽 규칙 삭제 확인



3) 방화벽 규칙 적용 확인



진단
기준

양호기준

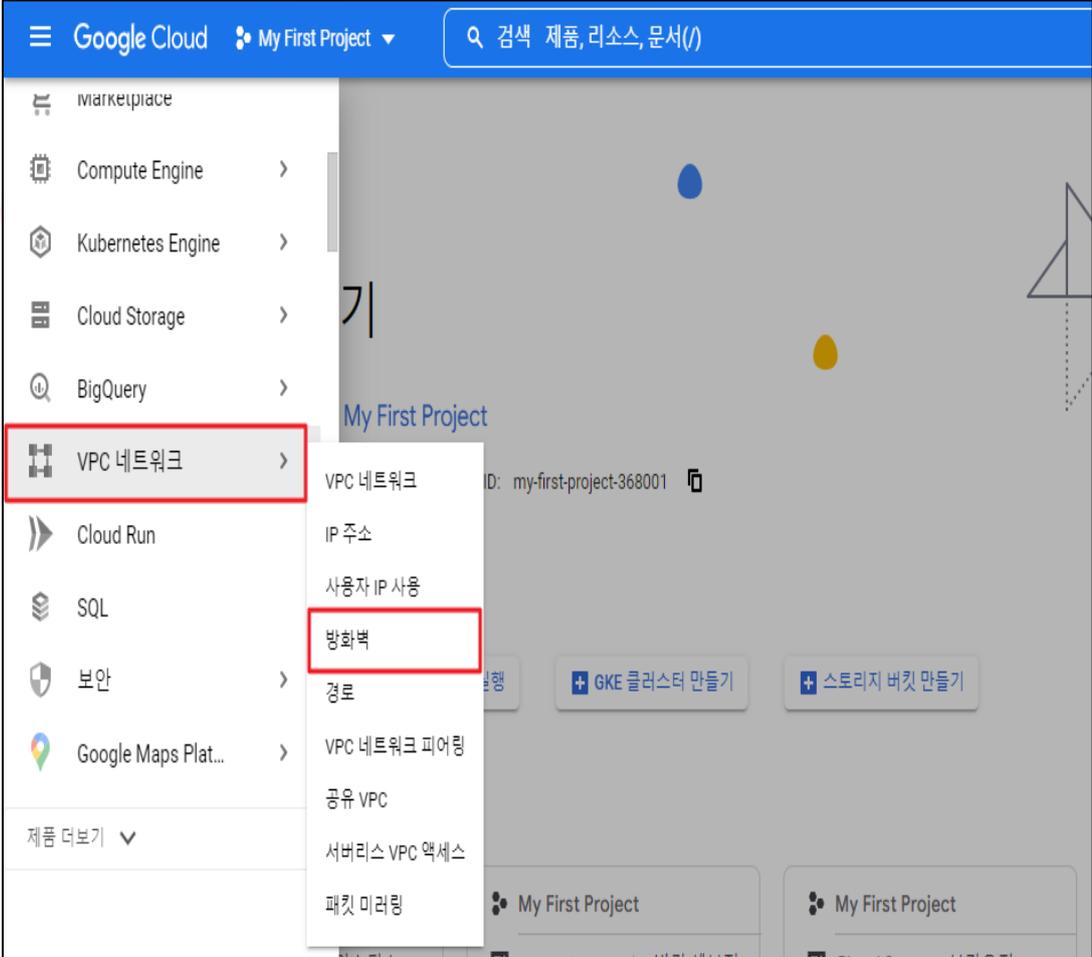
: IP 범위가 모두 허용(*) 설정이 되어 있지 않는 경우

취약기준

: IP 범위가 모두 허용(*) 설정이 되어 있는 경우

비고

3.4 네트워크 방화벽 인/아웃바운드 ANY 설정 관리

분류	가상 리소스 관리	중요도	상
항목명	네트워크 방화벽 인/아웃바운드 ANY 설정 관리		
항목 설명	<p>Virtual 프라이빗 Cloud(VPC) 방화벽 규칙이 특정 프로젝트 및 네트워크에 적용됩니다. VPC 방화벽 규칙을 사용하면 지정한 구성을 기준으로 가상 머신(VM) 인스턴스 간의 연결을 허용하거나 거부할 수 있습니다. 사용 설정한 VPC 방화벽 규칙은 인스턴스의 구성 및 운영 체제와 상관없이 인스턴스를 보호할 수 있도록 항상 실행됩니다.</p> <p>모든 VPC 네트워크는 분산형 방화벽으로 작동하며 방화벽 규칙은 네트워크 수준에서 정의되지만 연결은 인스턴스별로 허용되거나 거부됩니다. VPC 방화벽 규칙은 인스턴스와 다른 네트워크 사이뿐만 아니라 동일한 네트워크 내의 개별 인스턴스 간에 존재하는 것으로 볼 수 있으며 구성요소를 사용하면 트래픽의 프로토콜, 포트를 기준으로 특정 트래픽 유형을 대상으로 지정할 수 있습니다.</p>		
설정 방법	<p>가. VPC 네트워크 방화벽 설정</p> <p>1) [메인] > [VPC 네트워크] > [방화벽]</p> 		

2) 방화벽 규칙(송/수신) 내 프로토콜/포트 확인

The screenshot shows the Google Cloud Firewall Rules interface. A table lists firewall rules with columns for Name, Type, Target, Filter, Protocol/Port, Action, Priority, Network, and Log. The 'secu-test' rule is highlighted, and its 'tcp:22' protocol/port is enclosed in a red box.

이름	유형	대상	필터	프로토콜/포트	작업	우선순위	네트워크	로그
secu-test	수신	test	IP 범위: 0.0.0	tcp:22	허용	1000	default	사용 안 함
default-allow-icmp	수신	전체 적용	IP 범위: 0.0.0	icmp	허용	65534	default	사용 안 함

진단 기준

양호기준

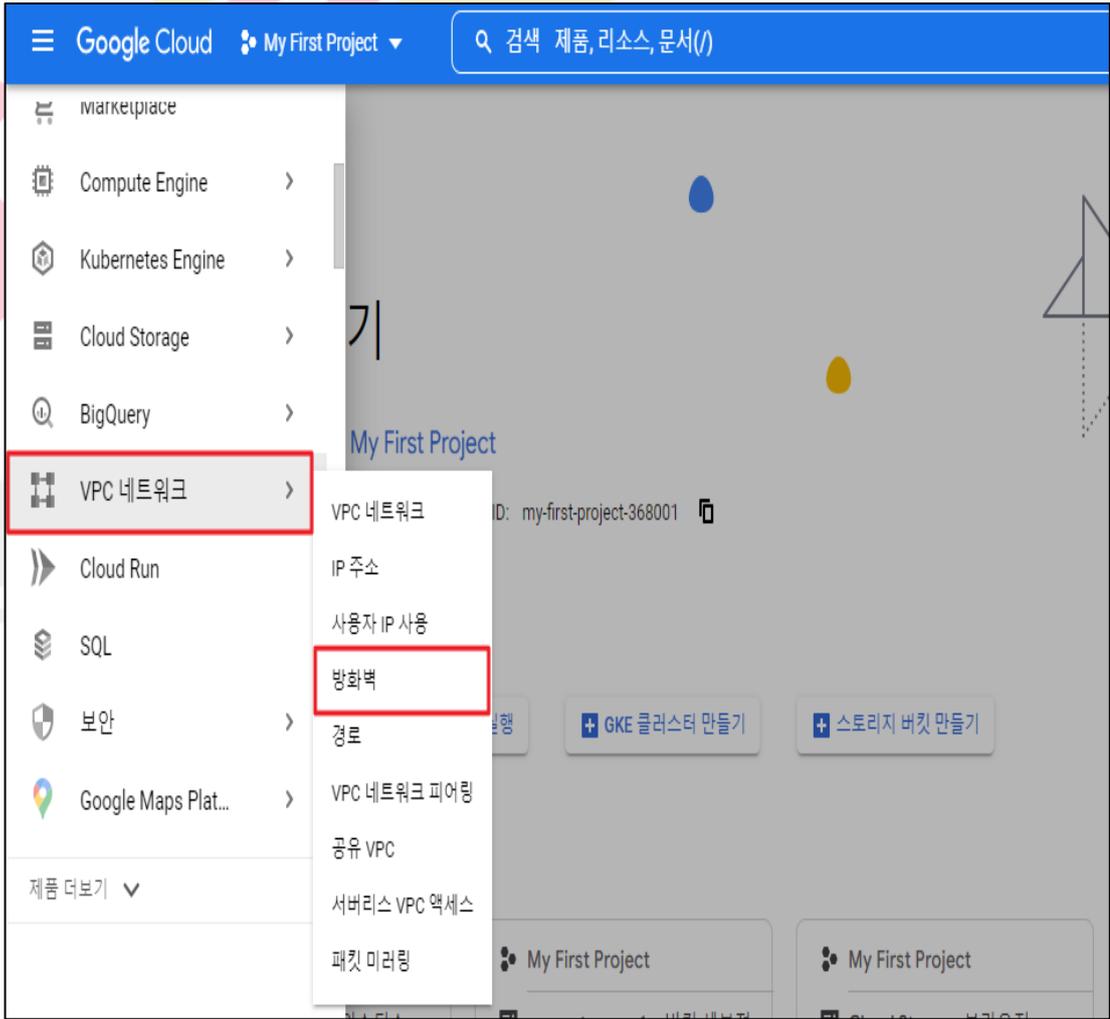
: 방화벽 내 인/아웃바운드의 포트가 Any 로 허용되어 있지 않을 경우

취약기준

: 방화벽 내 인/아웃바운드의 포트가 Any 로 허용되어 있을 경우

비고

3.5 네트워크 방화벽 인/아웃바운드 불필요 정책 관리

분류	가상 리소스 관리	중요도	상
항목명	네트워크 방화벽 인/아웃바운드 불필요 정책 관리		
항목 설명	<p>Virtual 프라이빗 Cloud(VPC) 방화벽 규칙이 특정 프로젝트 및 네트워크에 적용됩니다. VPC 방화벽 규칙을 사용하면 지정한 구성을 기준으로 가상 머신(VM) 인스턴스 간의 연결을 허용하거나 거부할 수 있습니다. 사용 설정한 VPC 방화벽 규칙은 인스턴스의 구성 및 운영 체제와 상관없이 인스턴스를 보호할 수 있도록 항상 실행됩니다.</p> <p>모든 VPC 네트워크는 분산형 방화벽으로 작동하며 방화벽 규칙은 네트워크 수준에서 정의되지만 연결은 인스턴스별로 허용되거나 거부됩니다. VPC 방화벽 규칙은 인스턴스와 다른 네트워크 사이뿐만 아니라 동일한 네트워크 내의 개별 인스턴스 간에 존재하는 것으로 볼 수 있으며 구성요소를 사용하면 트래픽의 소스, 목적지를 기준으로 특정 트래픽 유형을 대상으로 지정할 수 있습니다.</p>		
설정 방법	<p>가. VPC 네트워크 방화벽 설정</p> <p>1) [메인] > [VPC 네트워크] > [방화벽]</p> 		

2) 방화벽 규칙(송/수신) 내 필터(IP 범위) 확인

Google Cloud My First Project

방화벽 정책 만들기 방화벽 규칙 만들기

VPC 방화벽 규칙

방화벽 규칙은 인스턴스로 수신 또는 발신되는 트래픽을 제어합니다. 기본적으로 네트워크 외부에서 수신되는 트래픽은 차단됩니다. [자세히 알아보기](#)

참고: App Engine 방화벽은 [App Engine 방화벽 규칙 섹션](#)에서 관리됩니다.

SMTP port 25 disallowed in this project

새로고침 로그 구성 삭제

필터 속성 이름 또는 값 입력

<input type="checkbox"/>	이름	유형	대상	필터	프로토콜/포트	작업	우선순위	네트워크	로그
<input type="checkbox"/>	secu-test	수신	test	IP 범위: 192.168.2.0/24	tcp:22	허용	1000	default	사용 안함
<input type="checkbox"/>	default-allow-icmp	수신	전체 적용	IP 범위: 0.0.0.0/0	icmp	허용	65534	default	사용 안함
<input type="checkbox"/>	default-allow-internal	수신	전체 적용	IP 범위: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	허용	65534	default	사용 안함

양호기준

: 방화벽 내 인/아웃바운드 규칙 내 불필요한 정책(Source, Destination)이 존재하지 않는 경우

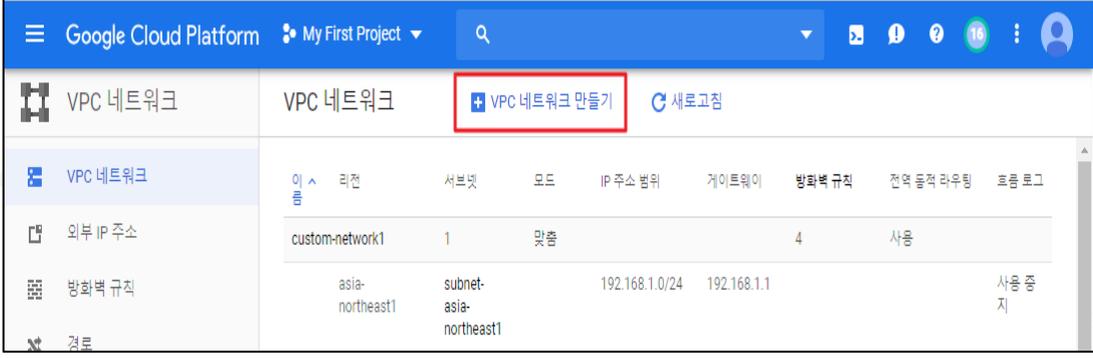
취약기준

: 방화벽 내 인/아웃바운드 규칙 내 불필요한 정책(Source, Destination)이 존재하는 경우

비고

안녕을 지키는 기술

3.6 VPC 네트워크 서브넷 관리

분류	가상 리소스 관리	중요도	상						
항목명	VPC 네트워크 서브넷 관리								
항목 설명	<p>VPC 네트워크는 Compute Engine 가상 머신(VM) 인스턴스, Kubernetes Engine Cluster, App Engine 가변형 인스턴스, 프로젝트의 다른 리소스를 위한 연결을 제공하며 하위 네트워크 또는 서브넷이라는 유용한 IP 범위 파티션 하나 그 이상으로 구성됩니다.</p> <p>※ 서브넷 속성</p> <table border="1" data-bbox="311 582 1428 1108"> <thead> <tr> <th data-bbox="311 582 470 627">구분</th> <th data-bbox="470 582 1428 627">설명</th> </tr> </thead> <tbody> <tr> <td data-bbox="311 627 470 952">자동모드</td> <td data-bbox="470 627 1428 952">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.</td> </tr> <tr> <td data-bbox="311 952 470 1108">커스텀 모드</td> <td data-bbox="470 952 1428 1108">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> </tbody> </table>			구분	설명	자동모드	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.
구분	설명								
자동모드	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.								
설정 방법	<p>가. VPC 네트워크 생성 방법</p> <p>1) [VPC 네트워크] > [VPC 네트워크 만들기]</p> <p>- VPC 네트워크 생성 시도</p>  <p>2) [VPC 네트워크 만들기] > [서브넷] > [새 서브넷]</p> <p>- 맞춤 설정을 통한 커스텀 서브넷 및 흐름로그 사용 설정</p>								

Google Cloud Platform My First Project

VPC 네트워크 VPC 네트워크 만들기

설명 (선택사항)
security_subnet_test

서브넷
서브넷을 사용하면 Google Cloud 내에 자체 사설 클라우드 토폴로지를 만들 수 있습니다. 각 리전에 서브넷을 만들려면 '자동'을 클릭하고, 서브넷을 직접 정의하려면 '맞춤설정'을 클릭하세요. [자세히 알아보기](#)

서브넷 생성 모드
맞춤설정 자동

새 서브넷

이름
security3

설명 추가

리전
asia-northeast1

IP 주소 범위
10.10.2.0/24

보통 IP 범위 만들기

비공개 Google 액세스
 사용
 사용 중지

플러그인
VPC 플러그인 사용 설정해도 상충되는 영향이 없지만 일부 시스템에서 대량의 플러그인 생성하여 Stackdriver 비용이 증가할 수 있습니다. [자세히 알아보기](#)

사용
 사용 중지

로그 구성

완료 취소

+ 서브넷 추가

VPC 네트워크 VPC 네트워크 만들기

이름
secu-subnet3

설명 (선택사항)
security_subnet_test

서브넷
서브넷을 사용하면 Google Cloud 내에 자체 사설 클라우드 토폴로지를 만들 수 있습니다. 각 리전에 서브넷을 만들려면 '자동'을 클릭하고, 서브넷을 직접 정의하려면 '맞춤설정'을 클릭하세요. [자세히 알아보기](#)

서브넷 생성 모드
맞춤설정 자동

security3

+ 서브넷 추가

동적 라우팅 모드
 지역
Cloud 라우터에서 자신이 생성된 리전의 경로만 학습합니다.

전역
전역 라우팅을 사용하면 단일 VPN 또는 상호 연결 및 Cloud 라우터가 있는 모든 지역과 통하는 경로를 동적으로 학습할 수 있습니다.

DNS 서버 정책 (선택사항)
서버 정책 없음

만들기 취소

Equivalent REST or command line

3) 생성된 VPC 네트워크 및 서브넷 내용 확인

VPC 네트워크	지역	네트워크 이름	주소 범위	서브넷 이름	주소 범위	상태	비고
europa-west6	default		10.172.0.0/20	10.172.0.1	사용 중지		
asia-northeast2	default		10.174.0.0/20	10.174.0.1	사용 중지		
secu-subnet1	2	맞춤		7	사용		
asia-northeast1	security1		10.146.0.0/20	10.146.0.1	사용 중지		
asia-northeast1	security4		10.144.0.0/20	10.144.0.1	사용		
secu-subnet2	1	맞춤		4	사용		
asia-northeast1	security2		10.144.0.0/20	10.144.0.1	사용 중지		
secu-subnet3	1	맞춤		0	사용 안함		
asia-northeast1	security3		10.10.2.0/24	10.10.2.1	사용		

항목	세부정보
VPC 네트워크	security3
외부 IP 주소	VPC 네트워크 secu-subnet3
방화벽 규칙	리전 asia-northeast1
경로	IP 주소 범위 10.10.2.0/24 게이트웨이 10.10.2.1
VPC 네트워크 피어링	비공개 Google 액세스 사용
공유 VPC	흐름 로그 사용 흐름 로그 보기
서버리스 VPC 액세스	로그 세부정보 동등한 REST

나. VPC 네트워크 삭제 방법

1) [VPC 네트워크] > [VPC 네트워크]

- 삭제 하고자 하는 VPC 네트워크 선택

Region	Network Name	Subnet Name	IP Range	Secondary IP Range	Usage
europa-west6	default		10.172.0.0/20	10.172.0.1	
asia-northeast2	default		10.174.0.0/20	10.174.0.1	
	secu-subnet1	1	맞춤	6	사용
asia-northeast1	security1		10.146.0.0/20	10.146.0.1	
	secu-subnet2	1	맞춤	3	사용
asia-northeast1	security2		10.144.0.0/20	10.144.0.1	
	secu-subnet3	1	맞춤	0	사용 안함
asia-northeast1	security3		10.10.2.0/24	10.10.2.1	

2) VPC 네트워크 삭제 시도

네트워크 삭제

네트워크를 삭제하면 하위 네트워크, 경로, 방화벽 규칙도 삭제됩니다. 이 작업은 취소할 수 없습니다.

'secu-subnet3' 네트워크를 삭제하시겠습니까?

취소 **삭제**

3) VPC 네트워크 삭제 완료 (secu-subnet3)

Region	Network	Subnet Name	IP Range	Start IP	End IP	Status
asia-east2	default		10.170.0.0/20	10.170.0.1		삭제 완료
europa-west6	default		10.172.0.0/20	10.172.0.1		삭제 완료
asia-northeast2	default		10.174.0.0/20	10.174.0.1		삭제 완료
		secu-subnet1	2	맞춤	7	사용
asia-northeast1	security1		10.146.0.0/20	10.146.0.1		삭제 완료
asia-northeast1	security4		10.144.0.0/20	10.144.0.1		사용
		secu-subnet2	1	맞춤	4	사용
asia-northeast1	security2		10.144.0.0/20	10.144.0.1		삭제 완료

진단
기준

양호기준

: 퍼블릭/프라이빗 서브넷을 단일 가상 네트워크 리소스 내 혼용하여 사용하지 않을 경우

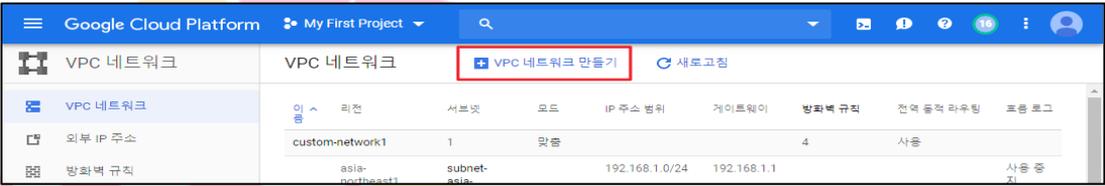
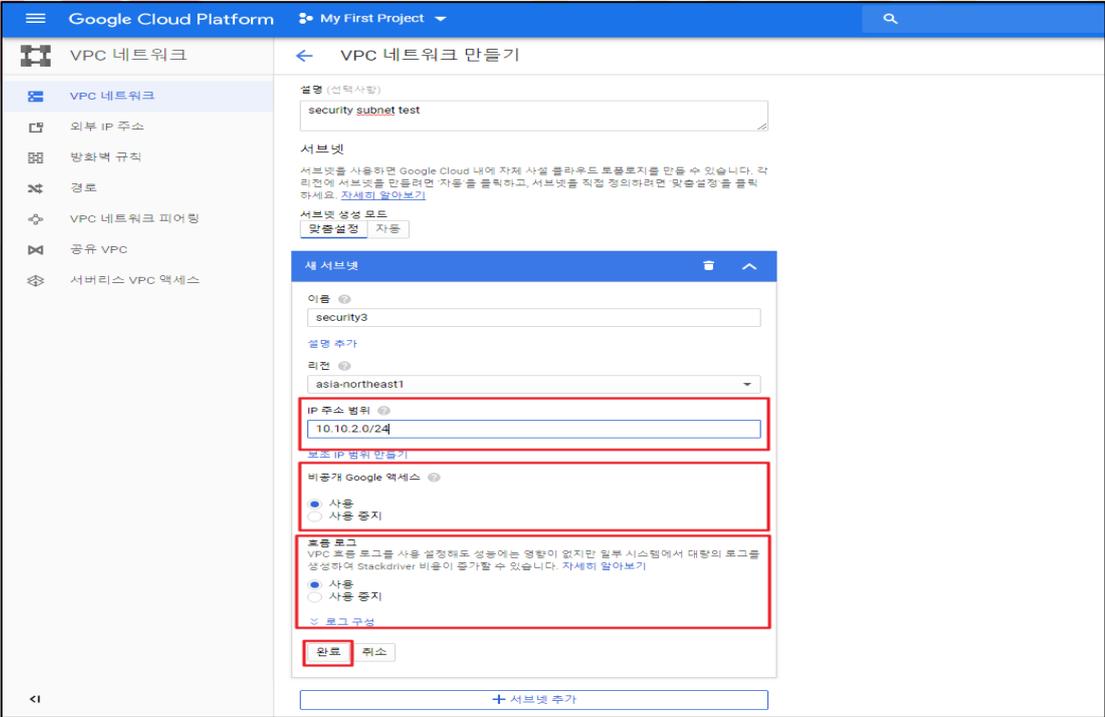
취약기준

: 퍼블릭/프라이빗 서브넷을 단일 가상 네트워크 리소스 내 혼용하여 사용하고 있을 경우

비고

안녕을 지키는 기술

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	<p>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.</p>		
설정 방법	<p>가. 비공개 구글 액세스 설정</p> <p>1) [VPC 네트워크] > [VPC 네트워크 만들기]</p> <p>- VPC 네트워크 생성 시도</p>  <p>2) [VPC 네트워크 만들기] > [서브넷] > [새 서브넷]</p> <p>- 비공개 Google 액세스 사용 설정</p> 		

VPC 네트워크 만들기

이름: secu-subnet3

설명 (선택사항): security subnet test

서브넷

서브넷 생성 모드: 맞춤설정 (선택사항)

동적 라우팅 모드: 지역 (선택사항)

DNS 서버 정책 (선택사항): 서버 정책 없음

만들기 취소

3) 생성된 VPC 네트워크 및 서브넷 내용 확인

VPC 네트워크	지역	서브넷	주소 범위	주소 범위	상태
europa-west6	default		10.172.0.0/20	10.172.0.1	사용 중지
asia-northeast2	default		10.174.0.0/20	10.174.0.1	사용 중지
secu-subnet1	2	맞춤	7		사용
asia-northeast1	security1		10.146.0.0/20	10.146.0.1	사용 중지
asia-northeast1	security4		10.144.0.0/20	10.144.0.1	사용
secu-subnet2	1	맞춤	4		사용
asia-northeast1	security2		10.144.0.0/20	10.144.0.1	사용 중지
secu-subnet3	1	맞춤	0		사용 안함
asia-northeast1	security3		10.10.2.0/24	10.10.2.1	사용

secu-subnet3 세부정보

지역: asia-northeast1

IP 주소 범위: 10.10.2.0/24

게이트웨이: 10.10.2.1

비공개 Google 액세스: 사용

흐름 로그: 사용

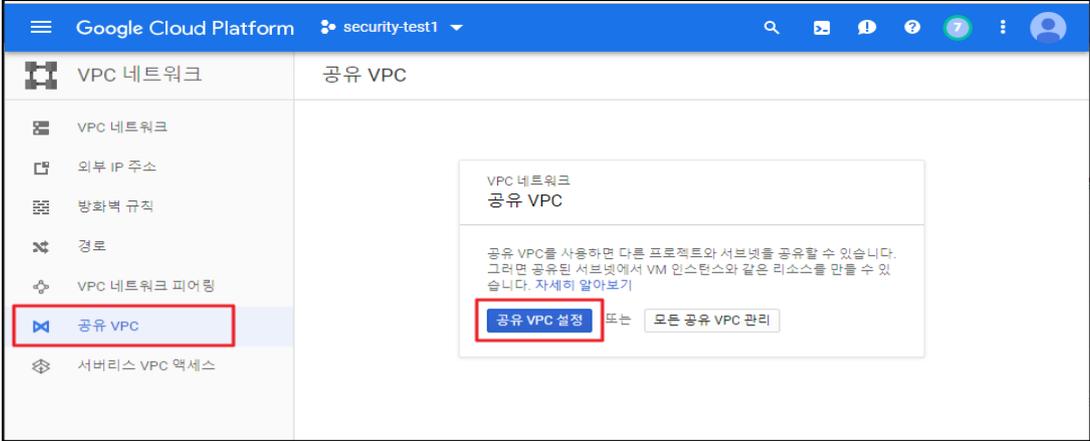
로그 세부정보

진단 기준	<p>양호기준 : 비공개 구글 액세스를 사용하지 않는 경우</p> <p>취약기준 : 비공개 구글 액세스를 사용하는 경우</p>
비고	



안녕을 지키는 기술

3.8 공유 VPC 관리

분류	가상 리소스 관리	중요도	중																																				
항목명	공유 VPC 관리																																						
항목 설명	<p>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.</p> <p>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.</p> <p>※ 공유 VPC List (예시)</p> <table border="1"> <thead> <tr> <th>호스트 프로젝트</th> <th>연결된(서비스) 프로젝트</th> <th>서브넷 명</th> <th>IP 주소 범위</th> <th>사용목적</th> <th>취약 유/무</th> </tr> </thead> <tbody> <tr> <td>ex) host-project</td> <td>ex) project1</td> <td>ex)default_subnet</td> <td>ex)192.168.0/24</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> </tbody> </table>			호스트 프로젝트	연결된(서비스) 프로젝트	서브넷 명	IP 주소 범위	사용목적	취약 유/무	ex) host-project	ex) project1	ex)default_subnet	ex)192.168.0/24	ex)사용목적	N/A						N/A																		
호스트 프로젝트	연결된(서비스) 프로젝트	서브넷 명	IP 주소 범위	사용목적	취약 유/무																																		
ex) host-project	ex) project1	ex)default_subnet	ex)192.168.0/24	ex)사용목적	N/A																																		
					N/A																																		
					N/A																																		
					N/A																																		
					N/A																																		
설정 방법	<p>가. 공유 VPC를 통한 조직 내 프로젝트 간 서브넷 공유</p> <p>1) [VPC 네트워크] > [공유 VPC] > [공유 VPC 설정]</p> <p>- 조직 내 프로젝트 간의 서브넷 공유를 위한 공유 VPC 설정 시도</p> 																																						

Google Cloud Platform security-test1

VPC 네트워크 < 공유 VPC 설정

1 호스트 프로젝트 사용 설정 2 서브넷 선택 3 권한 부여

공유 VPC 설정은 3단계로 구성됩니다.

1. 호스트 프로젝트 사용 설정
저장을 클릭하면 이 프로젝트가 호스트 프로젝트가 됩니다.
2. 서브넷 선택
공유할 서브넷을 선택합니다.
3. 권한 부여
사용자를 선택하고 서브넷에서 리소스를 만들 수 있는 권한을 부여합니다.

추가 정보가 필요하신가요? 공유 VPC 개념 및 생성에 대해 자세히 알아보세요.

저장하고 계속하기 취소

2) 조직 내 타 프로젝트와 공유할 서브넷 설정

Google Cloud Platform security-test1

VPC 네트워크 < 공유 VPC 설정

1 호스트 프로젝트 사용 설정 2 서브넷 선택 3 권한 부여

공유할 서브넷을 선택하세요. 이후에 생성되는 하위 서브넷을 포함해 프로젝트의 모든 서브넷을 공유하거나 개별적으로 선택할 수 있습니다.

공유 모드

모든 서브넷 공유(프로젝트 수준 권한)
이후에 생성되는 서브넷을 포함해 이 프로젝트의 모든 서브넷이 공유됩니다.

개별 서브넷(서브넷 수준 권한)
공유할 개별 서브넷입니다. 이후에 생성되는 서브넷은 자동으로 공유되지 않습니다.

공유할 서브넷	리전	VPC 네트워크	IP 주소 범위
<input checked="" type="checkbox"/> 서브넷 ^			
<input checked="" type="checkbox"/> security-subnet1	asia-northeast1	security-test	10.10.2.0/24

페이지당 행 수: 10 21 / 21 < >

서브넷 3개가 공유됩니다.

계속 취소

3) 연결할 프로젝트 설정

Google Cloud Platform security-test1

VPC 네트워크 < 공유 VPC 설정

호스트 프로젝트 사용 설정 서버넷 선택 3 권한 부여

서버넷을 공유하려면 사용자에게 Compute 네트워크 사용자 역할을 부여해야 합니다. 방법은 다음과 같습니다.

- 서비스 프로젝트 연결
- 역할을 기준으로 사용자 선택

서비스 프로젝트 연결

연결된 프로젝트의 사용자는 선택한 서버넷 또는 호스트 프로젝트의 Compute 네트워크 사용자 역할을 부여받을 수 있습니다.

프로젝트 이름 또는 ID로 필터링

<input checked="" type="checkbox"/>	프로젝트 이름	프로젝트 ID	라벨
<input checked="" type="checkbox"/>	security-test2	security-test2	

프로젝트 1개 선택함

역할을 기준으로 사용자 선택

역할을 하나 이상 선택하세요. 연결된 프로젝트에 속하며 선택한 역할을 갖는 사용자에게 선택한 서버넷 또는 호스트 프로젝트의 Compute 네트워크 사용자 역할이 부여됩니다.

- Compute 인스턴스 관리자
- Compute 네트워크 관리자
- 소유자
- 편집자

Kubernetes Engine 액세스

사용 설정됨

저장 취소

4) 설정된 공유 VPC 정보 확인

Google Cloud Platform security-test1

VPC 네트워크 < 공유 VPC > 모든 공유 VPC 관리 공유 VPC 사용 중지

이 프로젝트(security-test1)는 호스트입니다. 연결된 프로젝트와 서버넷을 공유하고 있습니다.

공유된 서버넷 및 권한 연결된 프로젝트

권한을 통해 공유된 서버넷에 액세스할 수 있는 사용자를 관리할 수 있습니다.

모든 서버넷 권한(프로젝트 수준 권한)

모든 서버넷에 대한 권한을 부여하려면 호스트 프로젝트를 선택하세요.

호스트 프로젝트 공유 대상

security-test1-250402 사용자 0명

개별 서버넷 권한(서버넷 수준 권한)

서버넷 사용 권한을 부여하려면 아래에서 하나 이상을 선택하세요.

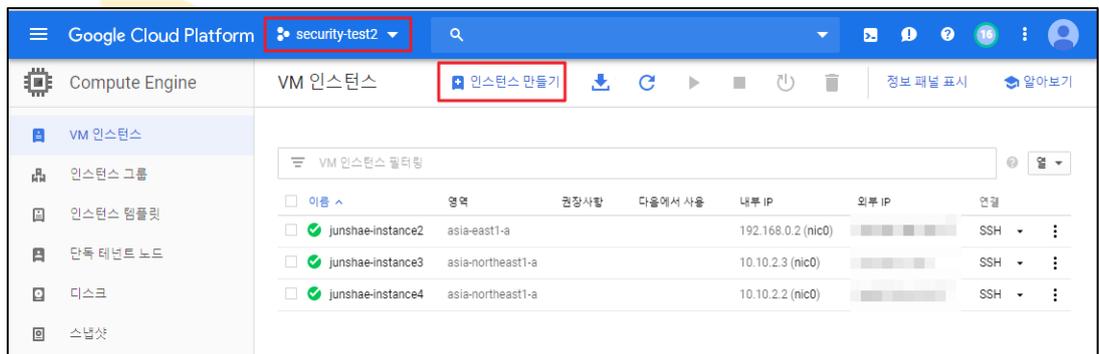
공유된 서버넷만 표시

<input type="checkbox"/>	서버넷	리전	VPC 네트워크	IP 주소 범위	공유 대상
<input type="checkbox"/>	default	asia-east1	default	10.140.0.0/20	사용자 3명
<input type="checkbox"/>	default	asia-northeast1	default	10.146.0.0/20	사용자 3명
<input type="checkbox"/>	security-subnet1	asia-northeast1	security-test	10.10.2.0/24	사용자 3명



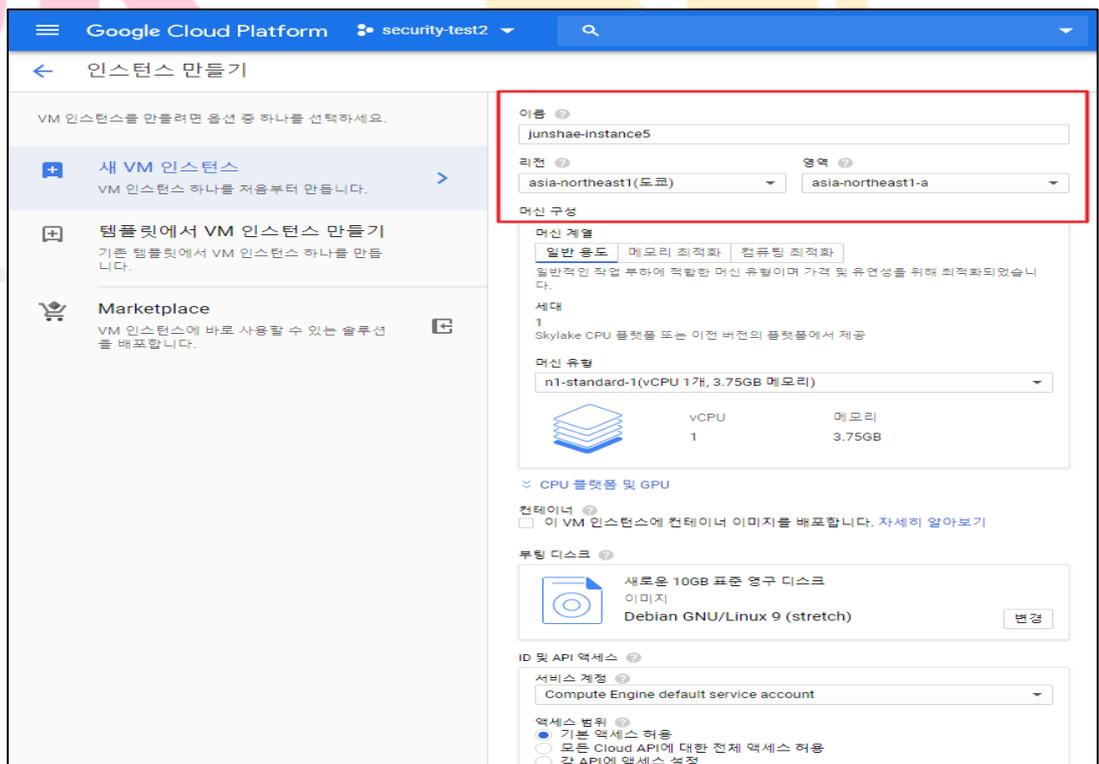
5) [Compute Engine] > [VM 인스턴스] > [인스턴스 만들기]

- 공유된 VPC 를 통한 VM 인스턴스 생성

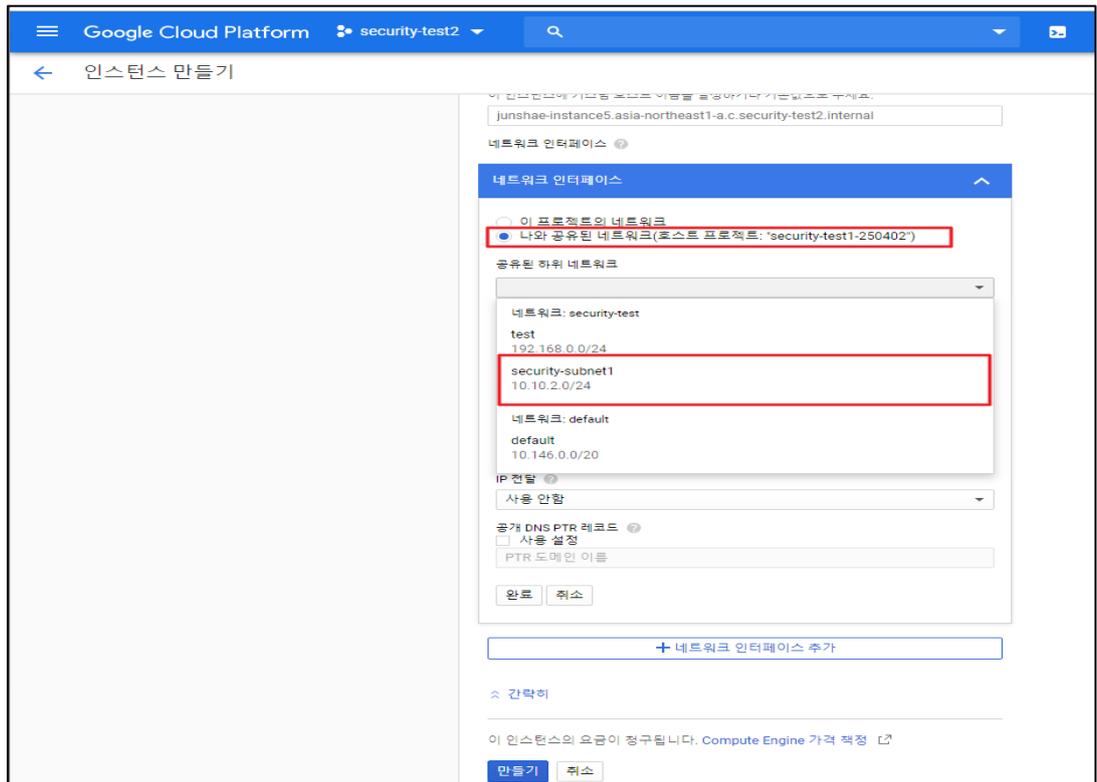


6) 새 VM 인스턴스 만들기

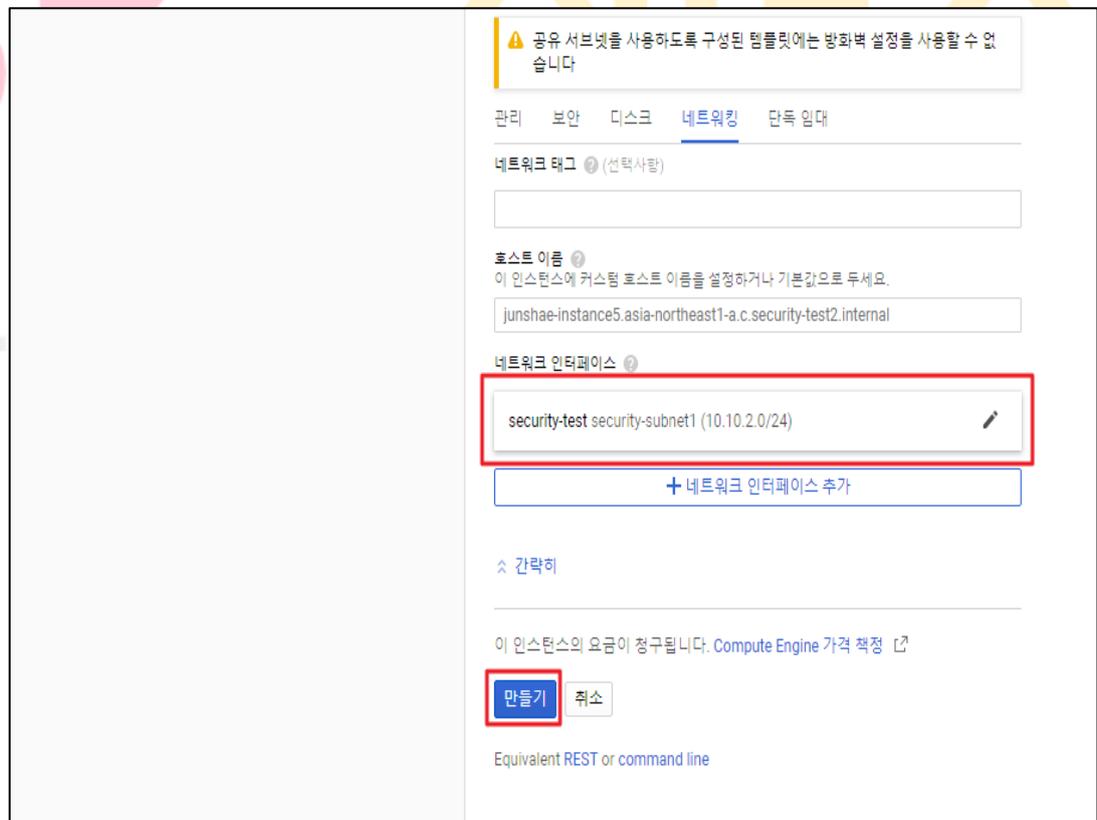
- 인스턴스 생성 시 리전을 공유 하려는 서브넷과 동일하게 설정되어야 함



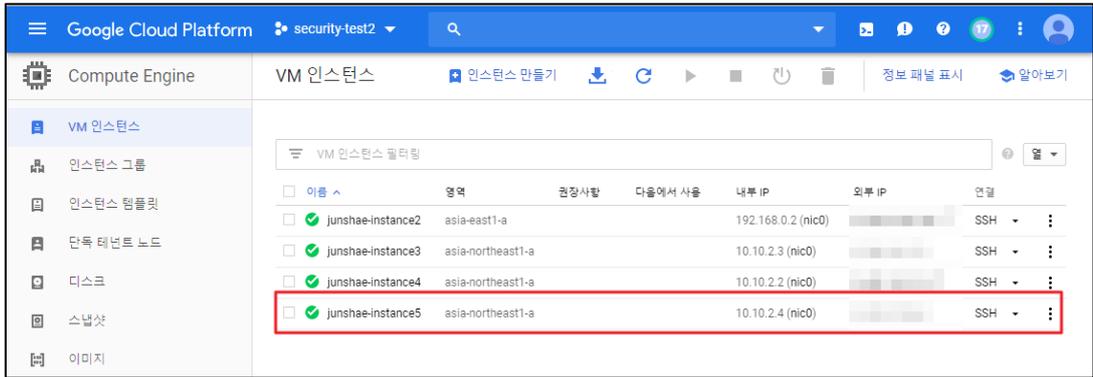
7) 네트워크 인터페이스 설정 시 '나와 공유된 네트워크' 선택



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



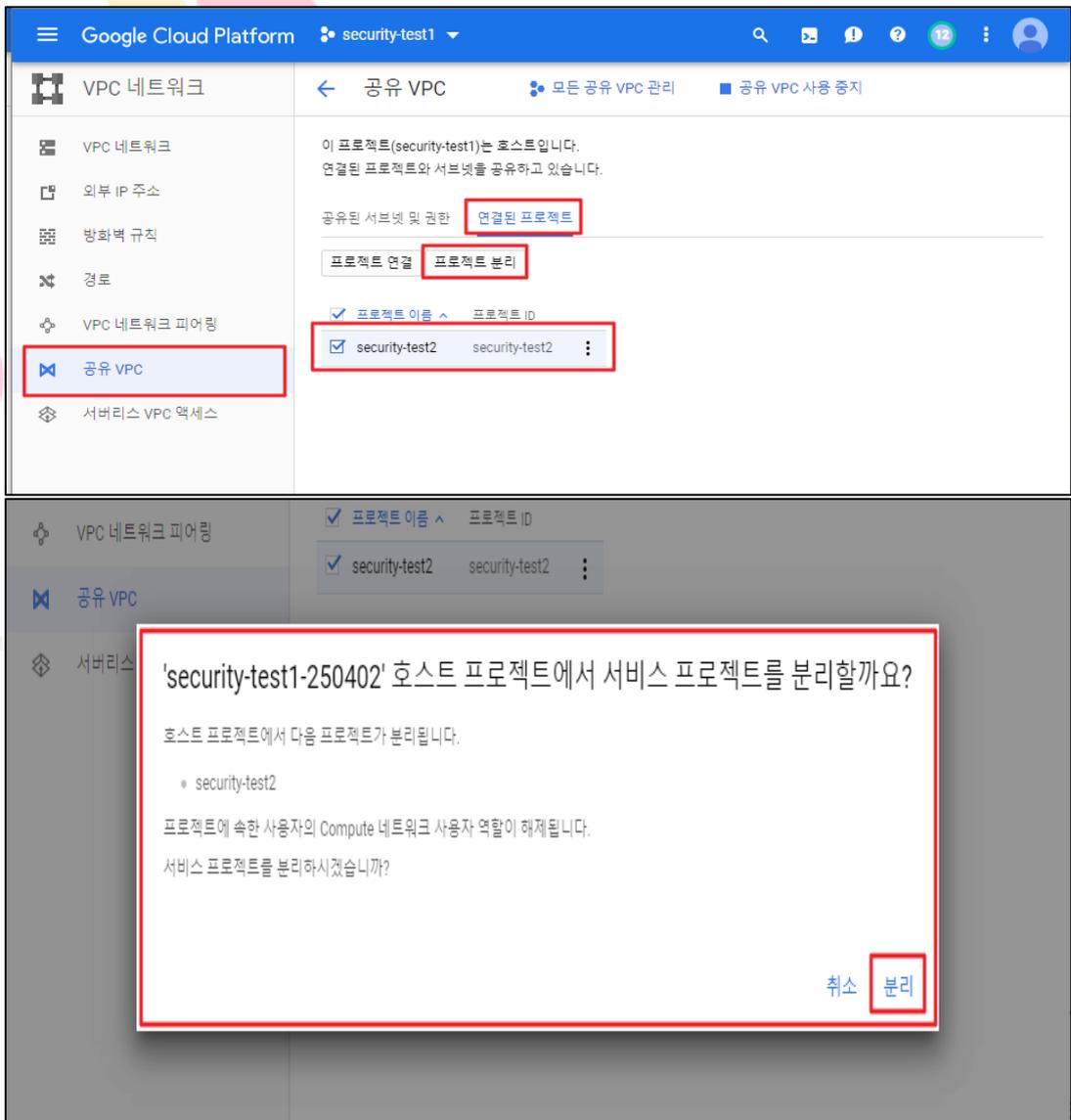
9) 공유된 서브넷을 통한 VM 인스턴스 생성 완료



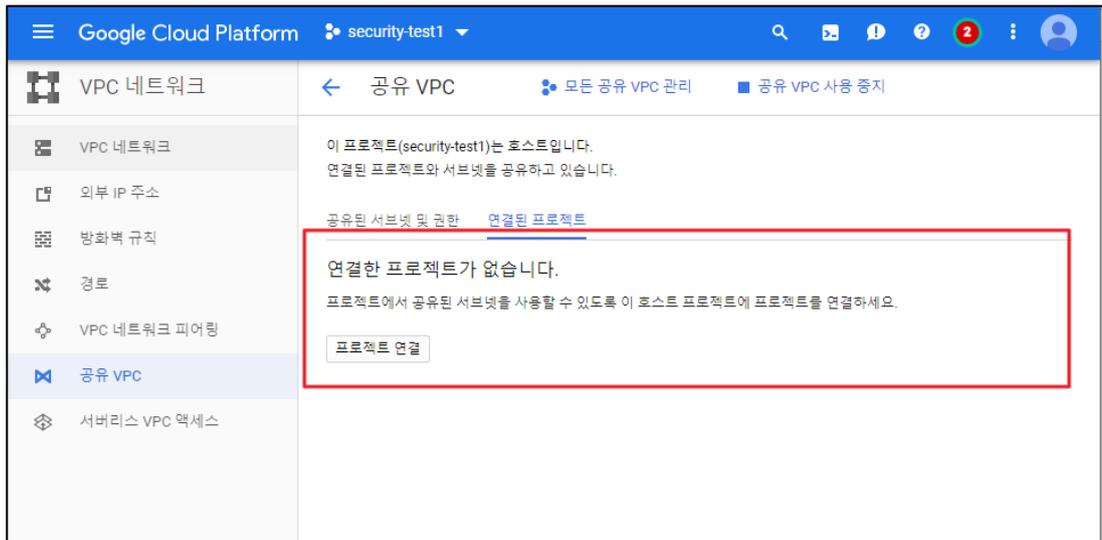
나. 공유 VPC 내 프로젝트 연결 해제

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

- 조직 내 불필요한 프로젝트 연결 해제를 위해 프로젝트 분리 시도



2) 프로젝트 연결 해제 확인



진단
기준

양호기준

: 사용 목적에 맞게 호스트 프로젝트와 서비스 프로젝트 서브넷이 공유되고 있을 경우

취약기준

: 사용 목적 없이 호스트 프로젝트와 서비스 프로젝트 서브넷이 공유되고 있을 경우

비고

3.9 VPN 연결 관리

분류	가상 리소스 관리	중요도	중																															
항목명	VPN 연결 관리																																	
항목 설명	<p>Cloud VPN 은 IPsec VPN 연결을 통해 온프레미스 네트워크를 GCP(Google Cloud Platform) Virtual Private Cloud 네트워크에 안전하게 연결합니다. 두 개의 네트워크 사이로 이동되는 트래픽은 하나의 VPN 게이트웨이에서 암호화된 후 다른 VPN 게이트웨이에서 암호 해독 됩니다. 인터넷에서 전송되는 데이터는 이러한 방식으로 보호됩니다.</p> <p>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 권장 사항에 따라 강력한 32 자 공유 보안 비밀을 생성하는 것을 권고합니다.</p> <p>※ IKEv1 지원되는 암호화</p> <table border="1"> <thead> <tr> <th>단계</th> <th>암호화 역할</th> <th>암호화</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>※ IKEv2 지원되는 암호화</p> <table border="1"> <thead> <tr> <th>단계</th> <th>암호화 역할</th> <th>암호화</th> </tr> </thead> <tbody> <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> </tbody> </table>			단계	암호화 역할	암호화	1 단계	암호화	AES-CBC-128	무결성	HMAC-SHA1-96	PFS 알고리즘(필수)	그룹 2(modp_1024)	PRF(의사 난수 함수)	PRF-SHA1-96	DH(Diffie-Hellman)	그룹 2(modp_1024)	1 단계 수명	36,600 초(10 시간, 10 분)	2 단계	암호화	AES-CBC-128	무결성	HMAC-SHA1-96	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)	단계	암호화 역할	암호화	1 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.
	단계	암호화 역할	암호화																															
	1 단계	암호화	AES-CBC-128																															
		무결성	HMAC-SHA1-96																															
		PFS 알고리즘(필수)	그룹 2(modp_1024)																															
		PRF(의사 난수 함수)	PRF-SHA1-96																															
		DH(Diffie-Hellman)	그룹 2(modp_1024)																															
		1 단계 수명	36,600 초(10 시간, 10 분)																															
	2 단계	암호화	AES-CBC-128																															
		무결성	HMAC-SHA1-96																															
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)																																
단계	암호화 역할	암호화																																
1 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	<ul style="list-style-type: none"> - HMAC-MD5-96 - HMAC-SHA1-96 - AES-XCBC-96, AES-CMAC-96 - HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256 <p>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.</p>
	PRF(의사 난수 함수)	<ul style="list-style-type: none"> - PRF-MD5-96 - PRF-SHA1-96 - PRF-AES-XCBC-96, PRF-AES-CMAC-96 - PRF-SHA2-256, PRF-SHA2-384, PRF-SHA2-512 <p>많은 장치에서 명시적인 PRF 설정이 필요하지 않습니다.</p>
	DH(Diffie-Hellman)	<ul style="list-style-type: none"> - 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)
	암호화	<ul style="list-style-type: none"> - 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 <p>일부 플랫폼에서 GCM 알고리즘은 비트(각각 64, 96, 128)로 지정된 해당 ICV 매개변수 옥텟(8, 12, 16)을 포함할 수 있습니다.</p>
2 단계	무결성	<ul style="list-style-type: none"> - HMAC-MD5-96 - HMAC-SHA1-96 - AES-XCBC-96, AES-CMAC-96 - HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256 <p>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.</p>
	PFS 알고리즘(필수)	<ul style="list-style-type: none"> - 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)

가. Cloud VPN 설정 방법

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

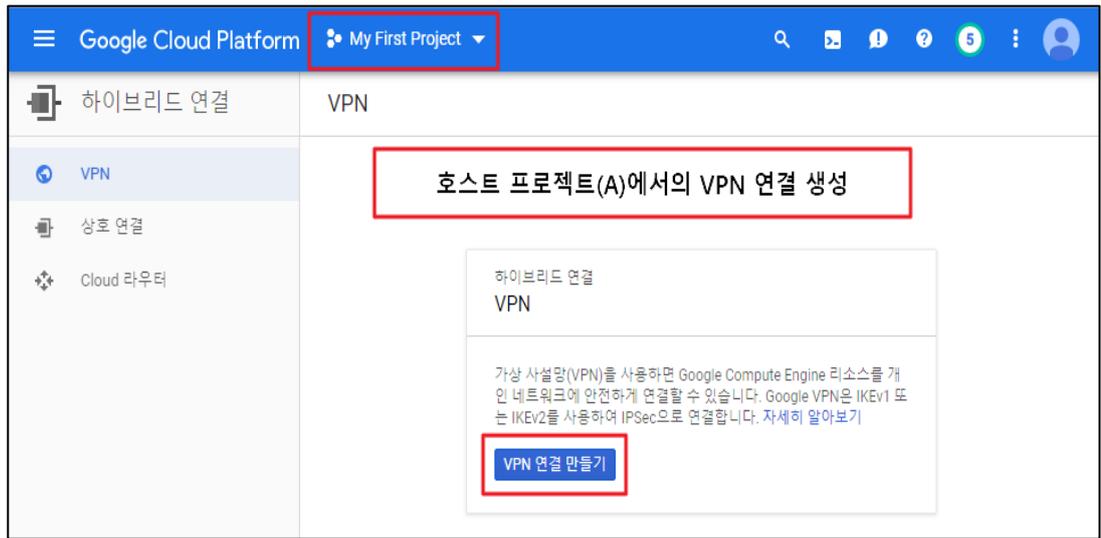
1) [Compute Engine] > [VM 인스턴스]

호스트 프로젝트(A) 내 VPN 연결에 사용하려는 VM 인스턴스 네트워크 정보 확인

설정
방법

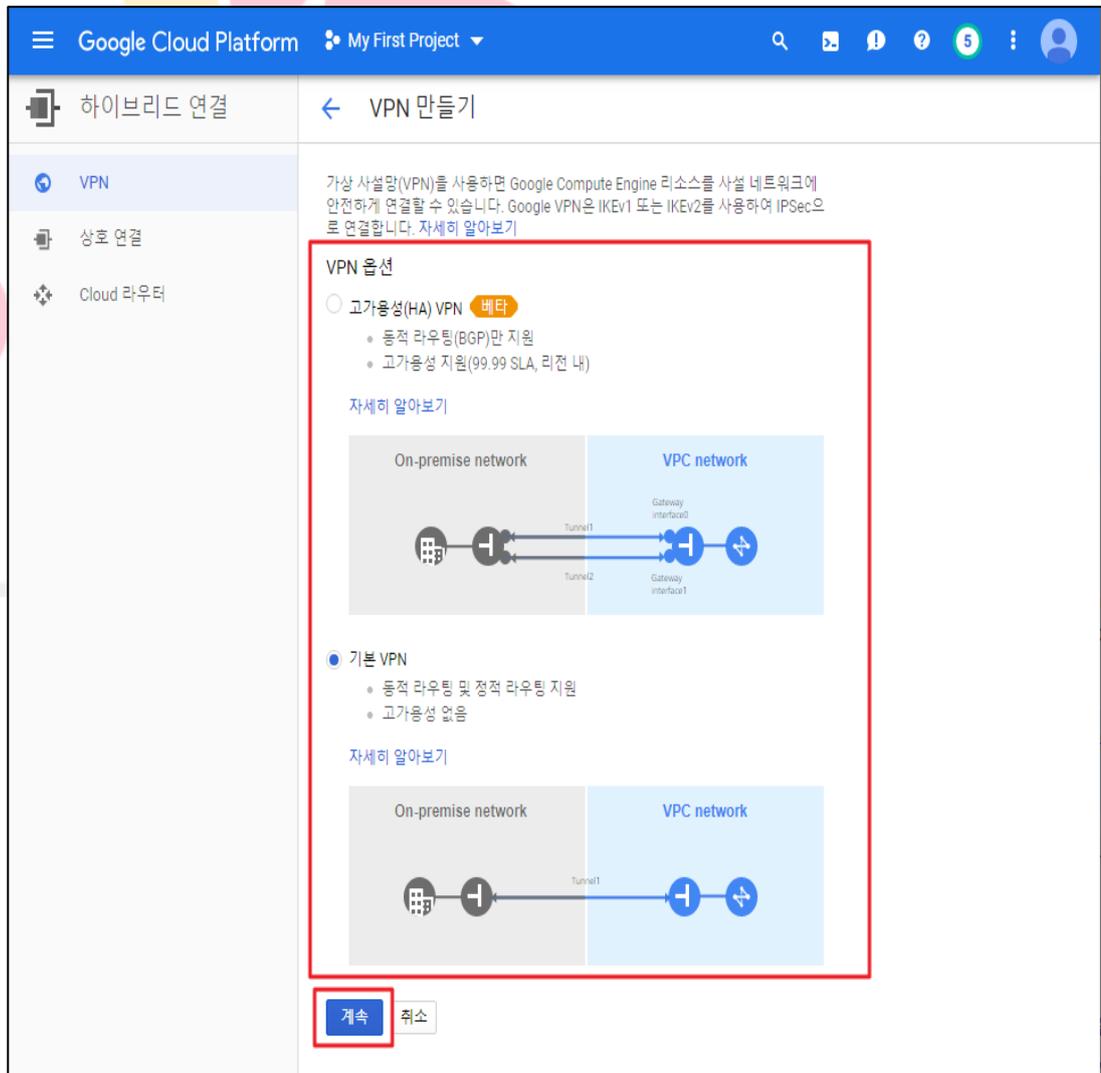
2) [하이브리드 연결] > [VPN]

3) [VPN 연결 만들기]



The screenshot shows the Google Cloud Platform interface for creating a VPN connection. The top navigation bar includes 'Google Cloud Platform' and 'My First Project'. The left sidebar has '하이브리드 연결' (Hybrid connection) selected, with sub-options for 'VPN', '상호 연결' (Mutual connection), and 'Cloud 라우터' (Cloud router). The main content area is titled 'VPN' and features a red-bordered box with the text '호스트 프로젝트(A)에서의 VPN 연결 생성' (Create VPN connection in host project (A)). Below this, there is a description of hybrid VPN connections and a blue button labeled 'VPN 연결 만들기' (Create VPN connection), which is also highlighted with a red box.

