업무참고 2025-클라우드대응-②-57

금융분야
상용 클라우드컴퓨팅서비스 보안 관리 참고서

Google Cloud

금융보안원
FINANCIAL SECURITY INSTITUTE

Google Cloud

CONTENTS

1. 가상자원 관리 ····· 1

1.1. 가상자원 생성 시 최초 계정에 대한 비밀번호 규칙 수립 ····· 2
1.2. 이용자 가상자원 접근 시 로그인 규칙 적용 ····· 5
1.3. 가상자원 루트 계정 접근 시 추가 인증수단 적용 ····· 7
1.4. 가상자원 생성 시 네트워크 설정 적용 ····· 9
1.5. 가상자원 접속 시 보안 방안 수립 ····· 12
1.6. 이용자 가상자원별 권한 설정 ····· 14
1.7. 이용자 가상자원 내 악성코드 통제방안 수립 ····· 17

2. 네트워크 관리 ····· 21

2.1. 업무 목적에 따른 네트워크 구성 ····· 22
2.2. 내부망 네트워크 보안 통제 ····· 27
2.3. 네트워크 보안 관제 수행 ····· 32
2.4. 공개용 웹서버 네트워크 분리 ····· 39
2.5. 네트워크 사설 IP주소 할당 및 관리 ····· 46
2.6. 네크워크(방화벽 등) 정책 주기적 검토 ····· 56

3. 계정 및 권한 관리 ····· 58

3.1. 클라우드 계정 권한 관리 ····· 59
3.2. 이용자별 인증 수단 부여 ····· 63
3.3. 인사변경 사항 발생 시 계정 관리 ····· 66
3.4. 클라우드 가상자원 관리시스템 관리자 권한 추가인증 적용 ····· 69
3.5. 클라우드 가상자원 관리 시스템 로그인 규칙 수립 ····· 73
3.6. 계정 비밀번호 규칙 수립 ····· 75
3.7. 공개용 웹서버 접근 계정 제한 ····· 77

4. 암호키 관리 ····· 81

4.1. 암호화 적용 가능 여부 확인 ····· 82
4.2. 암호키 관리 방안 수립 ····· 85
4.3. 암호키 서비스 관리자 권한 통제 ····· 91
4.4. 암호키 호출 권한 관리 ····· 95
4.5. 안전한 암호화 알고리즘 적용 ····· 100

5. 로깅 및 모니터링 관리 ····· 102

5.1. 가상자원 이용(생성, 삭제, 변경 등)에 관한 행위추적성 확보 ····· 103
5.2. 가상자원 이용 행위추적성 증적 모니터링 ····· 107
5.3. 이용자 가상자원 모니터링 기능 확보 ····· 110
5.4. API 사용(호출대상, 호출자, 호출일시 등)에 관한 행위추적성 확보 ····· 115
5.5. 네트워크 관련 서비스(VPC, 보안그룹, ACL 등)에 관한 행위추적성 확보 ····· 117
5.6. 계정 변동사항에 대한 행위추적성 확보 ····· 120
5.7. 계정 변경사항에 관한 모니터링 수행 ····· 123

6. API 관리 ····· 126

6.1. API 호출 시 인증 수단 적용 ····· 127
6.2. API 호출 시 무결성 검증 ····· 133
6.3. API 호출 시 인증키 보호대책 수립 ····· 134
6.4. API 이용 관련 유니크값 유효기간 적용 ····· 136
6.5. API 호출 구간 암호화 적용 ····· 142

7. 스토리지 관리 ····· 143

7.1. 스토리지 접근 관리 ····· 144
7.2. 스토리지 권한 관리 ····· 146
7.3. 스토리지 업로드 파일 제한 ····· 149

8. 백업 및 이중화 관리 ····· 150

8.1. 클라우드 이용에 관한 행위추적성 증적(로그 등) 백업 ····· 151
8.2. 행위추적성 증적(로그 등) 백업 파일 무결성 검증 ····· 158
8.3. 금융회사 전산자료 백업 ····· 161
8.4. 금융회사 전산자료 백업 파일 무결성 검증 ····· 168
8.5. 행위추적성 증적 및 전산자료등 백업에 관한 기록 및 관리 ····· 172
8.6. 백업파일 원격 안전지역 보관 ····· 174
8.7. 주요 전산장비 이중화 ····· 178

1. 가상자원 관리

1.1. 가상자원 생성 시 최초 계정에 대한 비밀번호 규칙 수립
1.2. 이용자 가상자원 접근 시 로그인 규칙 적용
1.3. 가상자원 루트 계정 접근 시 추가 인증수단 적용
1.4. 가상자원 생성 시 네트워크 설정 적용
1.5. 가상자원 접속 시 보안 방안 수립
1.6. 이용자 가상자원별 권한 설정
1.7. 이용자 가상자원 내 악성코드 통제방안 수립

1 가상자원 관리

1 기준

식별번호	기준	내용
1.1.	**가상자원 생성 시 최초 계정에 대한 비밀번호 규칙 수립**	**이용자 가상자원 생성 시 최초 계정에 대한 비밀번호 규칙을 수립하여야 한다.**