4) VPN 옵션 선택 (기본 VPN)



The screenshot displays the 'VPN 만들기' (Create VPN) page in Google Cloud Platform. The top navigation bar shows 'Google Cloud Platform' and 'My First Project'. The left sidebar has '하이브리드 연결' (Hybrid connection) selected, with sub-options for 'VPN', '상호 연결' (Mutual connection), and 'Cloud 라우터' (Cloud router). The main content area is titled 'VPN 만들기' and includes a description of virtual VPN connections. A red-bordered box highlights the 'VPN 옵션' (VPN options) section, which contains two radio button options: '고가용성(HA) VPN' (High availability VPN) and '기본 VPN' (Basic VPN). The '기본 VPN' option is selected. Below the options are two network diagrams. The first diagram shows an 'On-premise network' connected to a 'VPC network' via two tunnels (Tunnel1 and Tunnel2) and two gateway interfaces (Gateway interface0 and Gateway interface1). The second diagram shows a simpler connection with one tunnel (Tunnel1) and one gateway interface. At the bottom, there are '계속' (Continue) and '취소' (Cancel) buttons, with '계속' highlighted by a red box.

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

VPN 연결 만들기

가상 사설망(VPN)을 사용하면 Google Compute Engine 리소스를 개인 네트워크에 안전하게 연결할 수 있습니다. Google VPN은 IKEv1 또는 IKEv2를 사용하여 IPSec으로 연결합니다. [자세히 알아보기](#)

Google Compute Engine VPN 게이트웨이

이름

설명 (선택사항)

네트워크

리전

IP 주소

터널

피어 VPN 게이트웨이별로 여러 터널을 추가할 수 있습니다.

등등한 REST 또는 명령줄

VPN 연결을 하려는 호스트 프로젝트(A)의 네트워크 정보 기입

6) 호스트 프로젝트(A) Cloud VPN 게이트웨이 생성 확인

VPN 연결 만들기

VPN 게이트웨이 생성으로 필터링

게이트웨이 이름	IP 주소	VPC 네트워크	리전	VPN 터널
<input type="checkbox"/> security-vpn-1	34.84.138.201	secu-subnet1	asia-northeast1	<input type="button" value="+ VPN 터널 추가"/>

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

Google Cloud Platform security-test

Compute Engine VM 인스턴스

이름	영역	권장사항	다음에서 사용	내부 IP	외부 IP	연결
security-test5	asia-northeast1-c			10.192.0.2 (nic0)	35.200.24.148	SSH

대상 프로젝트(B) 내 VPN 연결에 사용하려는 VM 인스턴스 네트워크 정보 확인

8) 대상 프로젝트(B)에서의 VPN 연결 만들기

Google Cloud Platform security-test

하이브리드 연결 VPN

대상 프로젝트(B)에서의 VPN 연결 생성

하이브리드 연결 VPN

가상 사설망(VPN)을 사용하면 Google Compute Engine 리소스를 개인 네트워크에 안전하게 연결할 수 있습니다. Google VPN은 IKEv1 또는 IKEv2를 사용하여 IPsec으로 연결합니다. 자세히 알아보기

VPN 연결 만들기

9) VPN 연결 생성 옵션 선택

Google Cloud Platform security-test

하이브리드 연결 VPN 만들기

가상 사설망(VPN)을 사용하면 Google Compute Engine 리소스를 사설 네트워크에 안전하게 연결할 수 있습니다. Google VPN은 IKEv1 또는 IKEv2를 사용하여 IPsec으로 연결합니다. 자세히 알아보기

VPN 옵션

- 고가용성(HA) VPN **베타**
 - 동적 라우팅(BGP)만 지원
 - 고가용성 지원(99.99 SLA, 리전 내)
- 기본 VPN
 - 동적 라우팅 및 정적 라우팅 지원
 - 고가용성 없음

자세히 알아보기

On-premise network VPC network

계속 취소

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

VPN 연결 만들기

가상 사설망(VPN)을 사용하면 Google Compute Engine 리소스를 개인 네트워크에 안전하게 연결할 수 있습니다. Google VPN은 IKEv1 또는 IKEv2를 사용하여 IPSec으로 연결합니다. 자세히 알아보기

Google Compute Engine VPN 게이트웨이

이름
security-vpn-2

설명 (선택사항)
security-vpn-2

네트워크
secu-subnet3

리전
asia-northeast1

IP 주소
vpn-test2(34.84.254.13)

터널
피어 VPN 게이트웨이별로 여러 터널을 추가할 수 있습니다.

+ 터널 추가

만들기 취소

동등한 REST 또는 명령줄

VPN 연결을 하려는 대상 프로젝트(B)의 네트워크 정보 기입

11) 대상 프로젝트(B) Cloud VPN 게이트웨이 생성 확인

VPN 연결 만들기

VPN 연결 만들기

VPN 게이트웨이 속성으로 필터링

게이트웨이 이름	IP 주소	VPC 네트워크	리전	VPN 터널
security-vpn-2	34.84.254.13	secu-subnet3	asia-northeast1	VPN 터널 추가

12) 호스트 프로젝트(A) 내 VPN 터널 추가

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

VPN 터널 만들기

VPC 네트워크: secu-subnet1 리전: asia-northeast1
VPN 게이트웨이 이름: security-vpn-1 (기본 VPN 게이트웨이)
VPN 게이트웨이 IP 주소: 34.84.138.201

이름
security-vpn-1-tunnel-1

설명 (선택사항)

원격 피어 IP 주소
34.84.254.13

IKE 버전
IKEv2

IKE 사전 공유 키
자체 키를 입력하거나 자동으로 생성합니다.
gc/VmSqsu/dcYo... 생성 및 복사

⚠ 사전 공유 키를 안전한 위치에 기록해야 합니다. 이 양식을 담은 후에는 키를 가져올 수 없습니다. 자세히 알아보기

라우팅 옵션
동적(BGP) 경로 기반 정책 기반

원격 네트워크 IP 범위
여러 IP 주소 범위를 CIDR 표기법으로 입력하세요. 하나를 입력할 때마다 Enter 키를 누르세요.
10.192.0.0/20

로컬 하위 네트워크 (선택사항)
1개 선택됨...

로컬 IP 범위
10.146.0.0/20

만들기 취소

13) 호스트 프로젝트(A) 내 VPN 터널 생성 및 상태 값 확인

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

The screenshot shows the Google Cloud Platform console for a project named 'My First Project'. The page title is 'Google VPN 게이트웨이 세부정보' (Google VPN Gateway Details). The left sidebar shows navigation options: '하이브리드 연결' (Hybrid Connection), 'VPN', '상호 연결' (Mutual Connection), and 'Cloud 라우터' (Cloud Router). The main content area displays details for a VPN gateway named 'security-vpn-1', which is a basic Cloud VPN gateway. Key details include: VPC Network: secu-subnet1, Region: asia-northeast1, Description: security-vpn-1, IP Address: 34.84.138.201, High Availability: No, and a '로그 보기' (View Log) link. Below the details is a '전달 규칙' (Rule) section with a table of rules:

이름	프로토콜
security-vpn-1-rule-esp	esp
security-vpn-1-rule-udp4500	udp:4500
security-vpn-1-rule-udp500	udp:500

Underneath is the 'VPN 터널' (VPN Tunnel) section, which includes 'VPN 터널 추가' (Add VPN Tunnel) and '삭제' (Delete) buttons. A search bar for 'VPN 터널 속성으로 필터링' (Filter by VPN Tunnel Property) is present. A table below shows the status of the VPN tunnels:

VPN 터널 이름 ^	피어 게이트웨이 IP 주소	라우팅 유형	상태
<input type="checkbox"/> security-vpn-1-tunnel-1	34.84.254.13	정책 기반	⚠ 첫 번째 핸드셰이크

14) 대상 프로젝트(B) 내 VPN 터널 추가

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

The screenshot shows the 'VPN 터널 만들기' (Create VPN Tunnel) page in Google Cloud Platform. The interface includes the following fields and options:

- VPC 네트워크:** secu-subnet3 리전: asia-northeast1
- VPN 게이트웨이 이름:** security-vpn-2 (기본 VPN 게이트웨이)
- VPN 게이트웨이 IP 주소:** 34.84.254.13
- 이름:** security-vpn-2-tunnel-1
- 설명 (선택사항):** security-vpn-2-tunnel-1
- 원격 피어 IP 주소:** 34.84.138.201
- IKE 버전:** IKEv2
- IKE 사전 공유 키:** gc/VmSqsu/dcYoV (생성 및 복사 버튼 있음)
- 라우팅 옵션:** 동적(BGP), 경로 기반, 정책 기반
- 원격 네트워크 IP 범위:** 10.146.0.0/20
- 로컬 하위 네트워크 (선택사항):** 1개 선택됨...
- 로컬 IP 범위:** 10.192.0.0/24

15) 대상 프로젝트(B) 내 VPN 터널 생성 및 상태 값 확인

The screenshot shows the 'Google VPN 게이트웨이 세부정보' (Google VPN Gateway Details) page for 'security-vpn-2'. The page displays the following information:

- 기본 Cloud VPN 게이트웨이:**
 - VPC 네트워크: secu-subnet3
 - 리전: asia-northeast1
 - 설명: security-vpn-2
 - IP 주소: 34.84.254.13
 - 고가용성: 아니요
 - 로그: 보기
- 전달 규칙:**
 - 이름: 프로토폴름
 - security-vpn-2-rule-udp500: udp:500
 - security-vpn-2-rule-esp: esp
 - security-vpn-2-rule-udp4500: udp:4500
- VPN 터널:**
 - VPN 터널 추가 | 삭제
 - VPN 터널 속성으로 필터링

VPN 터널 이름	피어 게이트웨이 IP 주소	라우팅 유형	상태
security-vpn-2-tunnel-1	34.84.138.201	정책 기반	✓ 설정됨

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

The screenshots show the Google Cloud VPN console for two different projects. The top screenshot is for 'My First Project' and the bottom is for 'security-test'. Both show a table of VPN tunnels with columns for tunnel name, Cloud VPN gateway IP, peer VPN gateway IP, Cloud Router BGP IP, BGP peer IP, routing status, VPN tunnel status, BGP session status, Google network, and region. In both cases, the 'VPN 터널' row is highlighted with a red box, showing a status of '설정됨' (Configured).

터널 이름	Cloud VPN 게이트웨이(IP)	피어 VPN 게이트웨이(IP)	Cloud Router BGP IP	BGP 피어 IP	라우팅 유형	VPN 터널 상태	BGP 세션 상태	Google 네트워크	리전
security-vpn-1-tunnel-1 (기본)	security-vpn-1 34.84.138.201	34.84.254.13	없음	없음	장착 기반	✓ 설정됨	--	secu-subnet1	asia-northeast1
security-vpn-2-tunnel-1 (기본)	security-vpn-2 34.84.138.201	34.84.138.201	없음	없음	장착 기반	✓ 설정됨	--	secu-subnet3	asia-northeast1

진단 기준

양호기준

: On-Demand(프라이빗 Cloud)와 퍼블릭 Cloud 환경 간에 Cloud VPN 터널 및 게이트웨이를 연결하고 있지 않을 경우

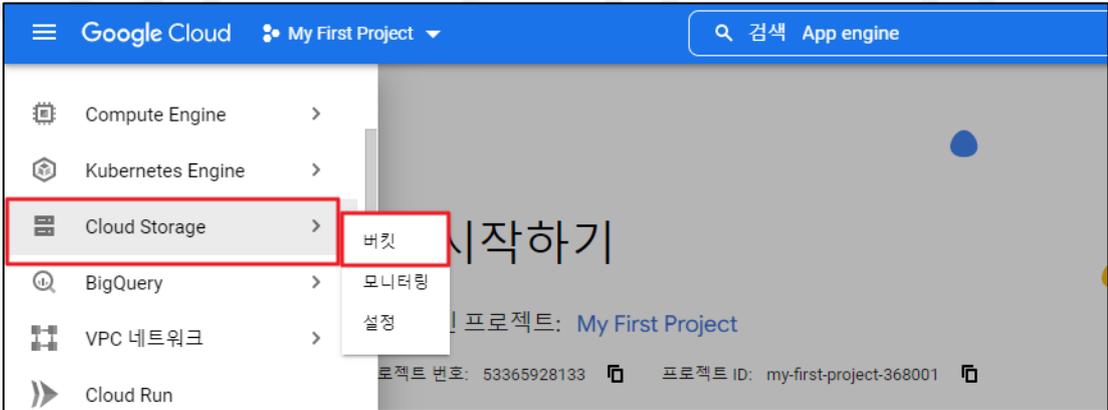
취약기준

: On-Demand(프라이빗 Cloud)와 퍼블릭 Cloud 환경 간에 Cloud VPN 터널 및 게이트웨이를 연결하고 있을 경우

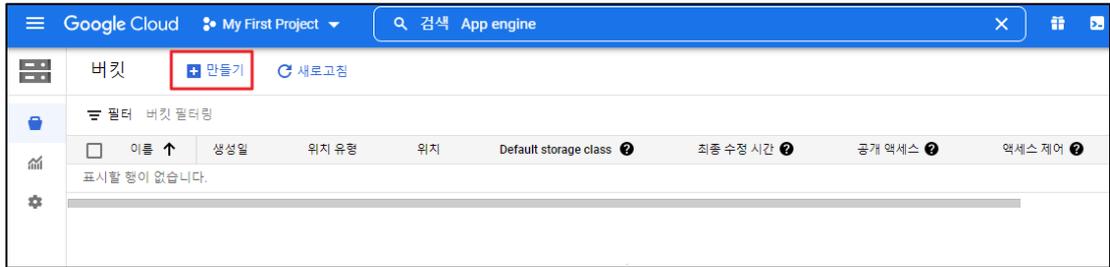
비고

안녕을 지키는 기술

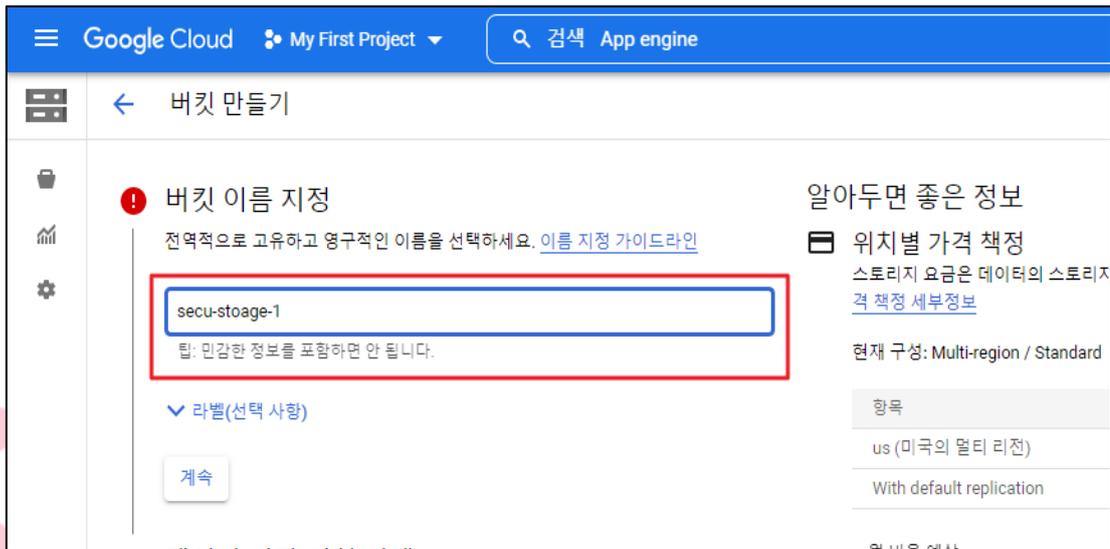
3.10 Storage 버킷 ACL 관리

분류	가상 리소스 관리	중요도	중								
항목명	Storage 버킷 ACL 관리										
항목 설명	<p>Cloud Storage는 버킷과 객체에 대한 액세스 권한을 사용자에게 부여하는데 사용되는 Cloud Identity and Access Management(Cloud IAM) 및 액세스 제어 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.</p> <p>※ Cloud Storage 버킷 및 객체 액세스 제어 옵션</p> <table border="1" data-bbox="279 768 1426 1417"> <thead> <tr> <th data-bbox="279 768 647 817">구분</th> <th data-bbox="647 768 1426 817">상세내용</th> </tr> </thead> <tbody> <tr> <td data-bbox="279 817 647 1003">Cloud Identity and Access Management(Cloud IAM)</td> <td data-bbox="647 817 1426 1003">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 data-bbox="279 1003 647 1189">액세스 제어 목록(ACL)</td> <td data-bbox="647 1003 1426 1189">사용자에게 개별 버킷이나 객체에 대한 읽기 또는 쓰기 액세스 권한을 부여합니다. 대부분의 경우 ACL 대신 Cloud IAM 권한을 사용해야 합니다. 개별 객체의 세부적인 제어가 필요한 경우에만 ACL을 사용하시기 바랍니다.</td> </tr> <tr> <td data-bbox="279 1189 647 1417">서명된 정책 문서</td> <td data-bbox="647 1189 1426 1417">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 Storage에 파일을 업로드 하도록 허용할 수 있습니다.</td> </tr> </tbody> </table>			구분	상세내용	Cloud Identity and Access Management(Cloud IAM)	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.	액세스 제어 목록(ACL)	사용자에게 개별 버킷이나 객체에 대한 읽기 또는 쓰기 액세스 권한을 부여합니다. 대부분의 경우 ACL 대신 Cloud IAM 권한을 사용해야 합니다. 개별 객체의 세부적인 제어가 필요한 경우에만 ACL을 사용하시기 바랍니다.	서명된 정책 문서	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 Storage에 파일을 업로드 하도록 허용할 수 있습니다.
구분	상세내용										
Cloud Identity and Access Management(Cloud IAM)	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.										
액세스 제어 목록(ACL)	사용자에게 개별 버킷이나 객체에 대한 읽기 또는 쓰기 액세스 권한을 부여합니다. 대부분의 경우 ACL 대신 Cloud IAM 권한을 사용해야 합니다. 개별 객체의 세부적인 제어가 필요한 경우에만 ACL을 사용하시기 바랍니다.										
서명된 정책 문서	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 Storage에 파일을 업로드 하도록 허용할 수 있습니다.										
설정 방법	<p>가. Cloud Storage IAM 권한 및 액세스제어 목록(ACL) 설정</p> <p>1) [관리 콘솔] > [Cloud Storage] > [버킷]</p> 										

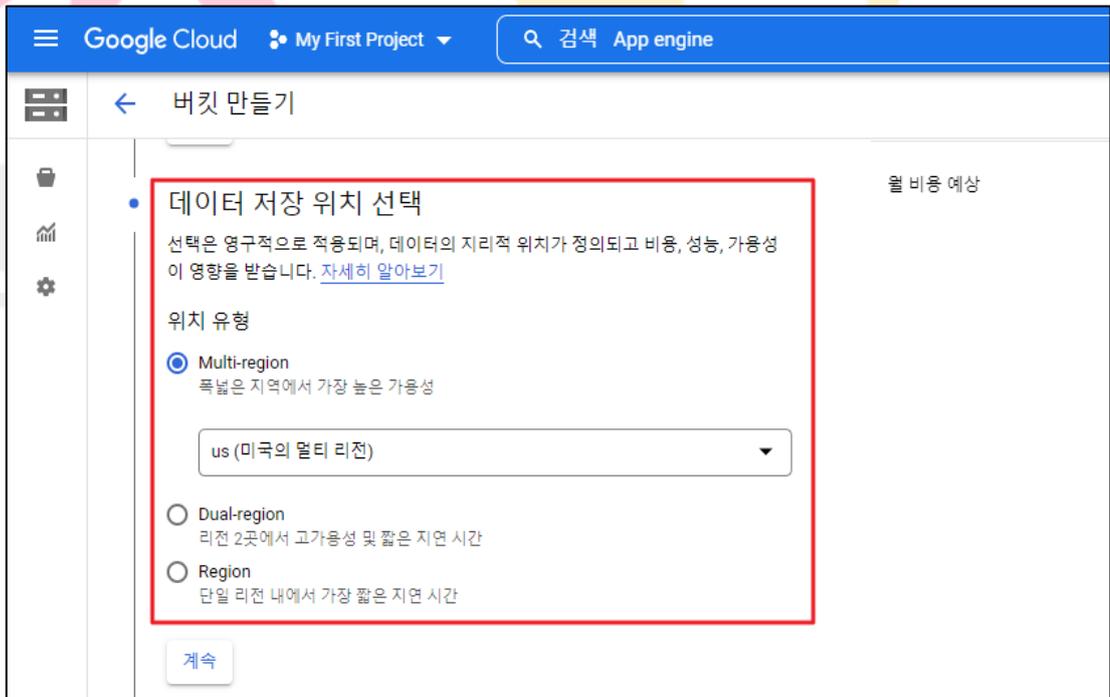
2) 버킷 생성



3) 버킷 정보 입력



4) 기본 스토리지 클래스 선택



5) 액세스 제어 모델 설정 및 버킷 만들기

선택 액세스를 제어하는 방식 선택

공개 액세스 방지
인터넷을 통해 공개적으로 데이터에 액세스할 수 없도록 제한합니다. 이 버킷이 웹 호스팅에 사용되지 않게 합니다. [자세히 알아보기](#)

이 버킷에 공개 액세스 방지 적용

액세스 제어

균일한 액세스 제어
버킷 수준 권한(IAM)만 사용하여 버킷의 모든 객체에 대한 균일한 액세스 권한을 가지도록 합니다. 90일이 지나면 이 옵션이 영구적으로 적용됩니다. [자세히 알아보기](#)

세분화된 액세스 제어
버킷 수준 권한(IAM) 외에도 객체 수준 권한(ACL)을 사용하여 개별 객체에 대한 액세스 권한을 지정합니다. [자세히 알아보기](#)

계속

객체 데이터를 보호하는 방법 선택

보호 도구: 없음
데이터 암호화: Google-managed key

만들기 취소

6) 생성된 버킷 접근

Google Cloud DHL 검색 제품, 리소스, 문서(/)

버킷 만들기 새로고침

필터 버킷 필터링

<input type="checkbox"/>	이름 ↑	생성일	위치 유형	위치	Default storage class
<input type="checkbox"/>	secu-storage-1	2022. 11. 9. AM 9:45:34	Multi-region	asia	Standard

7) 버킷 권한 및 구성원 추가 설정

secu-storage-1

위치: asia (아시아의 멀티 리전) | 스토리지 클래스: Standard | 공개 액세스: 공개 아님 | 보호: 1년

객체 구성 권한 보호 수명 주기

공개 액세스
공개 아님
공개 액세스가 차단되었으므로 이 버킷에 공개적으로 액세스할 수 없습니다. 이 제한으로 인해 인터넷을 통해 객체를 공개적으로 공유할 수 없습니다. [자세히 알아보기](#)
다음 주 구성원이 버킷 액세스로부터 제한됩니다.
allUsers, allAuthenticatedUsers

Access control
균일한 권한: 객체 수준 ACL 사용 설정되지 않음
설정 변경 잔여 기간: 90일
모든 객체 액세스가 버킷 권한으로 제어되며 객체는 자체 액세스 제어 목록(ACL)을 가질 수 없습니다. 객체별 액세스를 허용하려면 90일 내에 세분화된 액세스로 전환하십시오. [자세히 알아보기](#)
세분화된 권한으로 전환하기

권한 [+ 액세스 권한 부여](#) - 액세스 권한 삭제

주 구성원별로 보기 역할별로 보기

8) 새 구성원 및 IAM 역할 추가

The screenshot shows the Google Cloud IAM console interface. On the left, the bucket 'secu-storage-1' is selected. The main area is titled '"secu-storage-1"에 대한 액세스 권한 부여' (Grant access to 'secu-storage-1'). It includes instructions on adding members and roles. A red box highlights the '새 구성원' (New member) input field. Another red box highlights the '역할' (Role) dropdown menu, which is currently set to '보안 관리자' (Security Administrator). A '+ IAM 조건 추가' (Add IAM condition) button is also visible. At the bottom, there are '저장' (Save) and '취소' (Cancel) buttons.

9) 권한 추가 완료

The screenshot shows the '권한' (Permissions) page for the bucket 'secu-storage-1'. It displays a table of members and their roles. A red box highlights the '보안 관리자' (Security Administrator) role assigned to a member. The table includes columns for '유형' (Type), '주제' (Subject), '이름' (Name), '역할' (Role), and '상속' (Inheritance).

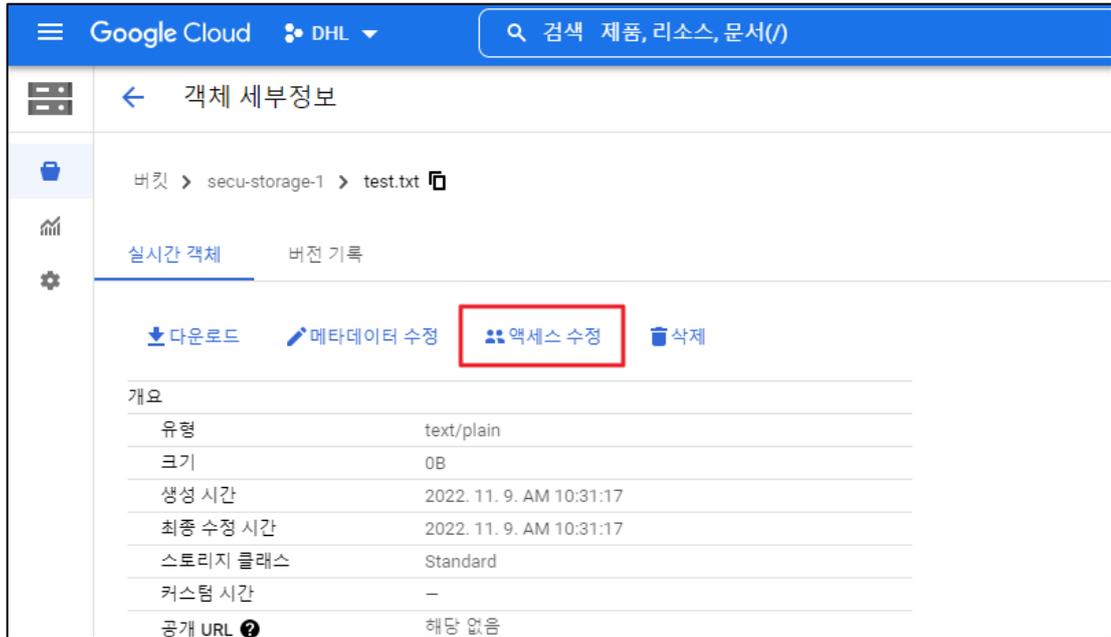
유형	주제	이름	역할	상속
프로젝트 뷰어	mystic-cirrus-367311	프로젝트 뷰어: mystic-cirrus-367311	저장소 기존 개체 리더	
프로젝트 소유자	mystic-cirrus-367311	프로젝트 소유자: mystic-cirrus-367311	저장소 이전 버킷 리더	
프로젝트 편집자	mystic-cirrus-367311	프로젝트 편집자: mystic-cirrus-367311	저장소 기존 개체 소유자	
			저장소 기존 버킷 소유자	
			보안 관리자	
			저장소 기존 개체 소유자	
			저장소 기존 버킷 소유자	
			보안 관리자	DHL
서비스 계정	service-379613018624@compute-system.iam.gserviceaccount.com	Compute Engine Service Agent for Project 379613018624	Compute Engine 서비스 에이전트	DHL

10) 생성된 버킷 내 객체 업로드

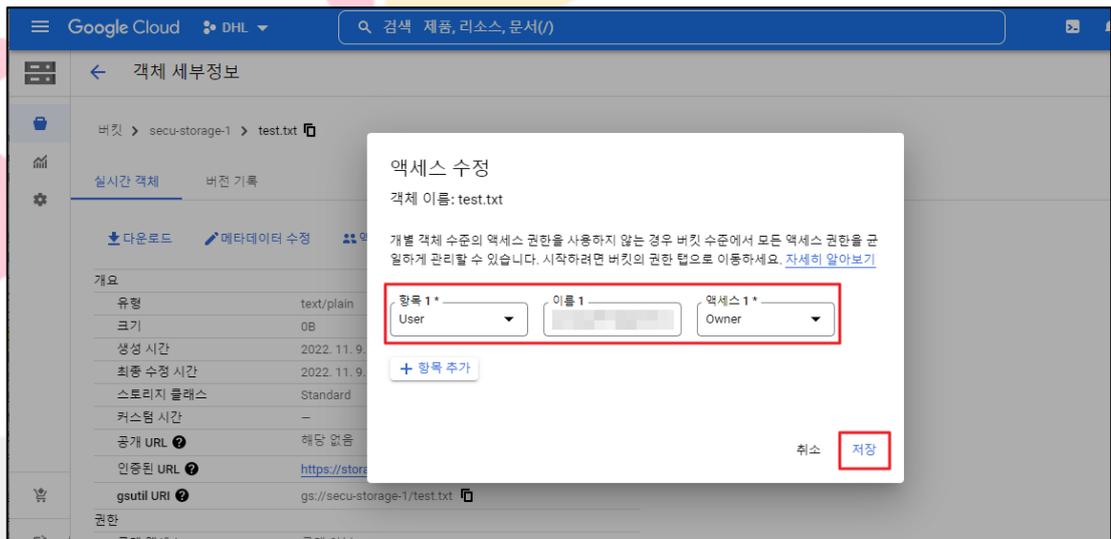
The screenshot shows the Google Cloud Storage console interface. The bucket 'secu-storage-1' is selected. The '객체' (Objects) tab is active, showing a list of objects. A red box highlights the newly uploaded object 'test.txt'. The table includes columns for '이름' (Name), '크기' (Size), '유형' (Type), '생성 시간' (Created), '스토리지 클래스' (Storage Class), '최종 수정 날짜' (Last Modified), '공개 액세스' (Public Access), '버전 기록' (Versioning), and '암호화' (Encryption).

이름	크기	유형	생성 시간	스토리지 클래스	최종 수정 날짜	공개 액세스	버전 기록	암호화
test.txt	0B	text/plain	2022. 11. 9...	Standard	2022. 11. 9...	공개 아님	-	Google-managed key

11) 객체 내 권한 수정



12) ACL 설정 추가



진단
기준

양호기준

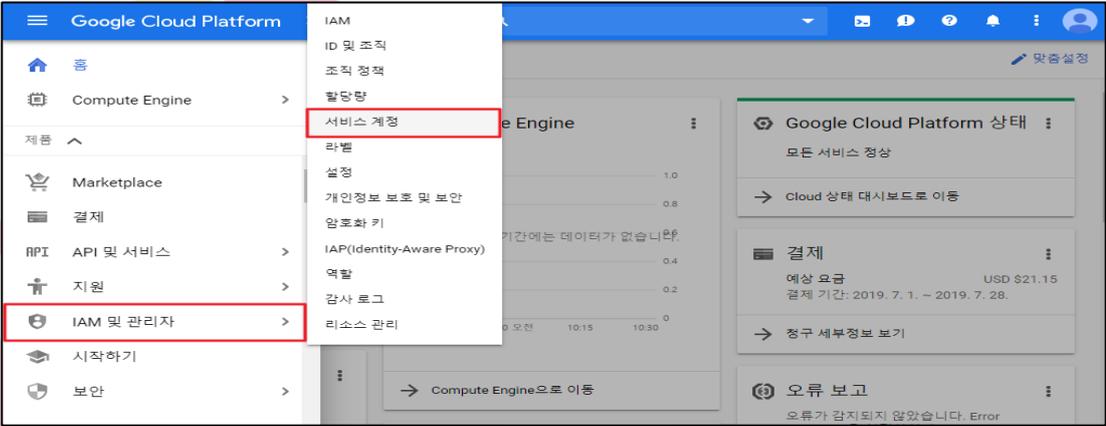
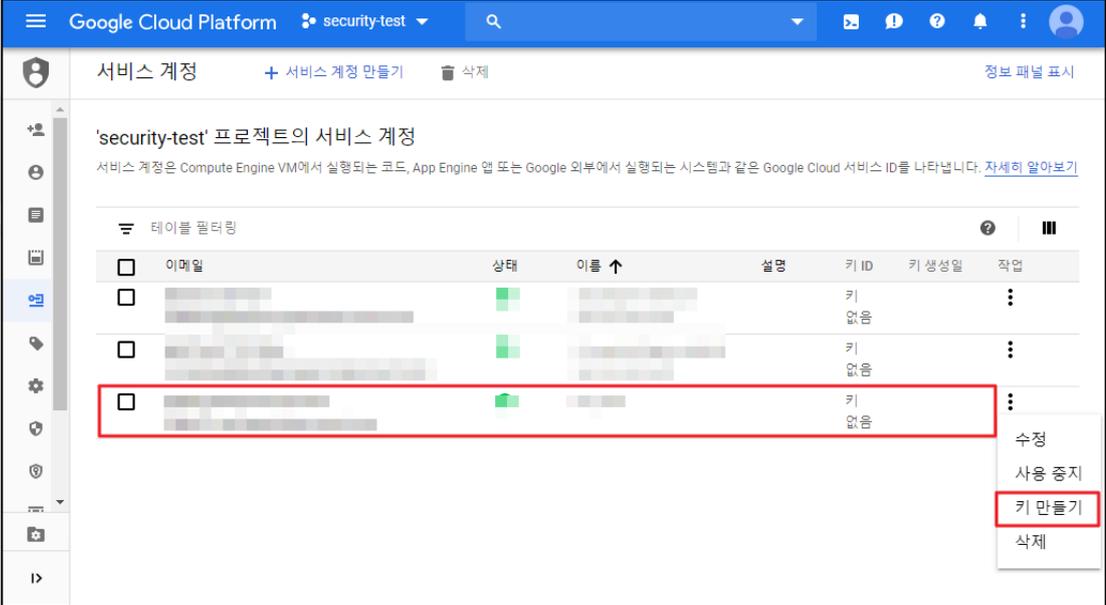
: Storage 버킷 서비스의 ACL 계정 사용 권한이 역할에 맞게 설정되어 있을 경우

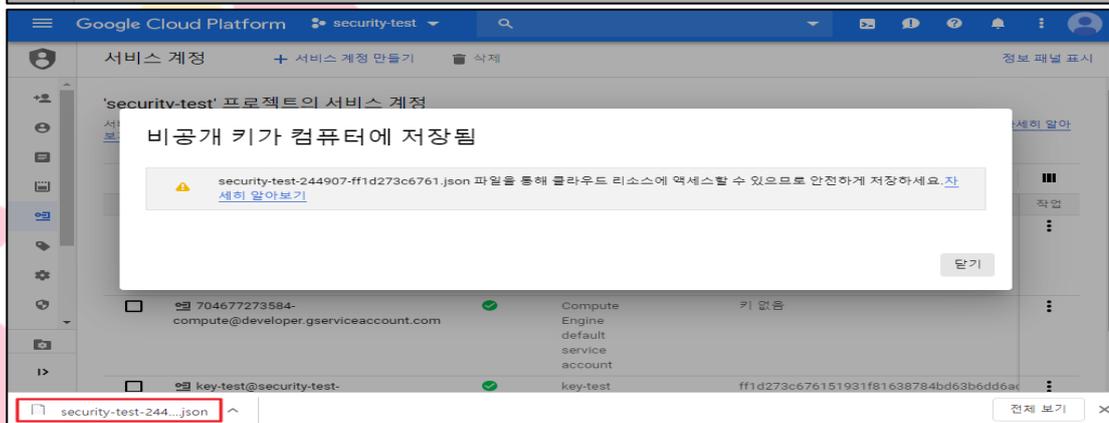
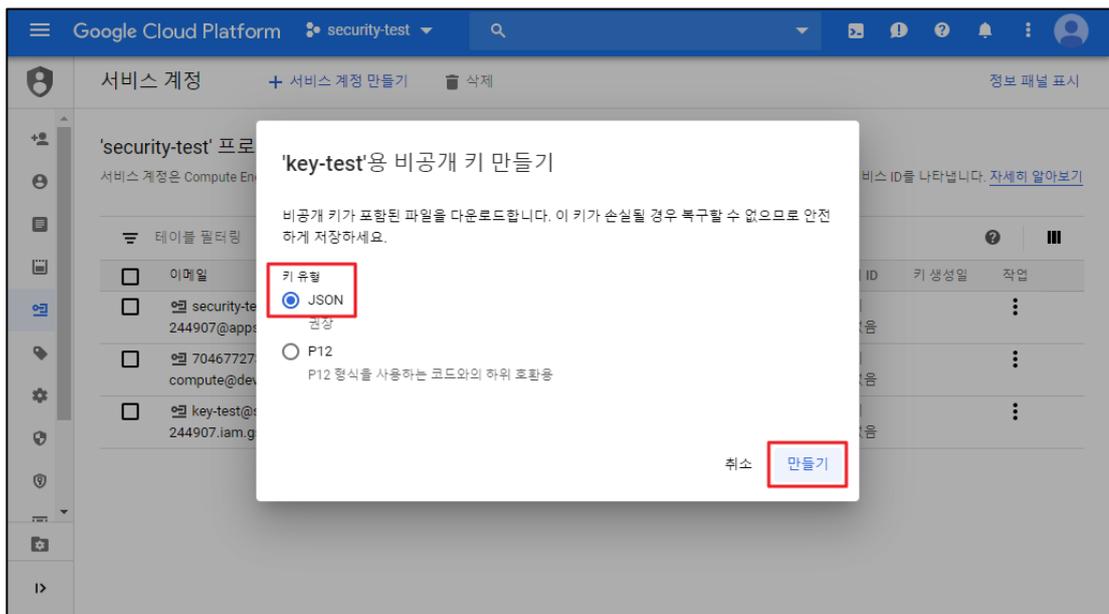
취약기준

: Storage 버킷 서비스의 ACL 계정 사용 권한이 역할에 맞게 설정되어 있지 않을 경우

비고

3.11 Storage 제어 관리

분류	가상 리소스 관리	중요도	중
항목명	Storage 제어 관리		
항목 설명	<p>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.</p>		
설정 방법	<p>가. 서명된 URL 설정</p> <p>1) [메인] > [IAM 및 관리자] > [서비스 계정]</p>  <p>2) 서명된 URL 생성에 필요한 키 만들기</p> 		



3) 생성된 키 정보 확인



4) 서명된 URL을 생성할 인스턴스 접근

Google Cloud Platform VM 인스턴스 관리 화면. 'secu-subnet3' 인스턴스가 선택되어 있으며, 연결 방법을 보여주는 팝업 메뉴가 표시되어 있습니다.

이름	영역	권장사항	다음에서 사용	내부 IP	외부 IP	연결
instance-1	us-east1-b			10.142.0.2 (nic0)	없음	SSH
instance-2	asia-northeast2-a	매월 \$21 절감		10.174.0.2 (nic0)	없음	SSH
secu-subnet3	asia-east1-b	매월 \$18 절감		10.146.0.2 (nic0)	35.236.188.141	SSH

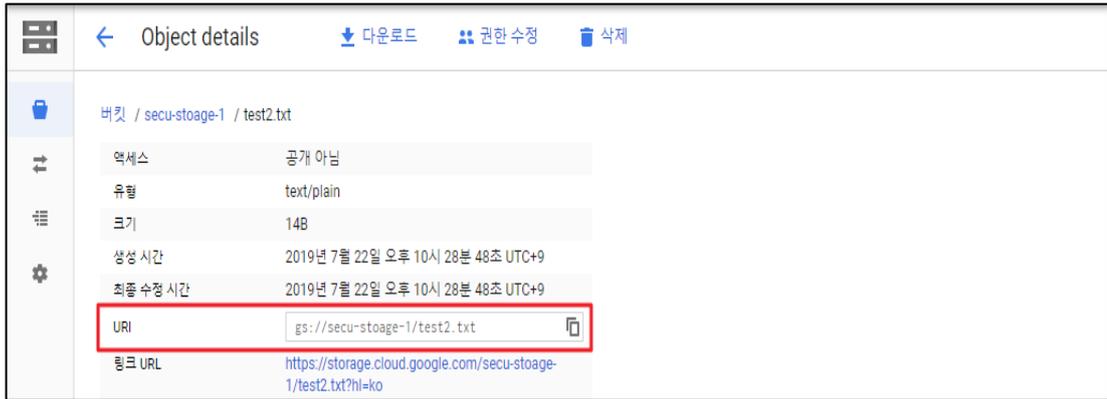
5) 인스턴스 내 생성한 키 저장

```
root@secu-subnet3:/infosec# ls -al
total 12
drwxr-xr-x  2 root root 4096 Jul 29 01:58 .
drwxr-xr-x 23 root root 4096 Jul 29 01:58 ..
-rw-r--r--  1 root root 2376 Jul 29 01:58 private-key.json
root@secu-subnet3:/infosec#
```

6) 서명된 URL 생성에 필요한 도구 설치

```
root@secu-subnet3:/infosec# pip install pyopenssl
DEPRECATION: Python 2.7 will reach the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 won't be maintained after that date. A future version of pip will drop support for Python 2.7. More details about Python 2 support in pip, can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support
Requirement already satisfied: pyopenssl in /usr/local/lib/python2.7/dist-packages (19.0.0)
Requirement already satisfied: cryptography>=2.3 in /usr/local/lib/python2.7/dist-packages (from pyopenssl) (2.7)
Requirement already satisfied: six>=1.5.2 in /usr/lib/python2.7/dist-packages (from pyopenssl) (1.10.0)
Requirement already satisfied: enum34; python_version < "3" in /usr/local/lib/python2.7/dist-packages (from cryptography>=2.3->pyopenssl) (1.1.6)
Requirement already satisfied: asn1crypto>=0.21.0 in /usr/local/lib/python2.7/dist-packages (from cryptography>=2.3->pyopenssl) (0.24.0)
Requirement already satisfied: cffi!=1.11.3,>=1.8 in /usr/local/lib/python2.7/dist-packages (from cryptography>=2.3->pyopenssl) (1.12.3)
Requirement already satisfied: ipaddress; python_version < "3" in /usr/local/lib/python2.7/dist-packages (from cryptography>=2.3->pyopenssl) (1.0.22)
Requirement already satisfied: pycparser in /usr/local/lib/python2.7/dist-packages (from cffi!=1.11.3,>=1.8->cryptography>=2.3->pyopenssl) (2.19)
root@secu-subnet3:/infosec#
```

7) 공유할 객체 URI 정보 확인



8) 서명된 URL 생성



양호기준

: 서명된 URL을 사용하지 않거나 사용시간을 최소한으로 설정되어 있을 경우

진단
기준

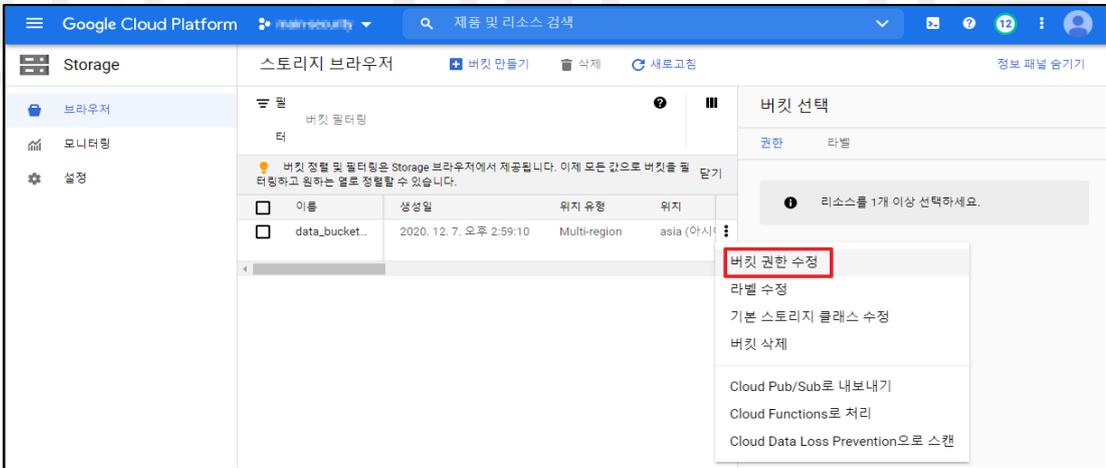
취약기준

: 서명된 URL 사용 시 사용시간을 최소한으로 설정하지 않은 경우

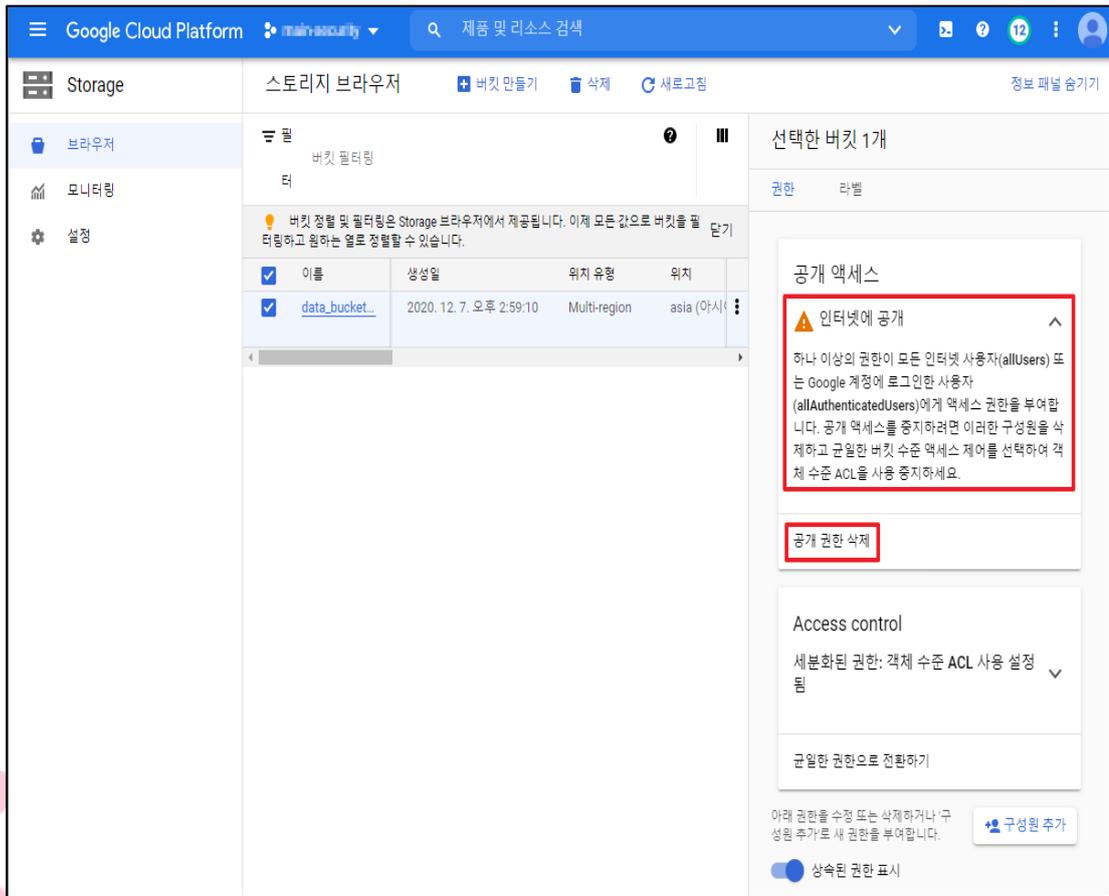
비고

안녕을 지키는 기술

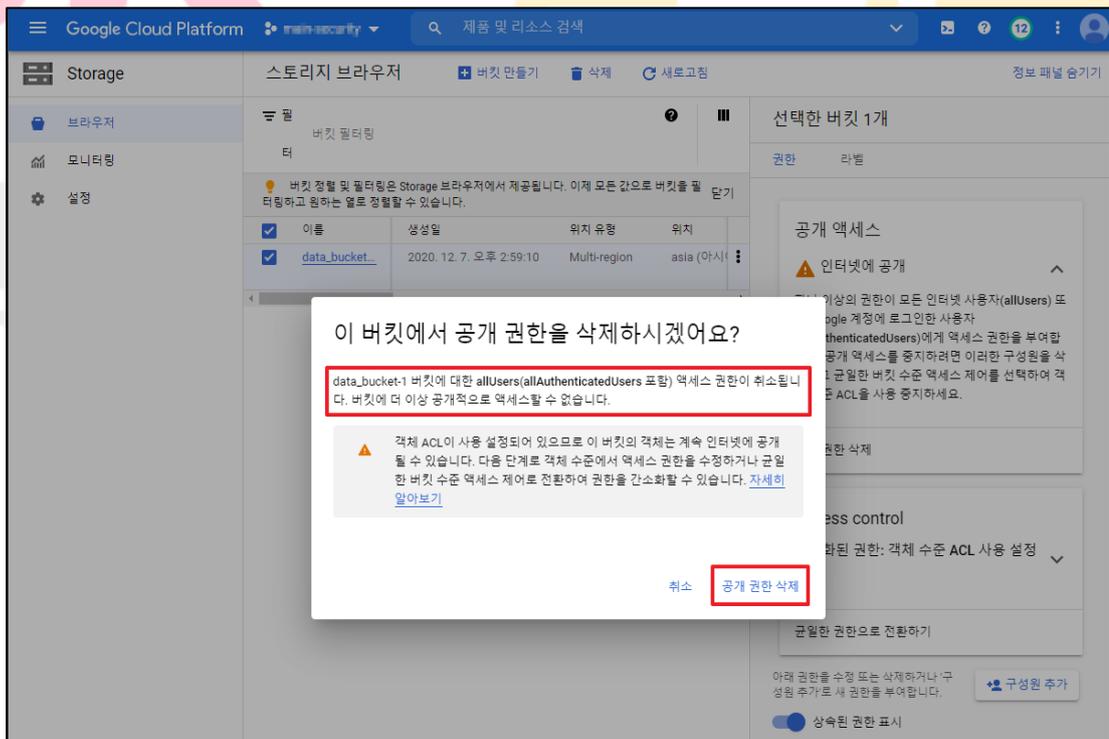
3.12 Storage 리소스 퍼블릭 Access 관리

분류	가상 리소스 관리	중요도	상
항목명	Storage 리소스 퍼블릭 Access 관리		
항목 설명	<p>공개 액세스는 모든 인터넷 사용자(allUsers) 또는 Google 계정에 로그인한 모든 사용자(allAuthenticatedUsers)가 버킷 또는 버킷 데이터에 액세스할 수 있는지를 나타냅니다.</p> <p>인터넷 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.</p> <p>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.</p>		
설정 방법	<p>가. 퍼블릭 Access 삭제 방법</p> <p>1) Storage 내 "작업 더 보기(:)" 클릭</p>  <p>2) 버킷 권한 수정 클릭</p> 		

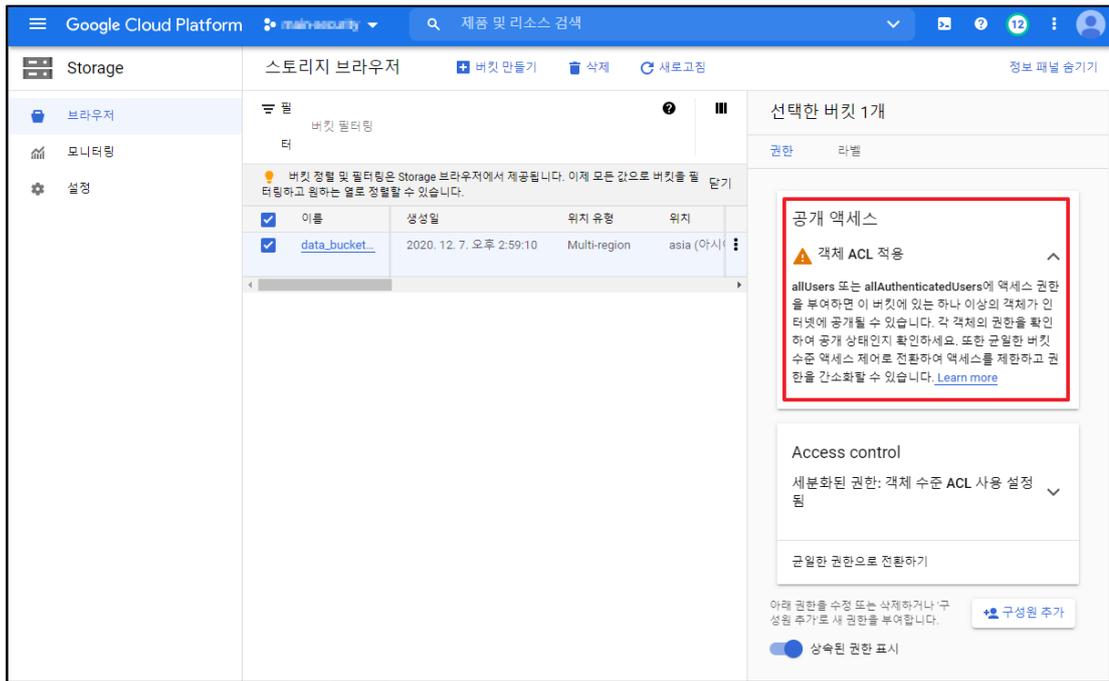
3) 퍼블릭 Access 권한 설정 확인 후 공개 권한 삭제 클릭



4) 퍼블릭 Access 삭제 버튼 클릭

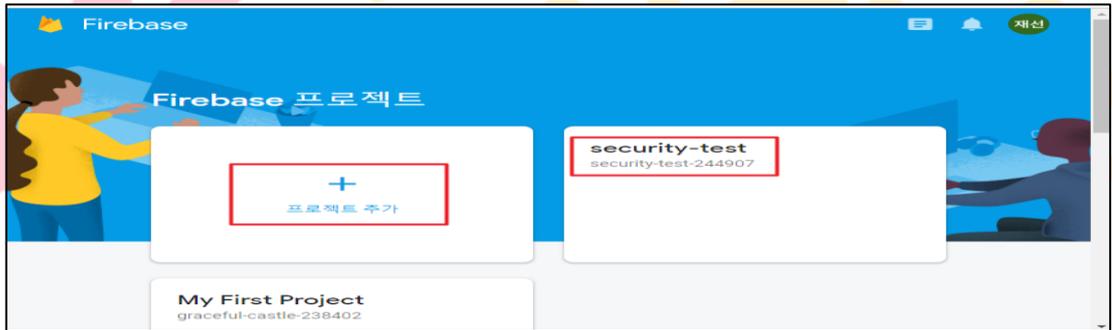


5) 퍼블릭 Access 권한 삭제 완료



나. Firebase Storage

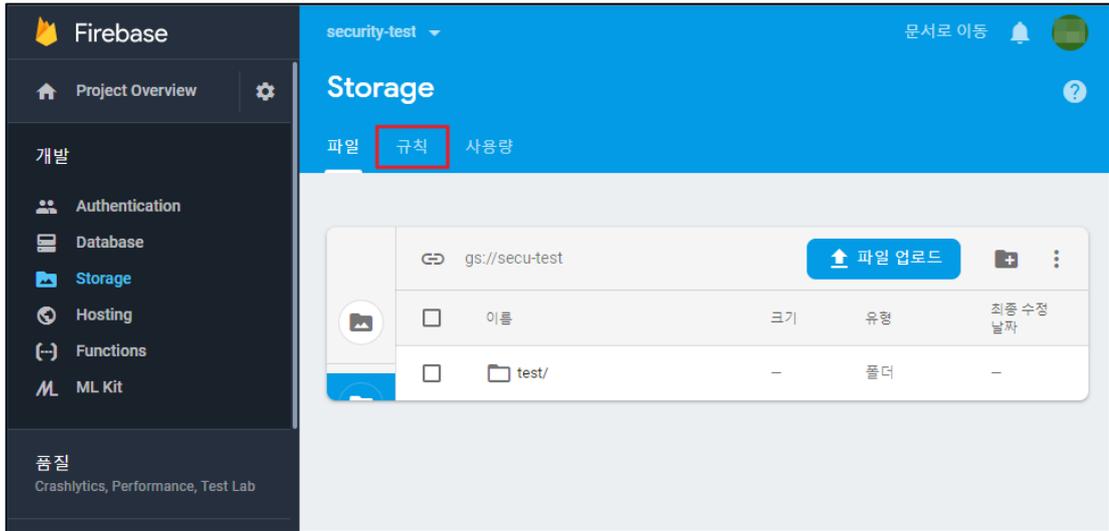
1) Firebase 프로젝트 추가



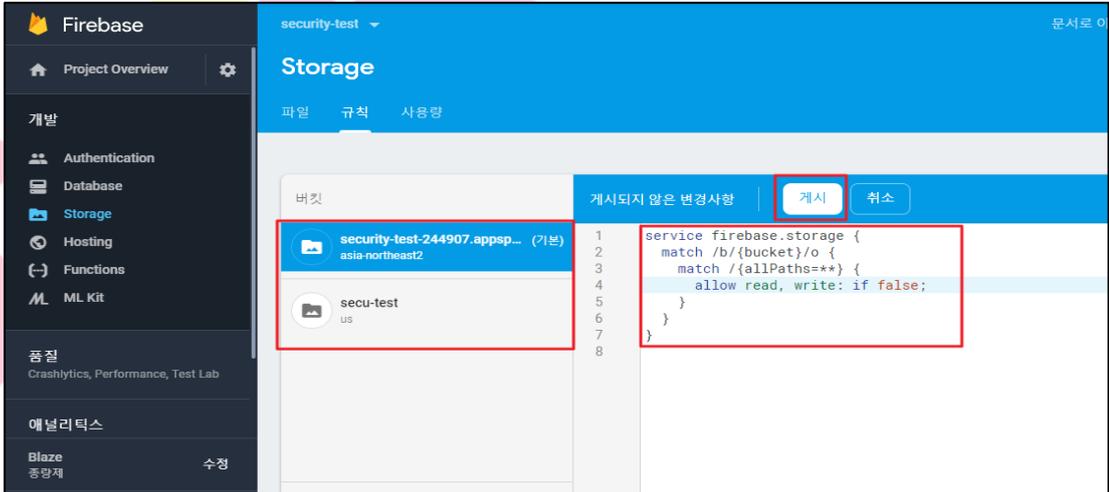
2) Storage 추가



3) 규칙 설정



4) 임의의 규칙 설정(모두 공개 제외)



진단
기준

양호기준

: Storage 버킷 내 불필요한 공개 액세스 설정이 되어 있지 않은 경우

취약기준

: Storage 버킷 내 불필요한 공개 액세스 설정이 되어 있는 경우

비고

3.13 GKE Pod 보안 정책 관리

분류	가상 리소스 관리	중요도	상																
항목명	GKE Pod 보안 정책 관리																		
항목 설명	<p>Kubernetes는 내장형 포드 보안을 제공하며 GCP에서의 PodSecurity는 GKE Cluster에서 실행되는 포드에 포드 보안 표준을 적용할 수 있는 Kubernetes 허용 컨트롤러입니다. 포드 보안 표준은 Kubernetes에서 포드 보안의 사전 정의된 보안 정책이며 상세 내용은 아래와 같습니다.</p> <p>(* Pod Security Standards (PSS))</p> <p>Kubernetes Cluster에서 실행되는 Pod의 보안 설정을 정의하는 규칙 집합이며 Cluster 안에서 실행되는 모든 Pod에 대해 일관된 보안 수준을 유지하고 일반적인 보안 문제를 방지하기 위해 사용됩니다. PSS는 Kubernetes Cluster 관리자가 정책을 구성하고 강제할 수 있으며, Pod의 보안 구성을 검사하여 규칙을 준수하지 않는 Pod를 거부할 수 있습니다.</p> <table border="1"> <thead> <tr> <th>Profile</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Privileged</td> <td>가장 광범위한 수준의 권한을 제공하는 제한되지 않은 정책입니다. 알려진 권한 에스컬레이션을 허용합니다.</td> </tr> <tr> <td>Baseline</td> <td>최소한으로 지정된 기본 포드 구성을 허용하는 최소 제한 정책입니다. 알려진 권한 에스컬레이션을 허용하지 않습니다.</td> </tr> <tr> <td>Restricted</td> <td>포드 강화 권장사항을 따르는 매우 제한적인 정책입니다.</td> </tr> </tbody> </table> <p>※ 각 Profile 별 세부 정보는 아래 링크 참고 https://kubernetes.io/docs/concepts/security/pod-security-standards</p> <p>(* Pod Security Admission (PSA))</p> <p>Kubernetes Cluster에 대한 사전 보안 검사를 수행하는 기능이며 PSA는 Cluster 내에서 Pod가 생성되기 전에 Pod의 보안 설정을 평가하고, 정의된 보안 정책을 준수하는지 확인합니다.</p> <table border="1"> <thead> <tr> <th>Mode</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enforce</td> <td>정책 위반에 대해 포드 생성을 거부 감사 이벤트가 감사 로그에 추가됨</td> </tr> <tr> <td>audit</td> <td>정책 위반에 대해 감사 로그에 감사 이벤트를 추가하는 것을 트리거함 (포드 만들기 허용)</td> </tr> <tr> <td>warn</td> <td>정책 위반은 사용자에게 표시되는 경고를 트리거합니다. 포드 만들기가 허용됩니다.</td> </tr> </tbody> </table>			Profile	Description	Privileged	가장 광범위한 수준의 권한을 제공하는 제한되지 않은 정책입니다. 알려진 권한 에스컬레이션을 허용합니다.	Baseline	최소한으로 지정된 기본 포드 구성을 허용하는 최소 제한 정책입니다. 알려진 권한 에스컬레이션을 허용하지 않습니다.	Restricted	포드 강화 권장사항을 따르는 매우 제한적인 정책입니다.	Mode	Description	enforce	정책 위반에 대해 포드 생성을 거부 감사 이벤트가 감사 로그에 추가됨	audit	정책 위반에 대해 감사 로그에 감사 이벤트를 추가하는 것을 트리거함 (포드 만들기 허용)	warn	정책 위반은 사용자에게 표시되는 경고를 트리거합니다. 포드 만들기가 허용됩니다.
	Profile	Description																	
	Privileged	가장 광범위한 수준의 권한을 제공하는 제한되지 않은 정책입니다. 알려진 권한 에스컬레이션을 허용합니다.																	
	Baseline	최소한으로 지정된 기본 포드 구성을 허용하는 최소 제한 정책입니다. 알려진 권한 에스컬레이션을 허용하지 않습니다.																	
Restricted	포드 강화 권장사항을 따르는 매우 제한적인 정책입니다.																		
Mode	Description																		
enforce	정책 위반에 대해 포드 생성을 거부 감사 이벤트가 감사 로그에 추가됨																		
audit	정책 위반에 대해 감사 로그에 감사 이벤트를 추가하는 것을 트리거함 (포드 만들기 허용)																		
warn	정책 위반은 사용자에게 표시되는 경고를 트리거합니다. 포드 만들기가 허용됩니다.																		
설정 방법	<p>가. 네임스페이스 내 PSS / PSA 설정 및 확인</p> <p>1) PSS / PSA를 적용하기 위한 네임스페이스 생성</p>																		

```
per_@cloudshell:~ (ethereal-audio-413401)$ kubectl create ns pod-sec-restricted-ns
namespace/pod-sec-restricted-ns created
per_@cloudshell:~ (ethereal-audio-413401)$
```

2) 생성된 네임스페이스 라벨 내 PSS / PSA 적용 (enforce=restricted)

```
per_@cloudshell:~ (ethereal-audio-413401)$ kubectl label --overwrite ns pod-sec-restricted-ns pod-security.kubernetes.io/enforce=restricted
namespace/pod-sec-restricted-ns labeled
per_@cloudshell:~ (ethereal-audio-413401)$ kubectl get ns --show-labels
NAME                STATUS   AGE   LABELS
baseline-ns        Active   6m20s  kubernetes.io/metadata.name=baseline-ns
default             Active   14d   kubernetes.io/metadata.name=default
gmp-public          Active   14d   addonmanager.kubernetes.io/mode=Reconcile, kubernetes.io/metadata.name=gmp-public
gmp-system          Active   14d   addonmanager.kubernetes.io/mode=Reconcile, kubernetes.io/metadata.name=gmp-system
kube-node-lease     Active   14d   kubernetes.io/metadata.name=kube-node-lease
kube-public         Active   14d   kubernetes.io/metadata.name=kube-public
kube-system         Active   14d   kubernetes.io/metadata.name=kube-system
pod-sec-restricted-ns Active   3m4s  kubernetes.io/metadata.name=pod-sec-restricted-ns, pod-security.kubernetes.io/enforce=restricted
restricted-ns       Active   6m20s  kubernetes.io/metadata.name=restricted-ns
per_@cloudshell:~ (ethereal-audio-413401)$ kubectl describe ns pod-sec-restricted-ns
Name:               pod-sec-restricted-ns
Labels:             kubernetes.io/metadata.name=pod-sec-restricted-ns
                   pod-security.kubernetes.io/enforce=restricted
Annotations:        <none>
Status:             Active

No resource quota.

No LimitRange resource.
per_@cloudshell:~ (ethereal-audio-413401)$
```

3) 네임스페이스 내 파드 생성 시도를 통해 PSS / PSA 적용 확인 (파드 생성 실패)

```
per_@cloudshell:~ (ethereal-audio-413401)$ kubectl apply -f psa-workload.yaml --namespace=pod-sec-restricted-ns
Error from server (Forbidden): error when creating "psa-workload.yaml": pods "nginx" is forbidden: violates PodSecurity "restricted:latest": privileged (container "nginx" must not set securityContext.privileged=true), allowPrivilegeEscalation != false (container "nginx" must set securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "nginx" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "nginx" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "nginx" must set securityContext.seccompProfile.type to "RuntimeDefault" or "Localhost")
per_@cloudshell:~ (ethereal-audio-413401)$
```

4) 로그 탐색기 내 PSS / PSA 적용 로그 확인 (파드 생성 실패)

<p>진단 기준</p>	<p>양호기준 : PSS Profile Baseline 및 PSA Audit 이상 설정을 적용해 사용하는 경우</p> <p>취약기준 : PSS 및 PSA 설정을 적용하여 사용하지 않거나 PSS Profile Privileged 및 PSA warn 설정을 적용해 사용하는 경우</p>
<p>비고</p>	

4. 운영 관리

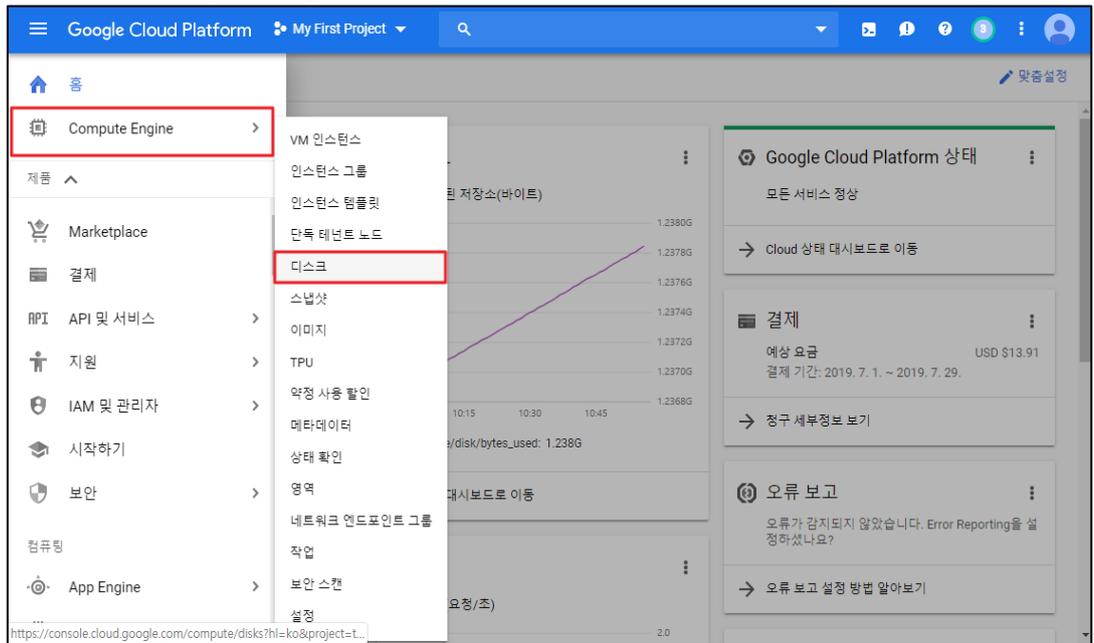
4.1 Compute Engine 디스크 암호화 설정

분류	운영 관리	중요도	중
항목명	Compute Engine 디스크 암호화 설정		
항목 설명	<p>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.</p> <p>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.</p> <p>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 방지할 수 있습니다.</p> <p>※ 암호화 키 방식</p>		
	암호화 키	상세내용	
	Google 관리 암호화 키	<p>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.</p>	
	고객 제공 암호화 키	<p>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.</p>	
고객 관리 암호화 키	<p>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.</p> <p>Cloud KMS 는 클라우드에서 호스팅 되는 키 관리 서비스로서 온프레미스와 동일한 방식으로 클라우드 서비스의 암호화 키를 관리할 수 있습니다. AES-256, RSA 2048, RSA 3072, RSA</p>		

4096, 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.

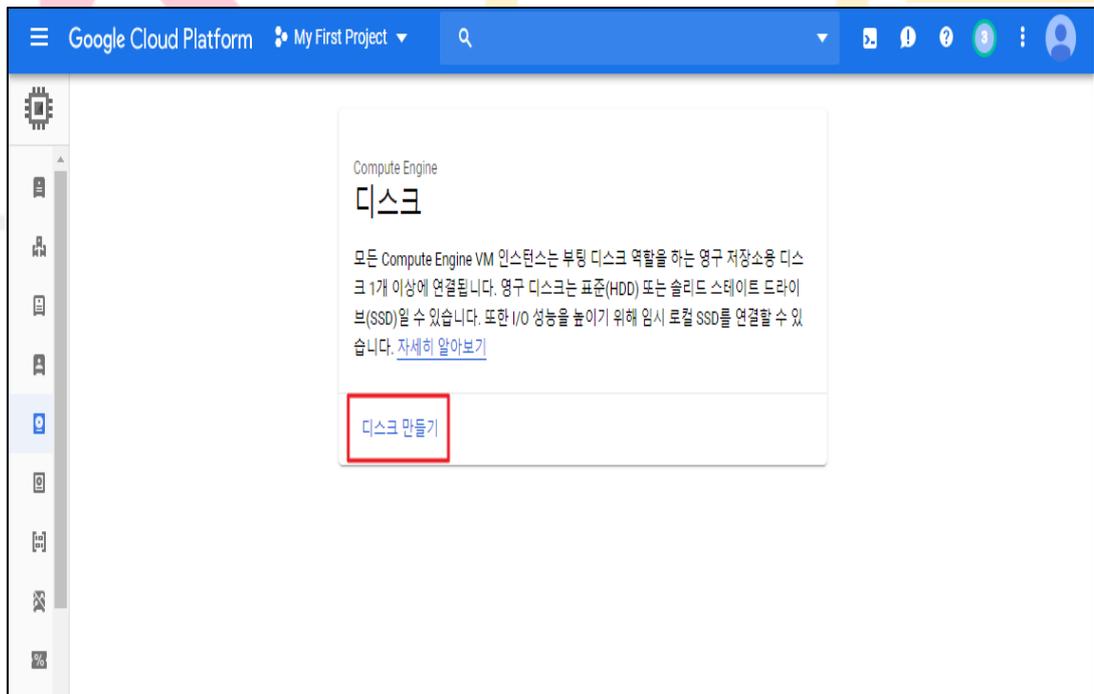
가. 디스크 암호화키 설정

1) [메인] > [Compute Engine] > [디스크]



설정
방법

2) 디스크 만들기



3) 디스크 정보 입력 및 리전 선택

The screenshot shows the '디스크 만들기' (Create Disk) page in the Google Cloud Platform console. The following fields are highlighted with red boxes:

- 이름 (Name):** disk-1
- 유형 (Type):** 표준 영구 디스크 (Standard Persistent Disk)
- 리전 (Region):** asia-northeast2(오사카) (asia-northeast2)
- 영역 (Zone):** asia-northeast2-a

Other visible options include '리전 내에서 이 디스크 복제' (checked), '스냅샷 설정' (Snapshot settings), and '소스 유형' (Source type) with options for '빈 디스크', '이미지', and '스냅샷'.

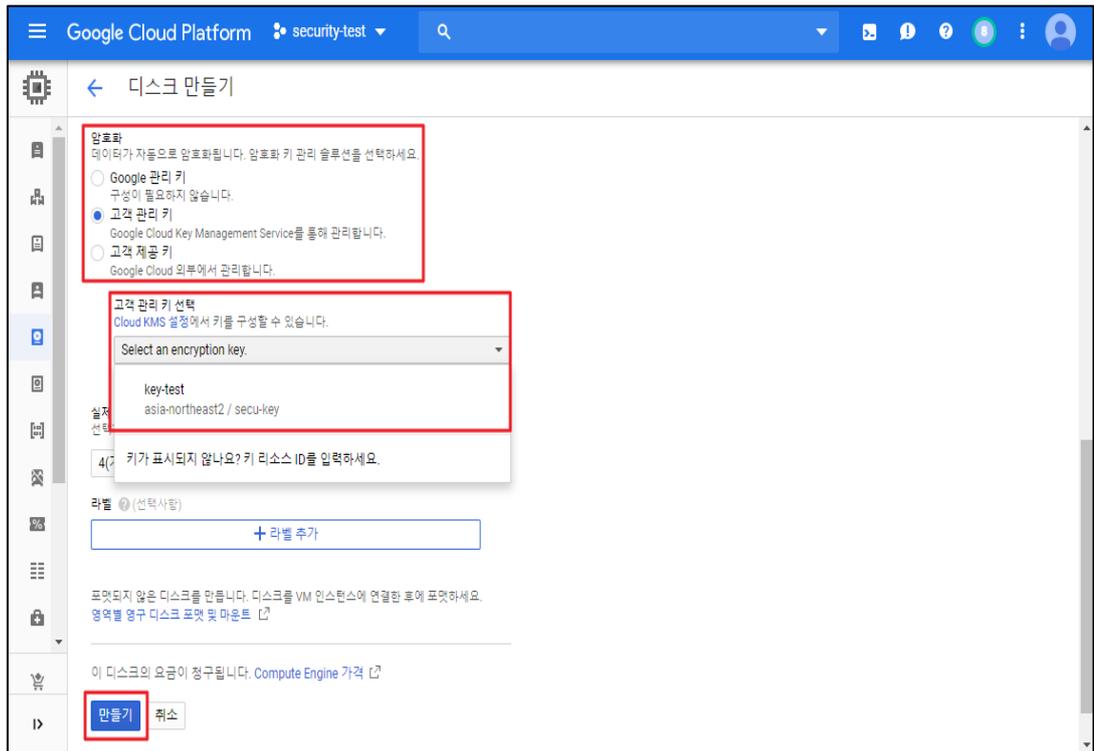
4) 'Google 관리 키' 암호화 방식 설정

The screenshot shows the '디스크 만들기' (Create Disk) page with encryption options highlighted in a red box:

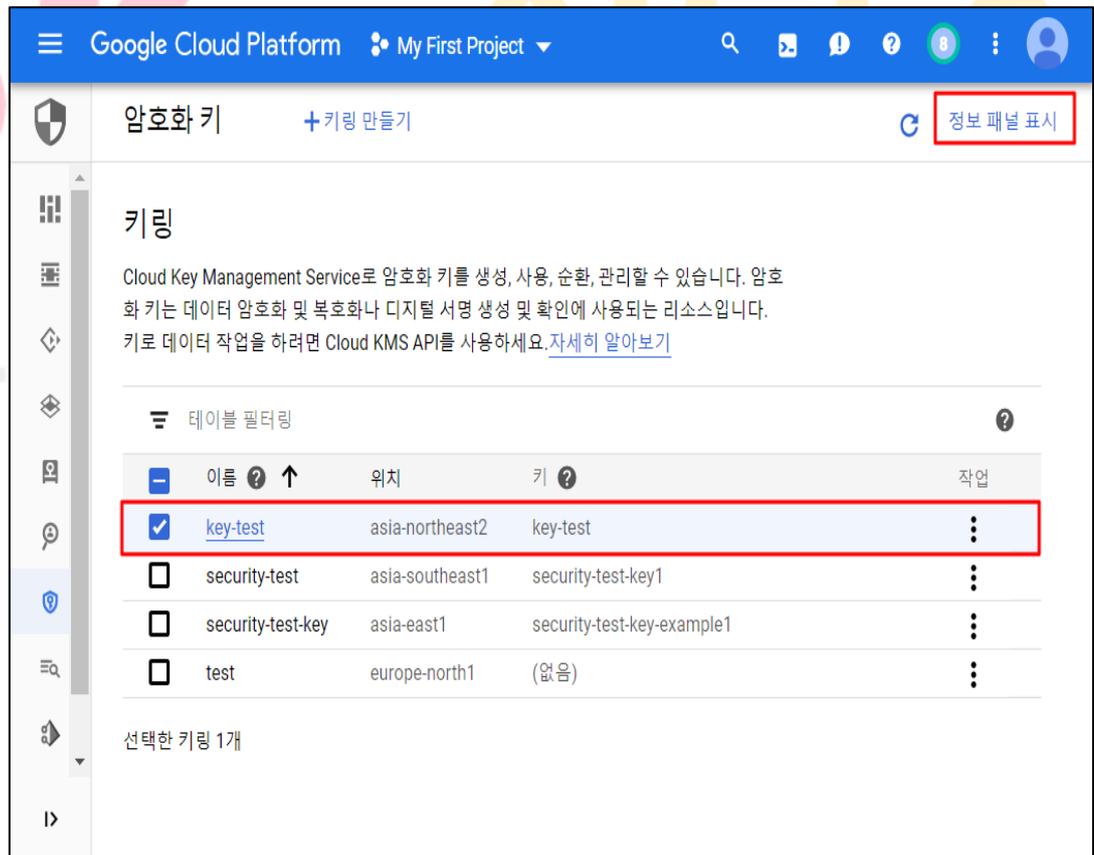
- 암호화 (Encryption):** 데이터가 자동으로 암호화됩니다. 암호화 키 관리 옵션을 선택하세요.
 - Google 관리 키 (Google-managed keys): 구성이 필요하지 않습니다.
 - 고객 관리 키 (Customer-managed keys): Google Cloud Key Management Service를 통해 관리합니다.
 - 고객 제공 키 (Customer-supplied keys): Google Cloud 외부에서 관리합니다.

Other visible options include '실제 블록 크기 (KB)' (4(기본값)), '라벨' (Labels), and a '만들기' (Create) button highlighted with a red box.

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

Google Cloud Platform My First Project

암호화 키 + 키링 만들기 정보 패널 숨기기

key-test

PERMISSIONS 활동

아래 권한을 수정 또는 삭제하거나 '구성원 추가'로 새 권한을 부여합니다. 구성원 추가

상속된 권한 표시

필터 트리

역할/구성원 ↑	상속
▼ 소유자 (1)	
gcpsecu@gmail.com	
▼ 편집자 (5)	
연 834963676861-compute@developer.gserviceaccount.com	
연 834963676861@cloudservices.gserviceaccount.com	
연 dulcet-answer-240900@appspot.gserviceaccount.com	
junshae1125@gmail.com	
연 service-834963676861@containerregistry.iam.gserviceaccount.com	

8) '고객 제공 키' 암호화 방식 설정 (256비트 키 사용)

Google Cloud Platform security-test

← 디스크 만들기

암호화
데이터가 자동으로 암호화됩니다. 암호화 키 관리 옵션을 선택하세요.

- Google 관리 키
구성이 필요하지 않습니다.
- 고객 관리 키
Google Cloud Key Management Service를 통해 관리됩니다.
- 고객 제공 키
Google Cloud 외부에서 관리됩니다.

⚠ Google Cloud Platform 외부에서 직접 관리하는 키를 분실할 경우 Google에서 데이터를 복구할 수 없습니다. 안전한 위치에 키를 보관하세요.

a

키는 표준 base64로 인코딩된 올바른 256비트 문자열이어야 합니다.

래핑된 키
이 키는 Compute Engine 공개 키로 래핑되었습니다.

실제 블록 크기(KB) Ⓜ
선택한 후에는 변경할 수 없습니다.

4(기본값)

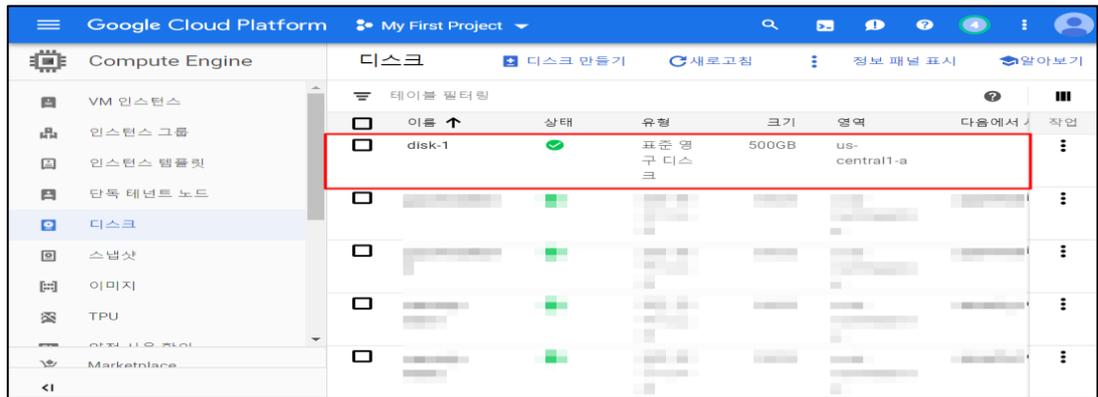
라벨 Ⓜ (선택사항)
+ 라벨 추가

포맷되지 않은 디스크를 만듭니다. 디스크를 VM 인스턴스에 연결한 후에 포맷하세요.
영역별 영구 디스크 포맷 및 마운트

이 디스크의 요금이 청구됩니다. Compute Engine 가격

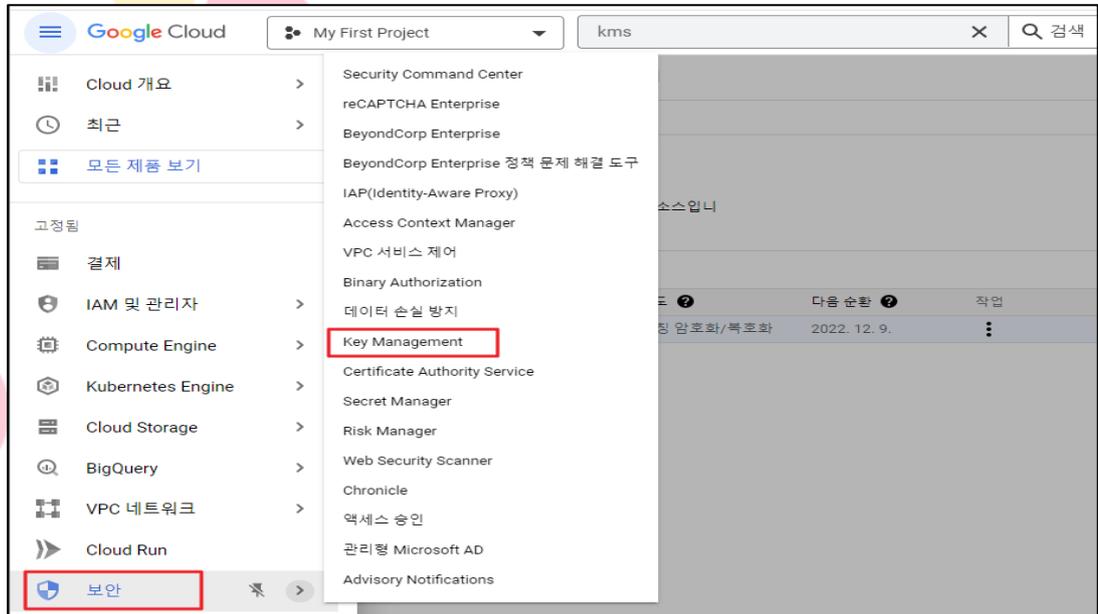
만들기 취소

9) 암호화된 디스크 생성 완료

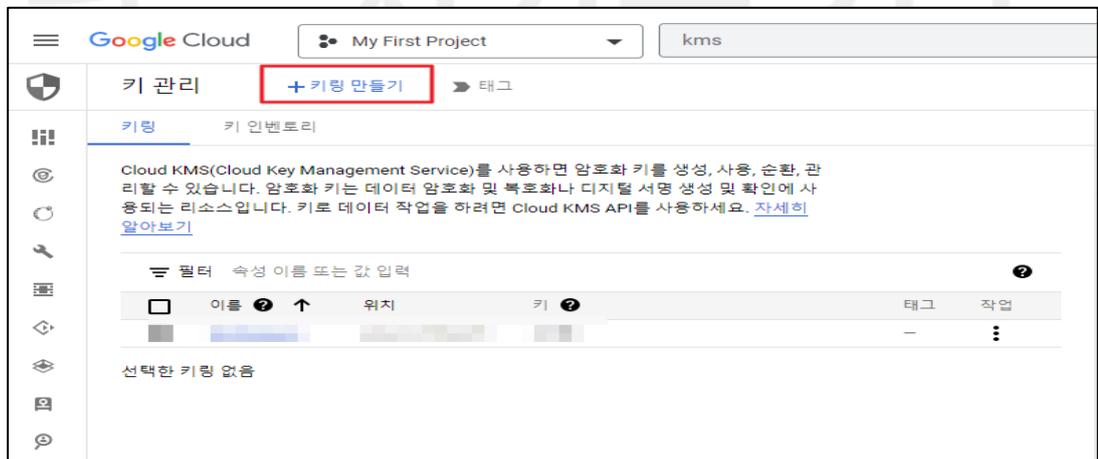


나. 암호화키 생성 및 순환주기 설정

1) [메인] > [보안] > [Key Management]



2) 키 생성을 위한 키링 만들기



3) 키링 이름 및 리전 선택 후 만들기

Google Cloud My First Project kms

키링 만들기

키링은 여러 키를 하나로 모아서 정리합니다. 다음 단계에서 키링에 속한 키를 만듭니다. [자세히 알아보기](#)

프로젝트 이름
My First Project

키링 이름 *
disk-enc-key

위치 유형
리전
 단일 리전 내에서 짧은 지연 시간
 멀티 리전
특별은 지역에서 가장 높은 가용성

리전 *
asia-northeast3 (서울)

만들기 취소

4) 키 순환 주기 설정 및 키 만들기

Google Cloud My First Project kms

키 만들기

암호화 키는 데이터 암호화 및 복호화나 디지털 서명 생성 및 확인에 사용되는 리소스입니다. 키에 여러 버전이 있을 수 있습니다. [자세히 알아보기](#)

프로젝트 이름 키링 위치

어떤 유형의 키를 만드시겠어요?
 생성된 키
일반 고객이 관리하는 암호화 키입니다. 키 자료가 자동으로 생성됩니다. [자세히 알아보기](#)
 가져온 키
GCP에 키 자료를 가져오려는 경우 선택합니다. [자세히 알아보기](#)
 외부 관리 키
키 자료는 외부 키 관리자에 저장됩니다. [자세히 알아보기](#)

키 이름 *
security-disk-key

보호 수준
소프트웨어

용도
대칭 암호화/복호화

알고리즘
Google 대칭 키 키

키 순환 기간
30일

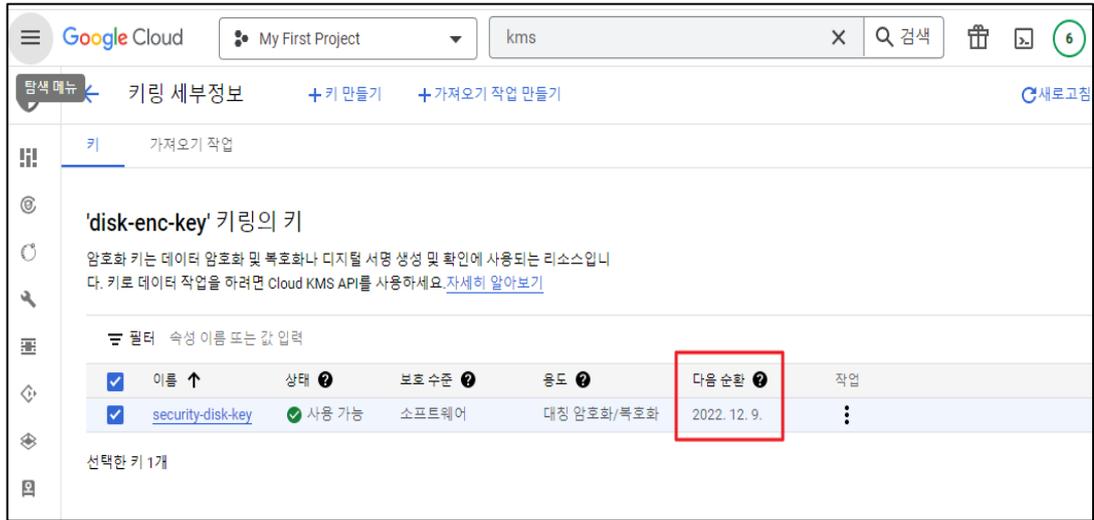
시작일
22. 12. 9.

순환 요약: 2022년 12월 9일부터 30일마다

설정(선택사항)
라벨
+ 라벨 추가

만들기 취소

5) 키 순환주기를 적용하여 키 생성 완료 확인



진단 기준

양호기준

: “고객 관리 키” 사용 시 키에 대한 순환 주기 설정이 되어 있을 경우

취약기준

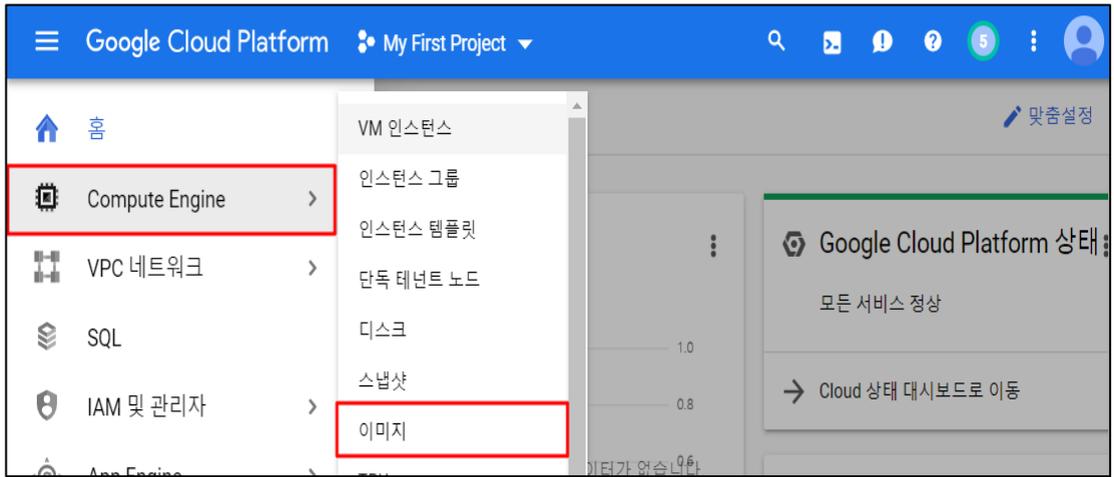
: “고객 관리 키” 사용 시 키에 대한 순환 주기 설정이 되어있지 않을 경우

비고

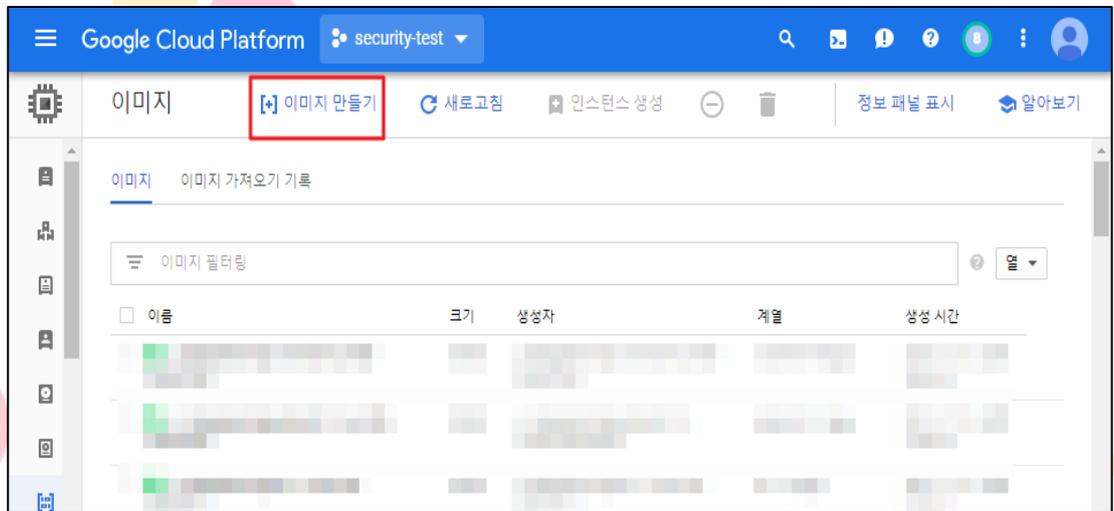
진단기준에서 하나라도 기준에 맞지 않는 설정을 보유하고 있을 경우 취약으로 간주함

4.2 Compute Engine 이미지 암호화 설정

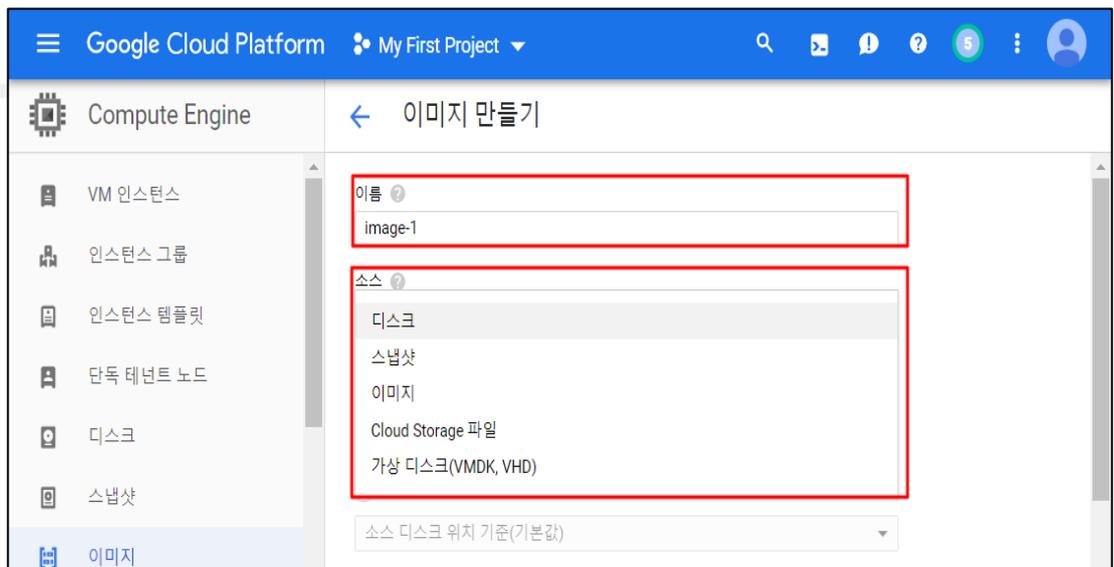
분류	운영 관리	중요도	중						
항목명	Compute Engine 이미지 암호화 설정								
항목 설명	<p>Compute Engine 내 이미지는 변경할 수 없는 디스크에 대한 참조를 제공하는 클라우드 리소스로서, 운영체제(OS) 이미지를 이용하여 인스턴스의 부팅 디스크를 만드는데 사용되며, Compute Engine의 모든 디스크는 기본적으로 Google의 암호화 키를 사용하여 암호화됩니다. 디스크에서 빌드된 이미지도 암호화됩니다. 또는 디스크를 만들 때 자체 암호화 키를 제공할 수도 있습니다. 디스크를 만든 다음 이미지 생성 명령어에 암호화 키를 제공하여 암호화된 이미지를 만들 수 있습니다. 이미지는 아래 두가지 방식으로 생성이 가능합니다.</p> <p>기본적으로 Compute Engine 은 생성된 이미지를 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.</p> <p>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 방지할 수 있습니다.</p> <p>※ 이미지 생성 방식</p> <table border="1"> <thead> <tr> <th>이름</th> <th>상세내용</th> </tr> </thead> <tbody> <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> </tbody> </table>			이름	상세내용	공개 이미지	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.	커스텀 이미지	커스텀 이미지는 사용자의 프로젝트에서만 사용할 수 있습니다. 부팅 디스크 및 다른 이미지에서 커스텀 이미지를 생성한 다음 해당 커스텀 이미지를 사용하여 인스턴스를 만들 수 있습니다.
	이름	상세내용							
공개 이미지	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.								
커스텀 이미지	커스텀 이미지는 사용자의 프로젝트에서만 사용할 수 있습니다. 부팅 디스크 및 다른 이미지에서 커스텀 이미지를 생성한 다음 해당 커스텀 이미지를 사용하여 인스턴스를 만들 수 있습니다.								
설정 방법	<p>가. 이미지 암호화키 설정</p> <p>1) [메인] > [Compute Engine] > [이미지]</p>								



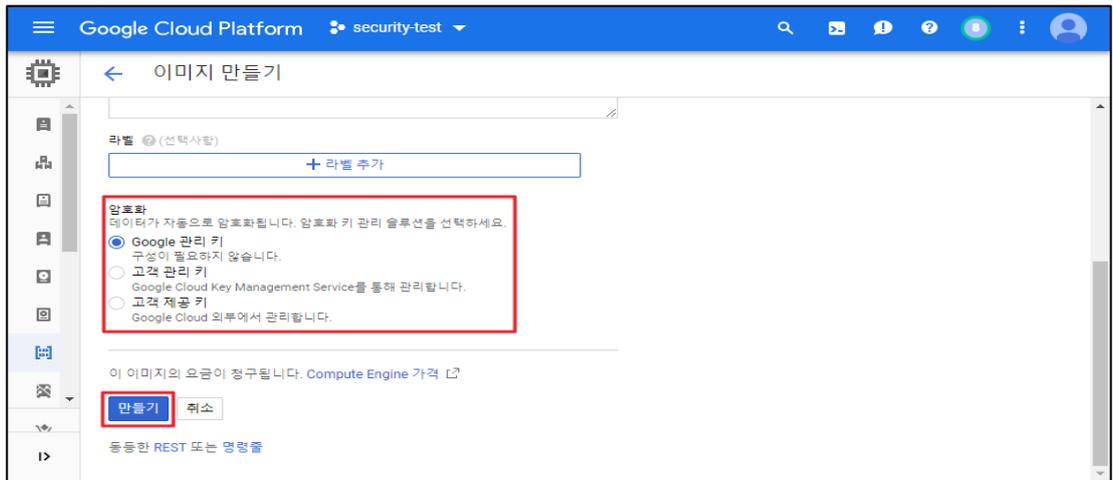
2) 이미지 만들기



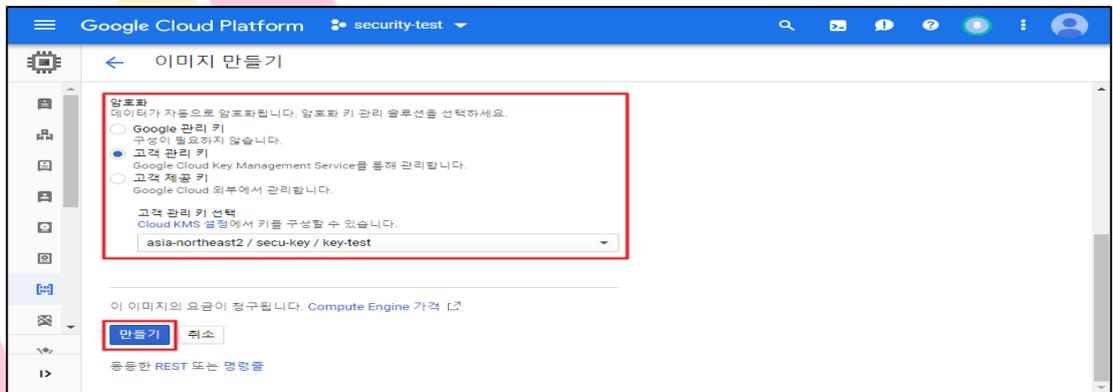
3) 이미지 정보 및 생성할 소스 대상 선택



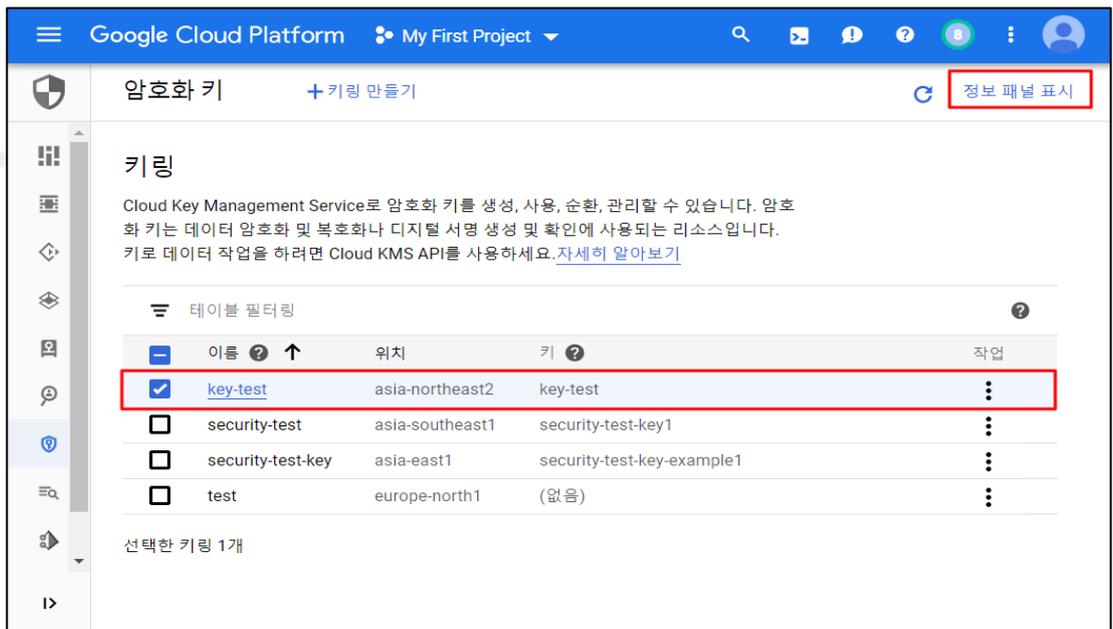
4) 'Google 관리 키' 암호화 방식 설정



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

Google Cloud Platform My First Project

암호화 키 +키링 만들기 정보 패널 숨기기

key-test

PERMISSIONS 활동

아래 권한을 수정 또는 삭제하거나 '구성원 추가'로 새 권한을 부여합니다. [구성원 추가](#)

상속된 권한 표시

필터 트리

역할/구성원 ↑	상속
▼ 소유자 (1)	
gcpsecu@gmail.com	
▼ 편집자 (5)	
연 834963676861-compute@developer.gserviceaccount.com	
연 834963676861@cloudservices.gserviceaccount.com	
연 dulcet-answer-240900@appspot.gserviceaccount.com	
junshae1125@gmail.com	
연 service-834963676861@containerregistry.iam.gserviceaccount.com	

8) '고객 제공 키' 암호화 방식 설정 (256비트 키 사용)

Google Cloud Platform security-test

← 이미지 만들기

암호화
데이터가 자동으로 암호화됩니다. 암호화 키 관리 솔루션을 선택하세요.

Google 관리 키
구성이 필요하지 않습니다.

고객 관리 키
Google Cloud Key Management Service를 통해 관리합니다.

고객 제공 키
Google Cloud 외부에서 관리합니다.

⚠ Google Cloud Platform 외부에서 직접 관리하는 키를 분실할 경우 Google에서 데이터를 복구할 수 없습니다. 안전한 위치에 키를 보관하세요.

a

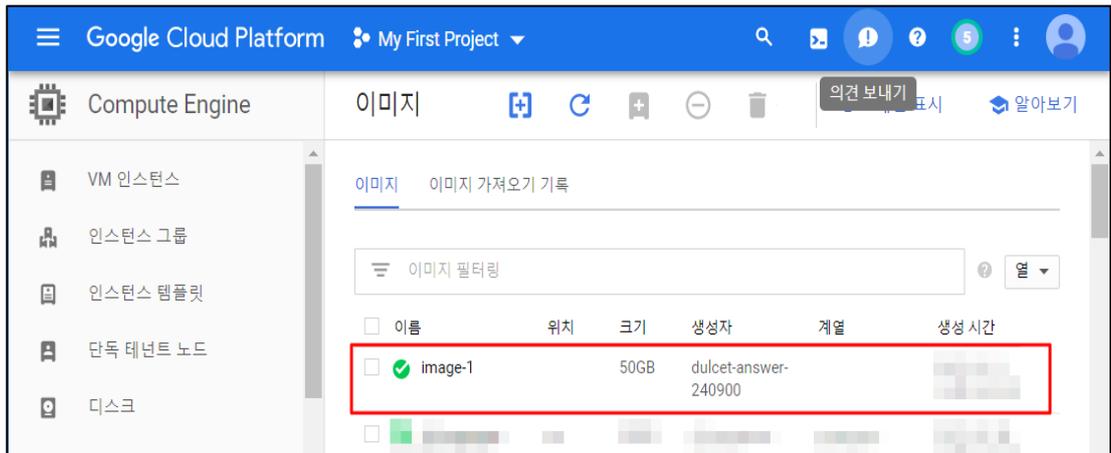
키는 표준 base64로 인코딩된 올바른 256비트 문자열이어야 합니다.

래핑된 키
이 키는 Compute Engine 공개 키로 래핑되었습니다.