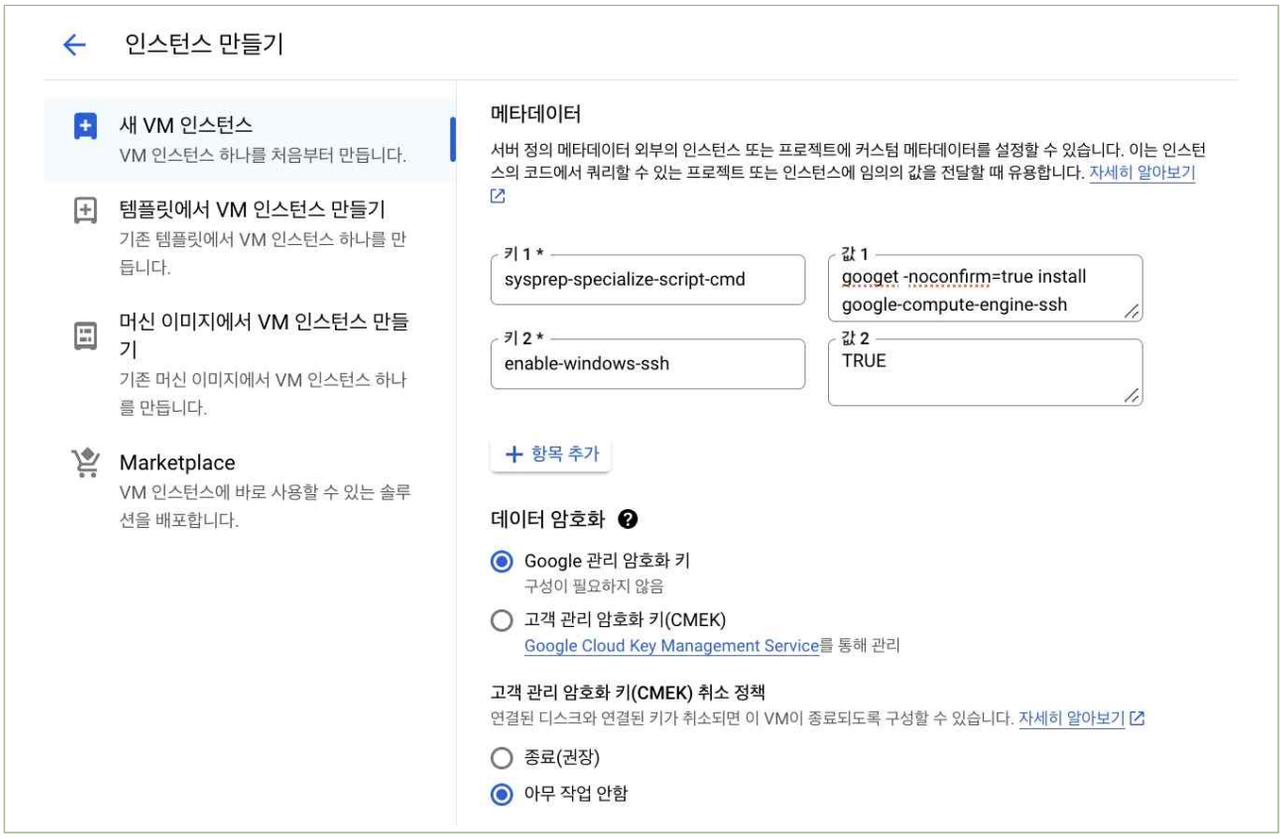
2 설명

- 이용자 가상자원에 접근하는 계정에 대한 비밀번호 규칙 보안통제 방안을 수립하여야 한다.
  - Google Cloud의 VM 서비스인 Google Compute Engine에서는 Linux와 Windows 두 가지 OS의 VM 자원을 제공합니다.
  - GCE에서 VM 인스턴스를 최초 생성 시, 이때 별도로 사용자 계정은 생성되지 않으며, 적절한 IAM 권한을 가진 관리자가 최초 접근을 시도할 때 OS 종류 및 접근 방법에 따라 생성됩니다.
  - Linux VM의 경우 PEM Key 기반의 SSH 인증을 제공하며, 패스워드를 이용한 인증은 제공되지 않습니다. Google Cloud에서는 SSH 키를 생성하고 관리할 필요 없이 IAM으로 인스턴스에 대한 SSH 액세스를 관리할 수 있는 OS Login 서비스를 사용하는 것을 권장합니다.
  - Windows VM의 경우 관리자가 Windows VM 최초 접근 전 Google Cloud 콘솔 혹은 CLI를 통해 계정을 생성 후 Windows VM 내부 Agent가 생성한 무작위 패스워드를 공개키로 암호화하여 전달받아 RDP 세션을 로그인 할 수 있습니다.
  - 이때 생성되는 무작위 패스워드는 Windows Server 제품군에서 요구하는 패스워드 복잡도를 만족하는 최소 15자에서 최대 225자 이내 패스워드가 생성됩니다. 패스워드에 대한 기본 요건은 아래와 같으며, 좀 더 자세한 내용은 윈도우 패스워드 복잡도 설명 문서를 참고해주십시오.
    - Windows 계정의 samAccountName, displayName 항목 정보가 재사용되어서는 안된다.
    - 패스워드는 다음 구성 요소 중 최소 세가지 이상을 포함하여야 한다. (1) 알파벳 대문자, (2) 알파벳 소문자, (3) 10진수 아라비아 숫자, (4) 특수문자.

- Windows VM 의 아래 계정들은 기본 비활성화 되어 있으며, 패스워드 초기화를 통해서도 재활성화 할 수 없습니다.
  - Administrator
  - Guest
  - DefaultAccount
  - WDAGUtilityAccount

3 우수 사례

- Google Cloud GCE에서는 Windows VM을 위한 SSH 접근 기능을 제공하며, 이를 이용하면 패스워드 없이 PEM Key 기반의 SSH 로그인이 가능합니다.
- Windows용 SSH 연결 기능은 아래의 방법을 통해 설정이 가능합니다.
  - Windows VM 생성 시 고급 옵션에서 관리 섹션을 펼칩니다.
  - 관리 섹션 아래 메타데이터 섹션에 항목 추가 버튼을 클릭하여 다음의 메타데이터 키-값 쌍을 입력합니다.
    - 키: sysprep-specialize-script-cmd
    - 값: googet -noconfirm=true install google-compute-engine-ssh
    - 키: enable-windows-ssh
    - 값: TRUE
  - 만들기 버튼을 클릭하여 VM을 만듭니다.



| 그림 1-1-1 | Windows VM 생성시 SSH 연결 설정

- 만약 Windows용 SSH 사용이 힘들다면, 관리형 Microsoft AD를 이용하여 Windows VM 사용자 계정을 관리합니다. 관리형 Microsoft AD를 이용하면, 계정 비밀번호에 대한 세분화된 비밀번호 정책을 아래와 같이 구성할 수 있습니다.
- 관리형 Microsoft AD의 세분화된 비밀번호 정책에 대한 자세한 내용은 세분화된 비밀번호 정책 구성 문서를 참고를 부탁드립니다.

4 참고 사항

- 위 내용에 대한 좀 더 자세한 정보는 아래에 첨부한 문서에서 확인하실 수 있습니다.
  - Windows VM에서 계정 및 사용자 인증 정보 관리
  - 세분화된 비밀번호 정책 정보
  - 세분화된 비밀번호 정책 구성
  - SSH를 사용하여 Windows VM에 연결

1 기준

식별번호	기준	내용
1.2.	**이용자 가상자원 접근 시 로그인 규칙 적용**	**이용자 가상자원 접근 계정에 대한 안전한 로그인 규칙을 수립하여야 한다.**

2 설명

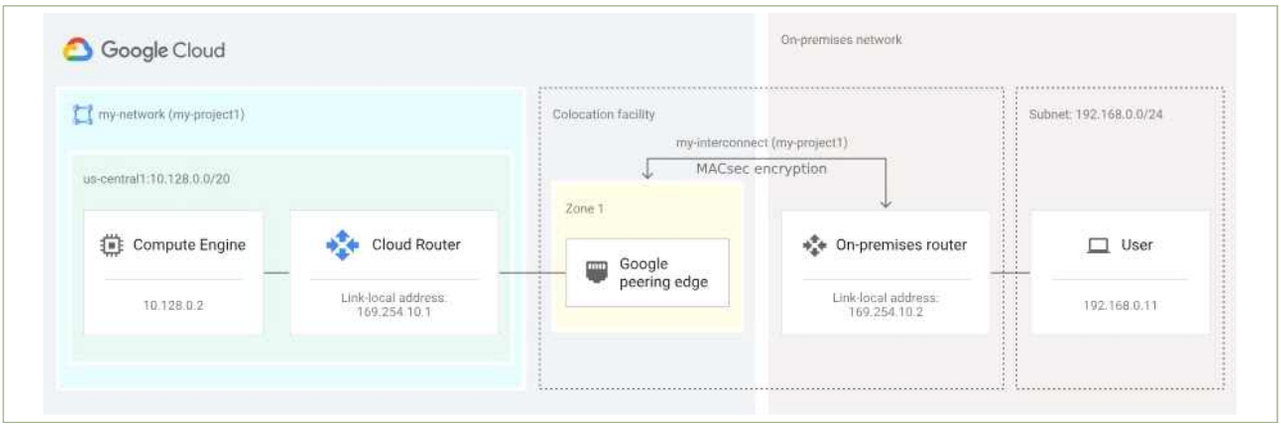
- 이용자는 패스워드 무작위 대입 공격 등에 대응하기 위해 가상자원 접근계정에 대한 안전한 로그인 규칙을 수립하여야 한다.
  - Google Cloud의 VM 서비스인, Google Compute Engine에서는 Linux와 Windows 두 가지 OS의 VM 자원을 제공합니다.
  - Linux VM의 경우 자동으로 관리되는 임시 PEM Key 기반의 SSH 인증을 제공하며, 패스워드를 이용한 인증은 제공되지 않습니다.
  - Windows VM의 경우 관리자가 Windows VM 최초 접근 전 Google Cloud 콘솔 혹은 CLI를 통해 계정을 생성 후 Windows VM 내부 Agent가 생성한 무작위 패스워드를 전달받아 RDP 세션을 로그인 할 수 있습니다.
  - 또한 Google Cloud의 Enterprise Foundation Blueprints에서는 사용자의 가상자원이 공용 IP 주소를 사용하지 않기를 권고하고 있으며, 가상자원에 대한 접근도 신뢰할 수 있는 장소에서만 가능하도록 VPC 방화벽 규칙 혹은 VPN과 같은 기술을 이용해 인프라를 구성하기를 권고하고 있습니다.