이 이미지의 요금이 청구됩니다. [Compute Engine 가격](#)

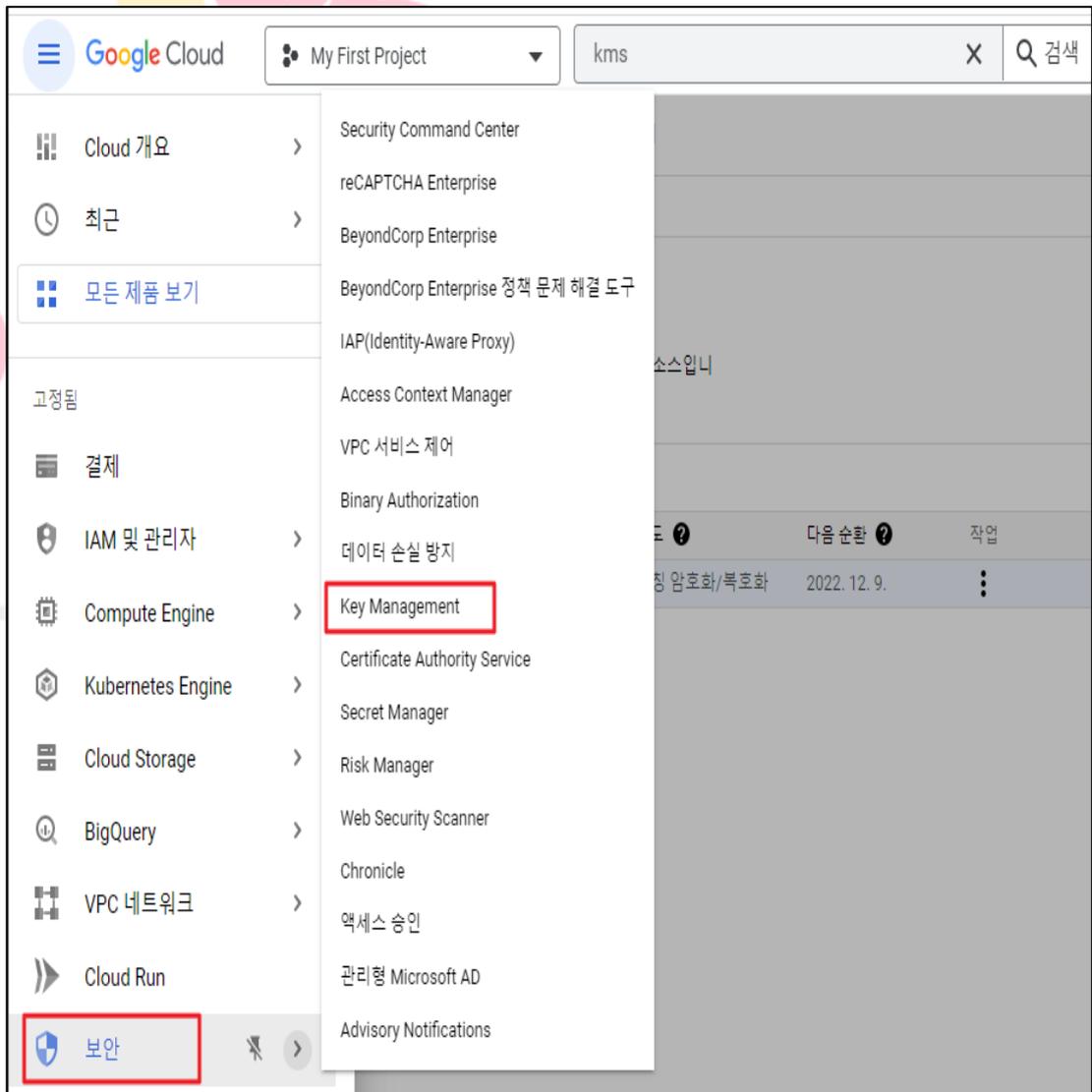
만들기 취소

9) 암호화된 이미지 생성 완료



나. 암호화키 생성 및 순환주기 설정

1) [메인] > [보안] > [Key Management]



2) 키 생성을 위한 키링 만들기

Google Cloud My First Project kms

키 관리 **+ 키링 만들기** 태그

키링 키 인벤토리

Cloud KMS(Cloud Key Management Service)를 사용하면 암호화 키를 생성, 사용, 순환, 관리할 수 있습니다. 암호화 키는 데이터 암호화 및 복호화나 디지털 서명 생성 및 확인에 사용되는 리소스입니다. 키로 데이터 작업을 하려면 Cloud KMS API를 사용하세요. [자세히 알아보기](#)

필터 속성 이름 또는 값 입력

<input type="checkbox"/>	이름 ? ↑	위치	키 ?	태그	작업
				-	⋮

선택한 키링 없음

3) 키링 이름 및 리전 선택 후 만들기

Google Cloud My First Project kms

키링 만들기

키링은 여러 키를 하나로 모아서 정리합니다. 다음 단계에서 키링에 속한 키를 만듭니다. [자세히 알아보기](#)

프로젝트 이름
My First Project

키링 이름 *
disk-enc-key

위치 유형 ?

리전
단일 리전 내에서 짧은 지연 시간

멀티 리전
특정 지역서 가장 높은 가용성

리전 *
asia-northeast3 (서울)

만들기 취소

4) 키 순환 주기 설정 및 키 만들기

Google Cloud My First Project kms

키 만들기

암호화 키는 데이터 암호화 및 복호화나 디지털 서명 생성 및 확인에 사용되는 리소스입니다. 키에 여러 버전이 있을 수 있습니다. [자세히 알아보기](#)

프로젝트 이름 키링 위치

어떤 유형의 키를 만드시겠습니까?

- 생성된 키
일반 고객이 관리하는 암호화 키입니다. 키 자료가 자동으로 생성됩니다. [자세히 알아보기](#)
- 가져온 키
GCP에 키 자료를 가져오려는 경우 선택합니다. [자세히 알아보기](#)
- 외부 관리 키
키 자료는 외부 키 관리자에 저장됩니다. [자세히 알아보기](#)

키 이름 * security-disk-key

보호 수준 소프트웨어

용도 대칭 암호화/복호화

알고리즘 Google 대칭 키 키

키 순환 기간 30일

시작일 22. 12. 9.

순환 요약: 2022년 12월 9일부터 30일마다

설정(선택사항)

라벨

+ 라벨 추가

만들기 취소

5) 키 순환주기를 적용하여 키 생성 완료 확인

Google Cloud My First Project kms

키링 세부정보

키링 세부정보 + 키 만들기 + 가져오기 작업 만들기 새로고침

키 가져오기 작업

'disk-enc-key' 키링의 키

암호화 키는 데이터 암호화 및 복호화나 디지털 서명 생성 및 확인에 사용되는 리소스입니다. 키로 데이터 작업을 하려면 Cloud KMS API를 사용하세요. [자세히 알아보기](#)

필터 속성 이름 또는 값 입력

<input checked="" type="checkbox"/>	이름 ↑	상태	보호 수준	용도	다음 순환	작업
<input checked="" type="checkbox"/>	security-disk-key	사용 가능	소프트웨어	대칭 암호화/복호화	2022. 12. 9.	

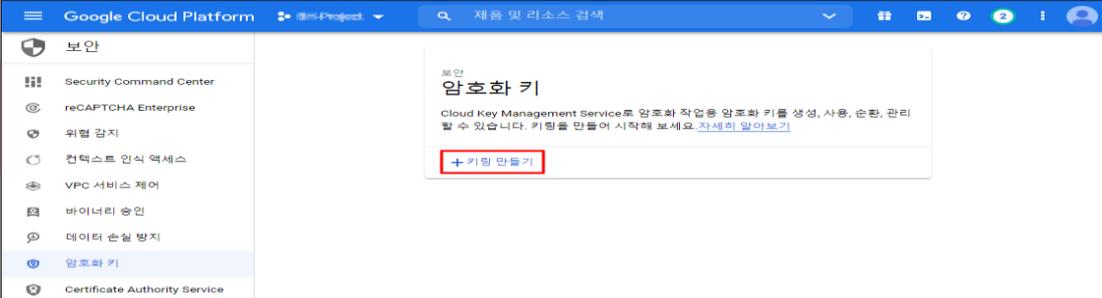
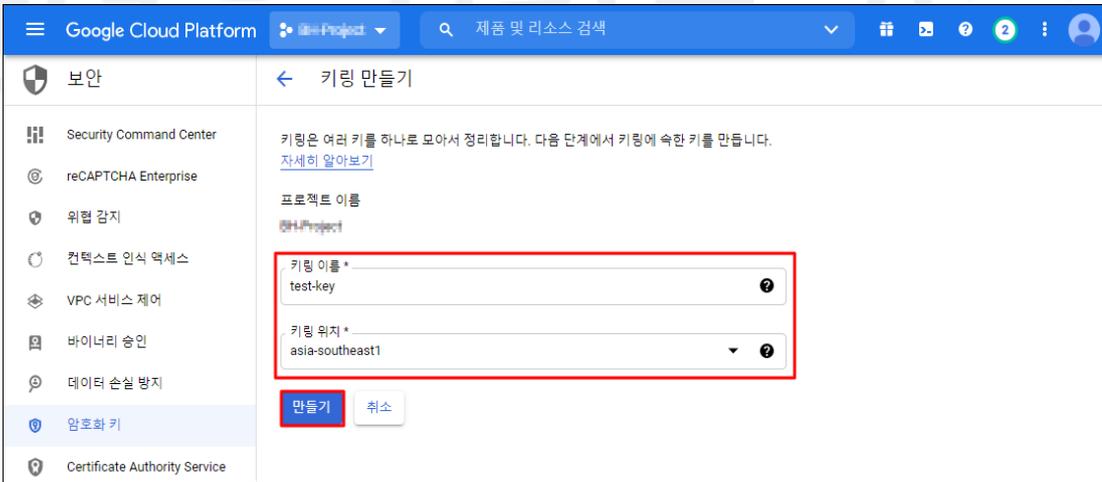
선택한 키 1개

진단 기준	<p>양호기준 : “고객 관리 키” 사용 시 키에 대한 순환 주기 설정이 되어 있을 경우</p> <p>취약기준 : “고객 관리 키” 사용 시 키에 대한 순환 주기 설정이 되어있지 않을 경우</p>
비고	



안녕을 지키는 기술

4.3 SQL 암호화 설정

분류	운영 관리	중요도	중						
항목명	SQL 암호화 설정								
항목 설명	<p>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.</p> <p>"고객 관리 키"를 사용하는 경우 키에 대한 순환 주기 설정을 통해 키 유출 및 사용자 접근에 대한 보안 위협을 미연에 방지할 수 있습니다.</p> <p>(*) 사용 가능한 암호화 키 종류</p> <table border="1" data-bbox="280 768 1425 958"> <thead> <tr> <th>구분</th> <th>내용</th> </tr> </thead> <tbody> <tr> <td>Google 관리 키</td> <td>Google에서 제공하는 자체 암호화 키를 이용하여 데이터 암호/복호화</td> </tr> <tr> <td>고객 관리 키</td> <td>CKMS(Cloud Key Management Service)를 이용하여 암호화 키 관리 및 데이터 암호/복호화</td> </tr> </tbody> </table>			구분	내용	Google 관리 키	Google에서 제공하는 자체 암호화 키를 이용하여 데이터 암호/복호화	고객 관리 키	CKMS(Cloud Key Management Service)를 이용하여 암호화 키 관리 및 데이터 암호/복호화
구분	내용								
Google 관리 키	Google에서 제공하는 자체 암호화 키를 이용하여 데이터 암호/복호화								
고객 관리 키	CKMS(Cloud Key Management Service)를 이용하여 암호화 키 관리 및 데이터 암호/복호화								
설정 방법	<p>가. CKMS(Cloud Key Management Service)를 통한 암호화 키 생성 방법</p> <p>1) 보안 > 암호화 키 내 키링 만들기 클릭</p>  <p>2) 키링 이름 및 키링 위치 설정 후 만들기 클릭</p> 								

3) 생성할 암호화 키의 유형, 이름, 보호 방법, 용도(순환 주기) 설정 후 만들기 클릭

Google Cloud Platform - 키 만들기

암호화 키는 데이터 암호화 및 복호화나 디지털 서명 생성 및 확인에 사용되는 리소스입니다. 키에 여러 버전이 있을 수 있습니다. [자세히 알아보기](#)

프로젝트 이름: test-key | 키링: test-key | 위치: asia-south

어떤 유형의 키를 만드시겠습니까?

- 생성된 키
일반 고객이 관리하는 암호화 키입니다. 키 자료가 자동으로 생성됩니다. [자세히 알아보기](#)
- 가져온 키
GCP에 키 자료를 가져오려는 경우 선택합니다. [자세히 알아보기](#)
- 외부 관리 키
키 자료는 외부 키 관리자에 저장됩니다. [자세히 알아보기](#)

키 이름 *
test-key-1

보호 수준
소프트웨어

용도
대칭 암호화/복호화

키 유형 및 알고리즘
Google 대칭 키 키

순환 주기: 90일 | 시작일: 21. 3. 20.

순환 요약: 2021년 3월 20일부터 90일마다

라벨: + 라벨 추가

만들기 취소

4) 생성된 암호화 키 확인

Google Cloud Platform - 키링 세부정보

키링 세부정보 | 키 만들기 | 가져오기 작업 만들기 | 정보 패널 표시

키링: test-key

키링의 키

암호화 키는 데이터 암호화 및 복호화나 디지털 서명 생성 및 확인에 사용되는 리소스입니다. 키로 데이터 작업을 하려면 Cloud KMS API를 사용하세요. [자세히 알아보기](#)

이름	상태	보호 수준	용도	다음 순환	작업
test-key-1	사용 가능	소프트웨어	대칭 암호화/복호화	2021. 3. 20.	

선택한 키 없음

나. 등록되어 있는 암호화 키 확인 및 순환 주기 설정 확인

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

Google Cloud Platform console showing the 'test-key' key details. The table below shows the key information:

이름	상태	보호 수준	종도	다음 순환	작업
test-key-1	사용 가능	소프트웨어	대칭 암호화/복호화	2021. 3. 20.	⋮

2) 보안 > 암호화 키 내 키링 클릭을 통해 순환 주기 설정 확인

Google Cloud Platform console showing the 'test-key' key details. The table below shows the key information:

이름	상태	보호 수준	종도	다음 순환	작업
test-key-1	사용 가능	소프트웨어	대칭 암호화/복호화	2021. 3. 20.	⋮

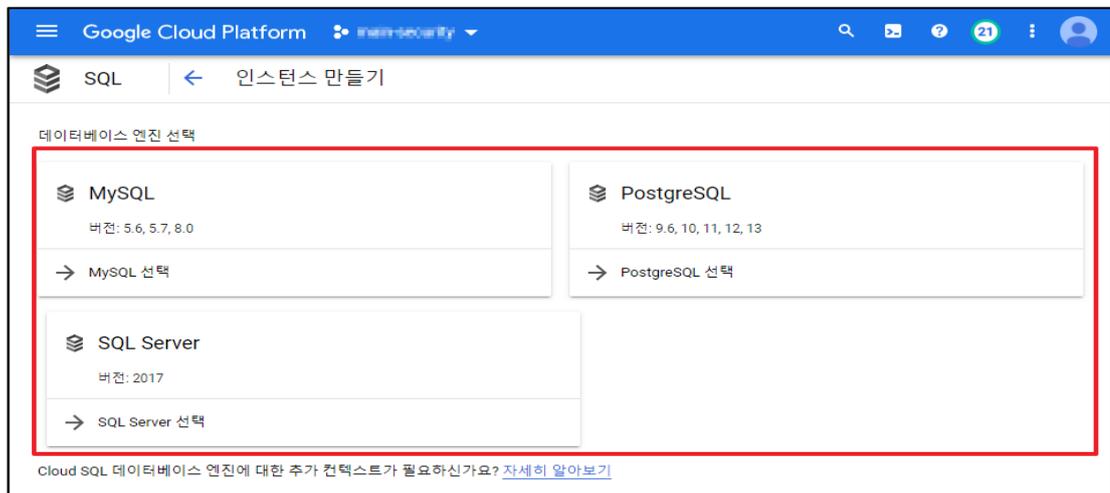
다. Cloud SQL 인스턴스 암호화 설정 방법

1) SQL 내 인스턴스 만들기 클릭

Google Cloud Platform console showing the 'SQL' section. The table below shows the instance information:

인스턴스 ID	유형	공개 IP 주소	비공개 IP 주소	인스턴스 연결 이름
main-security-mysql	MySQL 5.7	04.04.180.104		main-security...

2) 데이터베이스 엔진 선택

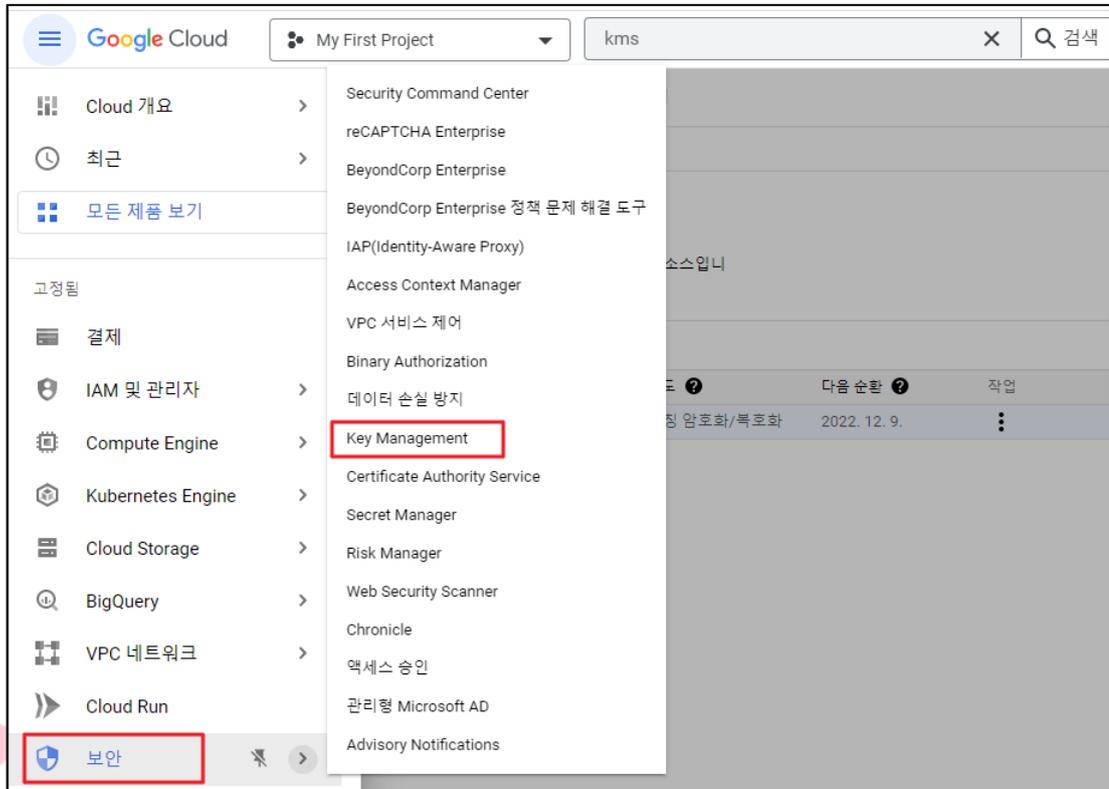


3) 구성 옵션 > 머신 유형 및 스토리지 내 암호화 유형 선택

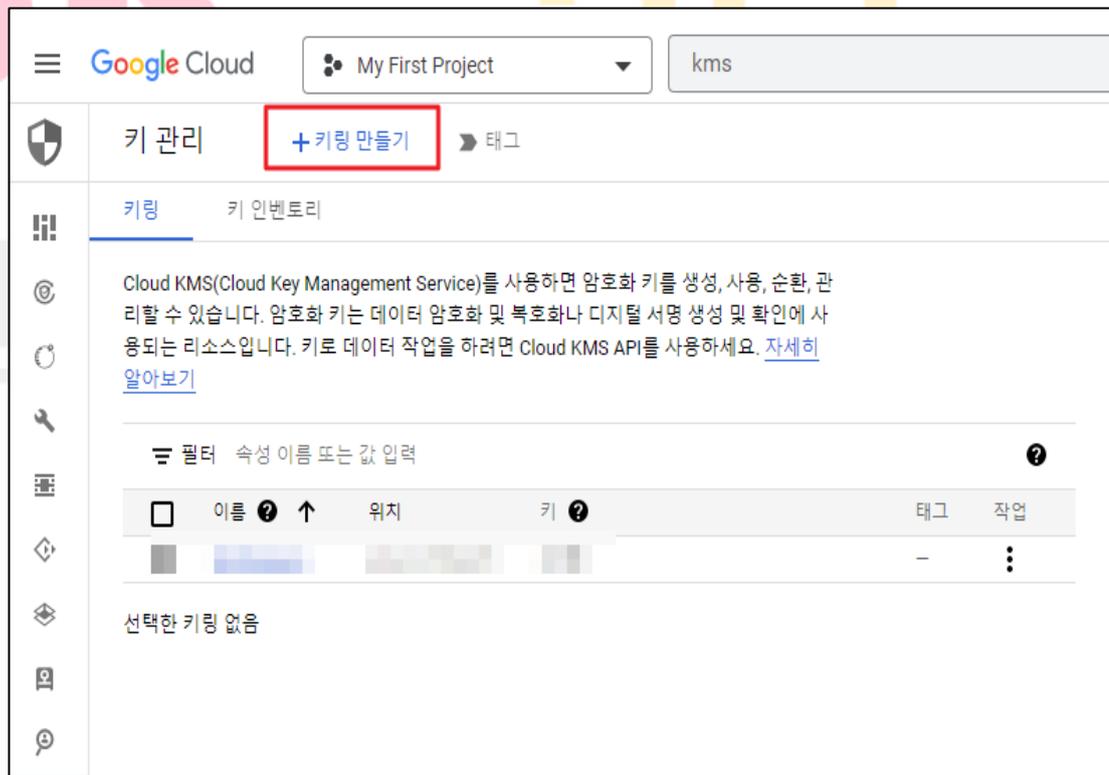


라. 암호화키 생성 및 순환주기 설정

1) [메인] > [보안] > [Key Management]



2) 키 생성을 위한 키링 만들기



3) 키링 이름 및 리전 선택 후 만들기

Google Cloud My First Project kms

키링 만들기

키링은 여러 키를 하나로 모아서 정리합니다. 다음 단계에서 키링에 속한 키를 만듭니다.
[자세히 알아보기](#)

프로젝트 이름
My First Project

키링 이름 *
disk-enc-key

위치 유형 ?

리전
 단일 리전 내에서 짧은 지연 시간

멀티 리전
 특정은 지역에서 가장 높은 가용성

리전 *
asia-northeast3 (서울)

만들기 취소

4) 키 순환 주기 설정 및 키 만들기

Google Cloud My First Project kms

키 만들기

암호화 키는 데이터 암호화 및 복호화나 디지털 서명 생성 및 확인에 사용되는 리소스입니다. 키에 여러 버전이 있을 수 있습니다.[자세히 알아보기](#)

프로젝트 이름 키링 위치 ?

어떤 유형의 키를 만드시겠어요?

생성된 키
 일반 고객이 관리하는 암호화 키입니다. 키 자료가 자동으로 생성됩니다. [자세히 알아보기](#)

가져온 키
 GCP에 키 자료를 가져오려는 경우 선택합니다. [자세히 알아보기](#)

외부 관리 키
 키 자료는 외부 키 관리자에 저장됩니다. [자세히 알아보기](#)

키 이름 *
security-disk-key

보호 수준
소프트웨어

중도
대칭 암호화/복호화

알고리즘
Google 대칭 키 키

키 순환 기간
30일

시작일
22. 12. 9.

순환 요약: 2022년 12월 9일부터 30일마다

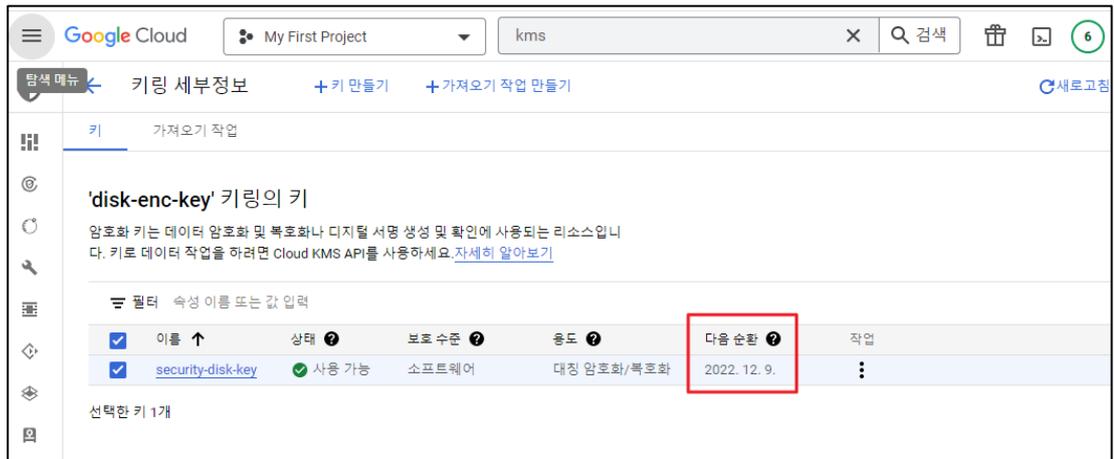
설정(선택사항)

라벨 ?

+ 라벨 추가

만들기 취소

5) 키 순환주기를 적용하여 키 생성 완료 확인



진단
기준

양호기준

: "고객 관리 키" 사용 시 키에 대한 순환 주기 설정이 되어 있을 경우

취약기준

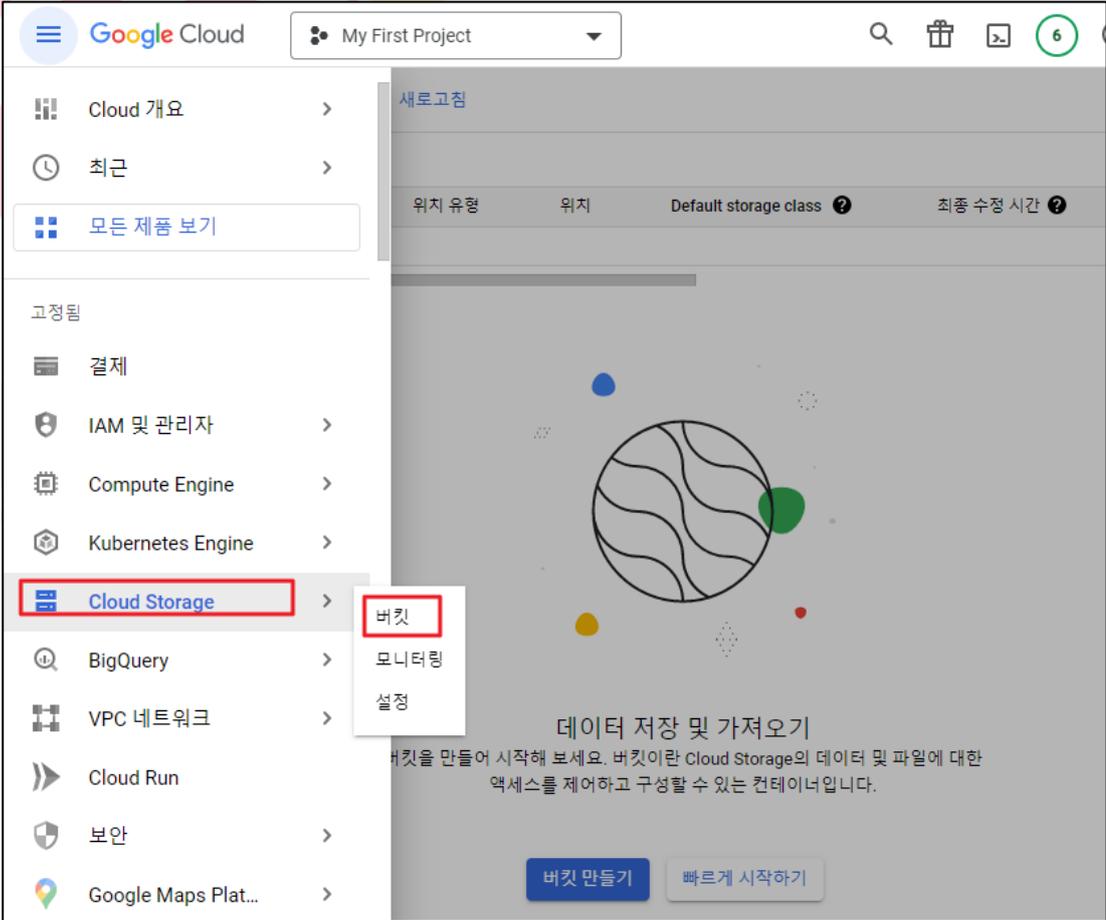
: "고객 관리 키" 사용 시 키에 대한 순환 주기 설정이 되어있지 않을 경우

비고

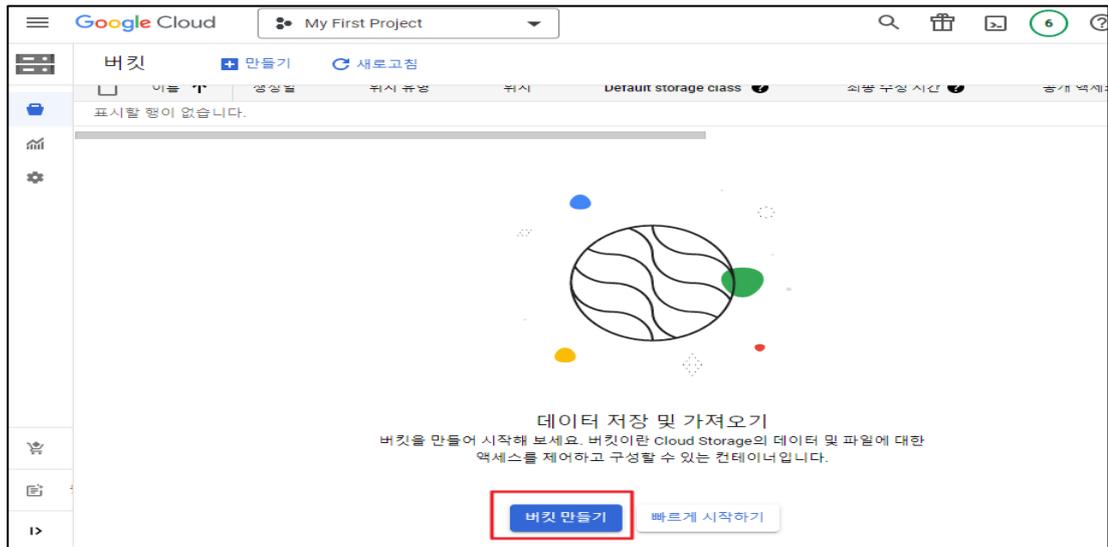


안녕을 지키는 기술

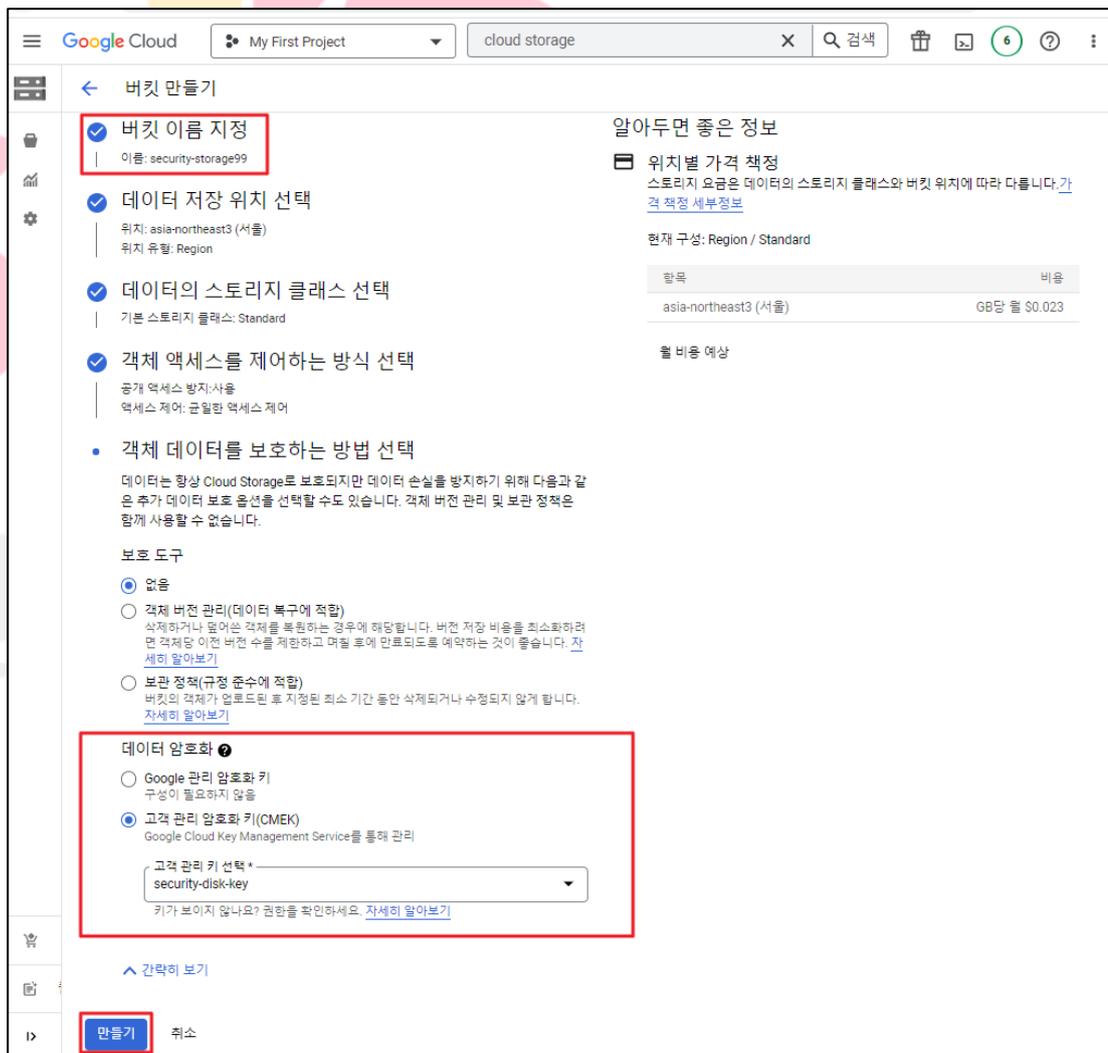
4.4 Storage 암호화 설정

분류	운영 관리	중요도	중						
항목명	Cloud Storage 암호화 설정								
항목 설명	<p>기본적으로 Cloud Storage는 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.</p> <p>"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.</p> <p>(*) 사용 가능한 암호화 키 종류</p> <table border="1" data-bbox="280 721 1423 911"> <thead> <tr> <th>구분</th> <th>내용</th> </tr> </thead> <tbody> <tr> <td>Google 관리 키</td> <td>Google에서 제공하는 자체 암호화 키를 이용하여 데이터 암호/복호화</td> </tr> <tr> <td>고객 관리 키</td> <td>CKMS(Cloud Key Management Service)를 이용하여 암호화 키 관리 및 데이터 암호/복호화</td> </tr> </tbody> </table>			구분	내용	Google 관리 키	Google에서 제공하는 자체 암호화 키를 이용하여 데이터 암호/복호화	고객 관리 키	CKMS(Cloud Key Management Service)를 이용하여 암호화 키 관리 및 데이터 암호/복호화
구분	내용								
Google 관리 키	Google에서 제공하는 자체 암호화 키를 이용하여 데이터 암호/복호화								
고객 관리 키	CKMS(Cloud Key Management Service)를 이용하여 암호화 키 관리 및 데이터 암호/복호화								
설정 방법	<p>가. Cloud Storage 암호화 설정</p> <p>1) [관리 콘솔] > [Cloud Storage] > [버킷]</p>  <p>The screenshot shows the Google Cloud console interface. On the left, a navigation menu is open, with 'Cloud Storage' highlighted in a red box. A sub-menu is visible, with '버킷' (Bucket) also highlighted in a red box. The main content area shows the '새로고침' (Refresh) button and a table with columns for '위치 유형', '위치', 'Default storage class', and '최종 수정 시간'. Below the table, there is a large graphic of a globe and text in Korean: '데이터 저장 및 가져오기' (Data storage and retrieval), '버킷을 만들어 시작해 보세요. 버킷이란 Cloud Storage의 데이터 및 파일에 대한 액세스를 제어하고 구성할 수 있는 컨테이너입니다.' (Try creating a bucket. A bucket is a container for data and files in Cloud Storage that you can control access to and configure.) At the bottom, there are two buttons: '버킷 만들기' (Create bucket) and '빠르게 시작하기' (Get started quickly).</p>								

2) 버킷 생성



3) 버킷 정보 입력 및 암호화 방식 설정



4) 버킷 생성 완료 및 암호화 적용 확인

The screenshot shows the Google Cloud Console interface for a bucket named 'security-storage99'. The bucket is located in the 'asia-northeast3 (서울)' region with a 'Standard' storage class. The 'Encryption' section is highlighted with a red box, showing '암호화 유형' (Encryption type) set to 'Customer-managed key' and '기본 암호화 키' (Default encryption key) set to 'key-utility-367900/asia-northeast3/disk-enc-key/security-disk-key'.

위치	스토리지 클래스	공개 액세스	보호
asia-northeast3 (서울)	Standard	공개 아님	없음

객체 구성 권한 보호 수명 주기

개요

- 생성 시간: 2022년 11월 9일 AM 10시 40분 25초 GMT+9
- 업데이트 시간: 2022년 11월 9일 AM 10시 40분 25초 GMT+9
- 위치 유형: Region
- 위치: asia-northeast3 (서울)
- 복제: -
- 기본 저장소 클래스: Standard
- 요청자 지름: 사용 안함
- 태그: 없음
- 라벨: 없음
- Cloud Console URL: [Redacted]
- gsutil URI: [Redacted]

권한

- 액세스 제어: 균일한 액세스 제어
- 공개 액세스 방지: 버킷 설정을 통해 사용 설정됨
- 공개 액세스 상태: 공개 아님

보호

- 객체 버전 관리: 사용 안함
- 보관 정책: 없음
- 암호화 유형: Customer-managed key
- 기본 암호화 키: key-utility-367900/asia-northeast3/disk-enc-key/security-disk-key

나. 암호화키 생성 및 순환주기 설정

1) [메인] > [보안] > [Key Management]

The screenshot shows the Google Cloud Console navigation menu. The '보안' (Security) menu item is highlighted with a red box, and the 'Key Management' option is also highlighted with a red box in the dropdown menu.

- Cloud 개요 >
- 최근 >
- 모든 제품 보기
- 고정됨
- 결제
- IAM 및 관리자 >
- Compute Engine >
- Kubernetes Engine >
- Cloud Storage >
- BigQuery >
- VPC 네트워크 >
- Cloud Run >
- 보안 >

- Security Command Center
- reCAPTCHA Enterprise
- BeyondCorp Enterprise
- BeyondCorp Enterprise 정책 문제 해결 도구
- IAP (Identity-Aware Proxy)
- Access Context Manager
- VPC 서비스 제어
- Binary Authorization
- 데이터 손실 방지
- Key Management
- Certificate Authority Service
- Secret Manager
- Risk Manager
- Web Security Scanner
- Chronicle
- 액세스 승인
- 관리형 Microsoft AD
- Advisory Notifications

2) 키 생성을 위한 키링 만들기

Google Cloud My First Project kms

키 관리 **+ 키링 만들기** 태그

키링 키 인벤토리

Cloud KMS(Cloud Key Management Service)를 사용하면 암호화 키를 생성, 사용, 순환, 관리할 수 있습니다. 암호화 키는 데이터 암호화 및 복호화나 디지털 서명 생성 및 확인에 사용되는 리소스입니다. 키로 데이터 작업을 하려면 Cloud KMS API를 사용하세요. [자세히 알아보기](#)

필터 속성 이름 또는 값 입력

<input type="checkbox"/>	이름 ? ↑	위치	키 ?	태그	작업
				-	⋮

선택한 키링 없음

3) 키링 이름 및 리전 선택 후 만들기

Google Cloud My First Project kms X 검색

← 키링 만들기

키링은 여러 키를 하나로 모아서 정리합니다. 다음 단계에서 키링에 속한 키를 만듭니다. [자세히 알아보기](#)

프로젝트 이름
My First Project

키링 이름 *
disk-enc-key

위치 유형 ?

- 리전
단일 리전 내에서 짧은 지연 시간
- 멀티 리전
특별한 지역에서 가장 높은 가용성

리전 *
asia-northeast3 (서울)

만들기 취소

4) 키 순환 주기 설정 및 키 만들기

암호화 키는 데이터 암호화 및 복호화나 디지털 서명 생성 및 확인에 사용되는 리소스입니다. 키에 여러 버전이 있을 수 있습니다. [자세히 알아보기](#)

프로젝트 이름 키링 위치 ?

어떤 유형의 키를 만드시겠어요?

- 생성된 키
일반 고객이 관리하는 암호화 키입니다. 키 자료가 자동으로 생성됩니다. [자세히 알아보기](#)
- 가져온 키
GCP에 키 자료를 가져오려는 경우 선택합니다. [자세히 알아보기](#)
- 외부 관리 키
키 자료는 외부 키 관리자에 저장됩니다. [자세히 알아보기](#)

키 이름*
security-disk-key

보호 수준
소프트웨어

용도
대칭 암호화/복호화

알고리즘
Google 대칭 키 키

키 순환 기간
30일

시작일
22. 12. 9.

순환 요약: 2022년 12월 9일부터 30일마다

설정(선택사항)

라벨 ?
[+ 라벨 추가](#)

만들기 취소

5) 키 순환주기를 적용하여 키 생성 완료 확인

키링 세부정보 + 키 만들기 + 가져오기 작업 만들기 새로고침

키 가져오기 작업

'disk-enc-key' 키링의 키

암호화 키는 데이터 암호화 및 복호화나 디지털 서명 생성 및 확인에 사용되는 리소스입니다. 키로 데이터 작업을 하려면 Cloud KMS API를 사용하세요. [자세히 알아보기](#)

필터 속성 이름 또는 값 입력

<input checked="" type="checkbox"/>	이름 ↑	상태 ?	보호 수준 ?	용도 ?	다음 순환 ?	작업
<input checked="" type="checkbox"/>	security-disk-key	사용 가능	소프트웨어	대칭 암호화/복호화	2022. 12. 9.	⋮

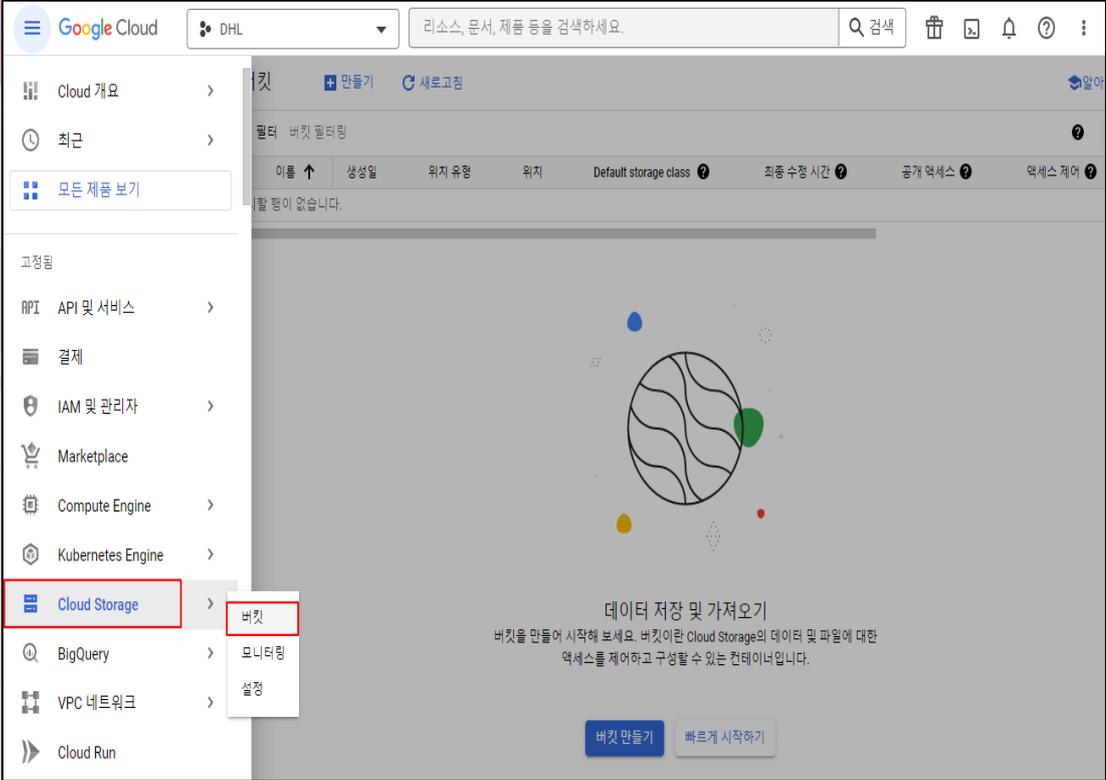
선택한 키 1개

진단 기준	<p>양호기준 : “고객 관리 키” 사용 시 키에 대한 순환 주기 설정이 되어 있을 경우</p> <p>취약기준 : “고객 관리 키” 사용 시 키에 대한 순환 주기 설정이 되어있지 않을 경우</p>
비고	

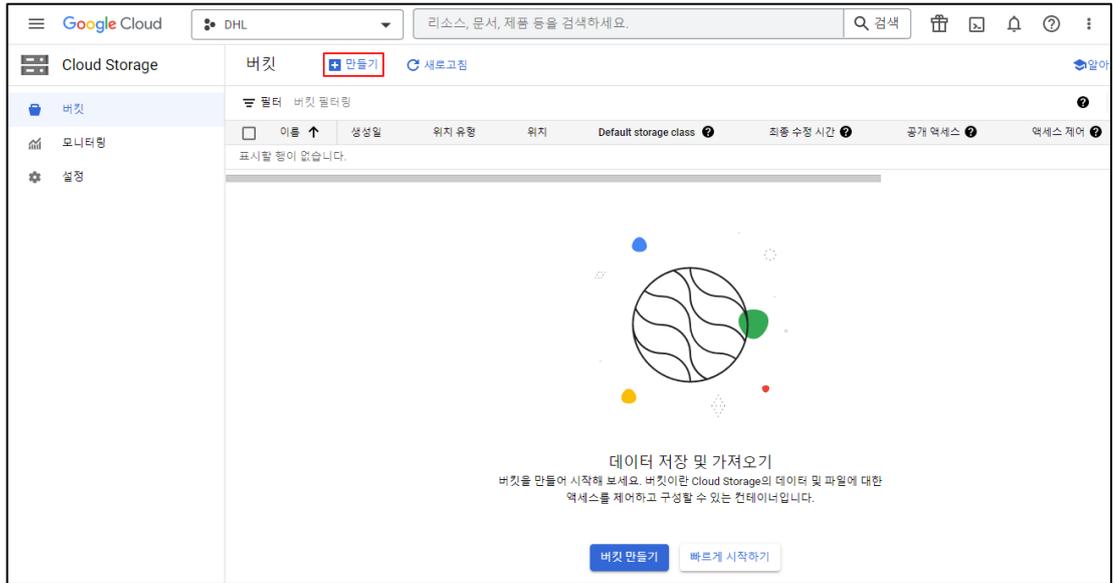


안녕을 지키는 기술

4.5 Storage 데이터 보존 정책 관리

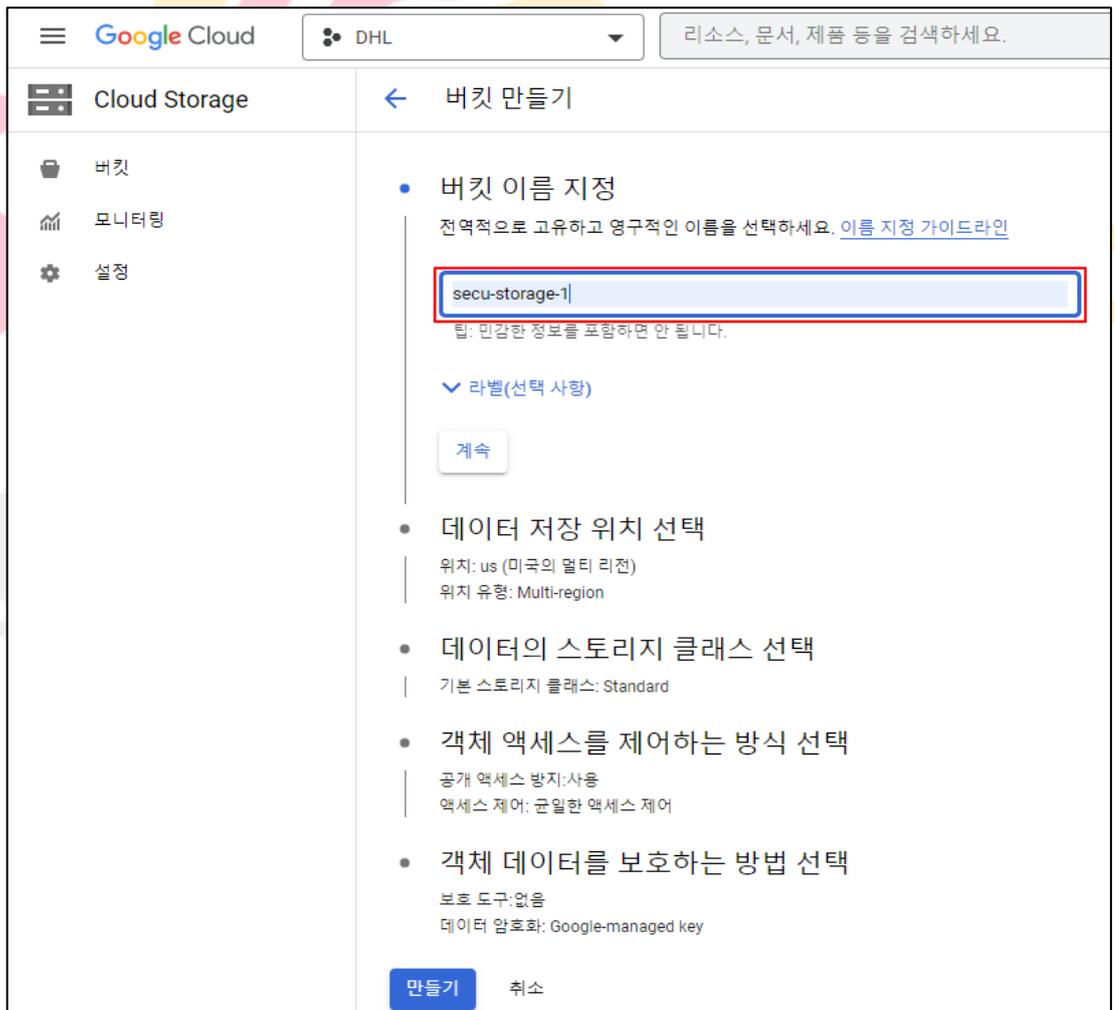
분류	운영 관리	중요도	중
항목명	Storage 데이터 보존 정책 관리		
항목 설명	<p>Cloud Storage를 사용하면 데이터 양에 관계없이 언제 어디서나 데이터를 저장하고 가져올 수 있습니다. Cloud Storage를 통해 웹사이트 콘텐츠를 제공하거나, 보관 및 재해 복구를 위해 데이터를 저장하거나, 직접 다운로드를 통해 사용자에게 대량의 데이터 객체를 배포하는 등 다양한 용도로 사용할 수 있으며 Storage 내 보관 정책을 설정하여 이 버킷의 객체가 업로드 된 후 삭제되거나 수정되지 않도록 보호해야 하는 최소 기간을 지정합니다.</p> <p>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 보호해야 합니다.</p> <p>"고객 관리 키"를 사용하는 경우 키에 대한 순환 주기 설정을 통해 키 유출 및 사용자 접근에 대한 보안 위협을 미연에 방지할 수 있습니다.</p> <p>※ 일정 기간을 정해두고 필수로 보관해야 하는 자료(계약서, 개인정보 등)는 장기간 보관을 고려해야 합니다.</p>		
설정 방법	<p>가. Storage 데이터 보존 정책 설정</p> <p>1) [관리 콘솔] > [Storage] > [버킷]</p>  <p>The screenshot shows the Google Cloud console interface. On the left, the navigation menu is open, and 'Cloud Storage' is selected. A sub-menu is visible with '버킷' (Bucket) highlighted. The main content area shows a '버킷' (Bucket) page with a search bar and a '버킷 만들기' (Create bucket) button. Below the search bar, there are tabs for '이름', '생성일', '위치 유형', '위치', 'Default storage class', '최종 수정 시간', '공개 액세스', and '액세스 제어'. The main content area is currently empty, displaying a large globe icon and the text '데이터 저장 및 가져오기' (Store and retrieve data).</p>		

2) 버킷 생성



The screenshot shows the Google Cloud Storage 'Create Bucket' page. The '버킷 만들기' (Create Bucket) button is highlighted with a red box. The page title is '버킷' (Bucket). Below the title, there are tabs for '버킷 만들기' (Create Bucket) and '새로고침' (Refresh). The main content area displays a large graphic with a globe and the text '데이터 저장 및 가져오기' (Data storage and retrieval). Below the graphic, there is a sub-header '데이터 저장 및 가져오기' and a paragraph: '버킷을 만들어 시작해 보세요. 버킷이란 Cloud Storage의 데이터 및 파일에 대한 액세스를 제어하고 구성할 수 있는 컨테이너입니다.' (Try creating a bucket. A bucket is a container that you can use to control and configure access to data and files in Cloud Storage.) At the bottom, there are two buttons: '버킷 만들기' (Create Bucket) and '빠르게 시작하기' (Get started quickly).

3) 버킷 정보 입력



The screenshot shows the Google Cloud Storage 'Create Bucket' configuration page. The page title is '버킷 만들기' (Create Bucket). The main content area is divided into several sections:

- 버킷 이름 지정** (Bucket naming): A text input field contains 'secu-storage-1', which is highlighted with a red box. Below the field, there is a tip: '팁: 민감한 정보를 포함하면 안 됩니다.' (Tip: Do not include sensitive information.)
- 라벨(선택 사항)** (Labels (optional)): A section with a dropdown arrow and the text '라벨(선택 사항)'.
- 데이터 저장 위치 선택** (Data storage location selection): A section with a dropdown arrow and the text '데이터 저장 위치 선택'. Below it, the location is set to 'us (미국의 멀티 리전)' and the location type is 'Multi-region'.
- 데이터의 스토리지 클래스 선택** (Storage class selection): A section with a dropdown arrow and the text '데이터의 스토리지 클래스 선택'. Below it, the storage class is set to '기본 스토리지 클래스: Standard'.
- 객체 액세스를 제어하는 방식 선택** (Access control selection): A section with a dropdown arrow and the text '객체 액세스를 제어하는 방식 선택'. Below it, the access control is set to '공개 액세스 방식: 사용' and '액세스 제어: 균일한 액세스 제어'.
- 객체 데이터를 보호하는 방법 선택** (Data protection selection): A section with a dropdown arrow and the text '객체 데이터를 보호하는 방법 선택'. Below it, the protection is set to '보호 도구: 없음' and '데이터 암호화: Google-managed key'.

At the bottom, there are two buttons: '만들기' (Create) and '취소' (Cancel).

4) 데이터 저장 위치 선택

Google Cloud | DHL | 리소스, 문서, 제품 등을 검색하세요.

Cloud Storage | 버킷 만들기

- 버킷 이름 지정 | 이름: secu-storage-1
- 데이터 저장 위치 선택**

선택은 영구적으로 적용되며, 데이터의 지리적 위치가 정의되고 비용, 성능, 가용성이 영향을 받습니다. [자세히 알아보기](#)

위치 유형

 - Multi-region**
폭넓은 지역에서 가장 높은 가용성
 - Dual-region
리전 2곳에서 고가용성 및 짧은 지연 시간
 - Region
단일 리전 내에서 가장 짧은 지연 시간

asia (아시아의 멀티 리전)
- 데이터의 스토리지 클래스 선택 | 기본 스토리지 클래스: Standard
- 객체 액세스를 제어하는 방식 선택 | 공개 액세스 방식: 사용 | 액세스 제어: 균일한 액세스 제어
- 객체 데이터를 보호하는 방법 선택 | 보호 도구: 없음 | 데이터 암호화: Google-managed key

Marketplace | 출시 노트

만들기 | 취소

5) 기본 스토리지 클래스 선택

Google Cloud | DHL | 리소스, 문서, 제품 등을 검색하세요.

Cloud Storage | 버킷 만들기

- 버킷 이름 지정 | 이름: secu-storage-1
- 데이터 저장 위치 선택 | 위치: asia (아시아의 멀티 리전) | 위치 유형: Multi-region
- 데이터의 스토리지 클래스 선택**

스토리지 클래스는 업타임의 차이를 최소화하면서 스토리지, 가져오기, 작업 비용을 설정합니다. 객체를 자동으로 관리할지 선택하거나, 데이터와 워크로드를 저장할 기간이나 사용 사례를 기준으로 기본 스토리지 클래스를 지정하세요. [Learn more](#)

 - Autoclass

객체 수준 활동에 따라 각 객체를 사용자가 높거나 낮은 스토리지로 자동 전환하여 비용 및 지연 시간에 맞게 최적화합니다. 사용 빈도를 예측할 수 없는 경우에 권장됩니다. 언제든지 기본 클래스로 변경할 수 있습니다. [가격 책정 세부정보](#)
 - 기본 클래스 설정**

객체별 클래스를 수동으로 수정하거나 객체 수명 주기 규칙을 설정하지 않는 한 버킷의 모든 객체에 적용됩니다. 사용량을 잘 예측할 수 있는 경우에 가장 적합합니다. 버킷을 만든 후에는 자동 클래스로 변경할 수 없습니다.