3 우수 사례

- 가상자원을 공개망에서 접근할 수 없도록 구성 후 필요하다면 VM의 OS 종류에 따라 좀 더 안전한 로그인을 위해 OS 레벨 이상에서 아래와 같은 구성을 검토해볼 수 있습니다.
  - Windows VM: 윈도우 계정 잠금 정책을 사용해 특정 로그인 실패 횟수 후 계정 잠금
  - Linux VM: fail2ban을 이용해 로그인 실패 감시 및 의심스러운 IP 주소 접근 제한
- 모든 가상자원은 공개망을 통해 직접 접근할 수 없도록 구성하는 것을 권장합니다.
  - Google Cloud 조직 정책 기능을 이용해 “compute.vmExternalIpAccess” 정책을 설정하여,

승인받은 가상자원만 공개 IP 주소를 가지도록 구성합니다.

- 네트워크 방화벽 규칙, NACL 등을 활용하여 모든 이용자 가상자원이 승인받은 관리자만이 접근할 수 있도록 네트워크 환경을 구축합니다.
- 승인받은 관리자는 회사 내부망에서만 VPN 혹은 Interconnect로 연결된 경로를 이용해 Google Cloud에 구동중인 가상자원은 접근할 수 있도록 구성합니다.
- 자세한 네트워크 구축 예시는 Enterprise Foundation Blueprints의 네트워크 토폴로지 예시를 참고하시어, 구성하는 것을 권장합니다.



| 그림 1-2-1 | Google Cloud Dedicated Interconnect 예시

4 참고 사항

- 위 내용에 대한 좀 더 자세한 정보는 아래에 첨부한 문서에서 확인하실 수 있습니다.
  - 허용되는 리소스 구성에 대한 예방형 제어
  - 엔터프라이즈 기반 청사진 – 네트워킹
- OS 레벨 이상의 영역은 Google Cloud의 책임 공유 및 공통된 운명 문서에 설명된 내용과 같이 따라 이용자의 재량으로 구성할 수 있습니다.
  - Google Cloud의 책임 공유 및 공통된 운명

1 기준

식별번호	기준	내용
1.3.	**가상자원 루트 계정 접근 시 추가 인증수단 적용**	**이용자 가상자원 루트 계정(root, administrator 등) 접근 시 추가인증 수단을 확보하여야 한다.**

2 설명

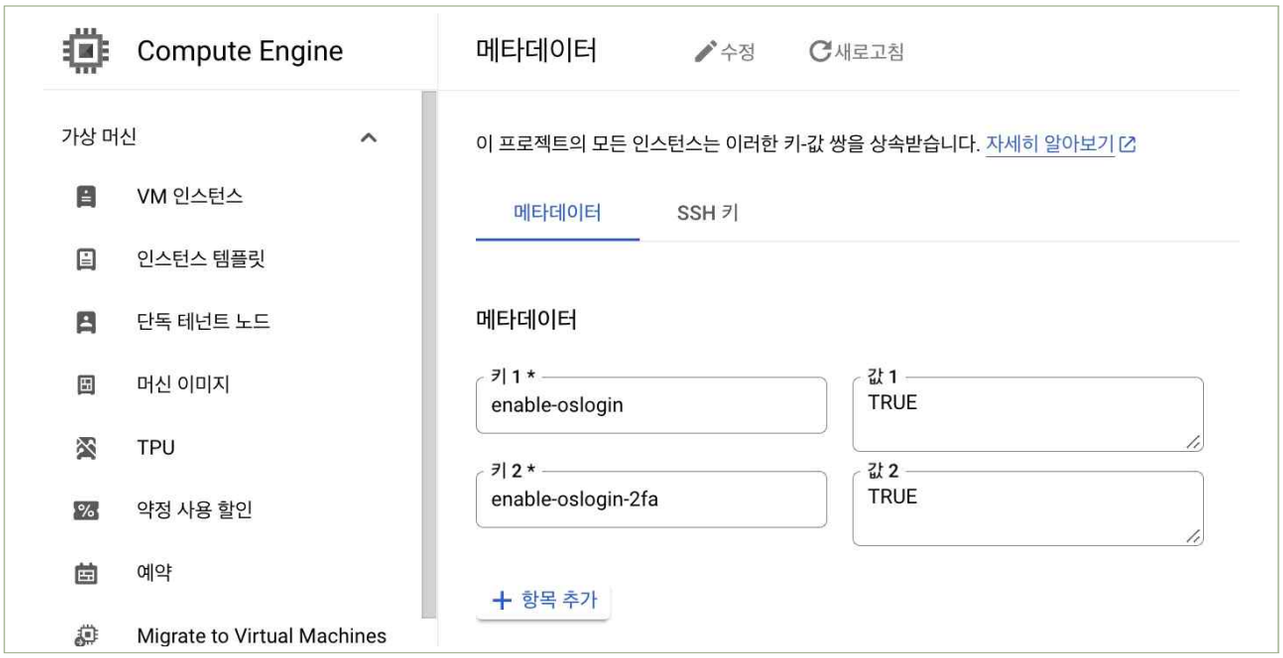
- 이용자 가상자원 루트 계정 접근 시 추가인증 수단이 확보되어야 한다.
  - Google Cloud의 VM 서비스인 Google Compute Engine에서는 가상자원의 OS 종류에 따라 다음과 같이 안전한 로그인 수단을 제공합니다.
    - Linux VM을 이용하는 경우 Cloud IAM의 InstanceAdmin IAM 역할을 가진 관리자만이 PEM Key 기반의 SSH 접근을 제공하며, 루트 계정은 기본적으로 SSH 로그인이 불가능합니다.
    - Windows VM에서는 Cloud IAM의 InstanceAdmin IAM 역할을 가진 관리자만이 RDP 접근을 위한 패스워드 생성 및 변경이 가능하며, Administrator 와 같은 루트 계정들은 비활성화되어 있습니다.
  - GCE에서는 추가적으로 OS Login 기능을 통해 가상자원 계정 로그인 시 아래와 같은 추가인증 수단 구성 및 고급기능을 사용하실 수 있습니다.
    - Google OTP
    - 문자 메시지 또는 전화 통화 확인
    - 전화 안내 메시지
    - 보안 키 일회용 비밀번호(OTP)
  - Google Cloud에서는 GCE VM 자원에 대한 접근시 OS Login을 구성해서 사용하시기를 권장합니다. (*참고: 현재 OS Login은 Linux VM만 지원합니다.)

3 우수 사례

- 프로젝트 전체 VM을 대상으로 OS Login 및 2FA 설정
  - 프로젝트의 모든 VM에 OS 로그인을 사용 설정하려면 프로젝트 메타데이터에서 다음 값을 설정합니다.
    - OS 로그인을 사용 설정합니다.

- 키: enable-oslogin
- 값: TRUE

- (선택사항) 2단계 인증을 사용 설정합니다.
  - 키: enable-oslogin-2fa
  - 값: TRUE



| 그림 1-3-1 | 프로젝트 메타데이터 화면에서 OS 로그인 설정

4 참고 사항

- 위 내용에 대한 좀 더 자세한 정보는 아래에 첨부한 문서에서 확인하실 수 있습니다.
  - OS 로그인 정보
  - OS 로그인 설정
  - VM 인스턴스에 안전하게 연결

1 기준

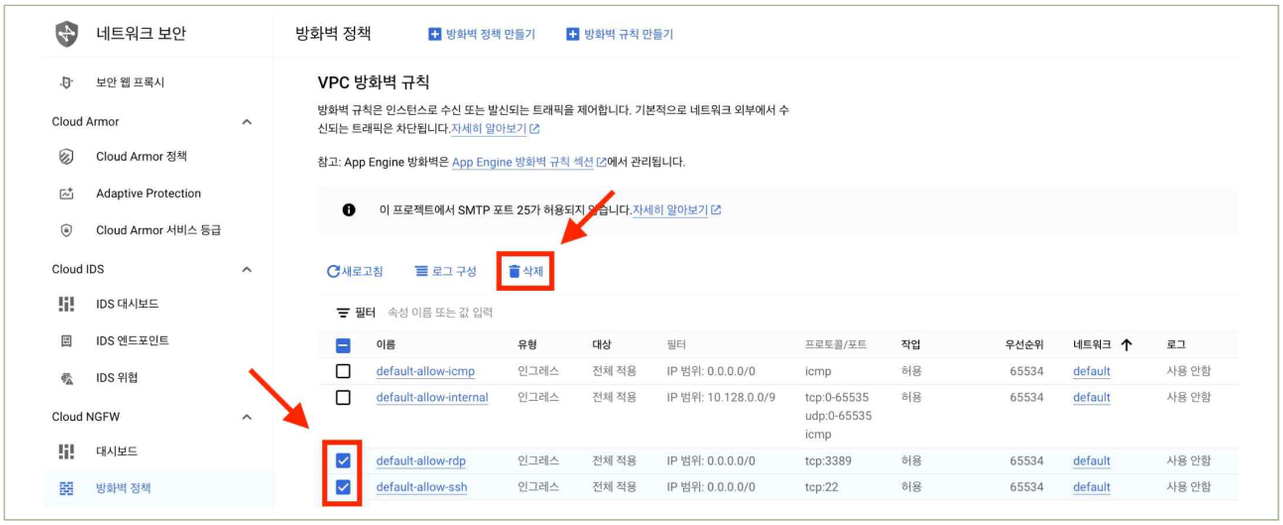
식별번호	기준	내용
1.4.	**가상자원 생성 시 네트워크 설정 적용**	**이용자의 가상자원 생성 시 안전한 네트워크 설정을 적용하여야 한다.**

2 설명

- 외부에서 직접 접속이 불필요한 경우 내부IP 또는 IP대역에서만 접근할 수 있도록 설정하여야 한다.
  - Google Cloud의 VM 서비스인 Google Compute Engine에서는 VM 가상자원에 신뢰할 수 있는 네트워크에서만 접근할 수 있도록 네트워크 및 인프라 환경을 구성할 수 있습니다.
  - 신뢰하는 네트워크에서 GCE VM 자원이 배포된 VPC 간에 연결은 VPN 혹은 Interconnect를 이용할 수 있습니다.
  - 또한 공용망에서의 접근을 제한하기 위하여, 모든 VM 자원이 공용 IP 주소 없이 내부 IP 주소만을 가지도록 구성하며, 필요 시 조직정책을 이용하여 허가된 VM 자원만 공용 IP를 가질 수 있도록 제한합니다.

3 우수 사례

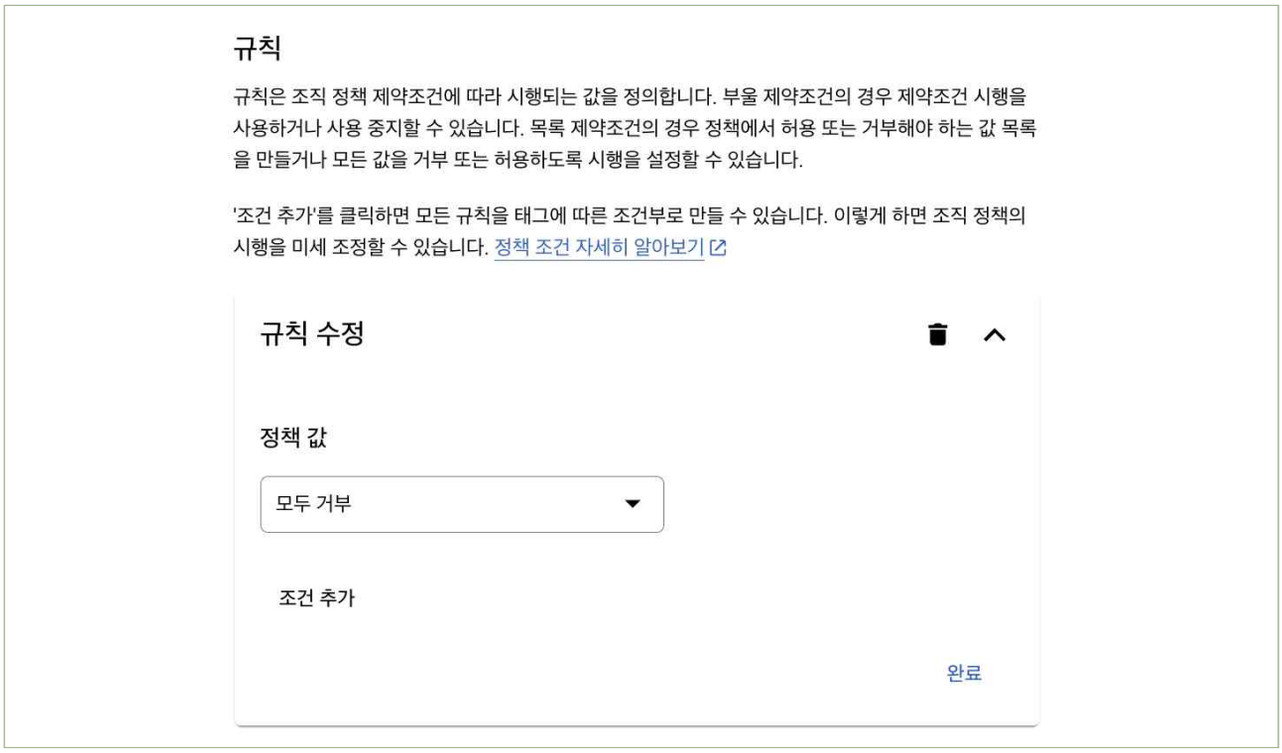
- 기본 SSH, RDP 방화벽 규칙 삭제하기
  - Google Cloud 콘솔 네트워크 보안 페이지로 이동합니다.
  - VPC 방화벽 규칙 중 “default-allow-rdp”, “default-allow-ssh” 삭제합니다.