 - Standard**

단기 스토리지 및 자주 액세스하는 데이터에 적합
 - Nearline

백업 및 월 1회 미만 액세스하는 데이터에 적합
 - Coldline

재해 복구 및 분기당 1회 미만 액세스하는 데이터에 적합
 - Archive

연 1회 미만 액세스하는 데이터의 디지털 장기 보존에 적합

Marketplace

계속

6) 데이터 보존 정책 설정

The screenshot shows the 'Bucket creation' page in Google Cloud Storage. The 'Retention policy' section is highlighted with a red box. It includes the following options:

- 버킷 이름 지정**
이름: secu-storage-1
- 데이터 저장 위치 선택**
위치: asia (아시아의 멀티 리전)
위치 유형: Multi-region
- 데이터의 스토리지 클래스 선택**
기본 스토리지 클래스: Standard
- 객체 액세스를 제어하는 방식 선택**
공개 액세스 방지: 사용
액세스 제어: 균일한 액세스 제어
- 객체 데이터를 보호하는 방법 선택**
데이터는 항상 Cloud Storage로 보호되지만 데이터 손실을 방지하기 위해 다음과 같은 추가 데이터 보호 옵션을 선택할 수도 있습니다. 객체 버전 관리 및 보관 정책은 함께 사용할 수 없습니다.
보호 도구
 - 없음
 - 객체 버전 관리(데이터 복구에 적합)
삭제하거나 덮어쓴 객체를 복원하는 경우에 해당합니다. 버전 저장 비용을 최소화하려면 객체당 이전 버전 수를 제한하고 며칠 후에 만료되도록 예약하는 것이 좋습니다. [자세히 알아보기](#)
 - 보관 정책(규정 준수에 적합)**
버킷의 객체가 업로드된 후 지정된 최소 기간 동안 삭제되거나 수정되지 않게 합니다. [자세히 알아보기](#)

The 'Retention period' field is also highlighted with a red box, showing '1' year.

7) 버킷 생성 완료

The screenshot shows the 'Bucket list' page in Google Cloud Storage. The newly created bucket 'secu-storage-1' is highlighted with a red box. The table below shows the details of the bucket:

이름	생성일	위치 유형	위치	Default storage class	최종 수정 시간
secu-storage-1	2022. 11. 9. AM 9:45:34	Multi-region	asia	Standard	2022. 11. 9. AM 9:45:34

양호기준

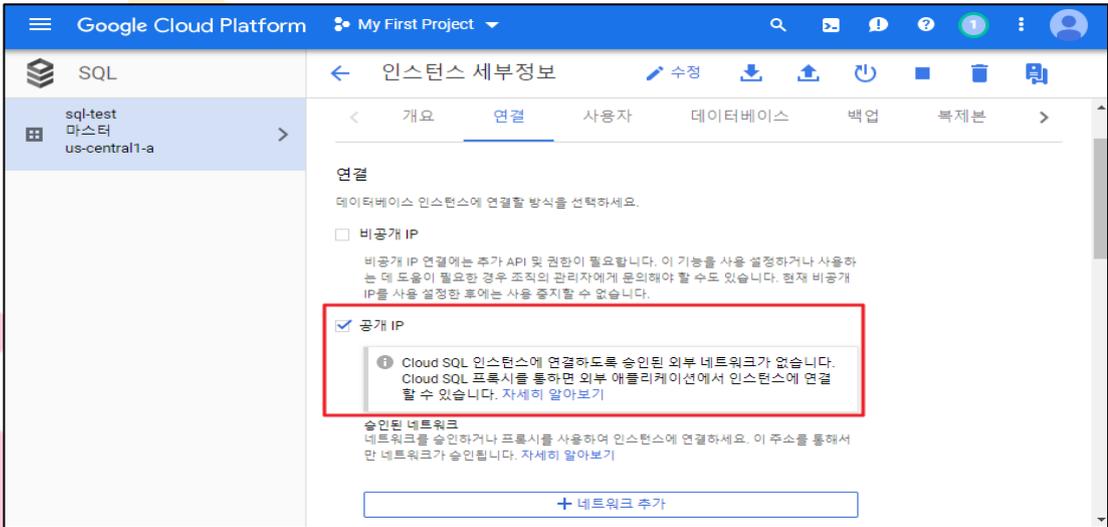
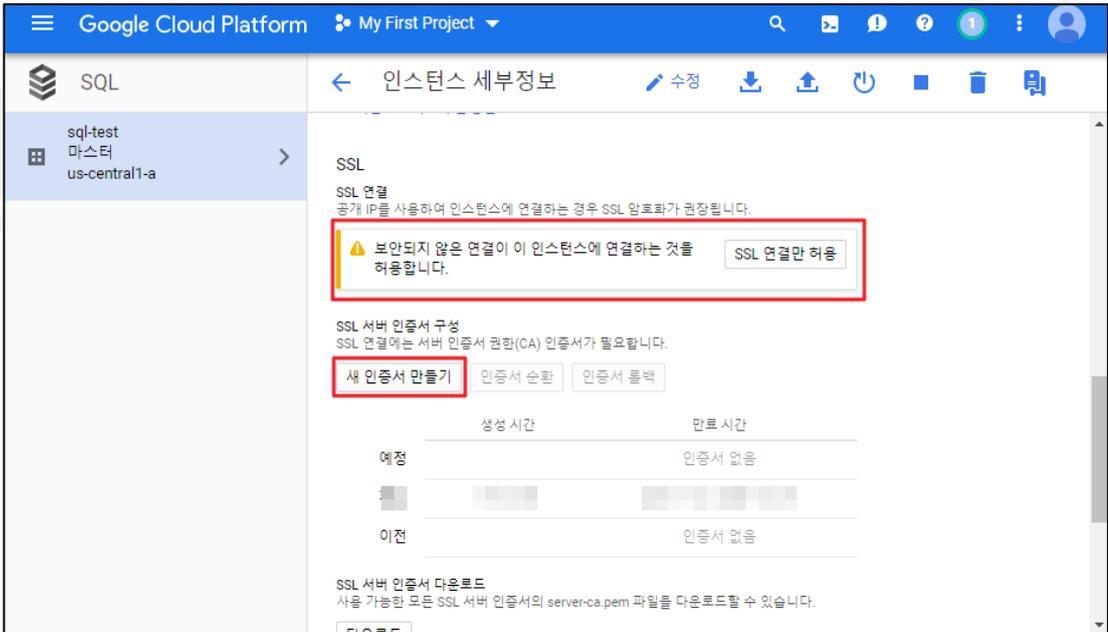
: 장기간 보관해야 하는 객체(데이터)에 보존 정책이 설정되어 있는 경우

취약기준

: 장기간 보관해야 하는 객체(데이터)에 보존 정책이 설정되어 있지 않은 경우

비고

4.6 SQL SSL 정책 관리

분류	운영 관리	중요도	중
항목명	SQL SSL 정책 관리		
항목 설명	<p>Cloud SQL은 GCP(Google Cloud Platform)에서 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.</p>		
설정 방법	<p>가. SQL 접근 시 SSL 설정 방법</p> <p>1) [생성된 인스턴스] > [연결] > 공개 IP/비공개 IP 설정</p>  <p>2) SSL 새 인증서 만들기</p> 		

3) SSL 클라이언트 인증서 구성

Google Cloud Platform My First Project

SQL

sql-test 마스터 us-central1-a

인스턴스 세부정보

예정	인증서 없음
활성	15시간 전 2029. 7. 26. 오후 7:02:17
이전	인증서 없음

SSL 서버 인증서 다운로드
사용 가능한 모든 SSL 서버 인증서의 server-ca.pem 파일을 다운로드할 수 있습니다.

다운로드

SSL 클라이언트 인증서 구성
SSL 인증서는 클라이언트 인증서와 클라이언트 비공개 키로 구성됩니다. 모두 SSL 연결에 필요합니다. 기존 클라이언트 인증서로는 클라이언트 인증서에만 액세스할 수 있습니다. 클라이언트 비공개 키는 인증서 생성 중에만 표시됩니다.

클라이언트 인증서 만들기

SSL 구성 재설정
서버의 SSL 구성을 재설정하면 모든 클라이언트 인증서가 취소되며 새로운 서버 CA 인증서가 생성됩니다.

SSL 구성 재설정

4) 클라이언트 인증서 만들기

Google Cloud Platform My First Project

SQL

sql-test 마스터 us-central1-a

인스턴스 세부정보

클라이언트 인증서 만들기

이름
SSL 인증서의 고유 식별자입니다.

test-cer1

닫기 만들기

5) 생성된 새 SSL 인증서 확인

새 SSL 인증서가 생성됨

이 인증서를 사용하여 연결하려면 아래 파일 3개의 콘텐츠를 가져오세요.

이 대화상자를 닫기 전에 client-key.pem 파일을 다운로드해야 합니다. 대화상자를 닫은 후에는 파일에 액세스할 수 없습니다.

[client-key.pem 다운로드](#)

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAhtkwtLTf48orIDCb0F0Q/Wy0wBcl07zWUj6FPWwWyznlI
wty9gImBdL00/AN6J3K/PFvRkJKTU+RohHA7fMdz8lq1EY/2z8XS42xLE664iBk
-----END RSA PRIVATE KEY-----
```

[client-cert.pem 다운로드](#)

```
-----BEGIN CERTIFICATE-----
MIIDTCCAKGqAwIBAgIEds37LDANBgkqhkiG9w0BAQsFAADCBgTELMAUUElMhk
ODU5MDZjZGQ1ZDAwMCOON6UzLWlWMDU1NGQ1YjJlMTdkNmVhNS0wKwY0QDEyRj
-----END CERTIFICATE-----
```

[server-ca.pem 다운로드](#)

```
-----BEGIN CERTIFICATE-----
MIIDfzCCAmegAwIBAgIBADANBgkqhkiG9w0BAQsFADE3MS0wKiwVODQLEyQ5YmU2
YmI4MCIhNzc1LTQyYmQ1OTY4MjI0OSNkz0TBjNjBmRkTgx1ZANBgkqhkiG9w0BAQ
-----END CERTIFICATE-----
```

인증서를 다운로드하면 다음 명령어를 사용하여 인스턴스에 연결할 수 있습니다.

```
$ mysql -uroot -p 'h 35-226-18-227 \
--ssl-ca=server-ca.pem --ssl-cert=client-cert.pem \
--ssl-key=client-key.pem
```

MySQL에서의 SSL 암호화에 대한 자세한 내용은 MySQL 문서를 참조하세요.

⚠ 대화상자를 닫으려면 client-key.pem 파일을 다운로드해야 합니다.

6) 'SSL 연결만 허용' 설정

인스턴스 세부정보

SSL

SSL 연결
공개 IP를 사용하여 인스턴스에 연결하는 경우 SSL 암호화가 권장됩니다.

⚠ 보안되지 않은 연결이 이 인스턴스에 연결하는 것을 허용합니다. [SSL 연결만 허용](#)

SSL 서버 인증서 구성
SSL 연결에는 서버 인증서 권한(CA) 인증서가 필요합니다.

[새 인증서 만들기](#) [인증서 순환](#) [인증서 롤백](#)

7) 웹 서비스 로그인 시도

WordPress

사용자명 또는 이메일 주소

AdiosL

암호

기억하기

[로그인](#)

8) 암호화된 SQL 쿼리 확인

Index	Protocol	Local Address	Remote Address	Local Port	Remote Port	Local Host	Remote Host	Service Name	Packets	Data
4	TCP	10.174.0.3	218.233.105.169	80	57095	gcpvmdiosl.asia...	gcpvmdiosl.asia...	http	12	3.1.4
5	TCP	10.174.0.3	249.24.100.11	49429	3306	gcpvmdiosl.asia...	111.170.97.34.bc...		47	1.0
5	TCP	10.174.0.3	34.97.170.111	49430	3306	gcpvmdiosl.asia...	111.170.97.34.bc...		105	30.0


```

00000000 0E 00 70 59 72 20 74 10 DF 63 E6 F3 00 E5 00 52 --(WrC...C...R
00000004 FE 4F E7 91 0A 19 20 0C 0D 37 09 14 00 EC 00 00 --.---(- -Y...H...
00000008 00 3E C0 13 C0 09 C0 14 C0 00 00 33 00 38 00 39 -->---...-3-8-9
0000000C 00 32 00 31 00 30 C0 0E C0 0A 00 2F 00 37 00 36 --2-1-0--.../Z-6
00000010 C0 0F C0 05 00 35 00 00 00 07 00 06 00 05 00 01 --...5-...-...
00000014 00 00 00 34 00 05 00 0A 00 03 00 02 00 01 00 0F --...E-0 -C-B-0--
00000018 01 00 00 47 00 00 00 12 00 10 00 00 00 33 34 2E --.G...-...-34.
0000001C 39 37 2E 31 37 30 2E 31 31 31 00 00 00 0A 03 00 97-70-1 11-...
00000020 01 02 00 0A 00 1C 00 10 00 17 00 19 00 1C 00 1B --...-...-...-...
00000024 00 18 00 1A 00 16 00 0E 00 0D 00 0B 00 0C 00 09 --...-...-...-...
00000028 00 00 00 23 00 00 00 0E 00 01 01 --...-...-...-...
00000030 16 03 01 00 30 02 00 00 37 03 01 5D 56 19 4F 60 --...-...-7-10-0h
00000034 ED 2F 2F 03 00 20 41 07 09 5E 60 30 07 7C 30 E0 --//...-...-...-...
00000038 51 91 68 F1 7F 70 0D F3 62 36 65 00 C8 13 00 00 00 0...h...-...-6e...-...
0000003C 0F FE 01 00 01 00 00 00 00 02 01 00 00 23 00 00 --...-...-...-...
00000040 16 03 01 03 50 00 00 03 4C 00 03 49 00 03 46 30 --...P...-...-...-...
00000044 02 03 02 30 02 02 20 00 03 02 01 02 02 0A 50 05 --...0...-...-...-...
00000048 03 06 30 00 06 09 20 06 48 06 F7 0D 01 01 00 05 --...-...-...-...
0000004C 00 30 77 31 2D 30 20 06 03 55 0A 2E 13 24 39 35 --003-0-...-...-...
00000050 34 31 04 32 62 31 2D 36 62 36 64 2D 34 31 61 32 4102b1-6 b0d-41a2
00000054 20 38 34 33 31 2D 37 34 69 38 64 31 62 31 36 62 --8031-74 b0d1b10
00000058 32 61 31 23 30 21 06 03 55 0A 03 13 10 47 6F 6F 241007-...-...-...
0000005C 67 6C 65 20 43 6C 6F 75 64 20 53 51 4C 20 53 65 61e Clou d SQL Se
00000060 72 76 65 72 20 43 61 31 14 30 12 06 03 55 0A 00 rver DB1 -...-...
00000064 13 00 47 6F 6F 67 6C 65 2D 20 49 6E 63 31 00 30 --...Google...-...-...
00000068 09 06 00 55 0A 06 13 02 55 53 30 1E 17 00 31 39 --...-...-...-...
0000006C 38 38 31 33 38 35 35 33 35 31 50 17 00 32 39 38 0010053 532-200
    