| 그림 1-4-1 | 기본 SSH, RDP 방화벽 규칙 삭제하기

- 조직 정책을 이용하여 VM 자원 공용 IP 주소 부여 제한
  - Google Cloud 콘솔 조직정책 페이지로 이동, 적용 범위를 조직으로 선택합니다.
  - 화면 아래 정책 목록에서 “vmExternalIpAccess”으로 필터링합니다.
  - 조회된 정책 중 “Define allowed external IPs for VM instances” 정책 클릭하여 상세 페이지로 이동합니다.
  - 정책 상세 페이지에서 우상단 “정책 관리” 버튼을 클릭하여 정책 관리 페이지로 이동하여 아래 규칙 부분의 정책 값을 “모두 거부"로 선택합니다.
  - 정책 관리 페이지 하단의 “정책 설정” 버튼을 클릭하여 조직 정책 적용합니다.

| 그림 1-4-2 | vmExternalIpAccess 조직 정책 필터링



| 그림 1-4-3 | 조직 정책 값 “모두 거부" 로 설정하기

4 참고 사항

- 위 내용에 대한 좀 더 자세한 정보는 아래에 첨부한 문서에서 확인하실 수 있습니다.
  - RDP를 사용하여 Windows VM에 연결
  - VPC 방화벽 규칙 - 기본 네트워크에 미리 입력된 규칙
  - 정적 외부 IP 주소 예약 - 외부 IP 주소를 특정 VM으로 제한

1 기준

식별번호	기준	내용
1.5.	**가상자원 접속 시 보안 방안 수립**	**이용자 가상자원 접속 시 안전한 인증절차를 통해 접속 하여야 한다.**

2 설명

- 이용자의 가상자원(인스턴스) 접속 시 안전한 방식을 통해 접근하여야 한다.
- SSH를 통한 접속 시 안전한 계정관리 수행 (ex. ID/PW 기반이 아닌 Certificate 기반 인증 방식 적용 등)
  - 클라우드 웹 콘솔에서 직접 실행 시 안전한 인증 방식 적용(해당 인스턴스를 호출할 수 있는 권한을 지닌 이용자인지 검증 등)
- Google Cloud의 VM 서비스인, Google Compute Engine에서는 VM 가상자원에 이용자가 안전한 방식으로 접근할 수 있도록 아래와 같이 기본 구성되어 있습니다.
  - Linux VM 의 경우, Cloud IAM에서 VM 자원에 접근 권한이 있는지 먼저 확인하고 PEM Key 를 기반한 SSH 연결을 기본 제공합니다.
  - 웹 콘솔에서 SSH 로그인시에는 웹브라우저에 로그인된 구글 계정이 적절한 Cloud IAM 역할 (예: roles/compute.instanceAdmin.v1)을 가지고 있는지 검증한 후 SSH 접근할 수 있습니다.
  - 또한 OS Login 기능을 이용해 MFA 인증 수단을 추가하여 보다 안전한 인증절차 및 루트 계정과 일반 계정을 분리하여 세밀한 권한 관리가 가능해집니다.

3 우수 사례

- Google Cloud의 GCE 서비스에서 SSH 접근을 위한 키를 수동으로 프로젝트 혹은 인스턴스 레벨에서 관리가 가능합니다. 하지만 수동으로 키를 관리하는 것은 필요한 기간 동안 제한적으로만 사용하고, 자동으로 키가 관리되는 OS Login을 사용하기를 권장드립니다.
- 프로젝트 메타데이터에서 공개 키 삭제
  - 프로젝트의 모든 VM에 대한 액세스 권한을 삭제하려면 프로젝트 메타데이터에서 공개 SSH 키를 삭제하십시오.
  - Google Cloud Console에서 메타데이터 페이지로 이동합니다.

- 메타데이터 페이지 상단에 있는 “수정" 버튼을 클릭합니다.
- 메타데이터 페이지에서 SSH 키 탭을 클릭 후 삭제하고자 하는 SSH 키 위에 마우스 커서를 이동 후 우측에 나타나는 휴지통 아이콘을 선택하여 삭제합니다.
- 페이지 하단에 있는 “저장” 버튼을 클릭하여 변경된 내용을 저장합니다.

| 그림 1-5-1 | 프로젝트 메타데이터에서 공개 키 삭제

4 참고 사항

- 위 내용에 대한 좀 더 자세한 정보는 아래에 첨부한 문서에서 확인하실 수 있습니다.
  - Linux VM에 연결
  - VM에서 SSH 키 제한
  - 수동 키 관리 위험
  - SSH를 사용하여 Windows VM에 연결
  - 회사 소유의 리소스에 균일한 MFA 적용

1 기준

식별번호	기준	내용
1.6.	**이용자 가상자원별 권한 설정**	**이용자 직무 및 권한에 따른 가상자원별 접근통제 방안(권한 설정 등)을 수립하여야 한다.**

2 설명

- 이용자 직무 및 권한에 따른 가상자원별 접근통제 방안(권한 설정 등)을 수립하여야 한다.
  - 가상자원 종류 별 접근통제 방안 수립(ex. IAM을 통한 접근권한 관리): 모든 가상자원에 접근 가능한 Role에 대해서는 최소 인원에 대해서만 부여
- Google Cloud의 VM 서비스인, Google Compute Engine에서는 VM 가상자원에 접근할 때 Cloud IAM 역할을 기반으로 이용자의 권한에 따른 가상자원 접근을 관리할 수 있습니다.
  - Cloud IAM 역할은 최대 조직 레벨에서 최소 가상자원(예: 인스턴스) 레벨까지 이용자가 원하는 범위에 해당 역할을 부여받은 사용자와 함께 설정할 수 있습니다.
  - 예를 들어 조직 레벨에서 “roles/compute.instanceAdmin.v1” 역할을 부여받은 관리자는 조직에 속한 모든 프로젝트의 GCE VM 인스턴스에 SSH 접근을 시도할 수 있습니다. 그러므로 최소 권한의 보안 원칙에 따라 필요한 기간동안 최소한의 인원만이 부여될 수 있도록 주의하여야 합니다.
  - GCE 의 OS Login 기능을 이용하면, 이용자의 SSH 접근 권한뿐만 아니라 루트 계정(“roles/compute.osAdminLogin”)과 일반 계정 사용자 (“roles/compute.osLogin”)로 사용하는 계정의 권한을 분리하여 설정할 수 있습니다.