```

진단 기준

양호기준

: 통신구간 암호화가 필요한 서비스 내 SSL 연결 설정이 존재하는 경우

취약기준

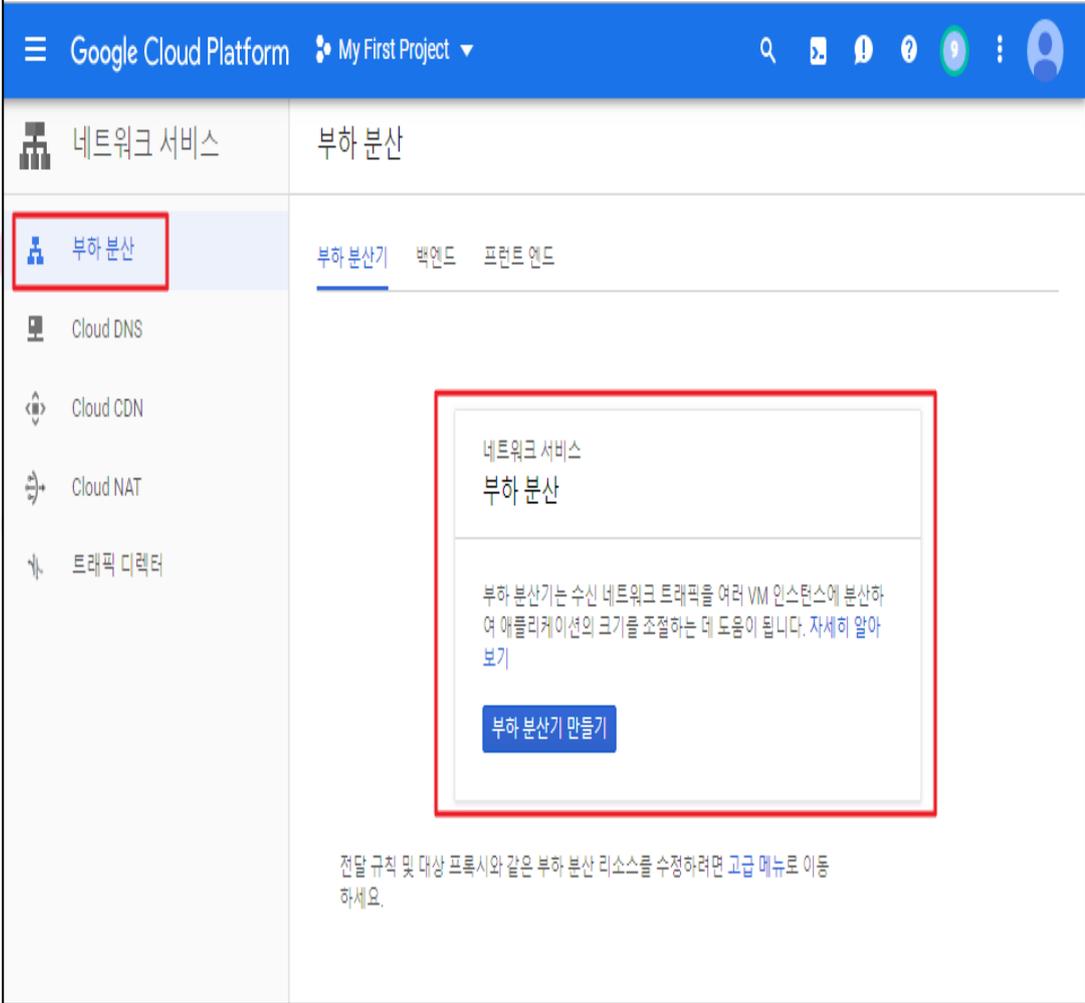
: 통신구간 암호화가 필요한 서비스 내 SSL 연결 설정이 존재하지 않는 경우

비고

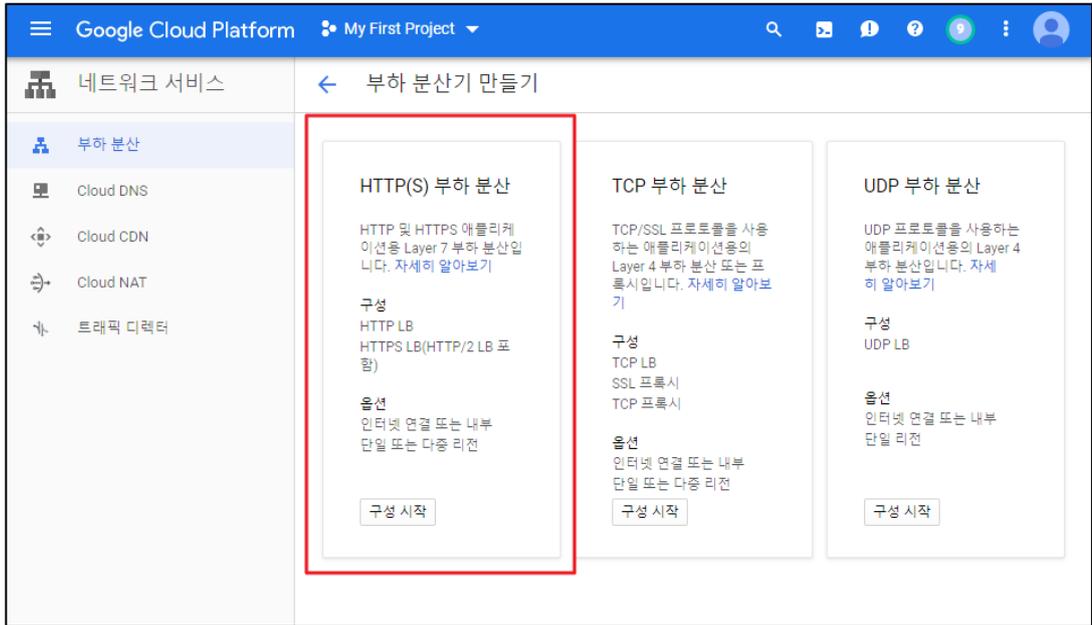


안녕을 지키는 기술

4.7 Load Balancing SSL 정책 관리

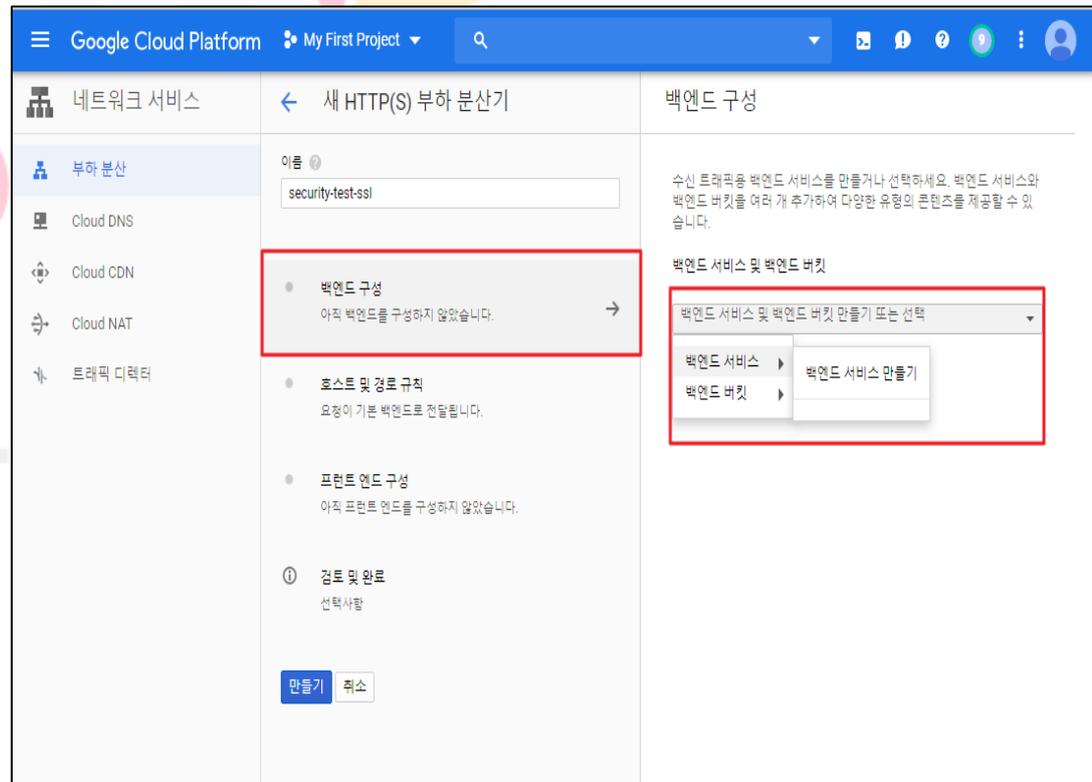
분류	운영 관리	중요도	상
항목명	Load Balancing SSL 정책 관리		
항목 설명	<p>Compute Engine 내 SSL 설정은 부하분산기가 클라이언트와 SSL을 협상하는 방식으로 제어를 하며, SSL/TLS 버전 및 암호화의 세밀한 제어를 위해 정책을 만들고 HTTPS 및 SSL 부하 분산기에 정책을 연결할 수 있습니다.</p> <p>기본적으로 HTTPS 로드 균형 조정과 SSL 프록시로드 균형 조정은 훌륭한 보안 및 광범위한 호환성을 제공하는 SSL 기능 세트를 사용합니다. 일부 응용 프로그램은 HTTPS 또는 SSL 연결에 사용되는 SSL 버전 및 암호를 보다 많이 제어해야 합니다. SSL 정책을 정의하여 로드 밸런서가 클라이언트와 협상하는 SSL 기능을 제어할 수 있습니다.</p>		
설정 방법	<p>가. 구글 관리형 SSL - Compute Engine</p> <p>1) [네트워크 서비스] > [부하 분산] > [부하 분산기 만들기]</p> <p>- Compute Engine 리소스 내 구글 관리형 SSL 인증서 발급 및 확인을 위한 부하 분산기 생성</p>  <p>The screenshot shows the Google Cloud Platform interface. The left sidebar has 'Network Services' selected, and 'Load Balancing' is highlighted in the main content area. A red box highlights the '부하 분산기 만들기' (Create Load Balancer) button. Below the button, there is a note: '전달 규칙 및 대상 프록시와 같은 부하 분산 리소스를 수정하려면 고급 메뉴로 이동하세요.'</p>		

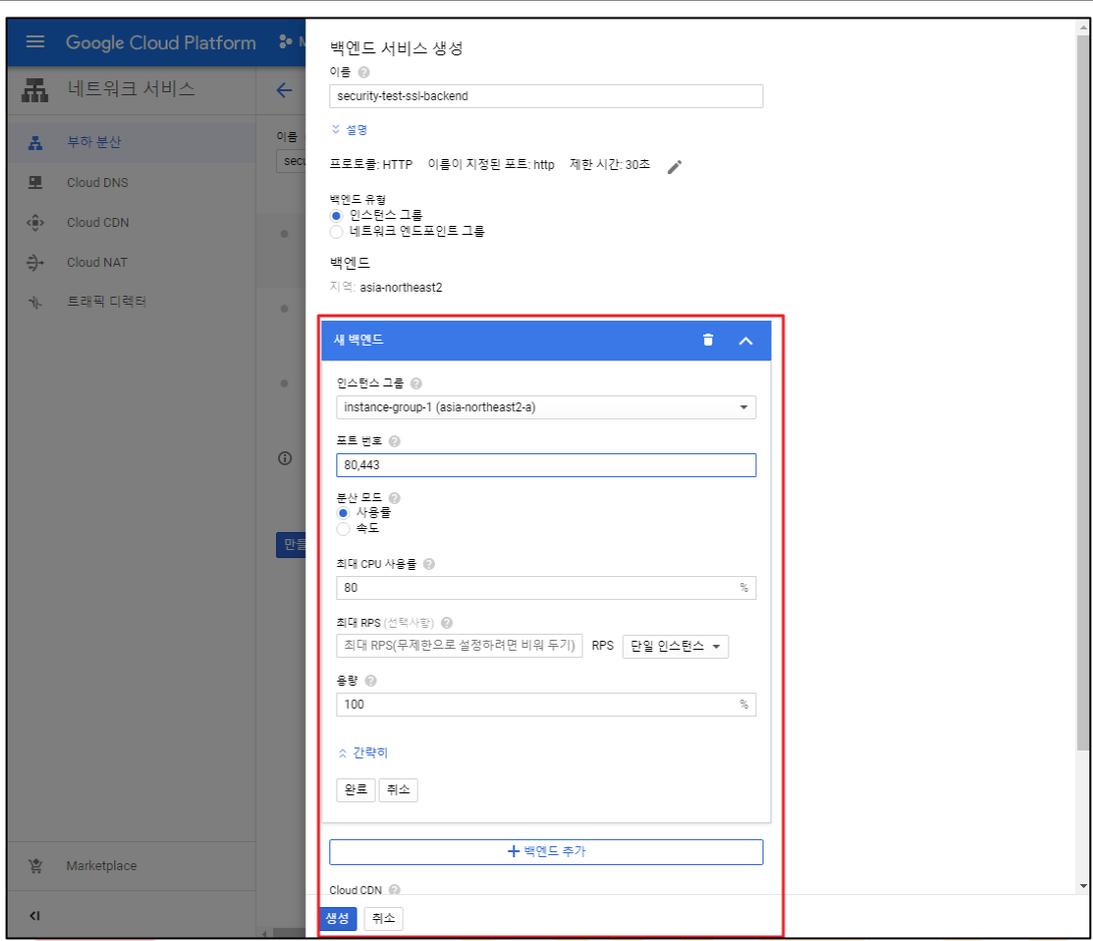
2) HTTP(S) 부하 분산으로 부하 분산기 구성



3) [백엔드 구성]

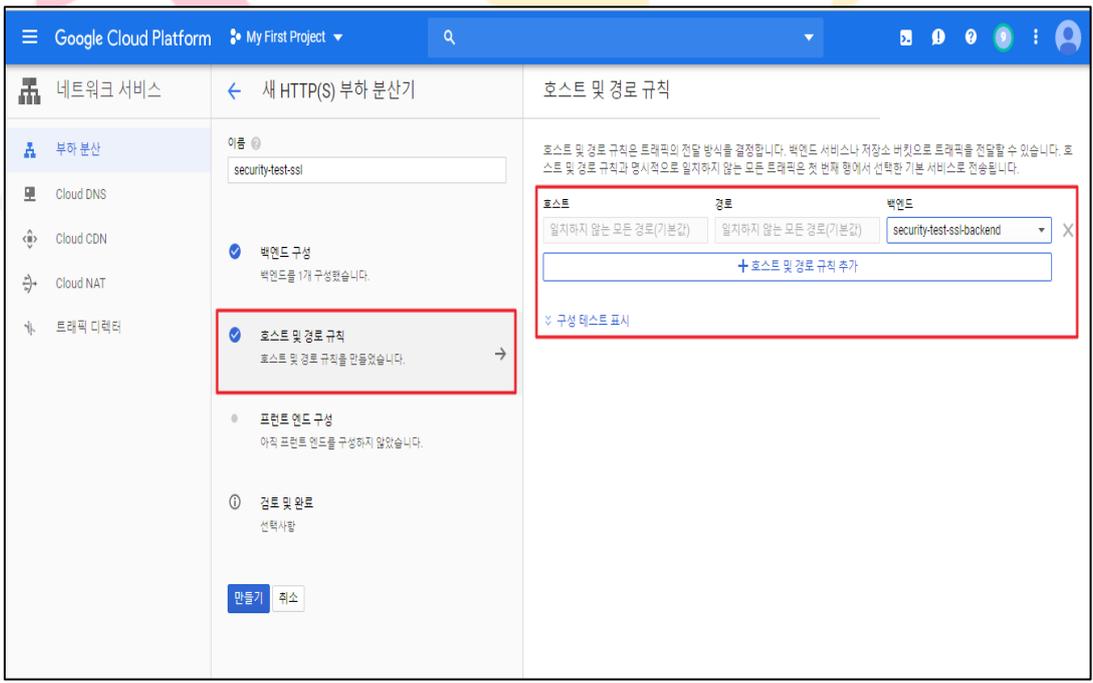
- VM 인스턴스 그룹을 이용해 백엔드 서비스 생성





4) [호스트 경로 및 규칙]

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



5) [프런트엔드 구성]

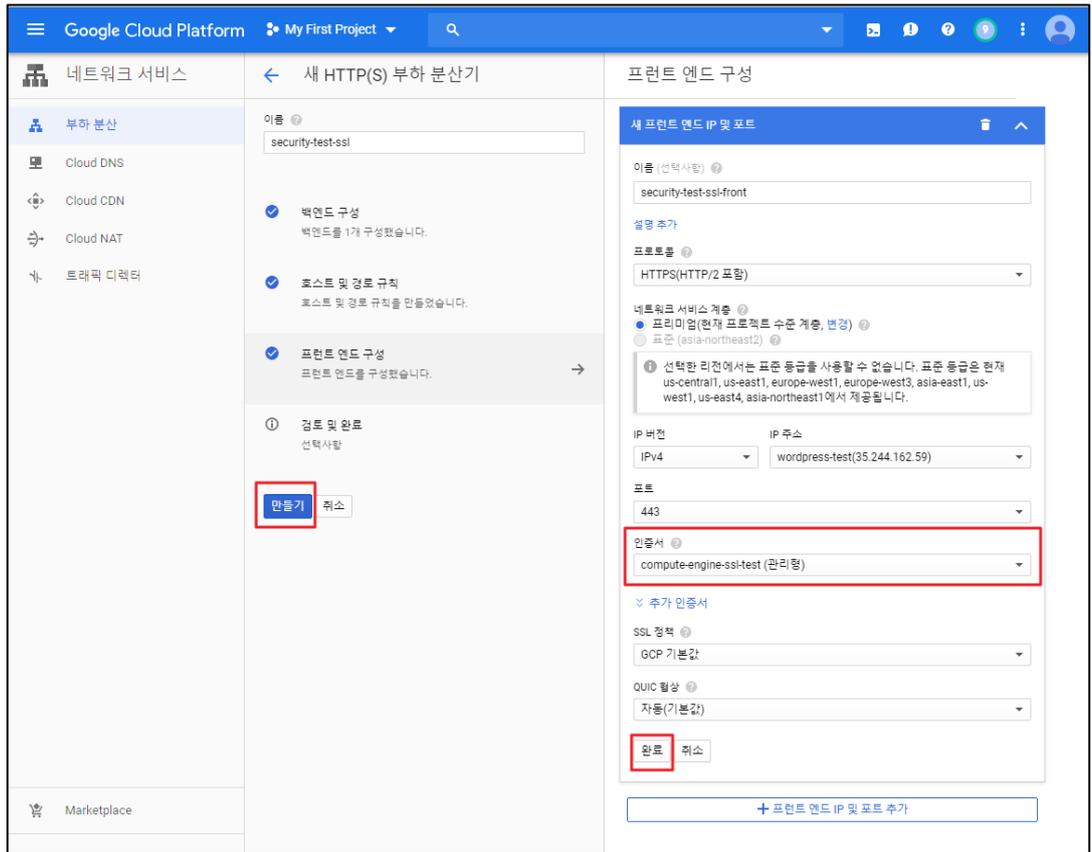
- 부하 분산기 이용을 위한 설정 (IP / 포트 / SSL 인증서)

The screenshot shows the Google Cloud Platform console for a new HTTP(S) load balancer. The 'Frontend configuration' section is highlighted with a red box. The 'New frontend IP and port' dialog is also highlighted with a red box, showing the 'HTTPS(HTTP/2 포함)' protocol, '443' port, and 'New certificate' option selected.

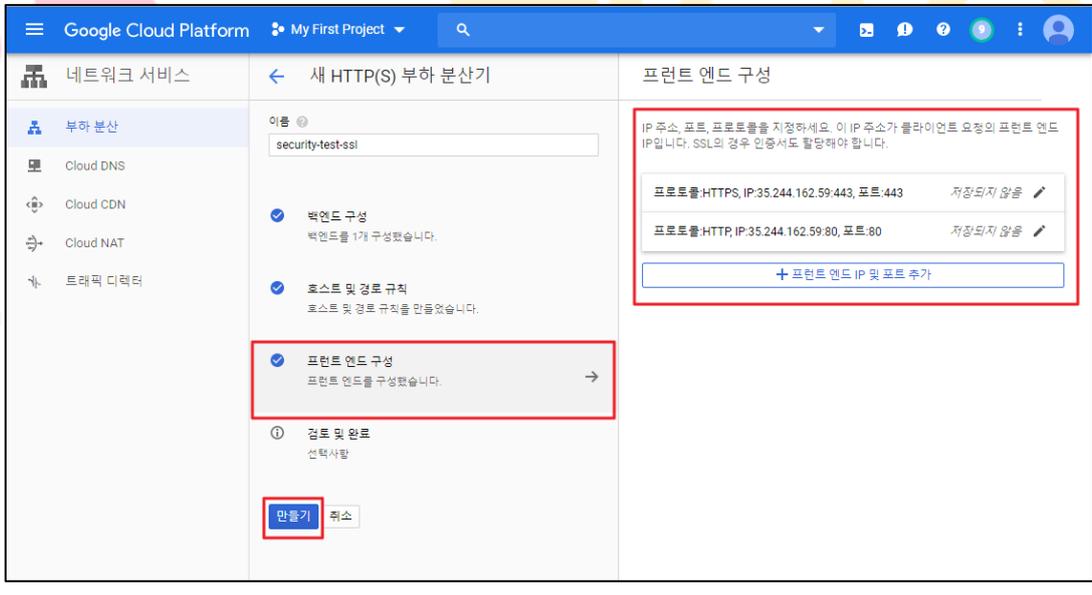
6) [SSL 인증서 생성]

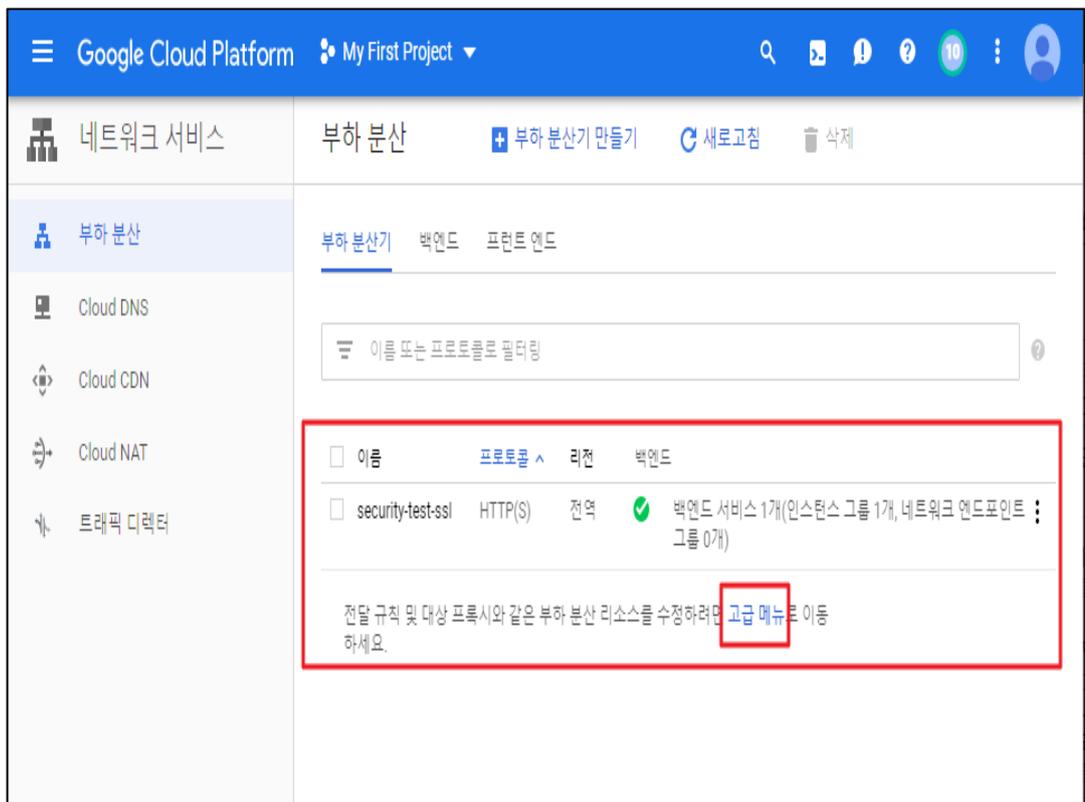
- 구글 관리형 인증서 생성 및 도메인 지정

The screenshot shows the Google Cloud Platform console for creating a new certificate. The 'Google-managed certificate creation' option is selected, and the domain 'tech.junshae.com' is entered. The 'Generate' button is highlighted with a red box.



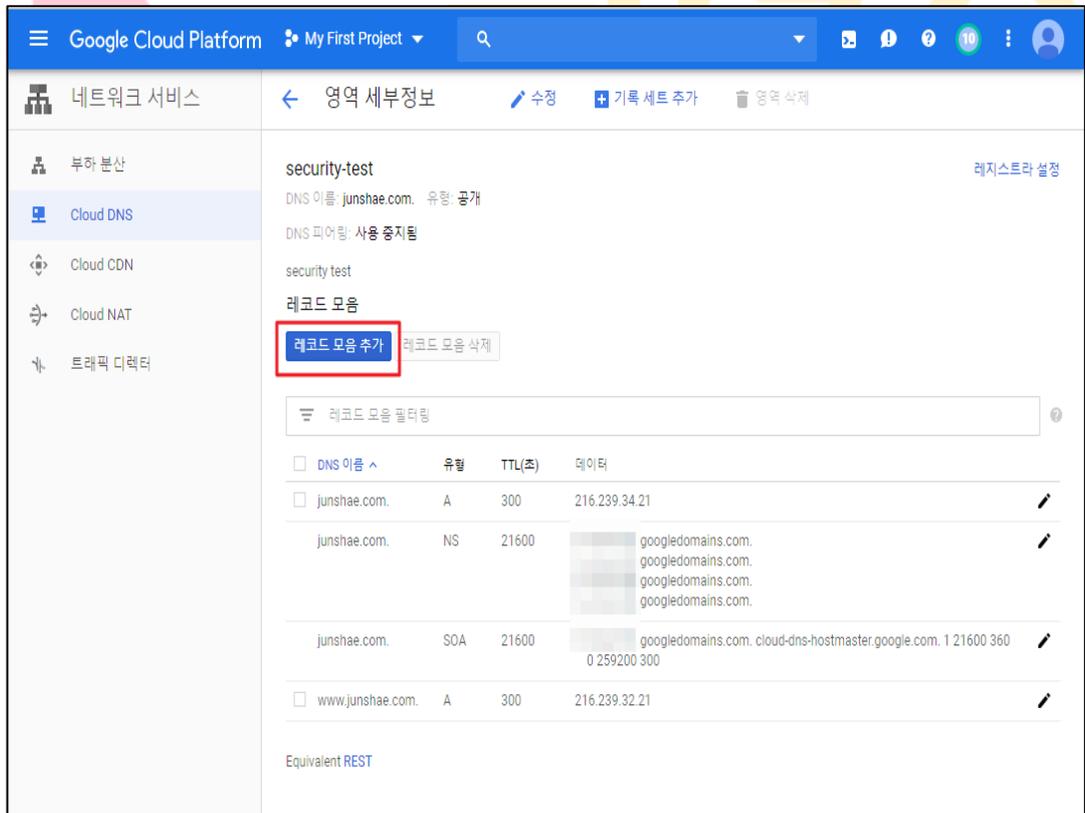
7) 부하 분산기 최종 설정 완료 및 생성





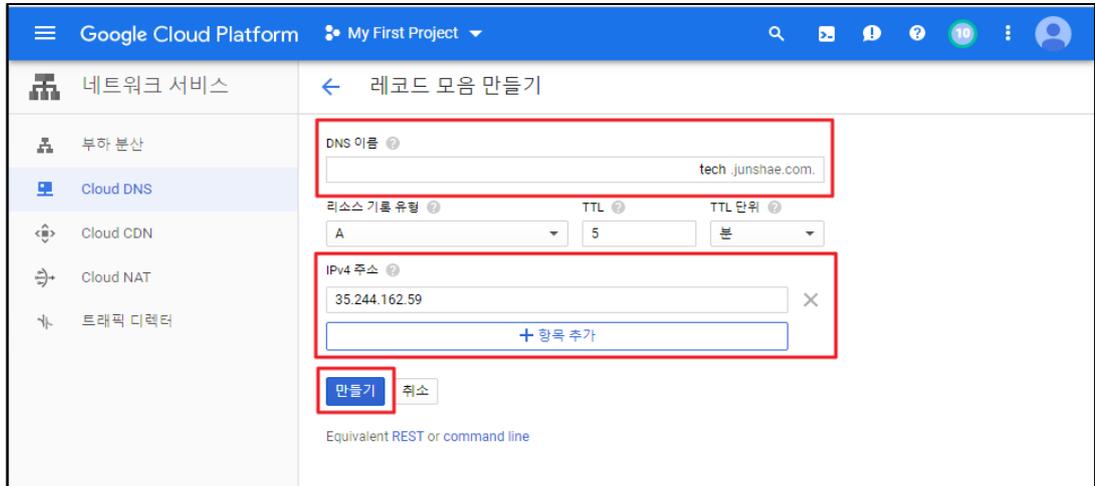
8) [네트워크 서비스] > [Cloud DNS] > [레코드 모음 추가]

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

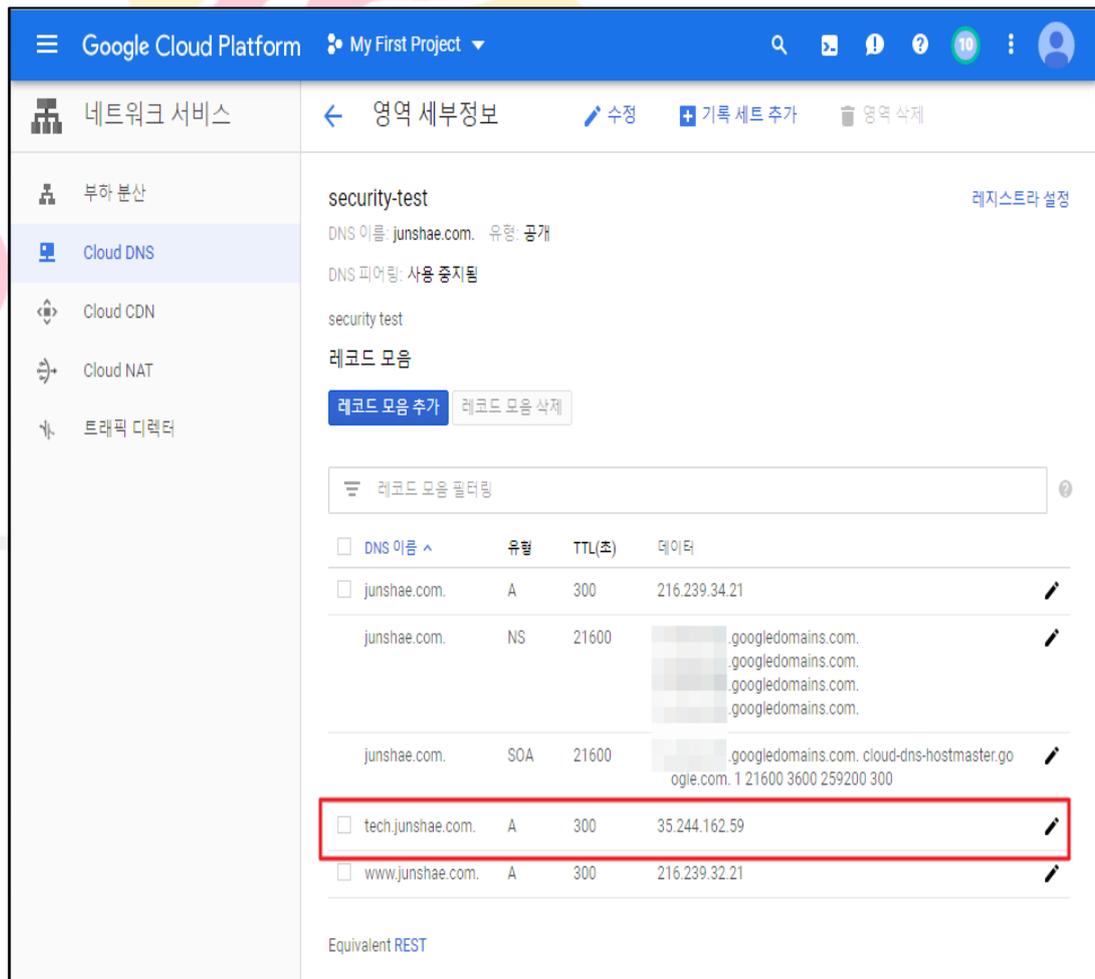


9) 웹서비스 연결에 사용할 도메인 및 IP(부하 분산기 외부 IP) 등록

※ 이때 DNS 이름은 부하 분산기 내 구글 관리형 SSL 인증서 생성 시 등록된 도메인과 동일해야함



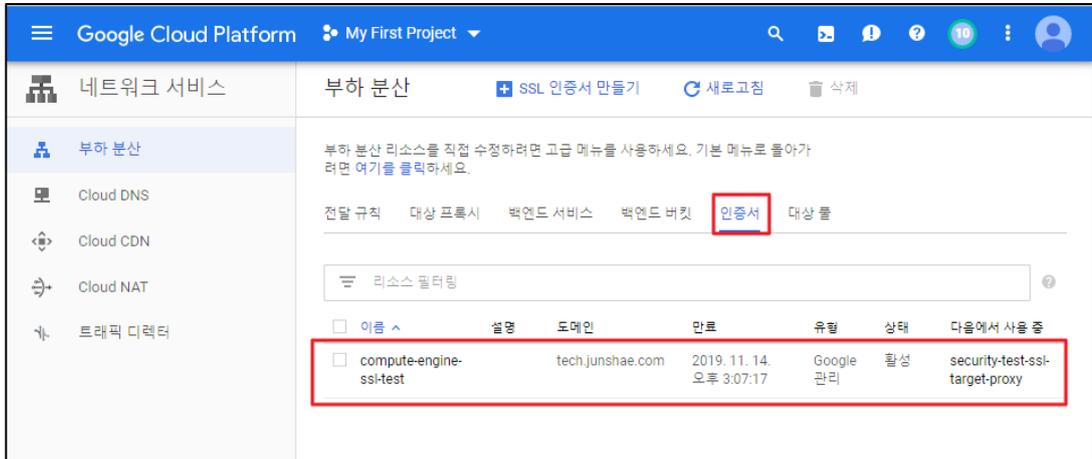
10) 레코드 정상 등록 확인



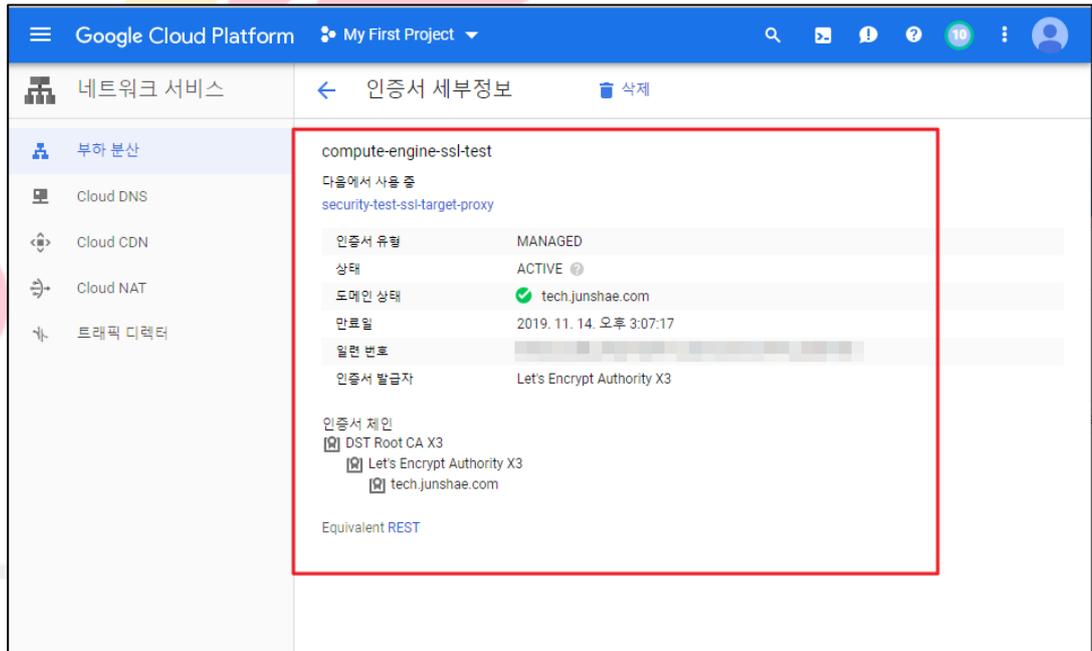
11) [네트워크 서비스] > [부하 분산] > [고급 설정] > [인증서]

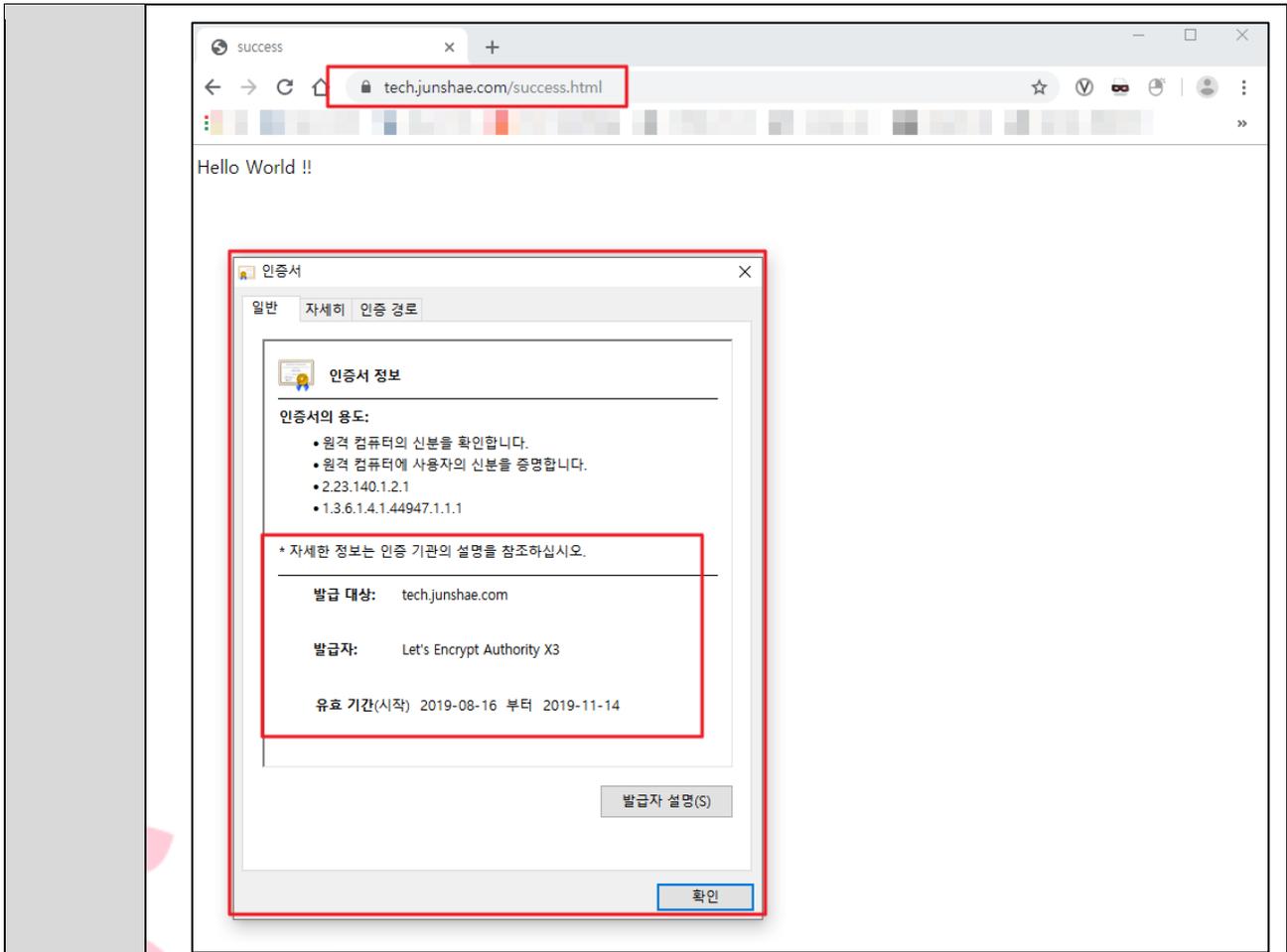
- 부하 분산기를 통한 웹서비스 접근 및 SSL 인증서 등록을 위한 Cloud DNS 설정 (레코드 추가)

※ 등록된 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)

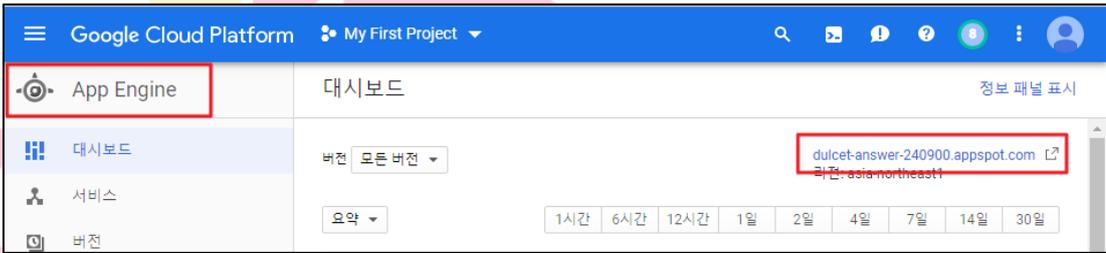




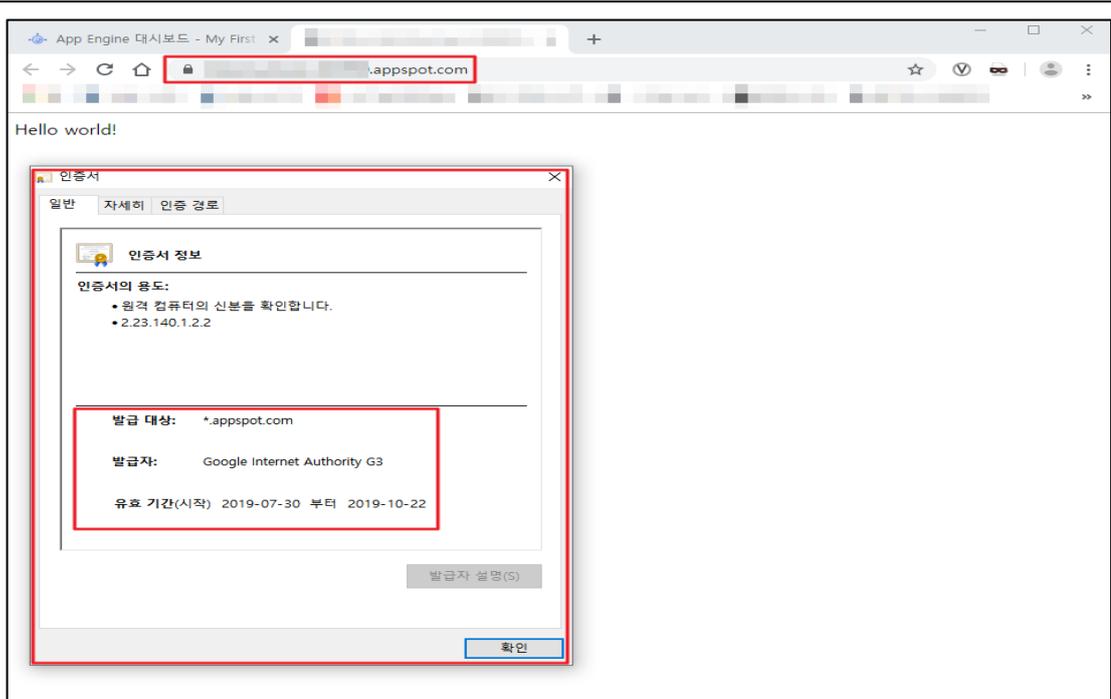
진단 기준	<p>양호기준 : 통신구간 암호화가 필요한 대상에 SSL 연결 설정이 존재하는 경우</p>
	<p>취약기준 : 통신구간 암호화가 필요한 대상에 SSL 연결 설정이 존재하지 않는 경우</p>

비고	
-----------	--

4.8 App Engine SSL 정책 관리

분류	운영 관리	중요도	상
항목명	App Engine SSL 정책 관리		
항목 설명	<p>App Engine 앱에 기본적인 SSL 보다 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.</p> <p>기본적으로 HTTPS 로드 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 암호를 보다 많이 제어 해야합니다. SSL 정책을 정의하여로드 밸런서가 클라이언트와 협상하는 SSL 기능을 제어할 수 있습니다.</p>		
설정 방법	<p>가. 구글 관리형 SSL – App Engine (기본 적용)</p> <p>1) [App Engine] > [대시보드]</p> <p>- App Engine 내 구동 서비스 확인</p>  <p>2) App Engine 내 구동 서비스 접근 및 인증서 확인</p> <p>- 기본적으로 App Engine을 통해 서비스를 운영할 경우 아래 그림과 같이 구글에서 자체적으로 SSL 인증서를 발급하여 *.appspot.com 도메인을 사용해 HTTPS 통신이 가능하게 해줍니다.</p>		

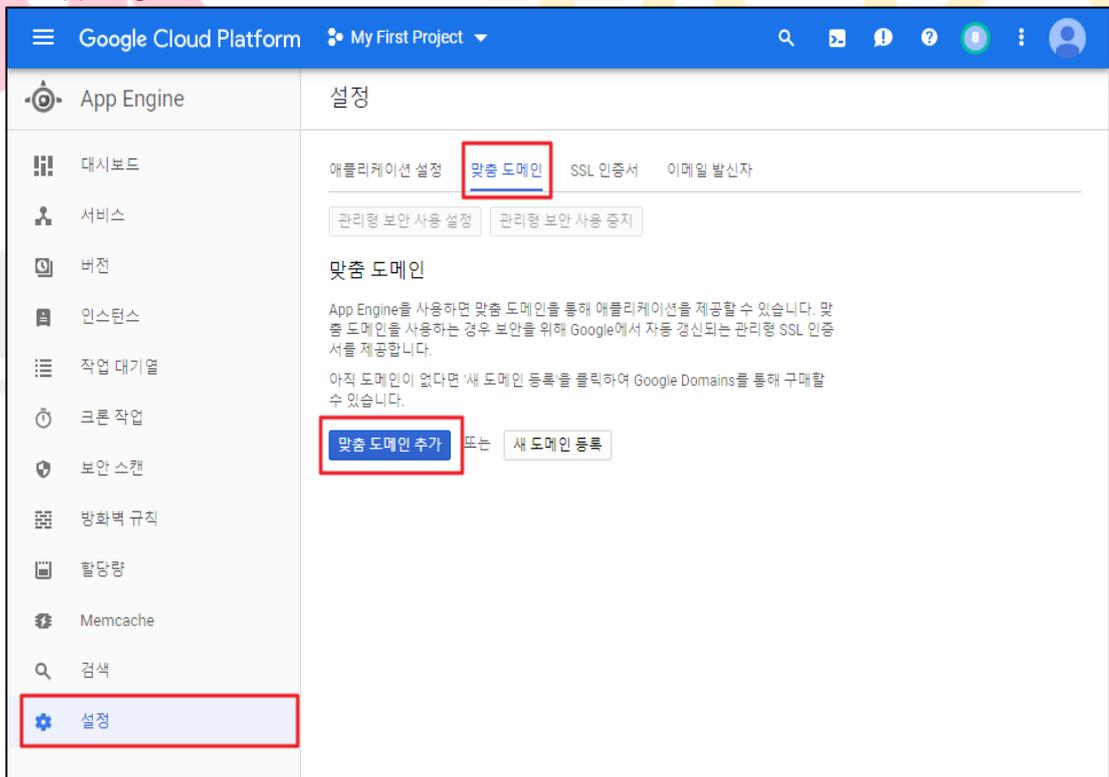
안녕을 지키는 기술



나. 구글 관리형 SSL – App Engine (커스텀 적용)

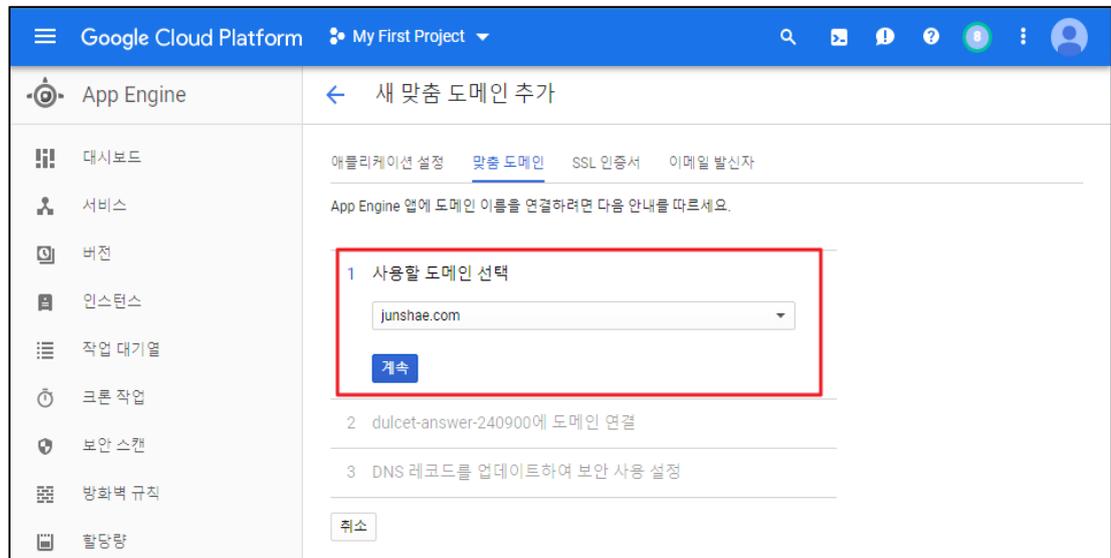
- App Engine 내 사용자가 별도 지정한 도메인에 대해 구글 관리형 SSL 인증서를 받기 위해서는 아래 그림을 참고해 주시기 바랍니다.

- 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



Google Cloud Platform My First Project

App Engine 새 맞춤 도메인 추가

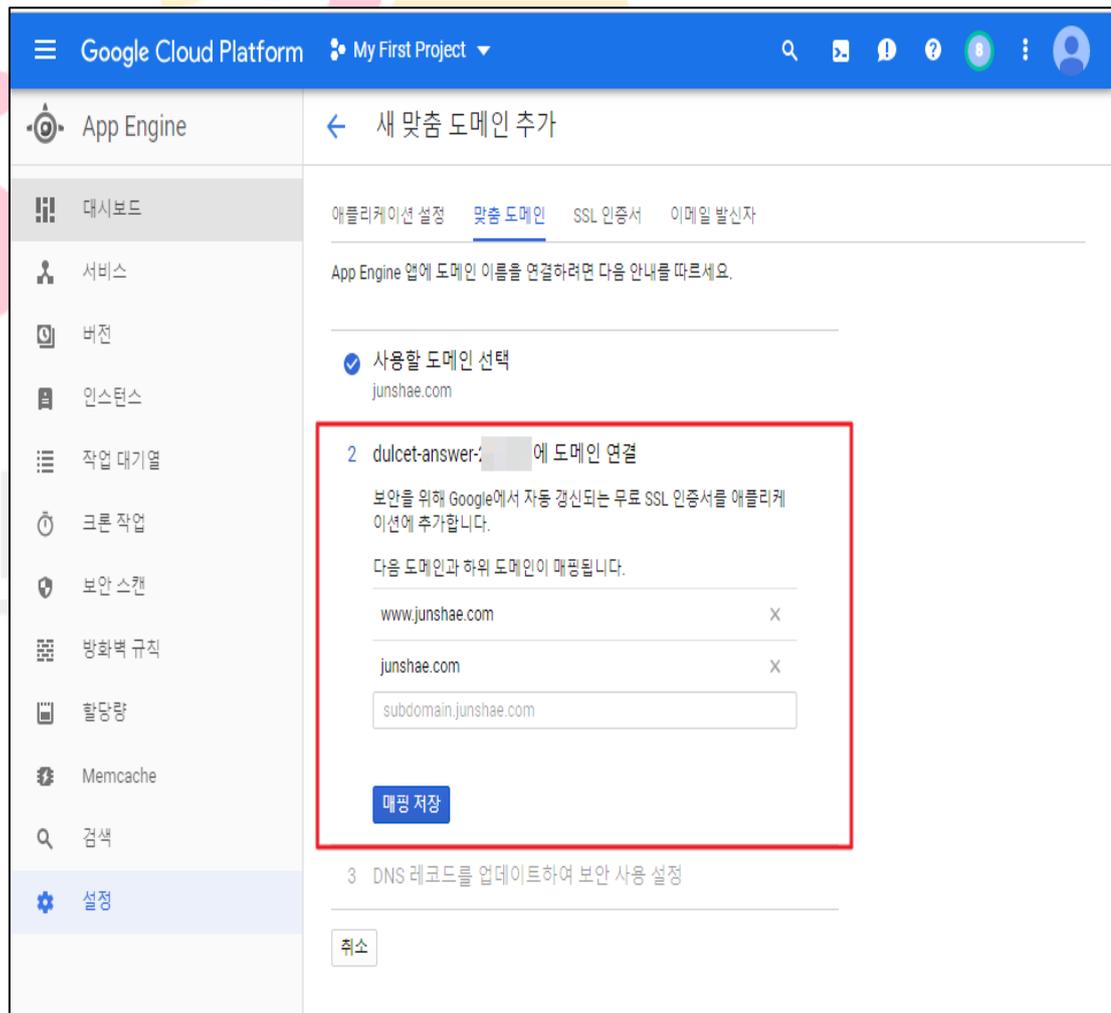
애플리케이션 설정 맞춤 도메인 SSL 인증서 이메일 발신자

App Engine 앱에 도메인 이름을 연결하려면 다음 안내를 따르세요.

- 1 사용할 도메인 선택
junshae.com
계속
- 2 dulcet-answer-240900에 도메인 연결
- 3 DNS 레코드를 업데이트하여 보안 사용 설정

취소

3) 사용할 하위 도메인 주소 등록



Google Cloud Platform My First Project

App Engine 새 맞춤 도메인 추가

애플리케이션 설정 맞춤 도메인 SSL 인증서 이메일 발신자

App Engine 앱에 도메인 이름을 연결하려면 다음 안내를 따르세요.

- 1 사용할 도메인 선택
junshae.com
- 2 dulcet-answer-240900에 도메인 연결
보안을 위해 Google에서 자동 갱신되는 무료 SSL 인증서를 애플리케이션에 추가합니다.
다음 도메인과 하위 도메인이 매핑됩니다.
www.junshae.com X
junshae.com X
subdomain.junshae.com
매핑 저장
- 3 DNS 레코드를 업데이트하여 보안 사용 설정

취소

4) 하위 도메인 유효성 확인

Google Cloud Platform My First Project

App Engine 새 맞춤 도메인 추가

애플리케이션 설정 맞춤 도메인 SSL 인증서 이메일 발신자

App Engine 앱에 도메인 이름을 연결하려면 다음 안내를 따르세요.

사용할 도메인 선택
junshae.com

2 dulcet-answer-...에 도메인 연결

보안을 위해 Google에서 자동 경신되는 무료 SSL 인증서를 애플리케이션에 추가합니다.

다음 도메인과 하위 도메인이 매핑됩니다.

상태	도메인
✓	www.junshae.com
✓	junshae.com

3 DNS 레코드를 업데이트하여 보안 사용 설정

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

Google Cloud Platform My First Project

App Engine 새 맞춤 도메인 추가

애플리케이션 설정 맞춤 도메인 SSL 인증서 이메일 발신자

App Engine 앱에 도메인 이름을 연결하려면 다음 안내를 따르세요.

사용할 도메인 선택
junshae.com

dulcet-answer-240900에 도메인 연결
www.junshae.com, junshae.com

3 DNS 레코드를 업데이트하여 보안 사용 설정

junshae.com용으로 도메인 등록기관에서 다음 DNS 레코드 추가:

유형	데이터	블링
A	216.239.32.21	
A	216.239.34.21	
A	216.239.36.21	
A	216.239.38.21	
AAAA	2001:4860:4802:32::15	
AAAA	2001:4860:4802:34::15	
AAAA	2001:4860:4802:36::15	
AAAA	2001:4860:4802:38::15	
CNAME	ghs.googlehosted.com	www

DNS 변경사항이 적용되는 데 최대 24시간이 걸릴 수 있습니다. SSL 인증서가 활성화되는 데 몇 분 정도 걸릴 수 있습니다.

6) 맞춤 도메인 추가 완료

The screenshot shows the 'App Engine' settings page in Google Cloud Platform. The '맞춤 도메인' (Custom Domain) tab is selected. A table lists the configured domains:

맞춤 도메인 이름	SSL 보안	인증서 ID	기록 유형	데이터	별칭
<input type="checkbox"/> junshae.com	Google에서 관리하며 자동 갱신됩니다.	-	A	216.239.32.21	(없음)
			A	216.239.34.21	
			A	216.239.36.21	
			A	216.239.38.21	
			AAAA	2001:4860:4802:32::15	
			AAAA	2001:4860:4802:34::15	
			AAAA	2001:4860:4802:36::15	
			AAAA	2001:4860:4802:38::15	
<input type="checkbox"/> www.junshae.com	Google에서 관리하며 자동 갱신됩니다.	-	CNAME	ghs.googlehosted.com.	www

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

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

The screenshot shows the 'DNS 영역 만들기' (Create DNS Zone) page in Google Cloud Platform. The form fields are filled as follows:

- 영역 유형: 공개
- 영역 이름: security-test
- DNS 이름: junshae.com
- DNSSEC: 사용 안함
- 설명 (선택사항): security test

Buttons for '만들기' (Create) and '취소' (Cancel) are visible at the bottom.

8) [레코드 모음 추가]

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

The screenshot shows the Google Cloud Platform interface for a project named 'My First Project'. The left sidebar shows '네트워크 서비스' (Network Services) with 'Cloud DNS' selected. The main content area is titled '영역 세부정보' (Zone Details) for 'security-test'. It shows the DNS name 'junshae.com' and type '공개' (Public). Under '레코드 모음' (Record Collection), there are buttons for '레코드 모음 추가' (Add Record Collection) and '레코드 모음 삭제' (Delete Record Collection). Below these is a table of records:

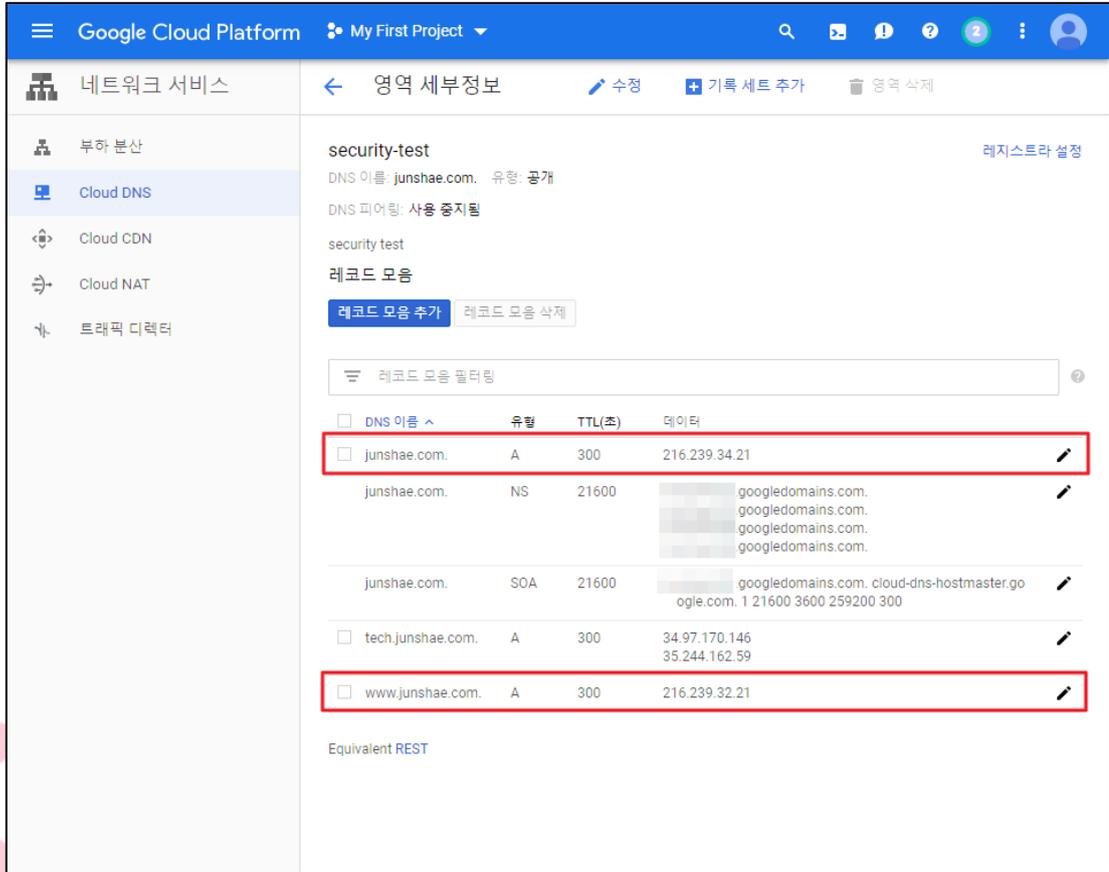
DNS 이름	유형	TTL(초)	데이터
junshae.com.	NS	21600	.googledomains.com. .googledomains.com. .googledomains.com. .googledomains.com.
junshae.com.	SOA	21600	.googledomains.com. cloud-dns-hostmaster.google.com. 1 21600 3600 259200 300

The screenshot shows the '레코드 모음 만들기' (Create Record Collection) form in the Google Cloud Platform. The form fields are:

- DNS 이름: junshae.com.
- 리소스 기록 유형: A
- TTL: 5
- TTL 단위: 분
- IPv4 주소: 216.239.34.21

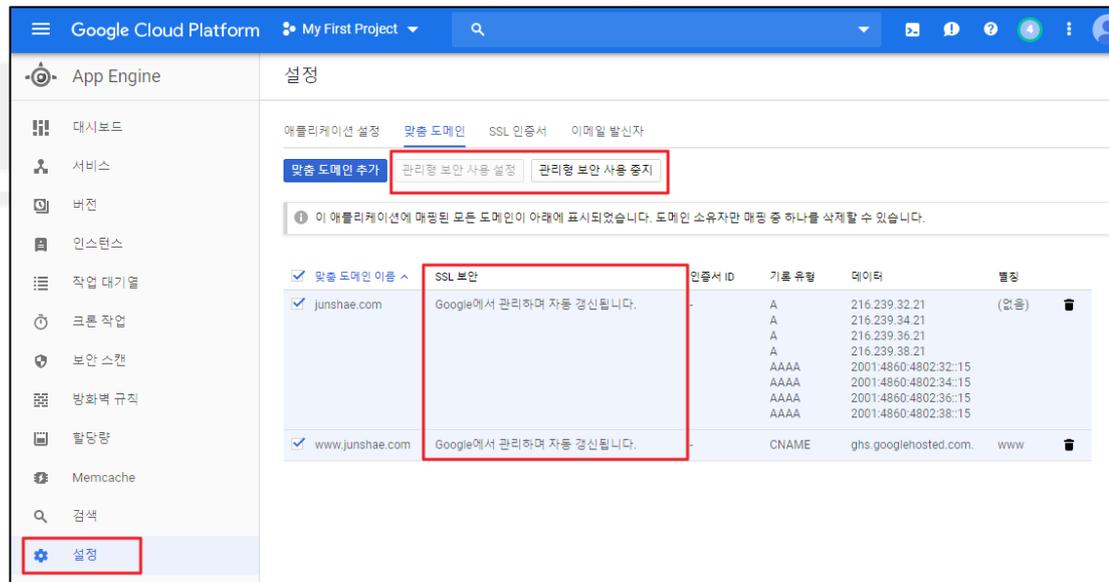
Buttons for '+ 항목 추가' (Add Item), '만들기' (Create), and '취소' (Cancel) are visible. The '만들기' button is highlighted with a red box.

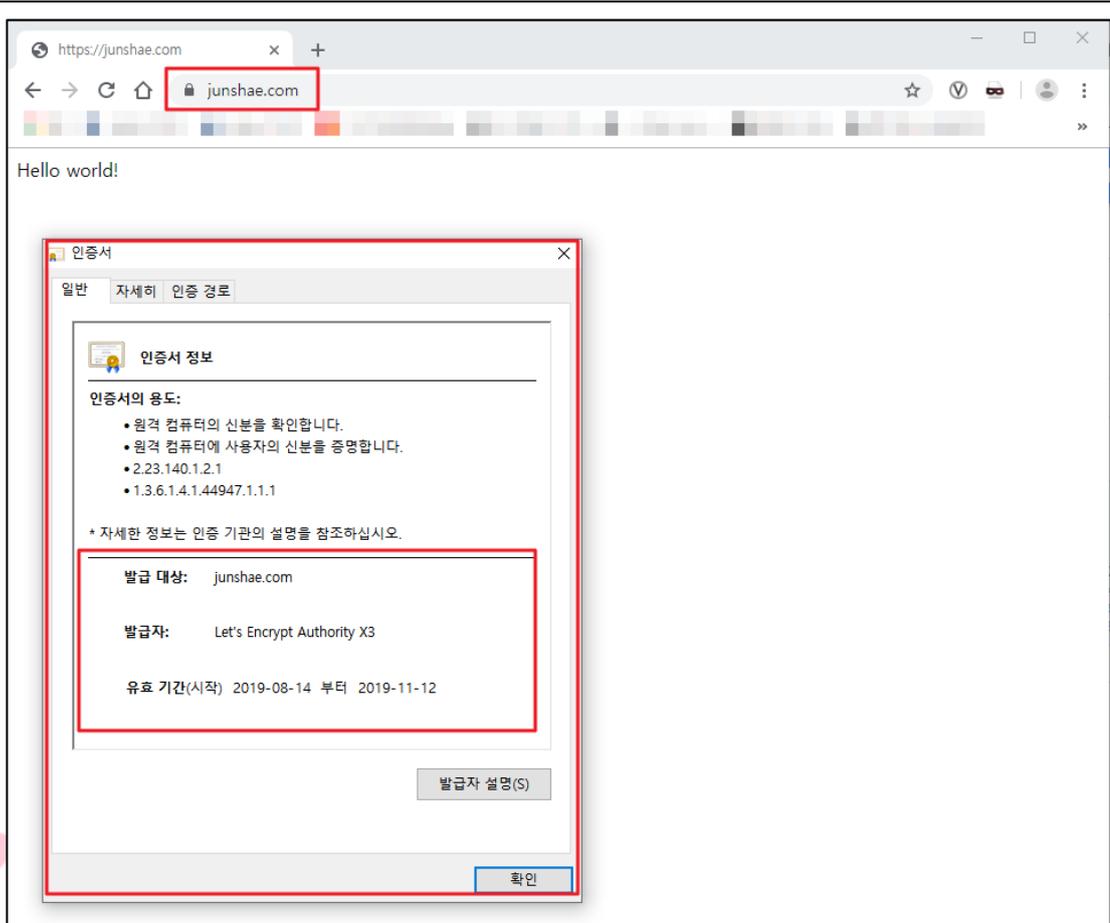
9) Cloud DNS 내 AppEngine 서비스와 연결하여 사용할 레코드 (도메인/IP) 추가 완료 확인



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





※ 상기 설정 방법은 구글 관리형 SSL 인증서에 대해 다루어졌으며, SSL 인증서 설정 시 참고용으로 이용하시기 바랍니다.

<p>진단 기준</p>	<p>양호기준 : App Engine을 사용할 때 SSL(TLS)의 설정이 적용되어 있을 경우</p> <p>취약기준 : App Engine을 사용할 때 SSL(TLS)의 설정이 적용되어 있지 않을 경우</p>
<p>비고</p>	

4.9 통신 구간 암호화 설정

분류	운영 관리	중요도	중									
항목명	통신 구간 암호화 설정											
항목 설명	클라우드 리소스를 통해 대/내외 서비스에서 정보를 송, 수신하는 경우 중간에서 공격자가 패킷을 가로채어 공격에 활용할 수 없도록 통신구간을 암호화하여 설정하여야 합니다.											
설정 방법	가. 중요정보 전송 시 암호화 정책 수립 1) 중요정보 전송 시 이동 구간 암호화 <ul style="list-style-type: none"> - 암호화된 통신 채널 사용 - 서버 원격 접근 시 암호화된 통신수단(VPN, SSH등)을 사용 - 공공기관 데이터 이관 시 VPN을 통해 이관 - 기타 관리를 위한 접근 시 OpenSSH 및 OpenSSL(TLS V1.2) 사용 											
	(*) 중요 정보 전송 및 저장 시 암호화 방안 예시 <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">구분</th> <th style="width: 50%;">암호화 방안</th> </tr> </thead> <tbody> <tr> <td>서버와 클라이언트 간 전송</td> <td>SSL 방식 응용프로그램</td> </tr> <tr> <td>개인정보처리시스템 간 전송</td> <td>IPSec 방식, SSL 방식, SSH 방식</td> </tr> <tr> <td>개인정보처리시스템 암호화 방식</td> <td>응용프로그램 자체 암호화 DB 서버 암호화 DBMS 자체 암호화 DBMS 암호화 기능 호출 운영체제 암호화</td> </tr> <tr> <td>업무용 컴퓨터 보조저장매체 암호화 방식</td> <td>문서 도구 자체 암호화 암호 유틸리티 이용 암호화 DRM 디스크 암호화</td> </tr> </tbody> </table> <p>※ 클라우드 서비스 보안인증제도(IaaS) 평가기준 해설서의 “11.1.4 네트워크 암호화 및 12.3.1 암호 정책 수립” 항목 참고</p>			구분	암호화 방안	서버와 클라이언트 간 전송	SSL 방식 응용프로그램	개인정보처리시스템 간 전송	IPSec 방식, SSL 방식, SSH 방식	개인정보처리시스템 암호화 방식	응용프로그램 자체 암호화 DB 서버 암호화 DBMS 자체 암호화 DBMS 암호화 기능 호출 운영체제 암호화	업무용 컴퓨터 보조저장매체 암호화 방식
구분	암호화 방안											
서버와 클라이언트 간 전송	SSL 방식 응용프로그램											
개인정보처리시스템 간 전송	IPSec 방식, SSL 방식, SSH 방식											
개인정보처리시스템 암호화 방식	응용프로그램 자체 암호화 DB 서버 암호화 DBMS 자체 암호화 DBMS 암호화 기능 호출 운영체제 암호화											
업무용 컴퓨터 보조저장매체 암호화 방식	문서 도구 자체 암호화 암호 유틸리티 이용 암호화 DRM 디스크 암호화											
진단 기준	양호기준 : 클라우드 리소스 통신 구간 내 암호화 설정이 되어 있는 경우 취약기준 : 클라우드 리소스 통신 구간 내 암호화 설정이 되어 있지 않는 경우											
비고												

4.10 감사 로그 기록 및 관리

분류	운영 관리	중요도	중																														
항목명	감사 로그 기록 및 관리																																
항목 설명	<p>Cloud 감사 로그 설정을 통해 Google Cloud 리소스에 '누가, 언제, 어디서, 무엇을 했는지' 파악할 수 있습니다.</p> <p>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.</p> <p>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.</p> <p>(*) 감사 로그 종류</p> <table border="1"> <thead> <tr> <th>구분</th> <th>내용</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>(*) 주요 리소스 별 감사 로그 기본 설정 현황</p> <table border="1"> <thead> <tr> <th>구분</th> <th>GCE(Google Cloud Engine)</th> <th>GCS(Google Cloud Storage)</th> <th>Google Cloud SQL</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>※ Cloud 감사 로그는 조직 구성원이 수행한 작업에 대한 로그를 제공하는 반면, 액세스 투명성 로그는 Google 직원이 수행한 작업에 대한 로그를 제공합니다. 또한, 중요 로그는 보관기간을 설정해 사용하시기 바랍니다.</p>			구분	내용	관리자 활동 감사 로그	API 호출이나 리소스의 구성 또는 메타데이터를 수정하는 기타 관리 작업과 관련된 로그 항목 포함	시스템 이벤트 감사 로그	리소스의 구성 또는 메타데이터를 읽는 API 호출뿐만 아니라 사용자가 제공한 리소스 데이터를 생성, 수정 또는 읽는 사용자 주도 API 호출까지 포함	데이터 액세스 감사 로그	리소스 구성을 수정하는 Google Cloud 관리 작업의 로그 항목을 포함	정책 거부 감사 로그	보안 정책 위반으로 인해 Google Cloud 서비스가 사용자 또는 서비스 계정에 대한 액세스를 거부 시 생성	구분	GCE(Google Cloud Engine)	GCS(Google Cloud Storage)	Google Cloud SQL	관리자 활동 감사 로그	사용	사용	사용	시스템 이벤트 감사 로그	사용 중지	사용 중지	사용	데이터 액세스 감사 로그	사용	X	사용 중지	정책 거부 감사 로그	X	X	X
	구분	내용																															
	관리자 활동 감사 로그	API 호출이나 리소스의 구성 또는 메타데이터를 수정하는 기타 관리 작업과 관련된 로그 항목 포함																															
	시스템 이벤트 감사 로그	리소스의 구성 또는 메타데이터를 읽는 API 호출뿐만 아니라 사용자가 제공한 리소스 데이터를 생성, 수정 또는 읽는 사용자 주도 API 호출까지 포함																															
	데이터 액세스 감사 로그	리소스 구성을 수정하는 Google Cloud 관리 작업의 로그 항목을 포함																															
	정책 거부 감사 로그	보안 정책 위반으로 인해 Google Cloud 서비스가 사용자 또는 서비스 계정에 대한 액세스를 거부 시 생성																															
	구분	GCE(Google Cloud Engine)	GCS(Google Cloud Storage)	Google Cloud SQL																													
	관리자 활동 감사 로그	사용	사용	사용																													
	시스템 이벤트 감사 로그	사용 중지	사용 중지	사용																													
	데이터 액세스 감사 로그	사용	X	사용 중지																													
정책 거부 감사 로그	X	X	X																														

가. 기본 감사 로그 설정

1) IAM 및 관리자 내 [감사 로그] 페이지 접근 및 기본 감사 설정 확인

2) 기본 감사 구성 설정 후 저장

3) 로그 탐색기 내 설정된 감사 로그 확인

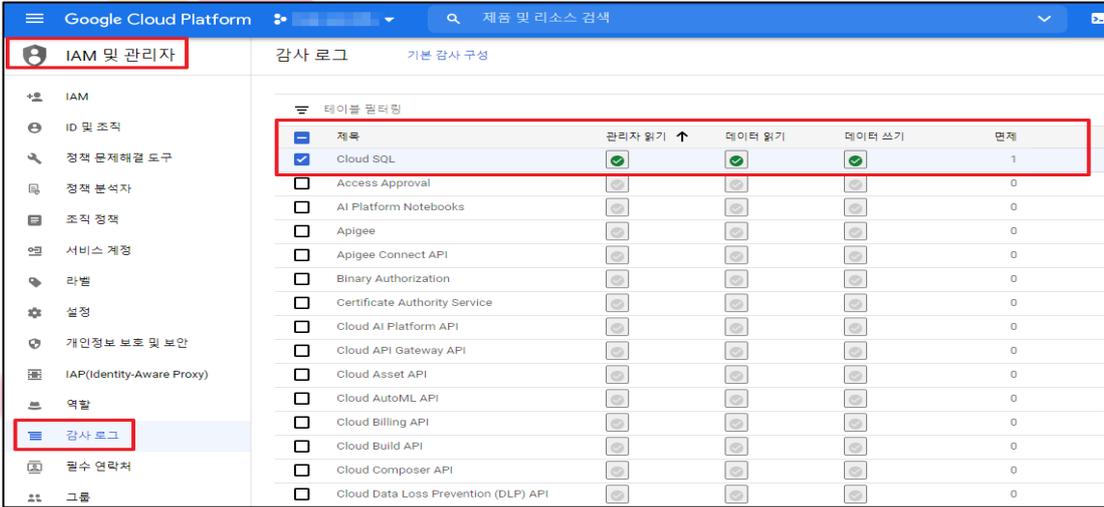
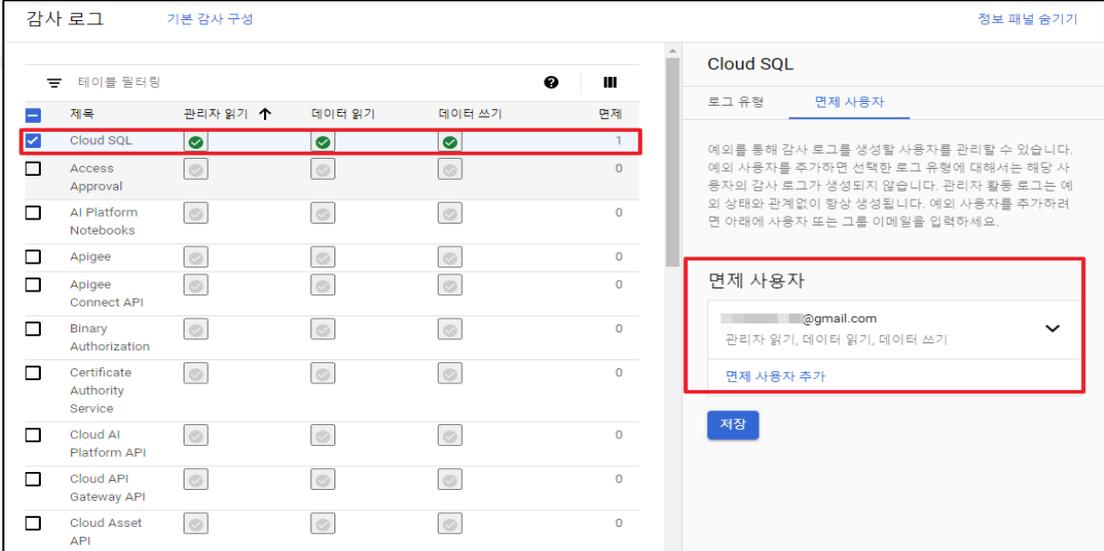
설정
방법

진단 기준	<p>양호기준 : 서비스 별 감사 로그가 설정되어 있을 경우</p> <p>취약기준 : 서비스 별 감사 로그가 설정되어 있지 않을 경우</p>
비고	



안녕을 지키는 기술

4.11 감사 로그 면제 사용자 존재 여부

분류	운영 관리	중요도	중
항목명	감사 로그 면제 사용자 존재 여부		
항목 설명	<p>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.</p> <p>면제 사용자는 [액세스] - [감사 로그] 내 [면제 사용자] 메뉴에서 추가/삭제할 수 있으며, 불필요한 면제 사용자가 존재하지 않도록 주기적 확인이 필요합니다.</p>		
설정 방법	<p>가. 감사 로그 내 면제 사용자 확인</p> <p>1) 감사 로그 면제 사용자가 존재하는 서비스 확인</p>  <p>2) 면제 사용자 확인</p> 		

나. 면제 사용자 삭제

1) 면제 사용자 삭제

The screenshot shows the Google Cloud IAM console. On the left, the 'IAM 및 관리자' (IAM and Admin) menu is visible, with '감사 로그' (Audit Logs) selected. The main area displays a table of audit logs for 'Cloud SQL'. The '면제' (Exempt) column shows a count of 1. On the right, the 'Cloud SQL' details panel is open, showing the '면제 사용자' (Exempt Users) section. A '삭제' (Delete) button is highlighted with a red box.

2) 면제 사용자 삭제 확인

The screenshot shows the Google Cloud IAM console after the deletion. The '면제 사용자' (Exempt Users) count for 'Cloud SQL' is now 0. The '삭제' (Delete) button in the panel is still highlighted with a red box.

진단
기준

양호기준

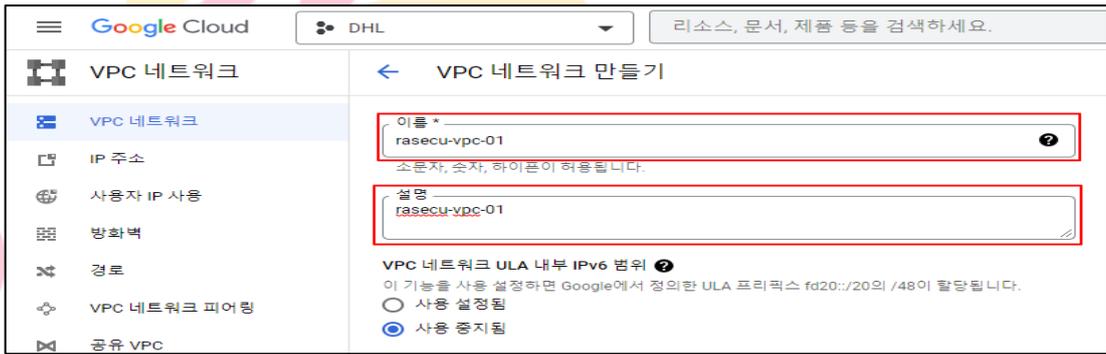
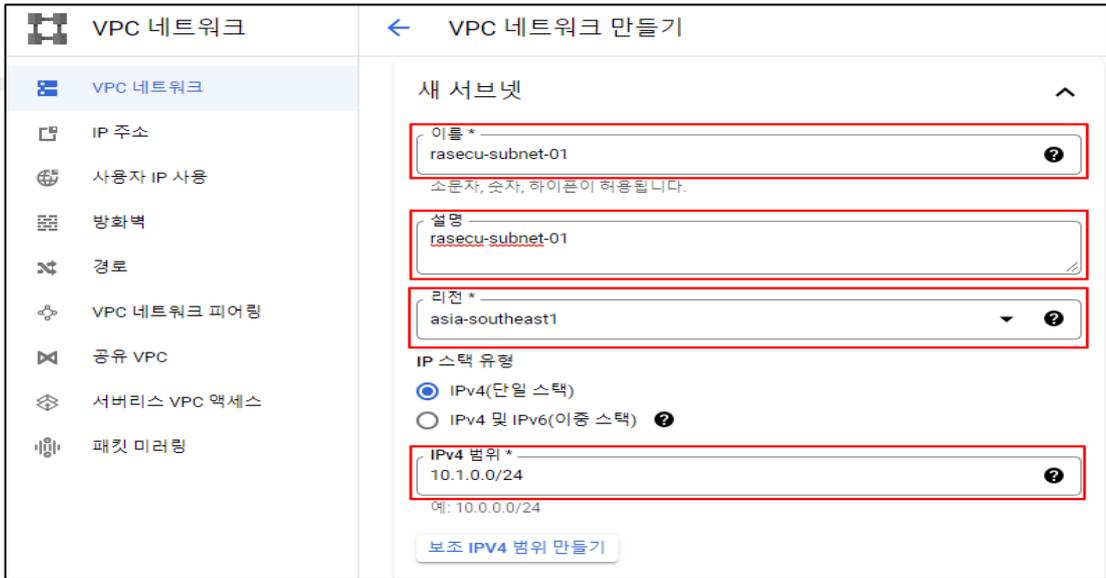
: 감사 로그 내 면제 사용자가 존재하지 않는 경우

취약기준

: 감사 로그 내 면제 사용자가 존재하는 경우

비고

4.12 VPC 네트워크 흐름 로그 설정 관리

분류	운영 관리	중요도	중
항목명	VPC 네트워크 흐름 로그 설정 관리		
항목 설명	<p>VPC 흐름 로그는 Google Kubernetes Engine 노드로 사용되는 인스턴스를 포함하여 VM 인스턴스에서 전송되거나 수신되는 네트워크 흐름의 샘플을 기록하며, 기존 네트워크가 아닌 VPC 네트워크에서 작동합니다. 서브넷별로 VPC 흐름 로그를 사용 설정하거나 사용 중지합니다. 서브넷에 대해 사용 설정된 경우 VPC 흐름 로그는 해당 서브넷의 모든 VM 인스턴스에서 데이터를 수집합니다.</p> <p>VPC 흐름 로그는 각 VM의 TCP, UDP, ICMP, ESP, GRE 흐름을 샘플링합니다. 인바운드 및 아웃바운드 흐름은 모두 샘플링됩니다. 이러한 흐름은 VM과 다른 VM, 온프레미스 데이터 센터의 호스트, Google 서비스, 인터넷 호스트 사이에 있을 수 있습니다. 흐름을 샘플링으로 캡처하는 경우 VPC 흐름 로그는 흐름의 로그를 생성합니다. 각 흐름 기록에는 레코드 형식 섹션에 설명된 정보가 포함됩니다.</p>		
설정 방법	<p>가. VPC 네트워크 생성 및 흐름 로그 설정</p> <p>1) VPC 네트워크 기본 정보 입력</p>  <p>2) 서브넷 기본정보 및 IP 범위 설정</p> 		

3) 흐름 로그 활성화 및 추가 설정

The screenshot shows the Google Cloud console interface for configuring a VPC network. The left sidebar lists various VPC network settings, with 'VPC 네트워크' selected. The main area is titled 'VPC 네트워크 만들기' (Create VPC Network). Under the '비공개 Google 액세스' (Private Google Access) section, the '사용 안함' (Do not use) option is selected. The '흐름 로그' (Flow Logs) section is highlighted with a red box and contains the following settings:

- 흐름 로그:** VPC 흐름 로그를 사용 설정해도 성능에는 영향이 없지만 일부 시스템에서 대량의 로그가 생성되어 Cloud Logging 비용이 증가할 수 있습니다. [자세히 알아보기](#)
- 사용:** Selected with a radio button.
- 사용 안함:** Unselected with a radio button.
- 집계 간격:** 5초, 30초, 1분, 5분, 10분, 15분. The '5분' (5 minutes) option is selected.
- 추가 필드:** '메타데이터 포함' (Include metadata) is checked with a blue checkbox.
- 샘플링 레이트:** A text input field containing '50' and a percentage sign.

At the bottom right of the configuration area, there are '취소' (Cancel) and '완료' (Done) buttons.

4) VPC 및 서브넷 생성 후 흐름 로그 설정 확인

The screenshot shows the Google Cloud console after VPC and subnet creation. A notification from Network Intelligence Center is displayed, stating that flow logs are enabled and providing a link to view details. Below the notification, a table lists the VPC subnets:

이름	리전	서브넷	MTU	모드	내부 IP 범위	외부 IP 범위	보조 IPv4 범위	게이트웨이	방화벽 규칙	전역 동적 라우팅	흐름 로그
rascu-vpc-01	asia-southeast1	rascu-subnet-01	1460	커스텀	10.1.0.0/24	없음	없음	10.1.0.1	0	사용 안함	사용

The '사용' (Used) status in the '흐름 로그' column is highlighted with a red box.

진단
기준

양호기준

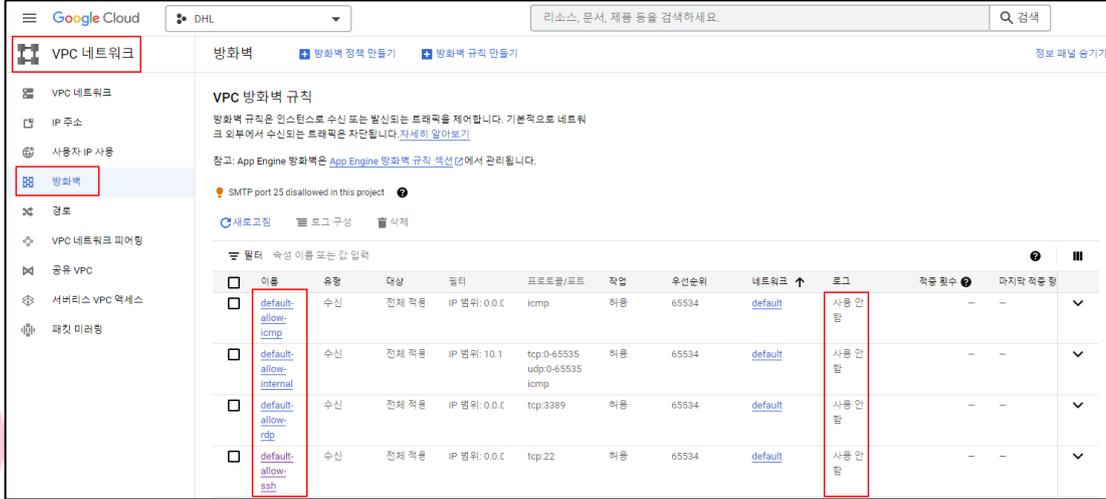
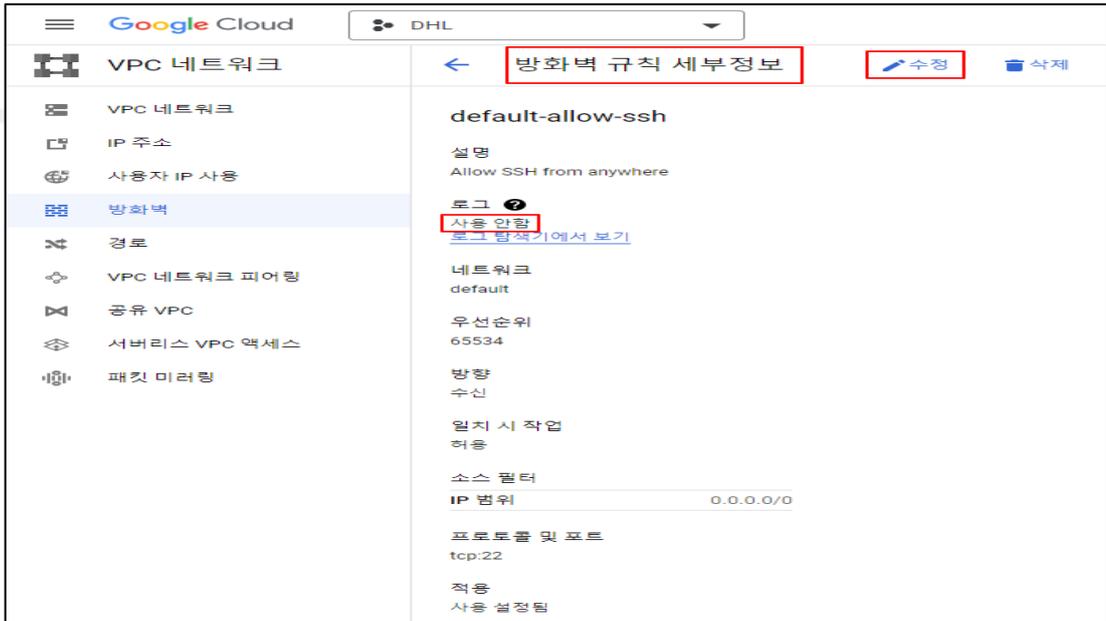
: VPC 네트워크 흐름 로그 설정이 활성화 되어있는 경우

취약기준

: VPC 네트워크 흐름 로그 설정이 활성화 되어있지 않은 경우

비고

4.13 방화벽 로그 관리

분류	운영 관리	중요도	중
항목명	방화벽 로그 관리		
항목 설명	<p>VPC 방화벽 규칙을 사용하면 지정한 구성을 기준으로 가상 머신(VM) 인스턴스 간의 연결을 허용하거나 거부할 수 있습니다. 사용 설정한 VPC 방화벽 규칙은 인스턴스의 구성 및 운영 체제와 상관없이 인스턴스를 보호할 수 있도록 항상 실행됩니다. 아직 시작하지 않은 인스턴스도 마찬가지입니다. 방화벽 규칙은 네트워크 수준에서 정의되지만 연결은 인스턴스별로 허용되거나 거부됩니다. VPC 방화벽 규칙은 인스턴스와 다른 네트워크 사이뿐만 아니라 동일한 네트워크 내의 개별 인스턴스 간에 존재할 수 있습니다.</p>		
설정 방법	<p>가. 방화벽 로그 설정</p> <p>1) 방화벽 현황 확인</p>  <p>2) 방화벽 규칙 세부 정보 확인</p> 		

3) 방화벽 규칙에 대한 로그 활성화

The screenshot shows the Google Cloud console interface for configuring a firewall rule. The left sidebar lists various VPC network settings, with '방화벽' (Firewall) selected. The main area displays the configuration for the 'default-allow-ssh' rule. The '로그' (Logging) section is highlighted, showing the '사용' (Use) radio button selected, indicating that logging is enabled for this rule. Other visible settings include the priority (65534), direction (Ingress), and target (All instances in the network).

4) 방화벽 규칙 로그 적용 완료

The screenshot shows the Google Cloud console displaying a list of firewall rules. The 'default-allow-ssh' rule is highlighted with a red box, and its '로그' (Logging) status is also highlighted with a red box, showing it is set to '사용' (Use). The table below lists several firewall rules with their respective logging statuses.

이름	유형	대상	필터	프로토콜/포트	작업	우선순위	네트워크	로그	적용 횟수	마지막 적용
default-allow-icmp	수신	전체 적용	IP 범위: 0.0.0	icmp	허용	65534	default	사용 안 함	-	-
default-allow-internal	수신	전체 적용	IP 범위: 10.1	tcp:0-65535 udp:0-65535 icmp	허용	65534	default	사용 안 함	-	-
default-allow-rdp	수신	전체 적용	IP 범위: 0.0.0	tcp:3389	허용	65534	default	사용 안 함	-	-
default-allow-ssh	수신	전체 적용	IP 범위: 0.0.0	tcp:22	허용	65534	default	사용	0	적용 횟수 없음

진단 기준	<p>양호기준 : Well-Known 정책에 대한 로그 설정이 존재하는 경우</p> <p>취약기준 : Well-Known 정책에 대한 로그 설정이 존재하지 않는 경우</p>
비고	



안녕을 지키는 기술

4.14 로그 보관 설정

분류	운영 관리	중요도	중										
항목명	로그 보관 설정												
항목 설명	<p>Cloud Logging은 GCP에서 사용중인 서비스 및 리소스에 대한 로그를 검색, 정렬, 분석할 수 있으며, 별도 리전 로그 버킷을 생성하여 별도 공간에 저장할 수 있습니다. 사용자 로그에 대한 로그는 Cloud 감사 로그 서비스를 통해 확인할 수 있으며 기본적으로 "관리자 활동", "데이터 액세스", "시스템 이벤트", "정책 거부"에 대한 부분을 제공합니다.</p> <p>※ Cloud 감사 로그 유형</p> <table border="1"> <thead> <tr> <th>서비스 구분</th> <th>서비스 상세</th> </tr> </thead> <tbody> <tr> <td>관리자 활동 감사 로그</td> <td>관리자 활동 감사 로그에는 API 호출이나 리소스의 구성 또는 메타데이터를 수정하는 기타 작업과 관련된 로그 항목이 포함됩니다. 관리자 활동 감사 로그는 항상 기록되며 구성하거나 제외하거나 사용 중지할 수 없습니다. Cloud Logging API를 사용 중지해도 관리자 활동 감사 로그는 계속 생성됩니다.</td> </tr> <tr> <td>데이터 액세스 감사 로그</td> <td>데이터 액세스 감사 로그에는 리소스의 구성 또는 메타데이터를 읽는 API 호출뿐만 아니라 사용자가 제공한 리소스 데이터를 생성, 수정 또는 읽는 사용자 주도 API 호출도 포함됩니다. 데이터 액세스 감사 로그(BigQuery 데이터 액세스 감사 로그 제외)는 감사가 상당히 클 수 있으므로 기본적으로 중지되어 있습니다. BigQuery 이외의 Google Cloud 서비스에 대해 데이터 액세스 감사 로그를 작성하려면 로그를 명시적으로 사용 설정해야 합니다.</td> </tr> <tr> <td>시스템 이벤트 감사 로그</td> <td>시스템 이벤트 감사 로그는 리소스 구성을 수정하는 Google Cloud 작업의 로그 항목을 포함합니다. 시스템 이벤트 감사 로그는 Google 시스템에서 사용 설정되며 사용자의 직접적인 작업을 통해서는 사용 설정되지 않습니다.</td> </tr> <tr> <td>정책 거부 감사 로그</td> <td>정책 거부 감사 로그는 보안 정책 위반으로 인해 Google Cloud 서비스가 사용자 또는 서비스 계정에 대해 액세스를 거부할 때 기록됩니다. 보안 정책은 Cloud Logging에 정책 거부 감사 로그를 제공하는 VPC 서비스 제어에 의해 결정됩니다.</td> </tr> </tbody> </table>			서비스 구분	서비스 상세	관리자 활동 감사 로그	관리자 활동 감사 로그에는 API 호출이나 리소스의 구성 또는 메타데이터를 수정하는 기타 작업과 관련된 로그 항목이 포함됩니다. 관리자 활동 감사 로그는 항상 기록되며 구성하거나 제외하거나 사용 중지할 수 없습니다. Cloud Logging API를 사용 중지해도 관리자 활동 감사 로그는 계속 생성됩니다.	데이터 액세스 감사 로그	데이터 액세스 감사 로그에는 리소스의 구성 또는 메타데이터를 읽는 API 호출뿐만 아니라 사용자가 제공한 리소스 데이터를 생성, 수정 또는 읽는 사용자 주도 API 호출도 포함됩니다. 데이터 액세스 감사 로그(BigQuery 데이터 액세스 감사 로그 제외)는 감사가 상당히 클 수 있으므로 기본적으로 중지되어 있습니다. BigQuery 이외의 Google Cloud 서비스에 대해 데이터 액세스 감사 로그를 작성하려면 로그를 명시적으로 사용 설정해야 합니다.	시스템 이벤트 감사 로그	시스템 이벤트 감사 로그는 리소스 구성을 수정하는 Google Cloud 작업의 로그 항목을 포함합니다. 시스템 이벤트 감사 로그는 Google 시스템에서 사용 설정되며 사용자의 직접적인 작업을 통해서는 사용 설정되지 않습니다.	정책 거부 감사 로그	정책 거부 감사 로그는 보안 정책 위반으로 인해 Google Cloud 서비스가 사용자 또는 서비스 계정에 대해 액세스를 거부할 때 기록됩니다. 보안 정책은 Cloud Logging에 정책 거부 감사 로그를 제공하는 VPC 서비스 제어에 의해 결정됩니다.
	서비스 구분	서비스 상세											
	관리자 활동 감사 로그	관리자 활동 감사 로그에는 API 호출이나 리소스의 구성 또는 메타데이터를 수정하는 기타 작업과 관련된 로그 항목이 포함됩니다. 관리자 활동 감사 로그는 항상 기록되며 구성하거나 제외하거나 사용 중지할 수 없습니다. Cloud Logging API를 사용 중지해도 관리자 활동 감사 로그는 계속 생성됩니다.											
	데이터 액세스 감사 로그	데이터 액세스 감사 로그에는 리소스의 구성 또는 메타데이터를 읽는 API 호출뿐만 아니라 사용자가 제공한 리소스 데이터를 생성, 수정 또는 읽는 사용자 주도 API 호출도 포함됩니다. 데이터 액세스 감사 로그(BigQuery 데이터 액세스 감사 로그 제외)는 감사가 상당히 클 수 있으므로 기본적으로 중지되어 있습니다. BigQuery 이외의 Google Cloud 서비스에 대해 데이터 액세스 감사 로그를 작성하려면 로그를 명시적으로 사용 설정해야 합니다.											
	시스템 이벤트 감사 로그	시스템 이벤트 감사 로그는 리소스 구성을 수정하는 Google Cloud 작업의 로그 항목을 포함합니다. 시스템 이벤트 감사 로그는 Google 시스템에서 사용 설정되며 사용자의 직접적인 작업을 통해서는 사용 설정되지 않습니다.											
	정책 거부 감사 로그	정책 거부 감사 로그는 보안 정책 위반으로 인해 Google Cloud 서비스가 사용자 또는 서비스 계정에 대해 액세스를 거부할 때 기록됩니다. 보안 정책은 Cloud Logging에 정책 거부 감사 로그를 제공하는 VPC 서비스 제어에 의해 결정됩니다.											
<p>국내에서 시행 중인 클라우드 보안인증제에서 보안감사 로그(접근기록 등)는 1년 이상 보존하도록 되어 있으며, 개인정보의 안전성 확보 조치 기준 8조(19.6, 행안부)에서도 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하도록 명시되어 있습니다.</p>													
<p>(*) 로그 분류</p> <p>1) 개인정보처리시스템 접근 기록</p>													

고객 주요 정보, 임직원 주요 정보 등
 관련 서비스: Storage, SQL, FileStore, Datastore 등

2) 보안관련 감사 로그
 사용자 접속 기록, 인증 성공/실패, 계정 생성/삭제 등
 관련 서비스: Cloud 감사 로그, IAM, Storage 등

3) 시스템 이벤트 로그
 운영체제 구성요소에 의해 발생하는 로그(시스템 시작, 종료, 상태, 에러 코드 등)
 주요 서버, 네트워크, 보안 장비 등의 로그(접근 기록 및 이벤트 로그 등)
 관련 서비스: Storage, 모니터링 등

※ 법적 근거
 국가정보보안기본지침 제55조(로그기록 유지) - 2019/03
 개인정보의 안전성 확보 조치 기준 제8조(접속 기록의 보관 및 점검) - 2019/06

가. 로그 버킷 생성 방법

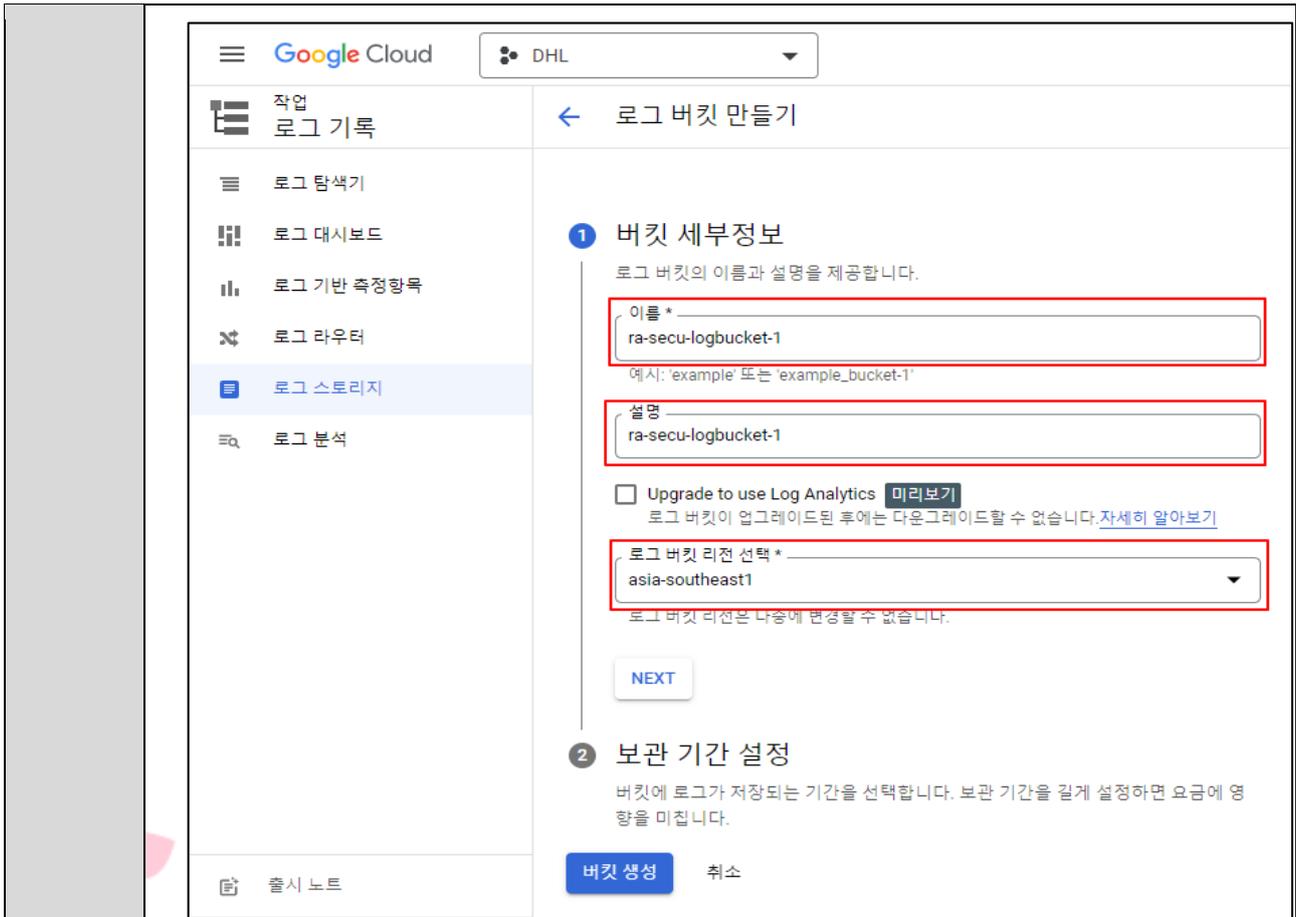
1) 로그 스토리지 메뉴 이동 후 로그 버킷 만들기 선택

The screenshot shows the Google Cloud console interface. On the left sidebar, the 'Log Storage' menu item is highlighted. The main content area shows the 'Log Buckets' section with a table of existing buckets. The table has columns for '이름' (Name), '설명' (Description), '지난달 사용량' (Last month usage), '월간 누적 사용량(이번 달 누적)' (Monthly cumulative usage), '로그 분석 사용 가능' (Log analysis available), and 'BigQuery 연결 데이터' (BigQuery connection data). Two buckets are listed: '_Default' and '_Required'.

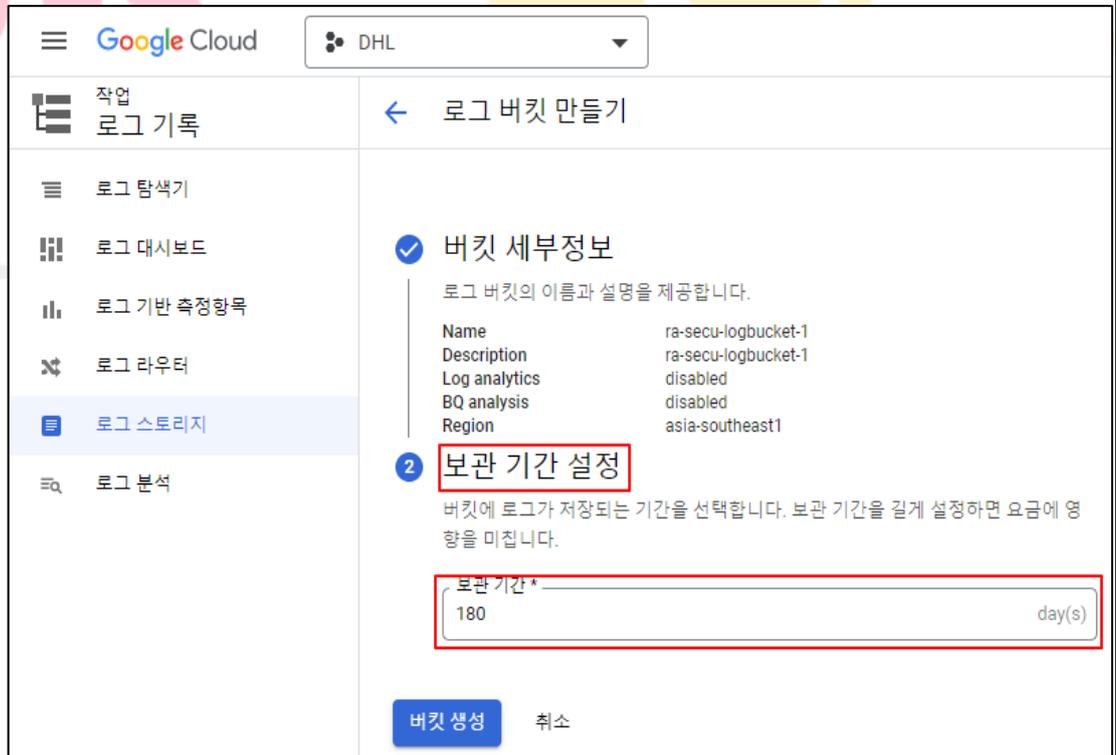
이름	설명	지난달 사용량	월간 누적 사용량(이번 달 누적)	로그 분석 사용 가능	BigQuery 연결 데이터
_Default	Default bucket	0 B	2.5 KIB	UPGRADE	-
_Required	Audit bucket	장구되지 않음	장구되지 않음	UPGRADE	-

2) 로그 버킷 기본 정보 기입 및 리전 선택

설정
 방법



3) 보관 기간 설정



4) 로그 버킷 생성 후 보관 기간 확인

이름	설명	지난달 사용량	올해 누적 사용량(이번 달 누적)	로그 분석 사용 가능	BigQuery 연결 데이터 세트	보관 기간	리전
ra-secu-logbucket-1	ra-secu-logbucket-1	0 B	0 B	업그레이드할 수 없음	-	180 days	asia-southeast1
._required	Audit bucket	중요되지 않음	중요되지 않음	UPGRADE	-	400 days	global
._default	Default bucket	0 B	2.5 KiB	UPGRADE	-	30 days	global

진단
기준

양호기준

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

취약기준

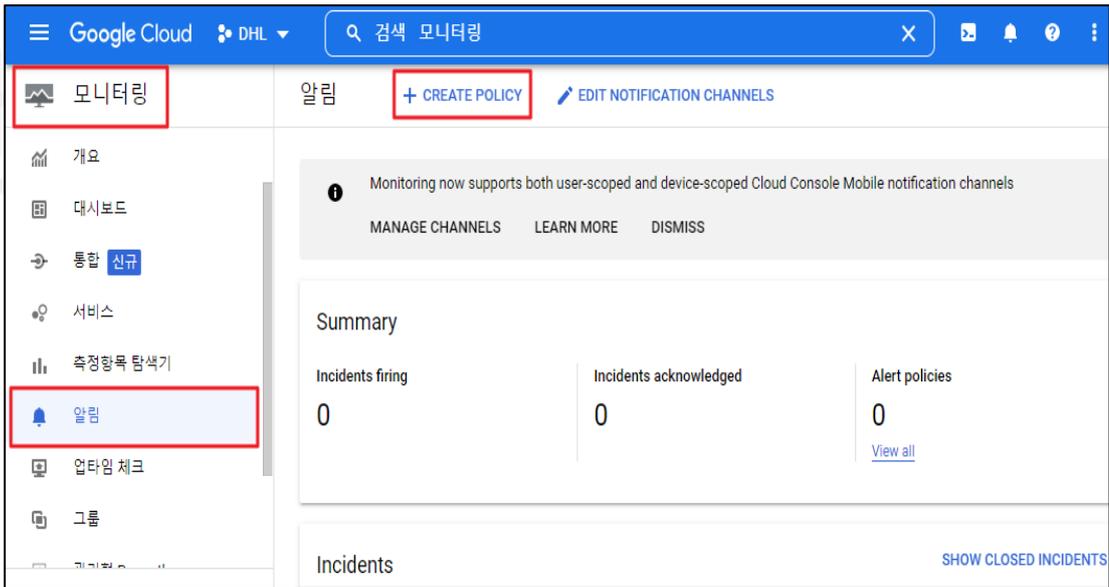
: GCP 서비스 로그를 기준(최소 1년 이상)에 맞게 보관하고 있지 않는 경우

비고

SK 실더스

안녕을 지키는 기술

4.15 Google 계정 사용자 이상징후 알림 설정

분류	운영 관리	중요도	중				
항목명 항목 설명	<p>Google 계정 사용자 이상징후 알림 설정</p> <p>Cloud Monitoring은 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 제품 군은 이러한 데이터를 수집하고 대시보드, 차트, 알림을 통해 유용한 정보를 제공합니다. BindPlane은 추가 비용 없이 Google Cloud 프로젝트에 포함되어 있습니다.</p> <p>안전한 Google 계정 사용을 위해 Cloud Monitoring 서비스 내 알림 정책 설정을 통해 Google 계정 사용자의 이상징후 확인이 가능합니다.</p> <p>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 측정 항목을 이용하여 임의의 알림 정책 설정도 가능합니다.</p> <p>(*) Google 계정 사용자 이상징후 확인을 위한 기본 정의 알림 정책 (참고)</p> <table border="1" data-bbox="304 1104 1428 1245"> <thead> <tr> <th>구분</th> <th>측정 항목</th> </tr> </thead> <tbody> <tr> <td>IAM</td> <td>service_account/authn_events_count service_account/key/authn_events_count</td> </tr> </tbody> </table>			구분	측정 항목	IAM	service_account/authn_events_count service_account/key/authn_events_count