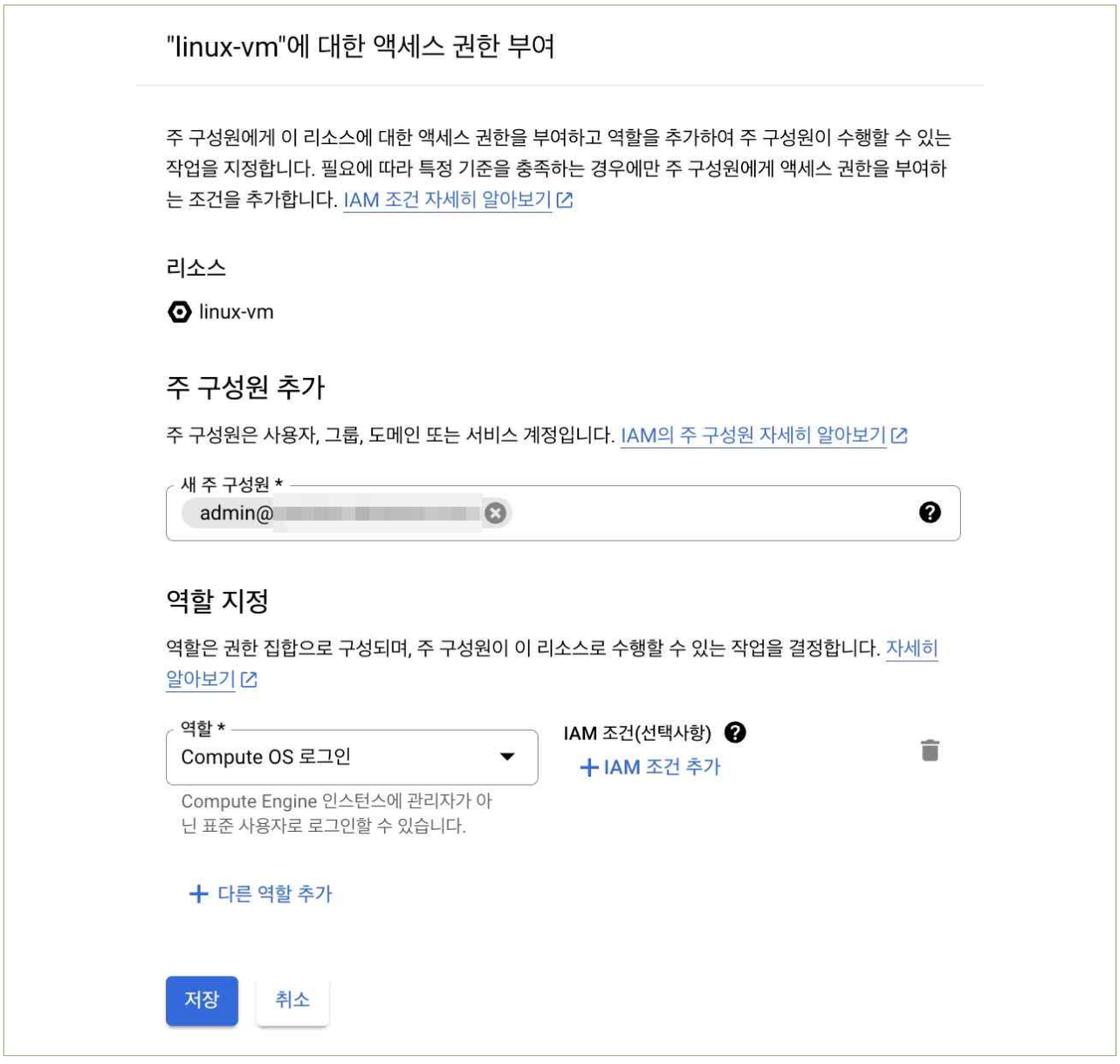
3 우수 사례

- GCE VM 인스턴스 레벨의 osLogin IAM 역할 부여
  - Google Cloud 콘솔의 Compute Engine 페이지를 엽니다.
  - osLogin IAM 역할을 부여하고자 하는 GCE VM 인스턴스를 목록에서 체크하고, 우측 상단의 “권한”을 클릭해 권한 상세 페이지를 엽니다.
  - 권한 상세 페이지에서 “주 구성원 추가” 버튼을 클릭하고, “새 주 구성원” 항목에 권한을 부여받은

이용자의 구글 계정 이메일 주소를 입력합니다.

- 아래 역할 섹션에서 “OS 로그인” IAM 역할을 선택한 뒤 “저장” 버튼을 클릭하여 변경된 권한을 저장합니다.

| 그림 1-6-1 | GCE VM 인스턴스 권한 페이지 열기



| 그림 1-6-2 | GCE VM 인스턴스 레벨 OS 로그인 IAM 역할 부여

4 참고 사항

- 위 내용에 대한 좀 더 자세한 정보는 아래에 첨부한 문서에서 확인하실 수 있습니다.
  - Compute Engine IAM 역할 및 권한

1 기준

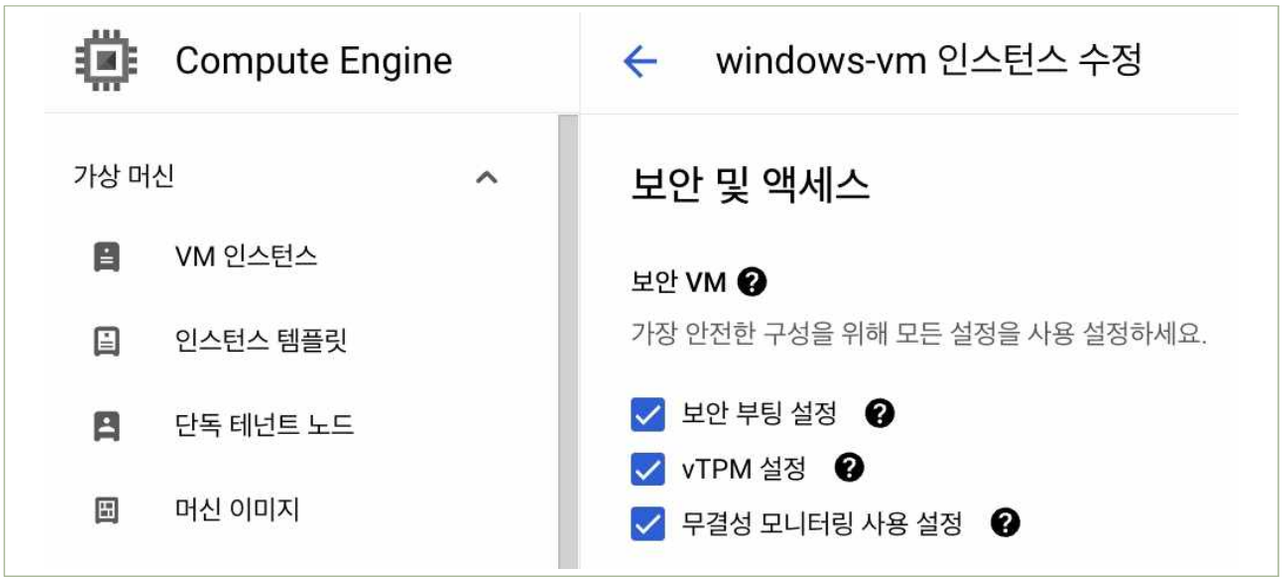
식별번호	기준	내용
1.7.	**이용자 가상자원 내 악성코드 통제 방안 수립**	**이용자 가상자원 내 악성코드 통제방안을 수립하여야 한다.**