구분	측정 항목						
IAM	service_account/authn_events_count service_account/key/authn_events_count						
설정 방법	<p>가. Google 계정 사용자 이상징후 경보 설정 방법</p> <p>1) 모니터링 내 [알림] 페이지 접근 및 정책 생성 클릭</p> 						

2) METRIC 설정 및 기타 세부 Condition 설정

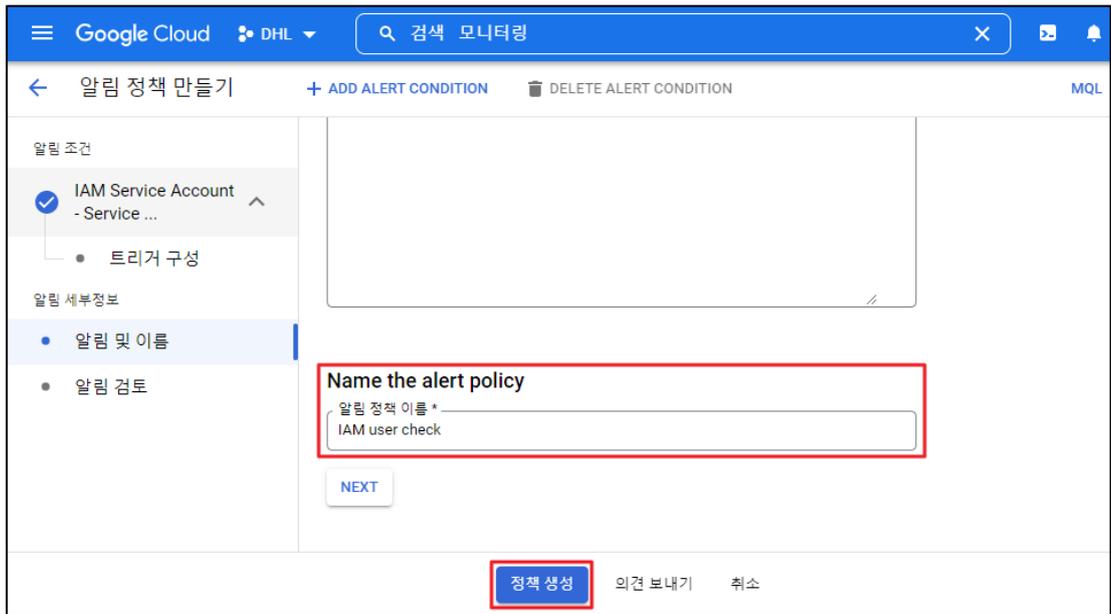
The first screenshot shows the 'Select a metric' step in the alert condition configuration. A red box highlights the '측정항목 선택' (Select metric) dropdown menu.

The second screenshot shows the '측정항목 선택' (Select metric) dialog box. A red box highlights the 'IAM Service Account' option in the list. Another red box highlights the 'Service account authentication events' metric under the 'Service_account' category. A '적용' (Apply) button is also highlighted with a red box.

3) 추가 설정 및 트리거 설정

The screenshot shows the 'Configure alert trigger' dialog box. A red box highlights the 'Threshold' condition type, the 'Alert trigger' dropdown (set to '임의 시계열 위반'), the '기준 위치' (Location) dropdown (set to '임계값 초과'), the '기준 값' (Threshold value) input field, and the '조건 이름*' (Condition name) field (set to 'IAM Service Account - Service account authentication events'). A 'NEXT' button is also visible.

4) 알림 이름 설정 및 정책 생성



5) 설정한 사용자 이상징후 알림 확인



진단
기준

양호기준

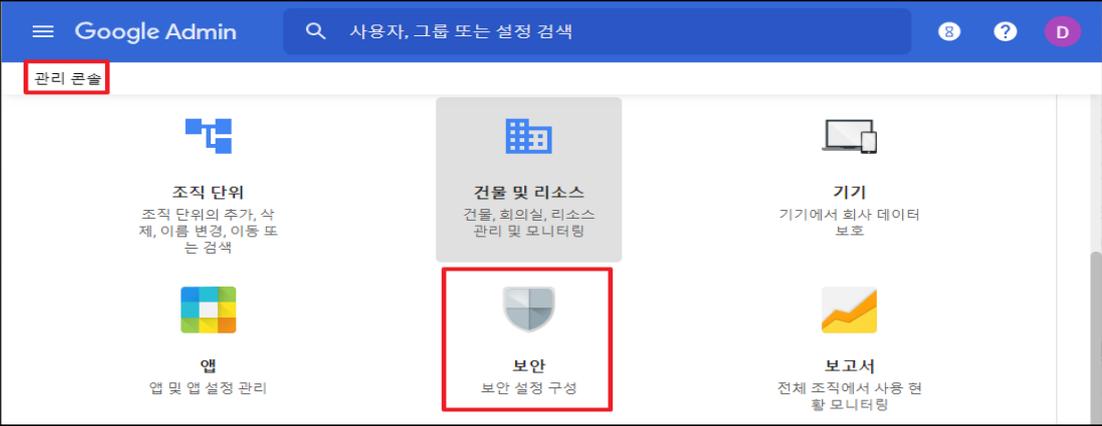
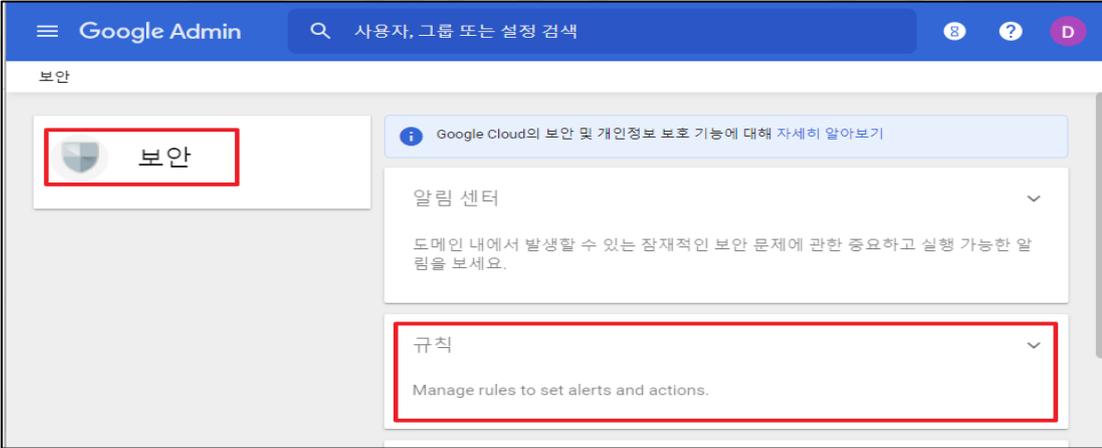
: Google 계정 사용자 이상징후에 대한 알림 설정이 되어 있을 경우

취약기준

: Google 계정 사용자 이상징후에 대한 알림 설정이 되어있지 않을 경우

비고

4.16 Cloud ID 계정 사용자 이상징후 알림 설정

분류	운영 관리	중요도	하
항목명	Cloud ID 계정 사용자 이상징후 알림 설정		
항목 설명	<p>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.</p> <p>(*) 알림이 필요한 이상징후</p> <ul style="list-style-type: none"> - 비밀번호 유출 - 사용중지된 사용자 활성화됨 - 의심스러운 로그인 - 사용자에게 관리자 권한 부여 - 사용자 사용중지됨(Google ID 알림) 		
설정 방법	<p>가. Cloud ID 사용자 이상징후 경보 설정 방법</p> <p>1) 관리 콘솔 (admin.google.com) 내 [보안] 페이지 클릭</p>  <p>2) 보안 페이지 내 [규칙] 클릭</p> 		

3) 설정하고자 하는 알림 클릭 (ex_ "사용자에게 관리자 권한 부여")

이름	상태	작업	알림	규칙 유형	최종 수정 시간
정부 지원 해킹 공격 국가 지원 해킹 공격 가능성에 대...	활성	알림 보내기	사용	시스템 정의됨	20. 10. 18. 오후 5:02
사용자가 신고한 피싱 발신자가 도메인으로 보낸 메일...	활성	-	사용	시스템 정의됨	-
사용자 비밀번호 변경됨 사용자의 비밀번호가 변경되었...	활동 안함	-	-	시스템 정의됨	-
사용자의 관리자 권한 취소됨 사용자의 관리자 권한이 취소되...	활동 안함	-	-	시스템 정의됨	-
필레이 스팸 발송으로 사용자 알... Google에서 SMTP 필레이 서비...	활성	-	사용	시스템 정의됨	-
스팸 발송 사용자 일시정지됨 Google에서 스팸과 같은 의심스...	활성	-	사용	시스템 정의됨	-
의심스러운 활동으로 사용자 알... Google에서 도용의 가능성을 감...	활성	-	사용	시스템 정의됨	-
사용자 사용중지됨(Google ID 알... Google에서 의심스러운 활동을 ...	활성	-	사용	시스템 정의됨	-
관리자가 정지한 사용자 관리자가 계정을 정지했습니다.	활동 안함	-	-	시스템 정의됨	-
사용자에게 관리자 권한 부여 사용자에게 관리자 권한이 부여...	활동 안함	-	-	시스템 정의됨	-
사용자 삭제됨 도메인에서 사용자가 삭제되었...	활동 안함	-	-	시스템 정의됨	-
TLS 실패 전송 레이어 보안(TLS)이 필요한...	활동 안함	-	-	시스템 정의됨	-
프로그램 방식으로 발생한 의심... Google에서 애플리케이션 또는 ...	활성	-	사용	시스템 정의됨	-

4) [작업] 필드 내 이메일 알림 클릭

규칙 세부정보

← 규칙

사용자에게 관리자 권한 부여
사용자에게 관리자 권한이 부여되었습니다.

규칙 수정

규칙 세부정보 및 범위

이름
사용자에게 관리자 권한 부여

설명
사용자에게 관리자 권한이 부여되었습니다.

범위
전체 도메인

조건
소스
관리자 권한

작업
이메일 알림
사용 안함

5) "이메일 알림 보내기" 체크 및 이메일 수신자 설정

× 규칙 수정

✓ 규칙 세부정보 및 범위 — ✓ 조건 — 3 작업 — 4 검토

알림

이메일 알림 보내기

모든 최고 관리자

+ 👤 이메일 수신자 추가 +

이전 취소 **다음: 검토**

6) 설정한 알림 규칙 확인 후 최종 업데이트

× 규칙 수정

✓ 규칙 세부정보 및 범위 — ✓ 조건 — ✓ 작업 — 4 검토

규칙 세부정보 및 범위

이름
사용자에게 관리자 권한 부여

설명
사용자에게 관리자 권한이 부여되었습니다.

범위
전체 도메인

조건

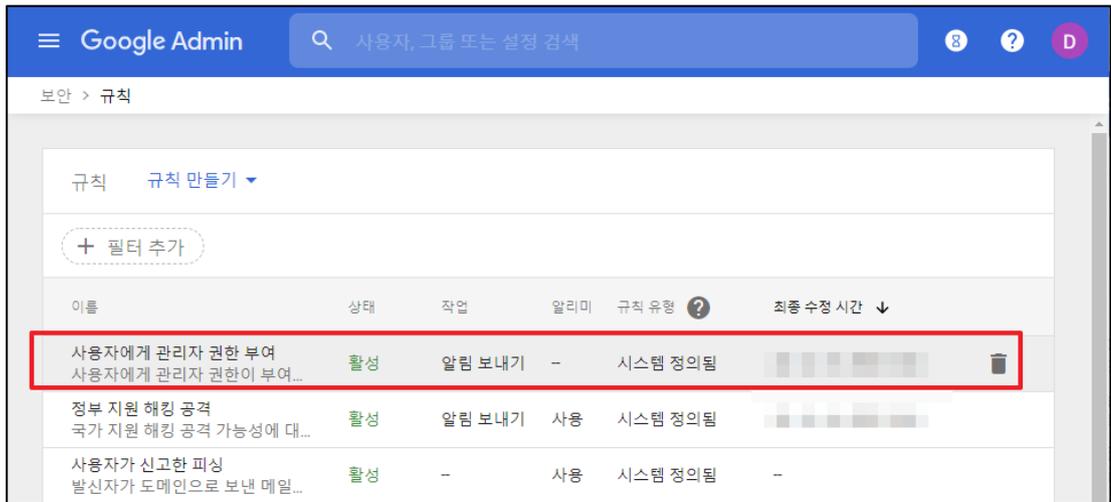
소스
관리자 권한

작업

이메일 알림
사용
이메일 알림 수신자
모든 최고 관리자

이전 취소 **규칙 업데이트**

7) 설정한 알림 규칙 확인



양호기준

: Google 계정 사용자 이상징후에 대한 알림 설정이 되어 있을 경우

취약기준

: Google 계정 사용자 이상징후에 대한 알림 설정이 되어 있지 않을 경우

비고

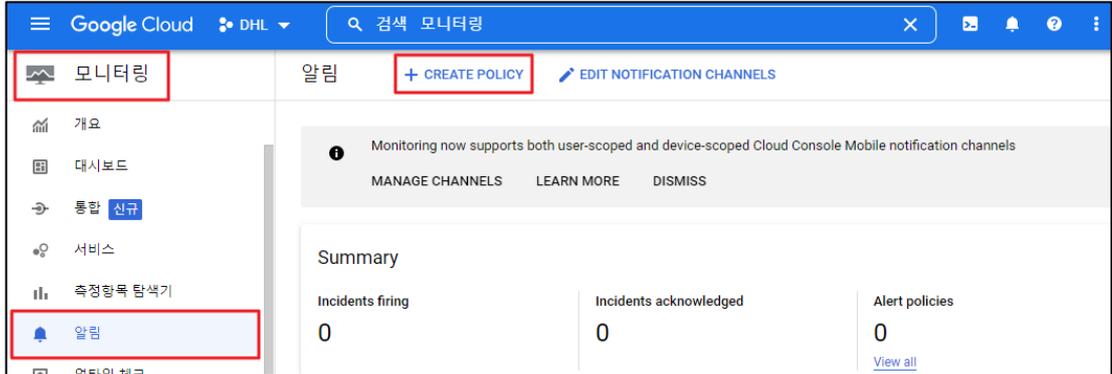
4.17 가상 리소스 이상징후 알림 설정

분류	운영 관리	중요도	중										
항목명	가상 리소스 이상징후 알림 설정												
항목 설명	<p>Cloud Monitoring은 호스팅 된 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.</p> <p>안전한 Google 계정 사용을 위해 Cloud Monitoring 서비스 내 알림 정책 설정을 통해 이용중인 Cloud 가상 리소스(Compute, Cloud SQL, Storage, Networking)에 대한 이상징후 확인이 가능합니다.</p> <p>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 측정 항목을 이용하여 임의의 알림 정책 설정도 가능합니다.</p> <p>(*) GCP 리소스 이상징후 확인을 위한 기본 정의 알림 정책 (참고)</p> <table border="1" data-bbox="272 1196 1414 2033"> <thead> <tr> <th data-bbox="272 1196 496 1245">구분</th> <th data-bbox="496 1196 1414 1245">측정 항목</th> </tr> </thead> <tbody> <tr> <td data-bbox="272 1245 496 1476">Compute</td> <td data-bbox="496 1245 1414 1476">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 data-bbox="272 1476 496 1706">Cloud SQL</td> <td data-bbox="496 1476 1414 1706">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 data-bbox="272 1706 496 1892">Storage</td> <td data-bbox="496 1706 1414 1892">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 data-bbox="272 1892 496 2033">Networking</td> <td data-bbox="496 1892 1414 2033">interconnect_attachment/ingress_bytes_count (GCP에서 온 프레미스 호스트로 전송된 바이트 수) vm_flow/rtt (TCP 연결을 통해 측정된 RTT 분포)</td> </tr> </tbody> </table>			구분	측정 항목	Compute	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	Cloud SQL	database/cpu/utilization (CPU 사용률) database/disk/utilization (디스크 사용률) database/instance_state (인스턴스 상태) database/memory/utilization (메모리 사용률) ... 등	Storage	network/received_bytes_count (수신 바이트) network/sent_bytes_count (전송 바이트) authz/object_specific_acl_mutation_count (ACL 변경 사항) ... 등	Networking	interconnect_attachment/ingress_bytes_count (GCP에서 온 프레미스 호스트로 전송된 바이트 수) vm_flow/rtt (TCP 연결을 통해 측정된 RTT 분포)
구분	측정 항목												
Compute	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												
Cloud SQL	database/cpu/utilization (CPU 사용률) database/disk/utilization (디스크 사용률) database/instance_state (인스턴스 상태) database/memory/utilization (메모리 사용률) ... 등												
Storage	network/received_bytes_count (수신 바이트) network/sent_bytes_count (전송 바이트) authz/object_specific_acl_mutation_count (ACL 변경 사항) ... 등												
Networking	interconnect_attachment/ingress_bytes_count (GCP에서 온 프레미스 호스트로 전송된 바이트 수) vm_flow/rtt (TCP 연결을 통해 측정된 RTT 분포)												

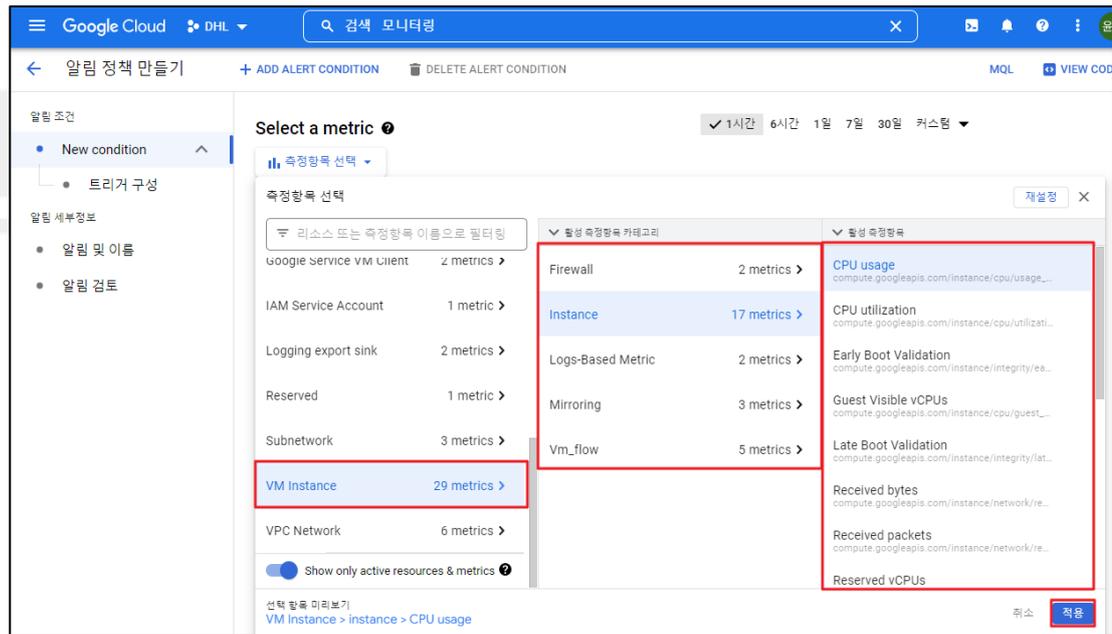
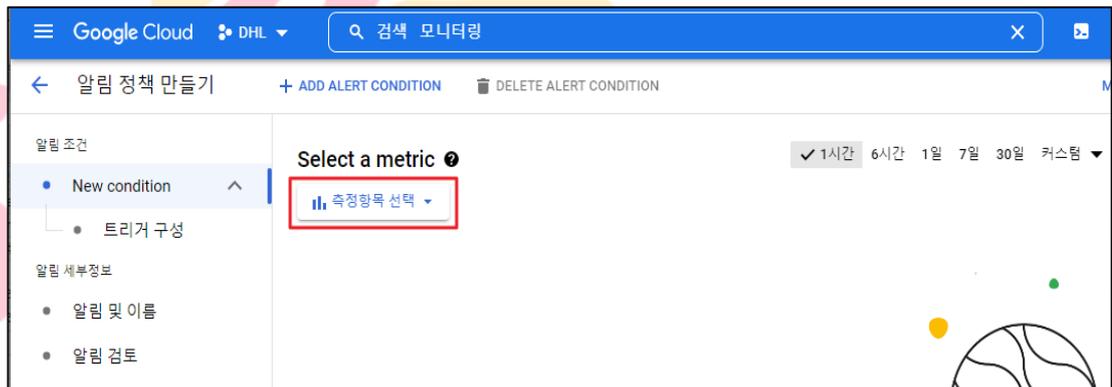
vpn_tunnel/egress_bytes_count, vpn_tunnel/ingress_bytes_count (VPN 터널을 통해 GCP에서 송·수신된 바이트 수)
... 등

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



설정
방법

3) 추가 설정 및 트리거 설정

The screenshot shows the 'Configure alert trigger' step in the Google Cloud Monitoring console. The left sidebar shows the navigation menu with '트리거 구성' (Configure trigger) selected. The main area is titled 'Configure alert trigger' and contains the following fields:

- Condition type:** Metric absence (selected), Threshold.
- Alert trigger:** A dropdown menu with '모든 시계열 위반' (All time series violations) selected.
- 트리거 부재 시간 *** (Trigger absence duration): A dropdown menu with '5분' (5 minutes) selected. Below it, the text '순환 기간이 재정의됩니다.' (Cyclic period is redefined.) is visible.
- 조건 이름 *** (Condition name): A text input field containing 'VM Instance - CPU usage'.

At the bottom of the configuration area is a 'NEXT' button. To the right, a preview of the alert policy is shown with a graph titled 'VM Instance - CPU usage' and a warning icon indicating a selected duration.

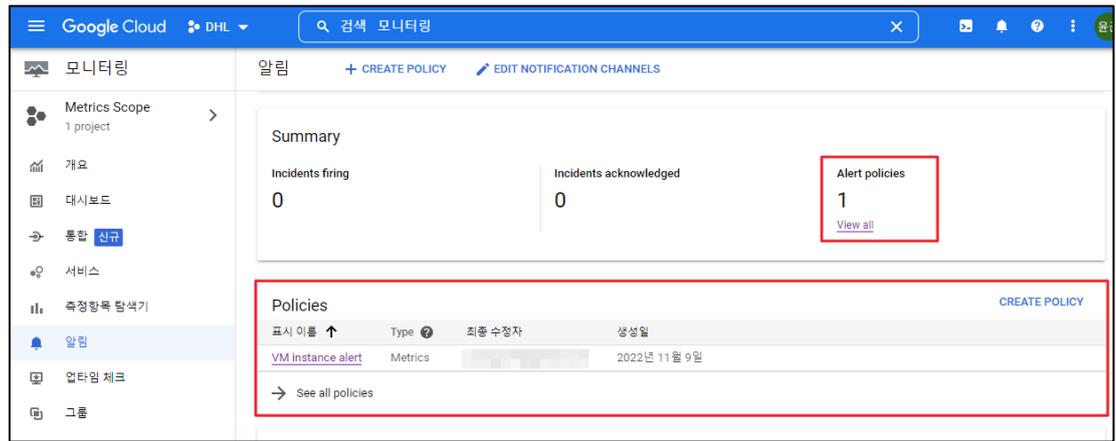
4) 알림 이름 설정 및 정책 생성

The screenshot shows the 'Name the alert policy' step in the Google Cloud Monitoring console. The left sidebar shows the navigation menu with '알림 및 이름' (Alert name) selected. The main area is titled 'Name the alert policy' and contains the following fields:

- 알림 정책 이름 *** (Alert policy name): A text input field containing 'VM instance alert'.

At the bottom of the configuration area is a 'NEXT' button. At the very bottom of the page, there are three buttons: '정책 생성' (Create policy), '의견 보내기' (Send feedback), and '취소' (Cancel). The '정책 생성' button is highlighted with a red box.

5) 설정한 가상 리소스 이상징후 알림 확인



진단
기준

양호기준

: 사용중인 GCP 리소스에 대한 경보가 설정되어 있을 경우

취약기준

: 사용중인 GCP 리소스에 대한 경보가 설정되어 있지 않을 경우

비고

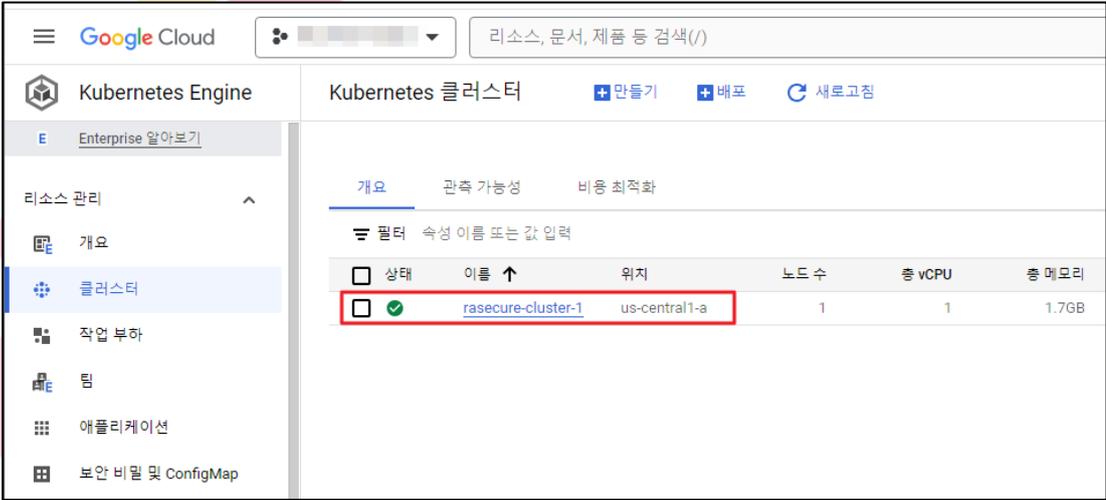
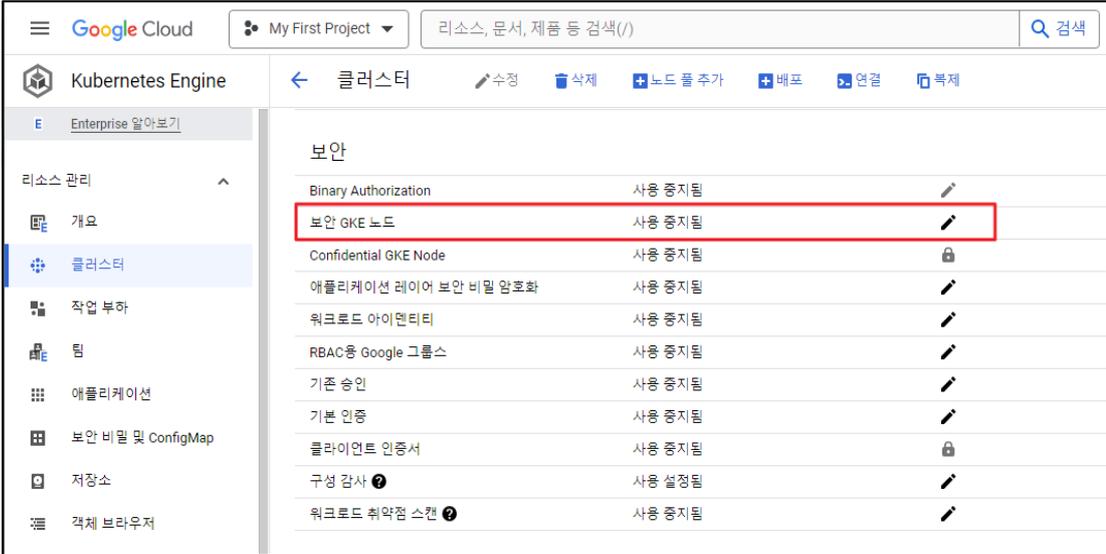


안녕을 지키는 기술

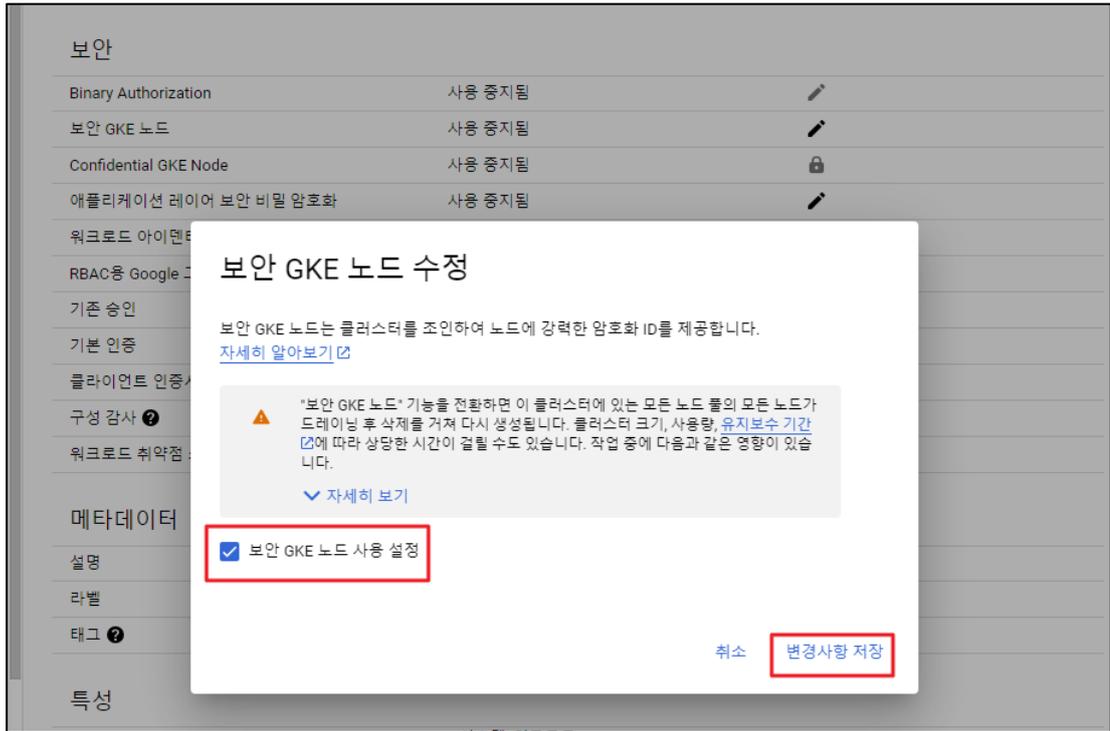
4.18 백업 사용 여부

분류	운영 관리	중요도	중
항목명	백업 사용 여부		
항목 설명	<p>운영중인 클라우드 리소스에 대한 시스템 충돌, 장애 발생, 인적 재해 등 기업의 사업 연속성을 해치는 모든 상황에 대비하기 위해 백업 서비스를 구성해야 데이터를 안전하게 보관할 수 있습니다. 이에 보안 담당자 및 관리자는 클라우드 리소스에 대한 백업을 설정하여 데이터 손실을 방지할 수 있도록 정책을 수립하고 관리하여야 합니다.</p>		
설정 방법	<p>가. 백업 및 복구 절차 수립</p> <p>1) 백업 및 복구 절차 수립, 담당자 지정</p> <ul style="list-style-type: none"> - 백업대상(서버 이미지, DB 데이터, 보안로그 등) 선정 - 백업대상별 백업 주기 및 보존기한 정의 - 백업 담당자 및 책임자 지정 - 백업방법 및 절차: 백업시스템 활용, 매뉴얼 방식 등(백업매체 관리 포함) - 복구절차 - 백업이력관리 (백업 관리 대장) - 백업 소산에 대한 물리적·지역적 사항 고려 - 백업 사이트 구축 및 운영 <p>※ 클라우드서비스 보안인증제도(laaS) 평가기준 해설서의 "6.2 서비스 가용성" 항목 참고</p>		
진단 기준	<p>양호기준 : 클라우드 리소스 백업 정책이 존재하는 경우</p> <p>취약기준 : 클라우드 리소스 백업 정책이 존재하지 않는 경우</p>		
비고			

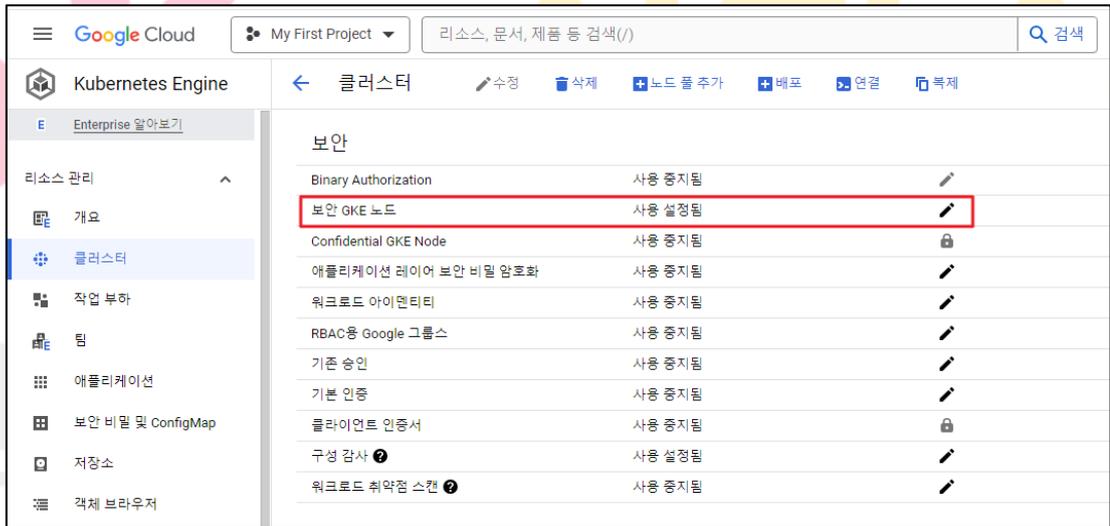
4.19 보안 GKE 노드 설정

분류	운영 관리	중요도	중
항목명	보안 GKE 노드 설정		
항목 설명	<p>보안 GKE 노드는 Compute Engine 보안 VM 위에 구축되며 보안 GKE 노드가 없으면 공격자가 Pod의 취약점을 악용하여 부트스트랩 사용자 인증 정보를 유출하고 Cluster에 있는 노드로 가장하여 Cluster 보안 비밀에 액세스할 수 있습니다.</p> <p>※ 보안 GKE 노드는 GKE 버전 1.13.6-gke.0 이상 조건에서 사용이 가능하며 GKE Autopilot Cluster의 경우 보안 GKE 노드 기능이 기본적으로 사용 설정되어 있으며 재정의될 수 없습니다.</p>		
설정 방법	<p>가. 보안 GKE 노드 설정</p> <p>1) Kubernetes Engine 내 Cluster 리소스 조회</p>  <p>2) 보안 GKE 노드 설정 확인 및 편집 (사용중지)</p> 		

3) 보안 GKE 노드 사용 설정



4) 보안 GKE 노드 설정 활성화 확인



진단
기준

양호기준

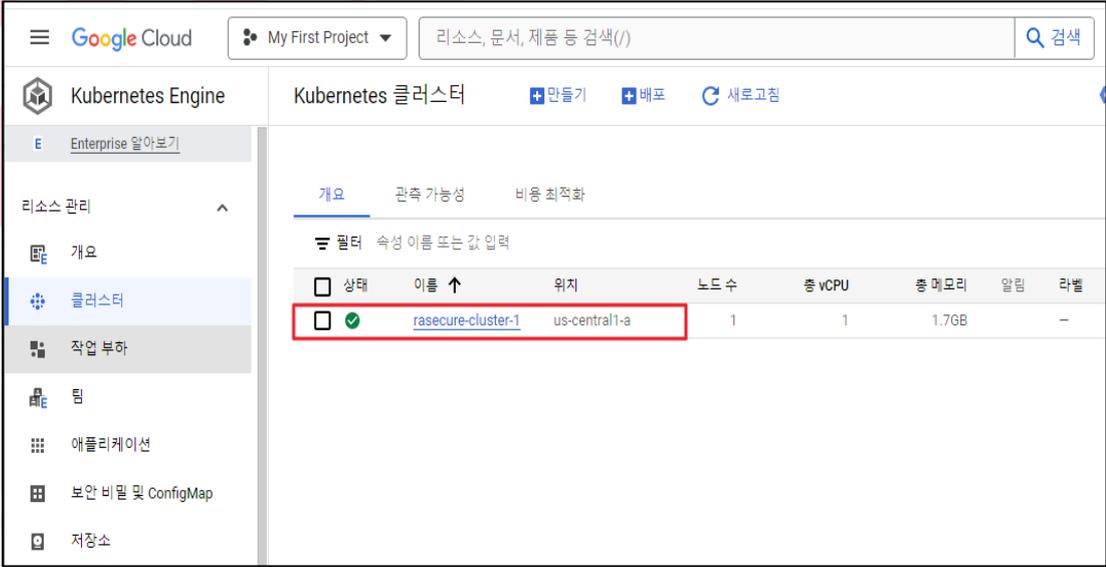
: 보안 GKE 노드 설정이 적용 되어있는 경우

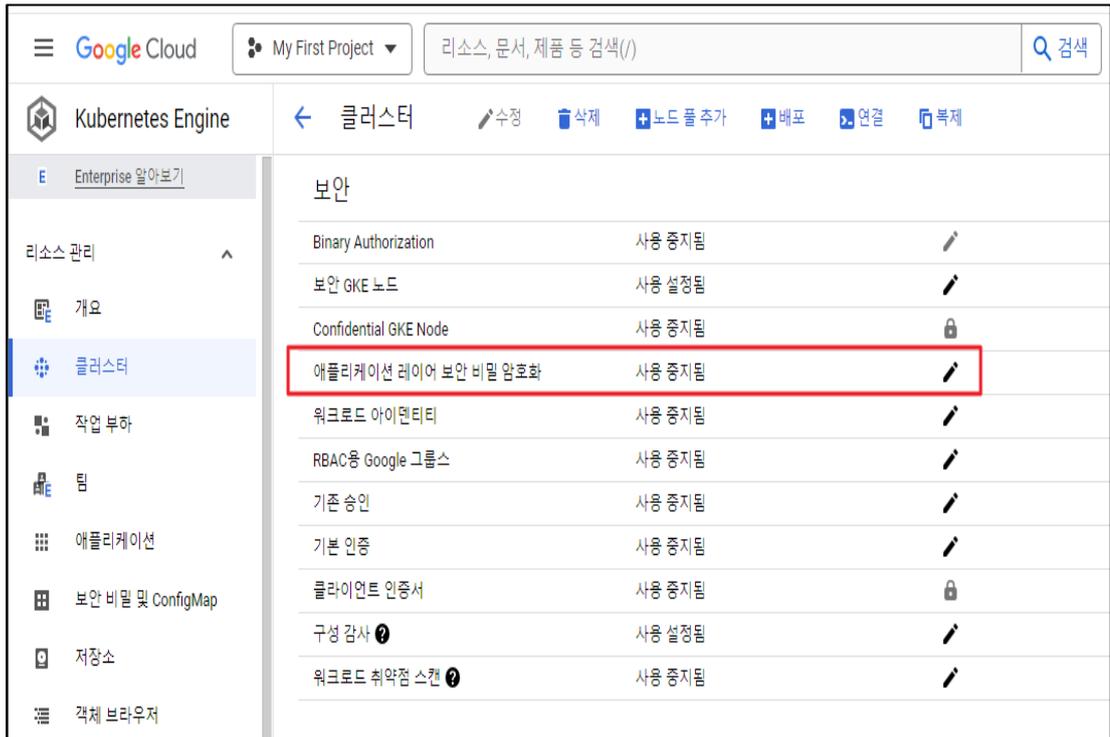
취약기준

: 보안 GKE 노드 설정이 적용 되어있지 않은 경우

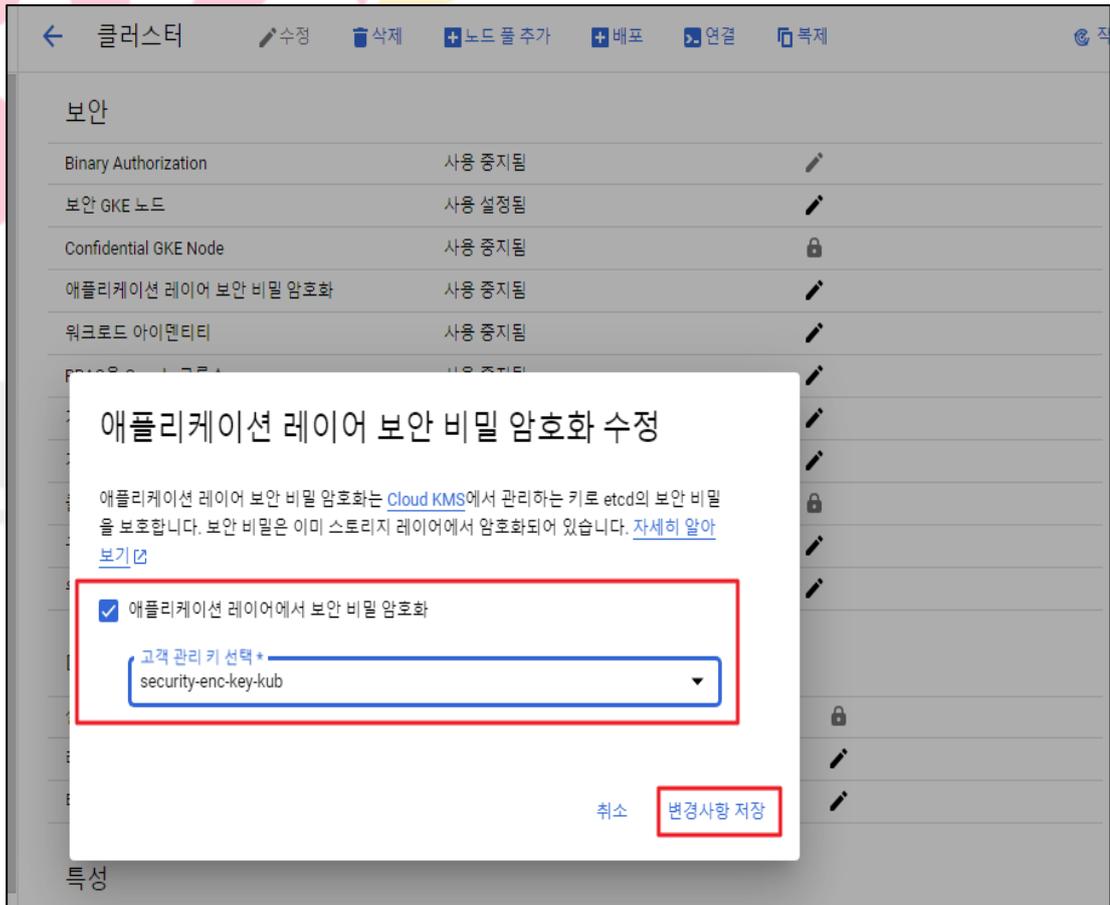
비고

4.20 애플리케이션 레이어 보안 비밀 암호화 설정

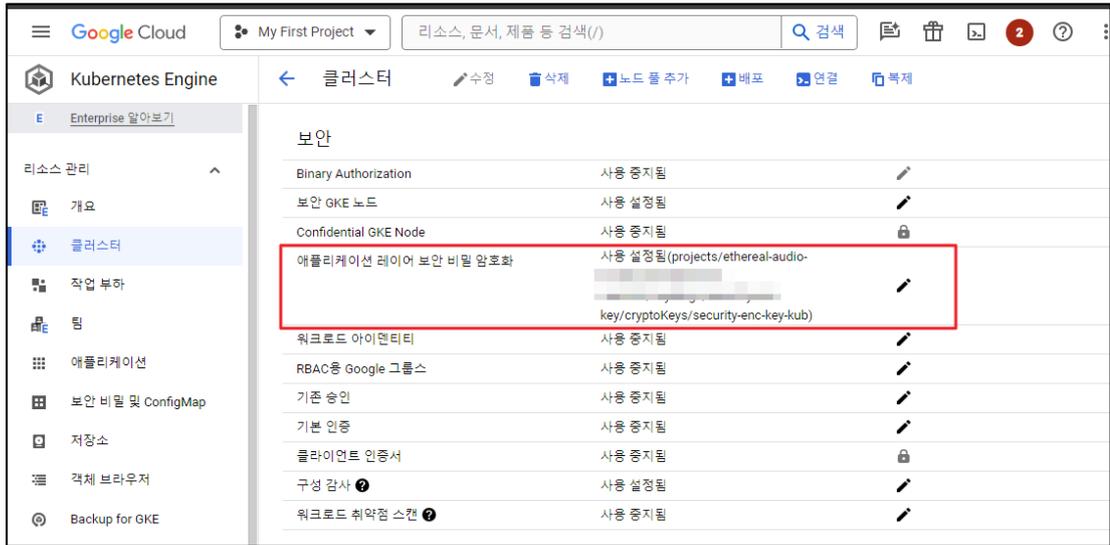
분류	운영 관리	중요도	중
항목명	애플리케이션 레이어 보안 비밀 암호화 설정		
항목 설명	<p>기본적으로 Google Kubernetes Engine(GKE)은 사용자가 추가 작업을 수행하지 않아도 보안 비밀을 포함하여 비활성 상태로 저장된 고객 콘텐츠를 암호화합니다.</p> <p>애플리케이션 레이어 보안 비밀 암호화는 etcd에 저장되는 보안 비밀과 같이 민감한 정보를 위한 추가 보안 레이어를 제공하며 Cloud KMS로 관리되는 키를 사용해 애플리케이션 레이어에서 데이터를 암호화할 수 있습니다. 이 설정은 etcd의 오프라인 사본에 액세스하는 공격자로부터 방어할 수 있습니다.</p> <p>애플리케이션 레이어 보안 비밀 암호화를 사용하려면 먼저 Cloud KMS 키를 만들고 이 키에 대한 액세스 권한을 GKE 서비스 계정에 부여해야 합니다. 추가적으로 지연 시간을 줄이고 리소스가 여러 장애 도메인에 분산된 서비스에 의존하는 경우를 방지하려면 키가 Cluster와 동일한 위치에 있어야 합니다.</p>		
설정 방법	<p>가. 애플리케이션 레이어 보안 비밀 암호화 설정</p> <p>1) Kubernetes Engine 내 Cluster 리소스 조회</p>  <p>2) 애플리케이션 레이어 보안 비밀 암호화 설정 확인 및 편집</p>		



3) KMS 내 키 선택 후 애플리케이션 레이어 보안 비밀 암호화 활성화 설정 적용



4) 애플리케이션 레이어 보안 비밀 암호화 활성화 설정 적용 확인



진단
기준

양호기준

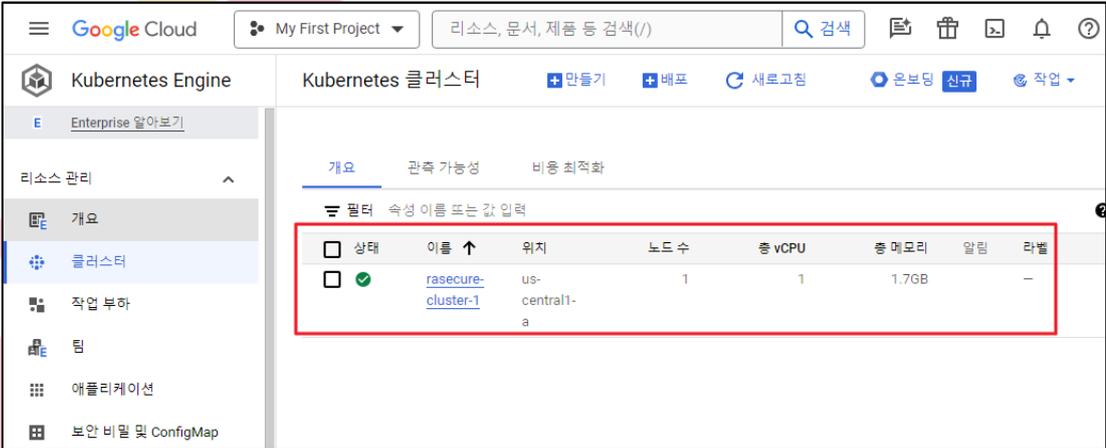
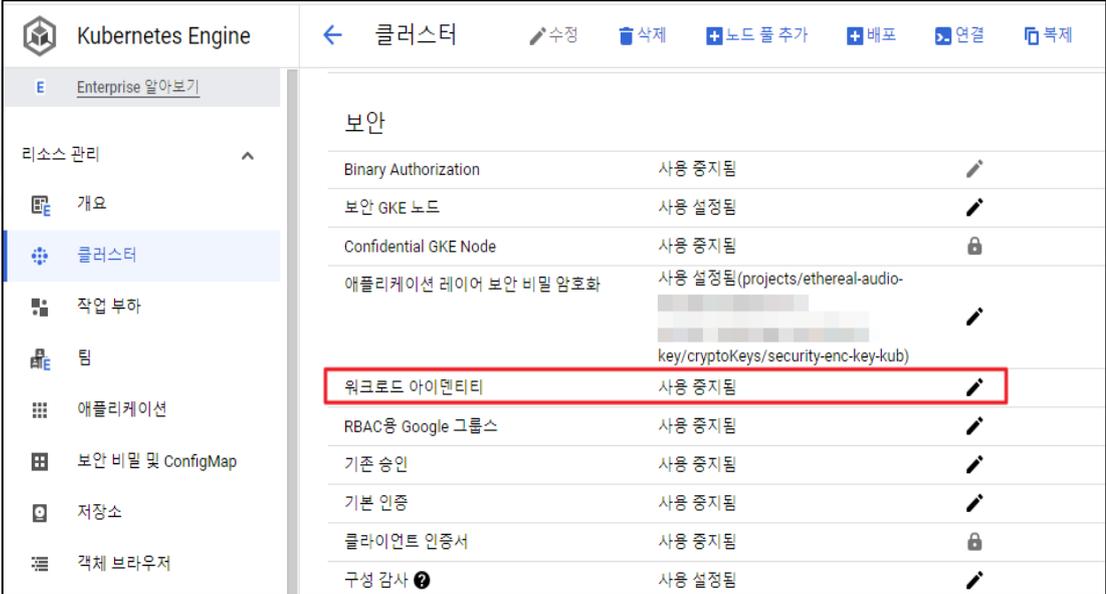
: 애플리케이션 레이어 보안 비밀 암호화 설정이 적용 되어있는 경우

취약기준

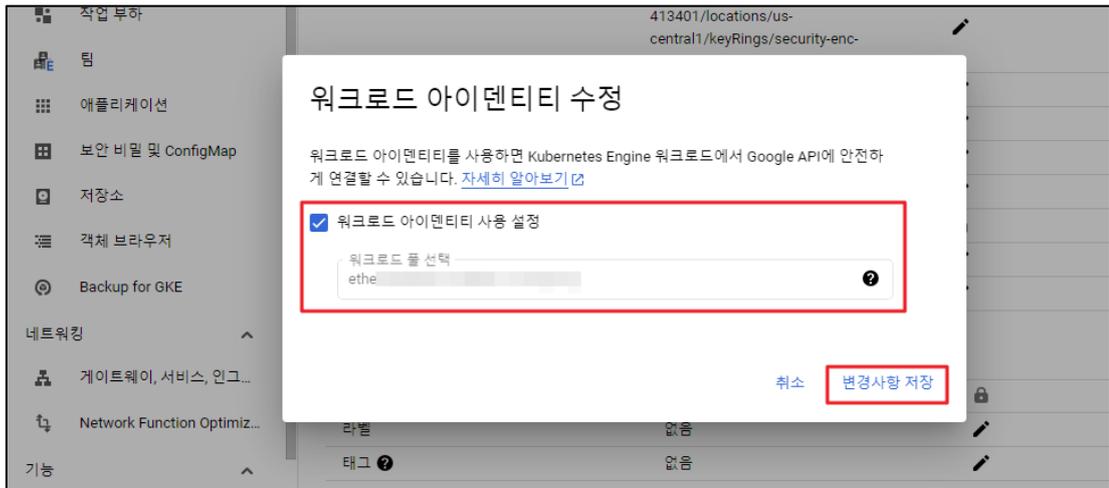
: 애플리케이션 레이어 보안 비밀 암호화 설정이 적용 되어있지 않은 경우

비고

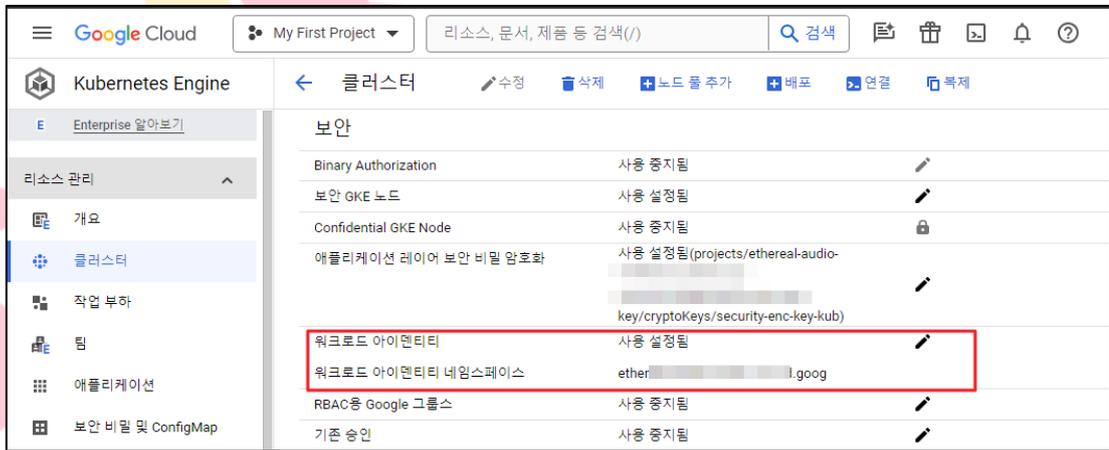
4.21 워크로드 아이덴티티 설정

분류	운영 관리	중요도	중
항목명	워크로드 아이덴티티 설정		
항목 설명	<p>GKE용 워크로드 아이덴티티 제휴는 GKE Cluster의 워크로드가 Google Cloud 서비스에 액세스하기 위해 Identity and Access Management(IAM) 서비스 계정을 사용할 수 있게 해주며 서비스 계정 키를 사용하지 않고도 온프레미스 또는 멀티 클라우드 워크로드에 Google Cloud 리소스에 대한 액세스 권한을 부여할 수 있습니다. 애플리케이션이 Google Cloud 리소스에 액세스하려면 서비스 계정 키를 사용하나 서비스 계정 키는 강력한 사용자 인증 정보이며 제대로 관리하지 않을 경우 보안상 위험할 수 있습니다. 그렇기에 워크로드 아이덴티티 제휴 ID를 사용하길 권장합니다.</p>		
설정 방법	<p>가. 워크로드 아이덴티티 설정</p> <p>1) Kubernetes Engine 내 Cluster 리소스 조회</p>  <p>2) 워크로드 아이덴티티 사용 설정 확인 (사용 중지됨)</p> 		

3) 워크로드 아이덴티티 사용 활성화 시도



4) 워크로드 아이덴티티 설정 적용 확인



진단
기준

양호기준

: Cluster 내 워크로드 아이덴티티 설정이 적용된 경우

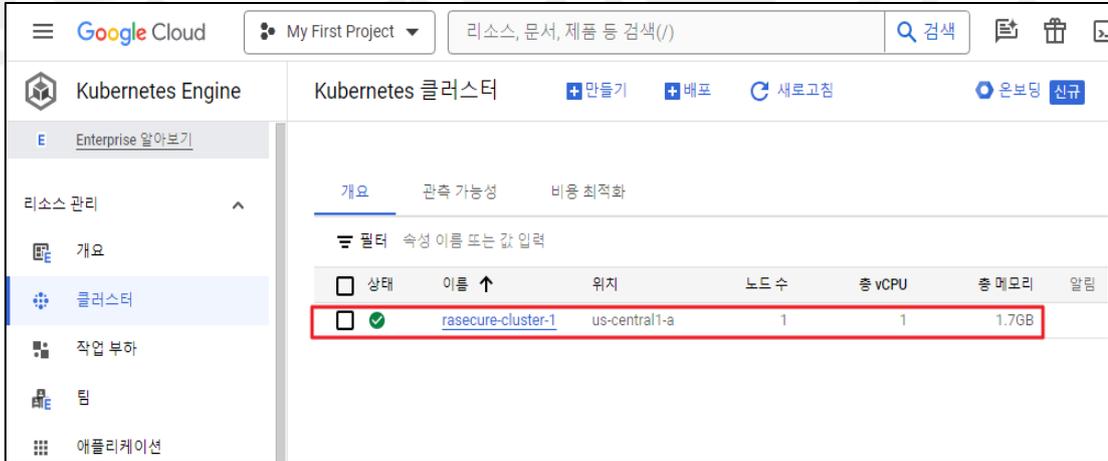
취약기준

: Cluster 내 워크로드 아이덴티티 설정이 적용되지 않은 경우

비고

※ Autopilot Cluster 는 기본적으로 GKE 용 워크로드 아이덴티티 제휴를 사용 설정함

4.22 워크로드 취약점 스캔 설정

분류	운영 관리	중요도	중									
항목명	보안 GKE 노드 설정											
항목 설명	<p>워크로드 취약점 스캔은 컨테이너 이미지 및 특정 언어 패키지에서 알려진 취약점을 자동으로 스캔하고 GKE에서 취약점이 감지되면 보안 상황 대시보드에 문제 세부정보가 표시되고 취약점 해결을 위한 실행 가능한 해결안을 제시해주는 서비스입니다.</p> <p>워크로드 취약점 스캔은 컨테이너 운영체제(OS) 취약점 스캔과 언어 패키지 취약점 스캔을 지원하며 컨테이너 OS 취약점 스캔은 NIST와 같은 공개 CVE 데이터베이스의 취약점 데이터를 사용해 GKE Cluster에서 실행되는 컨테이너 이미지를 지속적으로 스캔합니다. 언어 패키지 취약점 스캔은 GitHub Advisory Database와 같은 공개 소스에서 취약점 데이터를 활용해 Go 또는 Maven 패키지와 같은 언어 패키지에서 컨테이너의 알려진 취약점을 지속적으로 스캔합니다.</p> <p>※ GKE 취약점 스캔 사용 설정 옵션</p> <table border="1" data-bbox="276 907 1428 1373"> <thead> <tr> <th>구분</th> <th>제공 기능</th> <th>GKE 버전 요구사항</th> </tr> </thead> <tbody> <tr> <td>기본 (standard)</td> <td>- 컨테이너 OS 취약점 스캔</td> <td>- 버전 1.23.5-gke.700 이상 필요 - 기본적으로 버전 1.27 이상을 실행하는 Autopilot Cluster에서 사용 설정됩니다. - Standard Cluster에서 기본적으로 사용 중지됩니다.</td> </tr> <tr> <td>고급 (Advanced vulnerability insights)</td> <td>- 컨테이너 OS 취약점 스캔 - 언어 패키지 취약점 스캔</td> <td>- 버전 1.27 이상 필요 - Autopilot 및 Standard에서 기본적으로 사용 중지됩니다.</td> </tr> </tbody> </table>			구분	제공 기능	GKE 버전 요구사항	기본 (standard)	- 컨테이너 OS 취약점 스캔	- 버전 1.23.5-gke.700 이상 필요 - 기본적으로 버전 1.27 이상을 실행하는 Autopilot Cluster에서 사용 설정됩니다. - Standard Cluster에서 기본적으로 사용 중지됩니다.	고급 (Advanced vulnerability insights)	- 컨테이너 OS 취약점 스캔 - 언어 패키지 취약점 스캔	- 버전 1.27 이상 필요 - Autopilot 및 Standard에서 기본적으로 사용 중지됩니다.
구분	제공 기능	GKE 버전 요구사항										
기본 (standard)	- 컨테이너 OS 취약점 스캔	- 버전 1.23.5-gke.700 이상 필요 - 기본적으로 버전 1.27 이상을 실행하는 Autopilot Cluster에서 사용 설정됩니다. - Standard Cluster에서 기본적으로 사용 중지됩니다.										
고급 (Advanced vulnerability insights)	- 컨테이너 OS 취약점 스캔 - 언어 패키지 취약점 스캔	- 버전 1.27 이상 필요 - Autopilot 및 Standard에서 기본적으로 사용 중지됩니다.										
설정 방법	<p>가. 워크로드 취약점 스캔 설정</p> <p>1) Kubernetes Engine 내 Cluster 리소스 조회</p> 											

2) 워크로드 취약점 스캔 설정 확인 (사용 중지됨)

The screenshot shows the Google Cloud console interface for a Kubernetes Engine cluster. The left sidebar contains navigation options like '리소스 관리', '개요', '클러스터', '작업 부하', '팀', '애플리케이션', '보안 비밀 및 ConfigMap', '저장소', '객체 브라우저', and 'Backup for GKE'. The main content area is titled '보안' (Security) and lists various security features. The '워크로드 취약점 스캔' (Workload Vulnerability Audit) feature is highlighted with a red box and shows a status of '사용 중지됨' (Disabled).

기능	상태	액션
Binary Authorization	사용 중지됨	✎
보안 GKE 노드	사용 설정됨	✎
Confidential GKE Node	사용 중지됨	🔒
애플리케이션 레이어 보안 비밀 암호화	사용 설정됨 (projects/ethereal-audio-...)	✎
워크로드 아이덴티티	사용 설정됨	✎
워크로드 아이덴티티 네임스페이스		
RBAC용 Google 그룹스	사용 중지됨	✎
기존 승인	사용 중지됨	✎
기본 인증	사용 중지됨	✎
클라이언트 인증서	사용 중지됨	🔒
구성 감사	사용 설정됨	✎
워크로드 취약점 스캔	사용 중지됨	✎

3) 워크로드 취약점 스캔 설정 (기본)

The screenshot shows the '워크로드 취약점 스캔 수정' (Workload Vulnerability Audit Settings) dialog box. The dialog contains the following text: 'Enabling workload vulnerability audit shows you results for container runtime that manages the lifecycle of your containerized workloads. For example, CVEs that affect the container runtime.' Below this, there are two radio button options: '기본' (Basic) and '고급' (Advanced). The '기본' option is selected and highlighted with a red box. The '고급' option is also highlighted with a red box. At the bottom right, the '변경사항 저장' (Save Changes) button is highlighted with a red box.

워크로드 취약점 스캔 수정

Enabling workload vulnerability audit shows you results for container runtime that manages the lifecycle of your containerized workloads. For example, CVEs that affect the container runtime.

- 워크로드 취약점 스캔 사용 설정
 - 기본**
워크로드 OS 취약점 스캔입니다. 사용하려면 Kubernetes 버전 1.23 이상이 필요합니다.
 - 고급**
워크로드 OS 및 언어 패키지 취약점 스캔을 제공합니다. 사용하려면 Kubernetes 버전 1.27 이상이 필요합니다.

취소 **변경사항 저장**

4) 워크로드 취약점 스캔 설정 적용 확인

The screenshot shows the Google Cloud console for a Kubernetes Engine cluster. The left sidebar contains navigation options like 'Enterprise 알아보기', '리소스 관리', '개요', '클러스터', '작업 부하', '팀', '애플리케이션', '보안 비밀 및 ConfigMap', '저장소', '객체 브라우저', 'Backup for GKE', and '네트워크'. The main content area is titled '보안' (Security) and lists various security settings. The '워크로드 취약점 스캔' (Workload Vulnerability Scans) setting is highlighted with a red box and is currently set to '기본' (Basic).

설정명	현재 상태	수정
Binary Authorization	사용 중지됨	✎
보안 GKE 노드	사용 설정됨	✎
Confidential GKE Node	사용 중지됨	🔒
애플리케이션 레이어 보안 비밀 암호화	사용 설정됨 (projects/ethereal-audio-...)	✎
워크로드 아이덴티티	사용 설정됨	✎
워크로드 아이덴티티 네임스페이스	...	
RBAC용 Google 그룹스	사용 중지됨	✎
기존 승인	사용 중지됨	✎
기본 인증	사용 중지됨	✎
클라이언트 인증서	사용 중지됨	🔒
구성 감사	사용 설정됨	✎
워크로드 취약점 스캔	기본	✎

나. 워크로드 취약점 스캔 설정 여부에 따른 결과 확인

1) 워크로드 취약점 스캔 미설정 시 보안 상태 확인

The screenshot shows the 'GKE Security Posture' dashboard in the Google Cloud console. The dashboard includes three donut charts: '문제' (28 issues), '유형' (28 issues), and '클러스터' (1 cluster). Below the charts, there are sections for '워크로드 구성' (Workload Configuration) and '워크로드 OS 취약점' (Workload OS Vulnerabilities). The '보안 상태' (Security Status) section is highlighted with a red box, showing 28 issues and 1 cluster with GKE Security Posture.

문제 28 문제

- 0 심각
- 24 높음
- 4 보통
- 0 낮음

유형 28 문제

- 구성 2개
- 보안 개시판 26개
- 공급망 0개
- 취약점 0개

클러스터 1 GKE 클러스터

워크로드 OS 취약점

- 0 심각
- 0 높음
- 0 보통
- 0 낮음

취약점 스캔에 포함될 클러스터를 선택하세요.

클러스터 선택

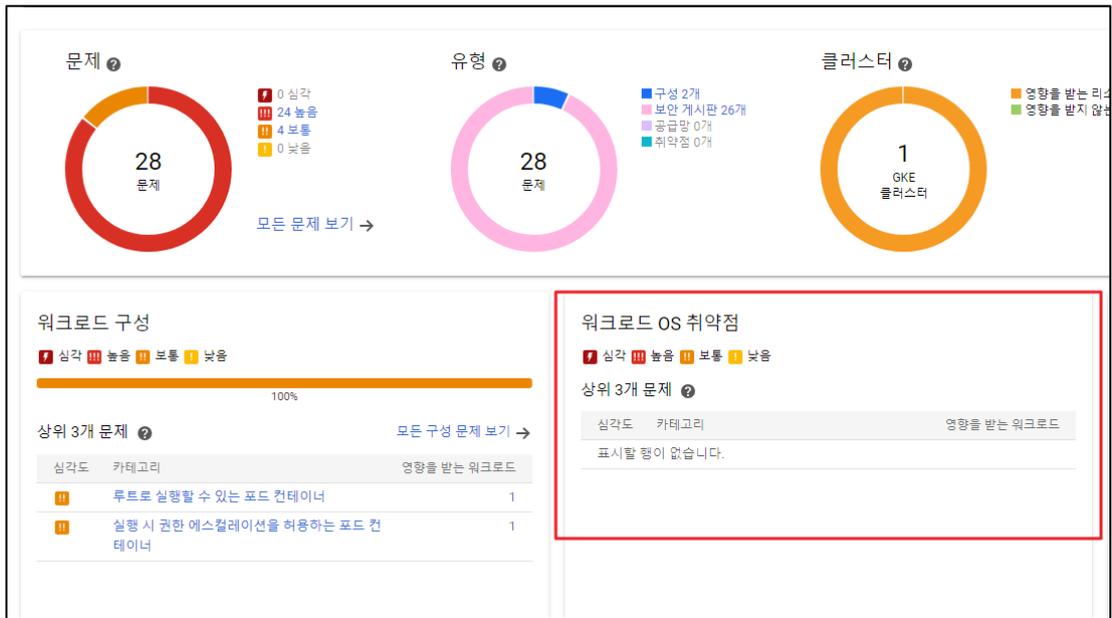
워크로드 구성

100%

상위 3개 문제

심각도	카테고리	영향을 받는 워크로드
높음	루트로 실행할 수 있는 코드 컨테이너	1
높음	실행 시 권한 에스컬레이션을 허용하는 코드 컨테이너	1

2) 워크로드 취약점 스캔 설정 후 보안 상태 확인



진단 기준

양호기준

: Cluster 내 워크로드 취약점 스캔 설정이 적용된 경우

취약기준

: Cluster 내 워크로드 취약점 스캔 설정이 적용되지 않은 경우

비고

안녕을 지키는 기술

4.23 GKE Cluster 로깅 설정

분류	운영 관리	중요도	중
-----------	-------	------------	---

항목명	GKE Cluster 로깅 설정		
------------	-------------------	--	--

GKE Cluster 생성 시 Cloud Logging, Cloud Monitoring, Google Cloud Managed Service for Prometheus에 시스템 로그 및 측정 항목(CPU, 메모리, 오류 등)들이 전송되며, Cluster에서 전송된 로그 및 측정 항목을 제어할 수 있습니다.

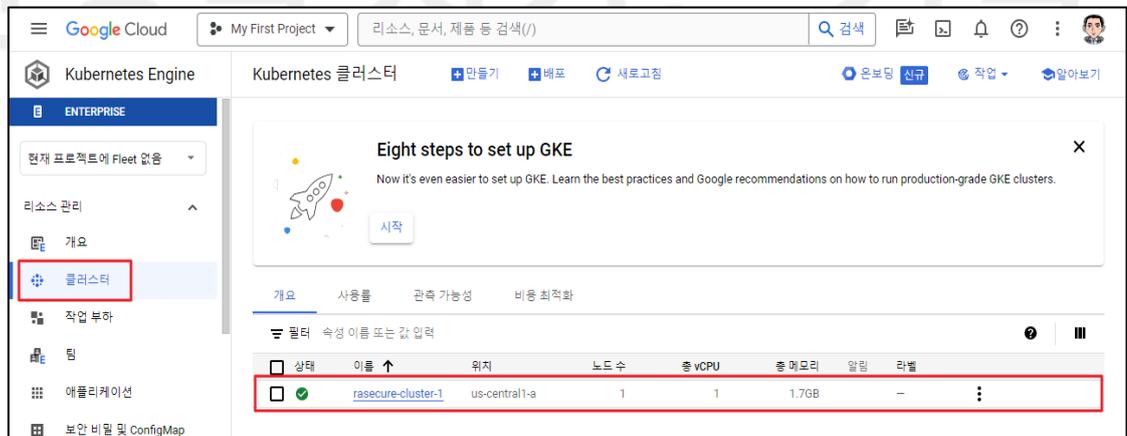
Kubernetes Engine의 [Cluster] 메뉴를 통해 생성된 Cluster를 선택하여 로깅 정책 설정이 가능하고, 아래와 같이 기본적으로 정의되어 있는 정책을 이용하여 Cluster 관련 로그를 수집 및 확인할 수 있습니다.

(*) GKE Cluster 로그 수집 유형 (참고)

구분	내용
시스템(기본)	네임스페이스(kube-system, istio-system, knative-serving, gke-system, config-management-system)에서 실행되는 모든 포드 docker/containerd 런타임, kubelet, kubelet-monitor, node-problem-detector, kube-container-runtime-monitor 등 컨테이너화되지 않은 키 서비스 VM 인스턴스 메타데이터 serial-port-logging-enable이 true로 설정된 경우 노드의 직렬 포트 출력. 또한 Kubernetes 이벤트를 수집
애플리케이션	사용자 노드에서 실행되는 비시스템 컨테이너로 생성되는 모든 로그
API 서버	Kubernetes API 서버(kube-apiserver)에서 생성된 모든 로그
스케줄러	Kubernetes 스케줄러(kube-scheduler)에서 생성된 모든 로그
컨트롤러 관리자	Kubernetes 컨트롤러 관리자(kube-controller-manager)에서 생성된 모든 로그

가. GKE Cluster 로깅 설정 방법

1) GKE Cluster 접근



2) 특성 메뉴 확인

Google Cloud My First Project 리소스, 문서, 제품 등 검색(/) 검색

Kubernetes Engine 클러스터 수정 삭제 +노드 풀 추가 +백포 연결 복제 작업

ENTERPRISE

현재 프로젝트에 Fleet 없음

리소스 관리

개요

클러스터

작업 부하

팀

애플리케이션

보안 비밀 및 ConfigMap

워크로드 취약점 스캔 사용 중지됨

메타데이터

설명	없음	🔒
라벨	없음	✎
태그	없음	✎

특성

로깅	시스템	✎
	View Logs	
Cloud Monitoring	시스템	✎
	GKE 대시보드 보기	
Prometheus용 관리형 서비스	사용 설정됨	✎
Cloud TPU	사용 중지됨	✎

3) 로깅 설정 확인

Google Cloud My First Project 리소스, 문서, 제품 등 검색(/) 검색

Kubernetes Engine 클러스터 수정 삭제 +노드 풀 추가 +백포 연결 복제 작업

ENTERPRISE

현재 프로젝트에 Fleet 없음

리소스 관리

개요

클러스터

작업 부하

팀

애플리케이션

보안 비밀 및 ConfigMap

저장소

객체 브라우저

Backup for GKE

리소스 관리

Marketplace

워크로드 취약점 스캔 사용 중지됨

메타데이터

설명

라벨

태그

특성

로깅

Cloud M

Prometh

Cloud TP

Kuberne

비용 할당

GKE 사용

GKE용 백업

구성 커넥터

Compute Eng

이미지 스트리

Logging 수정

Logging은 애플리케이션 및 GKE 인프라에서 내보낸 로그를 수집하는 Google Kubernetes Engine(GKE) 기능이 있습니다. [자세히 알아보기](#)

로깅 사용 설정
애플리케이션 및 GKE 인프라에서 내보낸 로그를 수집합니다. [각각의 설정 정보를 참조하십시오.](#) [자세히 알아보기](#)

구성요소

- 모두 선택
- 시스템
- 워크로드
- 제어 영역
 - API 서버
 - 스케줄러
 - 컨트롤러 관리자

나. GKE Cluster 로그 저장 확인

1) GKE Cluster 로그 탐색기 접근

Google Cloud My First Project 리소스, 문서, 제품 등 검색(/) 검색

Kubernetes Engine 클러스터 수정 삭제 +노드 풀 추가 +백포 연결 복제 작업

ENTERPRISE

현재 프로젝트에 Fleet 없음

리소스 관리

개요

클러스터

작업 부하

팀

애플리케이션

보안 비밀 및 ConfigMap

워크로드 취약점 스캔 사용 중지됨

메타데이터

설명	없음	🔒
라벨	없음	✎
태그	없음	✎

특성

로깅	시스템	✎
	View Logs	
Cloud Monitoring	시스템	✎
	GKE 대시보드 보기	
Prometheus용 관리형 서비스	사용 설정됨	✎
Cloud TPU	사용 중지됨	✎

2) 유형 별 로그 확인

The screenshot displays the Google Cloud Logging console for 'My First Project'. The search criteria are: Resource Type: Kubernetes 클러스터 +2, Severity: 기본값 (25,181), Location: us-central1-a. The log results show a series of 'leases.update' events from the 'rascure-cluster-1' namespace. A notification at the top indicates that 80% of results are truncated.

양호기준

진단 기준 : GKE Cluster 로깅을 설정하여 유형 별 로그를 기록하고 있는 경우

취약기준

: GKE Cluster의 유형 별 로그를 기록하고 있지 않는 경우

비고

안녕을 지키는 기술

4.24 GKE Cluster 모니터링 설정

분류	운영 관리	중요도	중
-----------	-------	------------	---

항목명	GKE Cluster 모니터링 설정		
------------	---------------------	--	--

GKE Cluster 생성 시 Cloud Logging, Cloud Monitoring, Google Cloud Managed Service for Prometheus에 시스템 로그 및 측정 항목(CPU, 메모리, 오류 등)들이 전송되며, Cluster에서 전송된 로그 및 측정 항목을 제어할 수 있습니다.

Kubernetes Engine의 [Cluster] 메뉴를 통해 생성된 Cluster를 선택하여 Cloud Monitoring 정책 설정이 가능하고, 아래와 같이 기본적으로 정의되어 있는 정책을 이용하여 Cluster 측정 항목(CPU, 메모리, 오류 등)을 확인할 수 있습니다.

(*) GKE Cluster 모니터링 유형 (참고)

구분	내용
시스템(기본)	CPU, 메모리, 네트워크 등 Cluster 관련 시스템 로그
API 서버	API 서버 측정 항목(지연시간, 트래픽, 오류율, 포화도)
스케줄러	스케줄러 측정 항목(지연시간, 리소스 문제)
컨트롤러 관리자	node_collector_evictions_total (NodeController의 현재 인스턴스가 시작되고 제거한 노드 수)
스토리지	스토리지 관련 정보
포드	포드 동작 및 오류 관련 정보
배포	개별 배포 관련 정보
StatefulSet	애플리케이션의 포드 집합 배포 및 확장을 관리하는 컨트롤러
DaemonSet	일부 노드 집합이 포드 사본을 실행하도록 보장하는 컨트롤러
수평형 포드 자동 확장 처리	CPU 또는 메모리 사용률과 같은 일부 측정항목에 따라 배포 또는 StatefulSet와 같은 워크로드의 포드 수를 주기적으로 변경하는 컨트롤러

가. GKE Cluster 모니터링 설정 방법

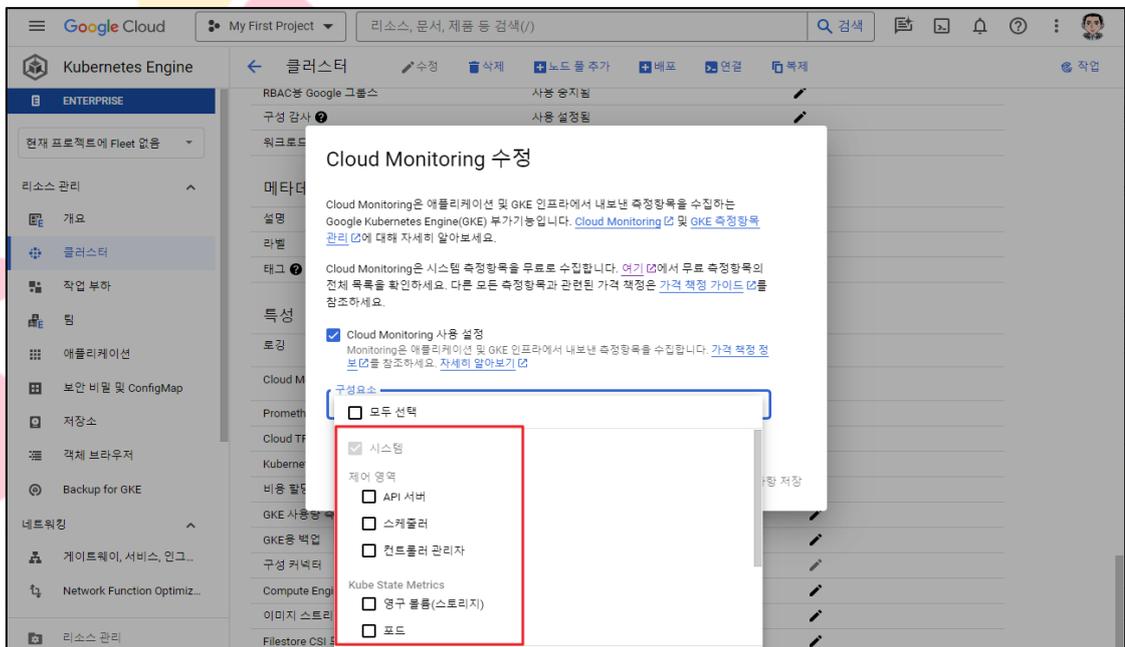
1) GKE Cluster 접근



2) 특성 메뉴 확인



3) 모니터링 설정 확인



나. GKE Cluster 모니터링 알림 확인

1) GKE Cluster 모니터링 대시보드 접근



2) 유형 별 알림 확인

The screenshot shows the Google Cloud Monitoring interface for a GKE cluster. The left sidebar has '모니터링' (Monitoring) and '대시보드' (Dashboard) highlighted. The main area displays the '타입라인' (Timeline) view for alerts. Below this, there are two tables: '클러스터' (Cluster) and '네임스페이스' (Namespace). The '클러스터' table shows one cluster with 4 alerts. The '네임스페이스' table shows several namespaces with their respective alert counts and resource usage.

이름	알림	라벨	컨테이너 재시작	오류 로그	CPU 사용률	메모리 사용량
rasecure-cluster-1	0	위치: us-central1-a	0	13	38.95%/CPU 0.6	32.05%/852.27MiB
클러스터 활성 알림 없음 활성 알림이 있는 클러스터 0개 전체 보기						
이름	알림	라벨	컨테이너 재시작	오류 로그	CPU 사용률	메모리 사용량
baseline-ns	0	클러스터: rasecure...	0	0	CPU 0	0B
default	0	클러스터: rasecure...	0	0	CPU 0	7.51MiB
gmp-public	0	클러스터: rasecure...	0	0	CPU 0	0B
gmp-system	0	클러스터: rasecure...	0	0	74.43%/CPU 0.01	59.95%/87.74MiB
네임스페이스 활성 알림 없음 활성 알림이 있는 네임스페이스 0개 전체 보기						

진단
기준

양호기준

: GKE Cluster 모니터링에서 유형 별 알림을 설정하고 있는 경우

취약기준

: GKE Cluster 모니터링 알림을 유형 별로 설정하지 않은 경우

비고

ETC. 부록

CSP(GCP)의 GKE를 사용하면서 발생하는 여러 보안 문제들에 대한 복잡한 클라우드 환경에서의 다양한 보안 사례를 제시함으로써 계층 및 영역별 보안을 다뤄 더 안전하게 클라우드를 운영할 수 있도록 도와주는 안내서입니다. 해당 부록은 GKE에 대한 보안을 중점적으로 다루며 GCP의 GKE 가이드를 참고하여 작성되었습니다. 하단에 기술되지 않은 내용에 대해서는 게시된 원문을 확인하시기 바랍니다. GKE 모범사례 가이드 : <https://cloud.google.com/kubernetes-engine/docs/concepts/security-overview?hl=ko>

가. 인증 및 접근 관리

GCP에서의 Kubernetes는 두가지 인증 유형(사용자 계정, 서비스 계정)을 지원하며, GKE Cluster에서의 Kubernetes 사용자 계정은 Google 계정과 Google Cloud 서비스 계정 두 가지 유형으로 구분됩니다. Kubernetes 서비스 계정은 Cluster의 일부이고 일반적으로 Cluster 내에서만 사용됩니다. Google Cloud 서비스 계정은 Google Cloud 프로젝트의 일부로서 Cluster 및 프로젝트 Cluster 자체, IAM을 사용하는 모든 Google Cloud 리소스에게 권한을 부여할 수 있습니다.

1. GKE RBAC 적용

Cluster 수준 또는 Kubernetes 네임스페이스 안에서 Kubernetes 리소스에 대한 상세한 액세스를 구성하기 위해서 역할 기반 액세스 제어(RBAC)를 사용해야 합니다. RBAC을 사용하게 되면 사용자와 서비스 계정의 액세스를 허용하는 작업과 리소스를 정의하는 상세한 정책을 생성할 수 있습니다.

2. 제어 영역 보안

GKE에서 Kubernetes 제어 영역 구성 요소는 Google에서 관리하고 유지되며 해당 구성 요소는 API 서버, 스케줄러, 컨트롤러 관리자 및 Kubernetes 구성이 유지되는 etcd 데이터베이스를 비롯한 제어영역을 실행하는 소프트웨어를 호스팅 합니다. 기본적으로 제어 영역 구성 요소는 공개 IP주소를 사용하기 때문에 제어 영역에 비공개 IP 주소를 할당하고 공개 IP 주소에 액세스 할 수 없도록 승인된 네트워크 및 비공개 Cluster를 적용하여 리소스를 보호해야 합니다.

3. Kubelet 인증 제어

Kubelet은 Kubernetes 각 노드에서 실행되는 Agent로서 Pod에 대해 정의된 YAML, JSON 형태의 PodSpec에 따라 컨테이너를 실행하고 관리하는 역할을 하며 Kubelet의 잘못된 인증 구현은 "Worker Node" 내 Pod, 컨테이너에 대한 비 인증 접근 후 정보 노출 및 리소스 수정과 같은 영향을 줄 수 있습니다.

3-1) Kubelet service 파일 사용 시 `"/source디렉터리/kubelet.service.d/xx-kubeadm.conf"`