2 설명

- 이용자 가상자원 내 악성코드 통제방안을 수립하여야 한다.
  - 이용자가 보유하고 있는 “악성코드 통제방안” 수립(백신 등)
  - 클라우드 사업자가 “악성코드 통제방안” 제공(백신 등)
  - 백신 등 설치가 불가능한 환경인 경우 그 수준에 준하는 악성코드 통제방안 수립
- 이용자가 보유하고 있는 백신 등 악성코드 통제방안을 구성하여 운영할 수 있습니다.
  - 특히 Google Cloud는 Windows를 실행하는 경우 바이러스 백신 소프트웨어를 실행할 것을 권고하고 있습니다.
- Google Cloud에서는 이용자의 VM 가상자원을 악성코드로부터 보호하고 안전한 사용을 위해서 Google Compute Engine의 보안 VM(Shielded VM), Security Command Center의 가상 머신 위협 감지(Virtual Machine Threat Detection)와 같은 서비스들을 제공합니다.
  - 보안 VM: GCE의 보안 VM은 GCE VM 인스턴스의 검증 가능한 무결성을 제공하는 서비스로, 부팅 또는 커널 수준의 멀웨어나 루트킷으로 인한 침해로부터 인스턴스의 안전을 보장합니다.
    - 보안 부팅(Secure Boot)
    - vTPM 을 사용한 신중한 부팅(Measured Boot)
    - 무결성 모니터링
  - 가상 머신 위협 감지: Security Command Center Premium 또는 Security Command Center Enterprise의 기본 서비스인 가상 머신 위협 감지(VMTD, Virtual Machine Threat Detection)은 하이퍼바이저 수준의 계측 및 영구 디스크 분석을 통해 사용자 인스턴스의 위협 감지를 제공합니다. VMTD 는 암호화폐 채굴 소프트웨어, 커널 모드 루트킷, 보안 침해된 클라우드 환경에서 실행되는 멀웨어 같은 잠재적 악성 애플리케이션을 감지합니다.

3 우수 사례

- GCE 보안 VM 옵션 사용 설정
  - Google Cloud 콘솔의 VM 인스턴스 페이지로 이동합니다.
  - 보안 VM 옵션 사용 설정하고자 하는 인스턴스의 이름을 클릭하여 VM 인스턴스 세부정보 페이지를 엽니다.
  - “중지”를 클릭하여, VM 인스턴스를 중지 후 “수정"을 클릭하여 수정 페이지를 엽니다.
  - 수정 페이지, 보안 VM 섹션에서 보안 VM 옵션을 수정합니다.
    - 보안 부팅 설정을 전환하여 보안 부팅을 사용 설정합니다.
    - vTPM 설정을 전환하여 Virtual Trusted Platform Module(vTPM)을 사용 설정합니다.
    - 무결성 모니터링 사용 설정을 전환하여 무결성 모니터링을 사용 설정합니다.
  - 저장을 클릭합니다.
  - 시작을 클릭하여 인스턴스를 시작합니다.

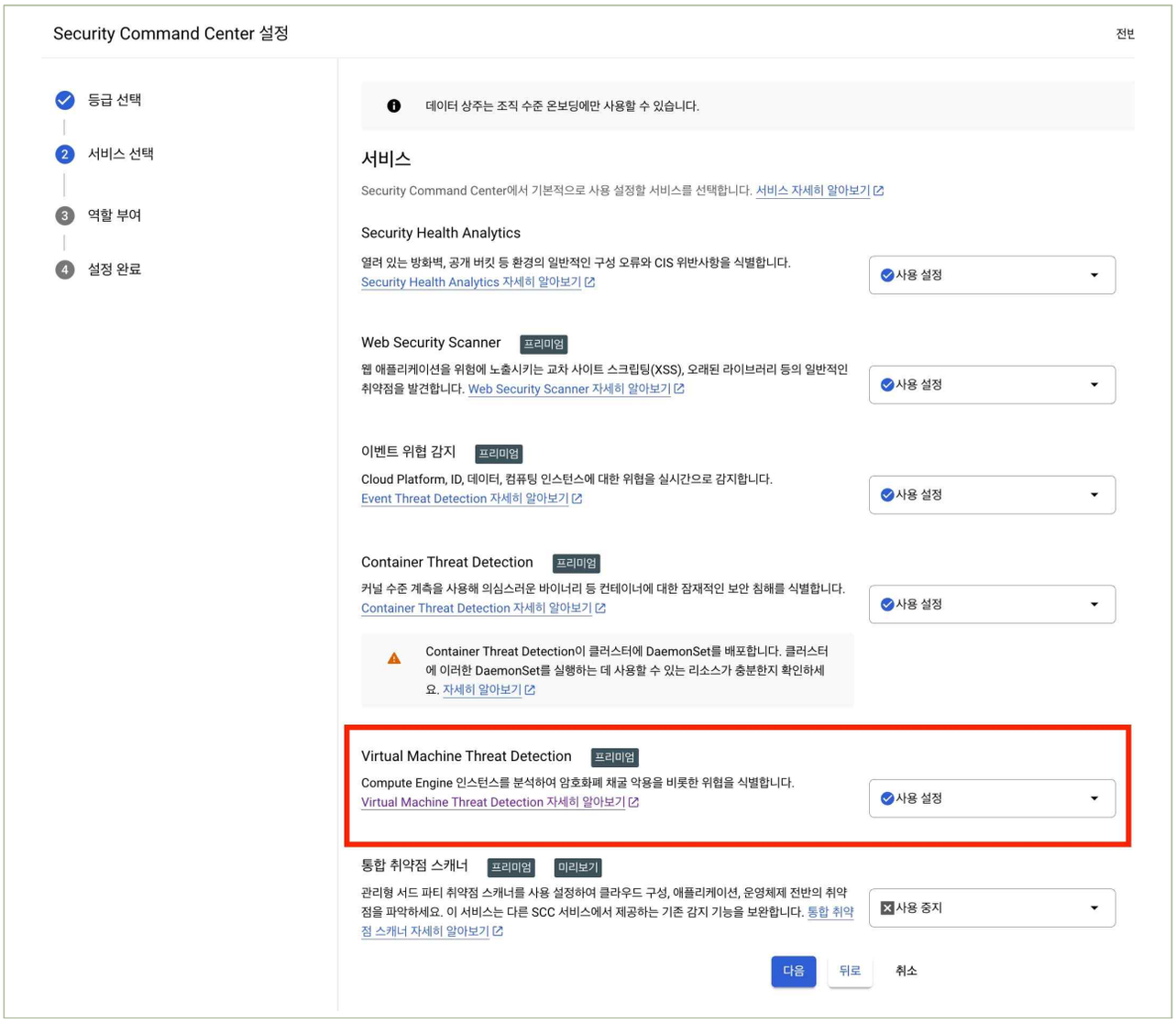


| 그림 1-7-1 | 보안 VM 섹션, 보안 VM 옵션 설정하기

- 가상 머신 위협 감지 설정하기
  - Google Cloud 콘솔의 Security Command Center 페이지로 이동합니다.
  - 만약 SCC 프리미엄 이상의 등급을 사용하고 있지 않다면, 가상 머신 위협 감지 기능이 활성화되는 SCC 프리미엄 이상 등급을 선택합니다. (* 참고: SCC 프리미엄 이상 등급을 사용할 경우, 서비스를 사용하는 양에 따라 과금이 발생할 수 있습니다. 활성화 이전 과금정책을 검토해

보시기를 바랍니다.)