```
KUBELET_SYSTEM_PODS_ARGS 내
```

```
--anonymous-auth=false  
--read-only-port=0
```

3-2) Kubelet config 파일 사용 시 `"/source디렉터리/kubelet/config.yaml"`

```
authentication:  
  anonymous:
```

```
enabled: false
```

```
readOnlyPort: 0
```

4. Kubelet 권한 제어

Kubelet은 기본적으로 Kubernetes Master API Server에서 전달되는 요청에 대해 권한 검사 없이 모두 허용하고 있기 때문에 설정 변경을 통해 권한 검증을 수행하여야 합니다.

4-1) Kubelet service 파일 사용 시 "/source디렉터리/kubelet.service.d/xx-kubeadm.conf"

```
KUBELET_AUTHZ_ARGS 내
```

```
--authorization-mode=Webhook
```

4-2) Kubelet config 파일 사용 시 "/source디렉터리/kubelet/config.yaml"

```
authorization:
```

```
mode: Webhook
```

5. GKE 서비스 에이전트

Kubernetes Engine 서비스 에이전트를 사용하여 노드, 디스크 부하 분산기와 같은 Cluster 리소스의 수명 주기를 자동으로 관리할 수 있으며 GKE API를 사용 설정하면 관리하고 있는 프로젝트에서 Kubernetes Engine 서비스 에이전트 역할이 부여됩니다.

6. Cluster 사용자 인증 정보 순환

Cluster 루트 인증 기관(CA)은 수명이 제한되어 있어 CA가 만료되면 Cluster 서명 인증서(MasterAuth API 필드), API 서버의 키 및 인증서, Kubelet 클라이언트 인증서를 포함하여 CA로 서명된 사용자 인증 정보가 더 이상 유효하지 않게됩니다. 이를 방지하기 위해 사용자 인증 정보 순환을 수행하여 사용자 인증 정보를 취소하고 Cluster에 새로운 사용자 인증 정보를 발급해야 합니다. 새 사용자 인증 정보를 사용하기 위해 노드를 신규 생성해야 합니다.

※ 현 사용자 인증 정보가 만료되기 전에 Cluster의 사용자 인증 정보 순환을 시작 및 종료해야 함

나. 파드 보안

GKE에서는 안전한 파드 사용과 파드 수준 보안 제어를 위해 아래 솔루션의 사용을 권고합니다.

1. PodSecurity 허용 컨트롤러 사용

GKE 표준 및 Autopilot Cluster에서 실행되는 파드에 파드 보안 표준을 적용할 수 있으며 이때 PodSecurity 허용 컨트롤러 사용이 가능합니다. PodSecurity란 GKE Cluster에서 실행되는 파드에 파드 보안 표준을 적용할 수 있는 Kubernetes 허용 컨트롤러이며 파드 보안 표준은 Kubernetes에서 파드 보안의 고급 요구사항을 다루는 사전 정의된 보안 정책입니다.

※ 해당 내용은 3.13 GKE Pod 보안 정책 관리 항목과 연계된 내용입니다.

2. 파드 보안 정책 번들과 함께 정책 컨트롤러 사용

정책 컨트롤러는 파드 보안 정책 번들과 함께 사용하여 Kubernetes 파드 보안 정책(PSP)과 동일한 보호수준을 제공하며 정책 시행 전 리소스 범위 제외, 사전 테스트 등 추가 기능을 제공합니다.

파드 보안 정책 번들과 같은 정책 컨트롤러 번들을 사용하면 리소스 범위에 대한 시험 이전 및 세분화된 제어와 같은 기능을 통해 PodSecurityPolicy와 동일한 검증을 시행할 수 있습니다.

3. 게이트키퍼 사용

게이트키퍼는 OPA(Open Policy Agent)를 사용하여 Kubernetes Cluster에서 파드 생성 및 업데이트 요청을 검증하는 허용 컨트롤러이며 게이트키퍼를 사용하면 관리자가 제약조건을 사용하여 정책을 정의할 수 있습니다. 이처럼 GKE Standard Cluster를 사용하면 게이트키퍼로 보안 정책을 적용할 수 있습니다. 게이트키퍼를 사용하면 PodSecurityPolicy와 동일한 기능을 적용할 수 있을 뿐만 아니라 테스트 실행, 점진적 출시, 감사 등의 기타 기능을 활용이 가능합니다.

4. GKE Autopilot Cluster 사용

GKE Autopilot은 Google에서 노드, 확장, 보안, 기타 사전 구성된 설정을 포함한 Cluster 구성을 관리하는 GKE의 작동 모드입니다. Autopilot Cluster는 대부분의 프로덕션 워크로드를 실행하고 Kubernetes 매니페스트에 따라 컴퓨팅 리소스를 프로비저닝해주며 Pod 보안관리에도 최적화 되어있습니다.

다. 네트워크 보안

GKE에서 실행되는 대부분의 워크로드는 Cluster 내부나 외부에서 실행될 수 있는 다른 서비스와 통신해야 하며 이를 안전하게 사용하기 위해서는 Cluster와 포드의 트래픽을 필터링하여 액세스를 제한해야 합니다.

1. 디폴트 거부(deny) 정책 생성

RBAC 정책과 마찬가지로 네트워크 정책에서도 네임스페이스 내에서 모든 인바운드 및 아웃바운드 트래픽을 제한하는 "모두 거부" 정책을 생성하시기 바랍니다.

2. 네트워크 격리 운영

조직에서 컨테이너를 통해 서비스를 운영하는 경우 때에 따라 외부에 오픈 된 웹 서비스, 내부 관리자 서비스와 같이 민감도 수준이 다른 기능을 수행하는 컨테이너들이 존재할 수 있으며, 컨테이너 구축 전 각각 서비스하고자 하는 바를 파악 후 별도 구분하여 서비스 특성에 따라 네트워크 정책 수립 후 격리 운영하는 것을 권고 드립니다.

3. 포드 간 통신 제한

Cluster 관리자와 사용자는 네트워크 정책을 사용하여 네임스페이스의 포드와의 수신 및 송신 연결을 제한할 수 있습니다. 기본적으로 정의된 네트워크의 정책이 존재하지 않을 경우 모든 인그레스 및 이그레스 트래픽이 모든 포드 액세스할 수 있기 때문에 네트워크 정책을 통해 트래픽을 정의해야 합니다.

4. 부하 분산 트래픽 필터링

LoadBalancer 서비스를 생성 후 LoadBalancerSourceRanges에 허용할 CIDR 범위를 지정하여 모든 IP 주소가 외부 IP를 통해 액세스하는 것을 차단해야 합니다. 만약 서비스에 대한 외부 액세스가 필요하지 않을 경우 내부 부하 분산기를 사용하시기 바랍니다.

5. 네트워크 정책 로깅 사용

Kubernetes 네트워크 정책은 포드가 전송 및 수신할 수 있는 네트워크 트래픽을 지정할 수 있습니다. 네트워크 정책 로깅을 설정하게 되면 네트워크 정책에 따라 연결이 허용되거나 거부되는 시점을 기록할 수 있으며 문제 발생시 서비스 감사로서 활용이 가능합니다.

상위필드	하위필드	유형	설명
cluster.allow	log	bool	true로 설정 시 Cluster 허용 연결이 로깅됨
	delegate	bool	false로 설정 시 허용된 모든 연결이 로깅됨
cluster.deny	log	bool	true로 설정 시 Cluster의 거부된 연결이 로깅됨
	delegate	bool	false로 설정 시 거부된 모든 연결이 로깅됨

라. 이미지 보안

컨테이너 이미지는 애플리케이션을 개발하고 실행할 때 중요한 우선 순위로서 오래된 기본 이미지 또는 패치되지 않은 애플리케이션 런타임이 있는 컨테이너는 보안 위험에 노출될 수 있습니다. 이는 빌드 및 런타임 시 컨테이너에서 검사 및 수정 도구를 통합하고 실행하여 해당 위험을 최소화할 수 있습니다.

1. Binary Authorization 설정

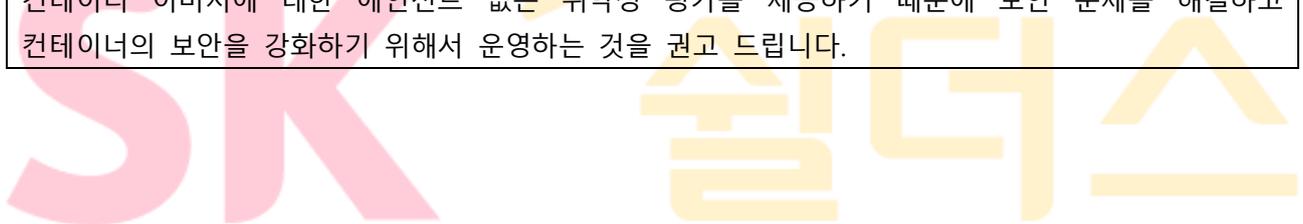
컨테이너 기반 애플리케이션을 개발 및 배포할 때 신뢰할 수 있는 컨테이너 이미지만 Kubernetes Engine에 배포하는 서비스입니다. 해당 기능(포드에 연결된 컨테이너 이미지 및 배포전 이미지의 정책을 준수하는지 확인하여 허용/비허용 진행)을 통해 Cluster 이미지를 관리 및 운영하는 것을 권고 드립니다.

2. GKE Cluster 생성 시 강화 노드 이미지 선택

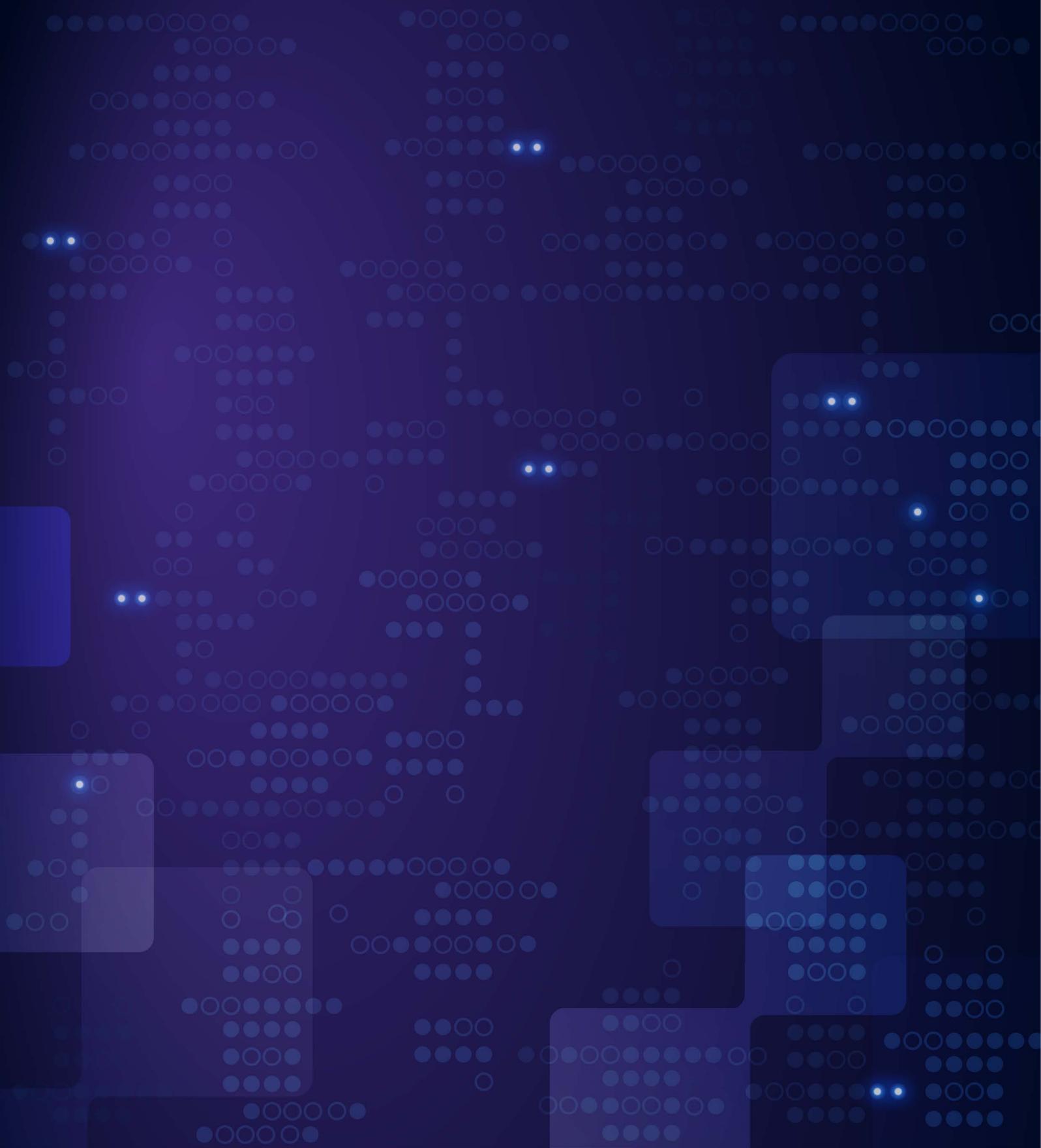
"containerd를 포함한 Container-Optimized OS(cos_containerd)" 이미지는 Kubernetes Container 런타임 인터페이스(CRI)의 핵심 컨테이너 기능을 제공하도록 설계되었으며, Docker 데몬보다 공격에 취약한 부분이 적기 때문에 Cluster 구성 시 강화 노드 이미지를 설정하여 운영하는 것을 권고 드립니다.

3. 컨테이너 스캔 설정

Artifact Registry에 업로드된 이미지를 검사하여 레지스트리 및 런타임 권장 사항, 이미지 검사 등 컨테이너 이미지에 대한 에인전트 없는 취약성 평가를 제공하기 때문에 보안 문제를 해결하고 컨테이너의 보안을 강화하기 위해서 운영하는 것을 권고 드립니다.



안녕을 지키는 기술



안녕을 지키는 기술 |  SK 쉴더스

SK쉴더스(주) 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
<https://www.skshieldus.com>

발행인 : SK쉴더스 취약점진단팀

제 작 : SK쉴더스 마케팅그룹

COPYRIGHT © 2024 SK SHIELDUS. ALL RIGHT RESERVED.

본 저작물은 SK쉴더스의 서면 동의 없이 사용될 수 없습니다.