- 서비스 선택 페이지에서 가상 머신 위협 감지(Virtual Machine Threat Detection) 기능이 사용설정 되었음을 확인합니다.
- Security Command Center 서비스를 위해 필요한 필수 권한을 부여하기 위하여, 새로운 서비스 계정을 생성 후 “securitycenter.serviceAgent” 역할을 부여합니다.
- 마지막 설정 완료 단계에서 “완료" 버튼을 클릭하여 설정을 완료합니다.
- 가상 머신 위협 감지에서 이상을 감지할 경우 SCC 페이지의 “발견항목” 항목에서 확인하실 수 있습니다.



| 그림 1-7-2 | 가상 머신 위협 감지 기능 활성화

- OS 레벨 이상의 영역은 Google Cloud의 책임 공유 및 공통된 운명 문서에 설명된 내용과 같이 따라 이용자의 영역으로 필요한 악성코드 통제방안 (예: 백신 등)을 이용자의 요구상황에 맞추어 설치 및 구성하시기를 권장 드립니다.

4 참고 사항

- 위 내용에 대한 좀 더 자세한 정보는 아래에 첨부한 문서에서 확인하실 수 있습니다.
  - 보안 VM이란 무엇인가요?
  - 빠른 시작: 보안 VM 옵션 사용 설정
  - 가상 머신 위협 감지 개요

2. 네트워크 관리

2.1. 업무 목적에 따른 네트워크 구성
2.2. 내부망 네트워크 보안 통제
2.3. 네트워크 보안 관제 수행
2.4. 공개용 웹서버 네트워크 분리
2.5. 네트워크 사설 IP 주소 할당 및 관리
2.6. 네크워크(방화벽 등) 정책 주기적 검토

2 네트워크 관리

1 기준

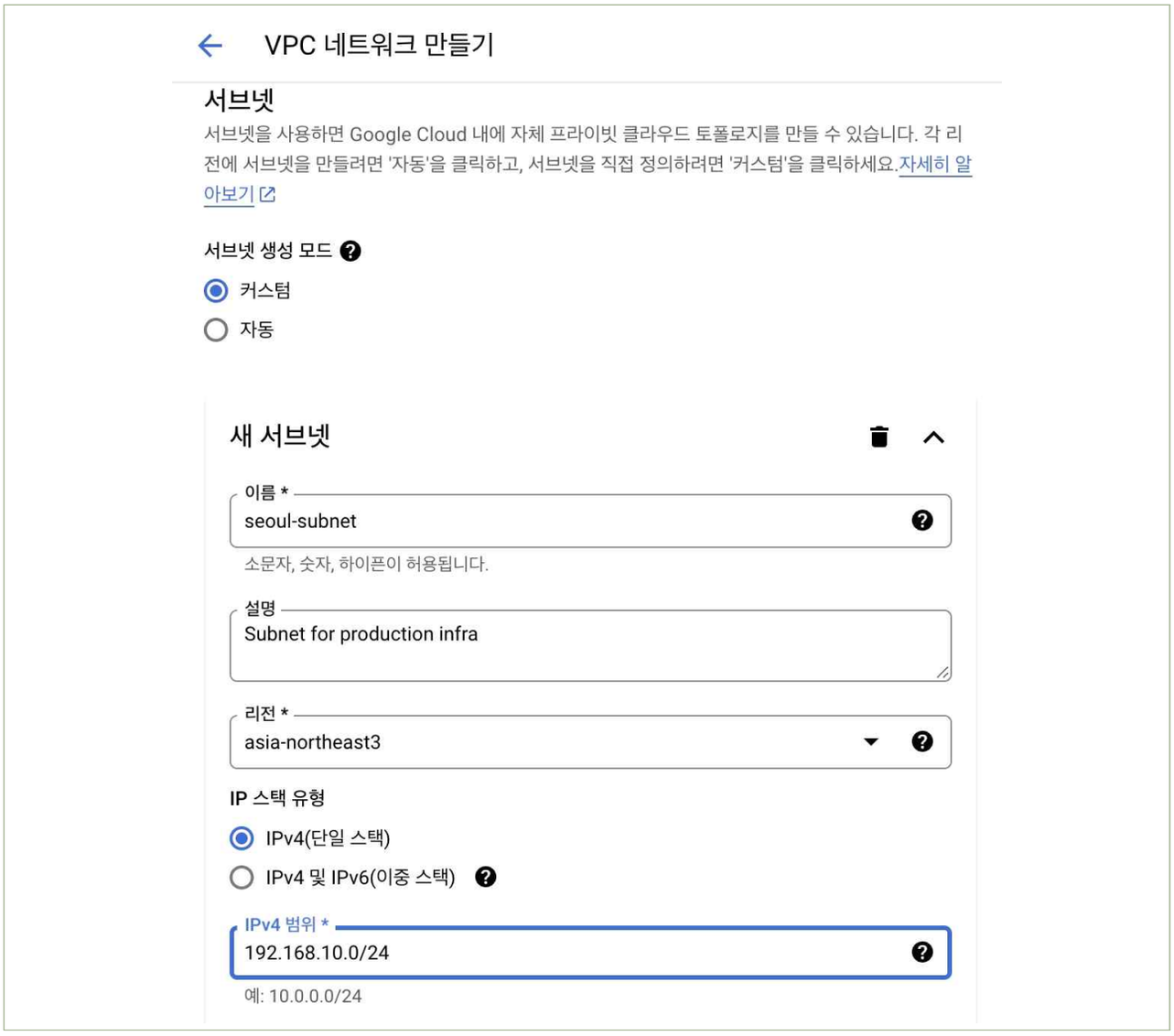
식별번호	기준	내용
2.1.	**업무 목적에 따른 네트워크 구성**	**클라우드 환경 내 업무 목적(개발, 운영, 업무 등)에 따른 네트워크를 구성하여야 한다.**

2 설명

- Google Cloud는 업무 목적에 따른 네트워크를 구성을 할 수 있도록 VPC (Virtual Private Cloud) 기능을 제공 합니다. VPC는 Compute Engine 가상 머신(VM) 인스턴스, Google Kubernetes Engine(GKE) 클러스터, 서버리스 워크로드 등과 같은 다양한 클라우드 리소스와 서비스에 네트워킹 기능을 제공합니다.
  - VPC 네트워크는 Google Cloud 내에서 가상화된다는 점을 제외하면 물리적 네트워크와 동일한 방식으로 생각할 수 있습니다. VPC 네트워크는 데이터 센터의 리전별 가상 서브 네트워크(서브넷) 목록으로 구성된 리소스로, 모든 리소스는 글로벌 통신망을 통해 연결됩니다. 이러한 VPC 네트워크는 Google Cloud에서 다른 VPC 네트워크와 논리적으로 서로 분리 및 격리됩니다.
  - 따라서 업무 목적에 따라 개별 생성된 VPC 간의 네트워크는 격리되어 있어 서로간의 통신이 불가능하며, 만약 서로 간의 통신이 필요한 경우에는 VPC 네트워크 피어링 기능 등을 사용하여 이를 허용하도록 구성할 수 있으며 VPC 방화벽 정책을 이용하여 트래픽을 통제할 수 있습니다.
  - VPC 네트워크 간의 연동은 VPC 네트워크 피어링 외에 HA VPN, 공유 VPC, Network Connectivity Center 등의 기능을 이용할 수 있으며 네트워크 연동을 위한 필요 기능과 요구사항에 맞게 선택할 수 있습니다. 이 경우에도 접근 통제 방안은 기본적으로 VPC 방화벽 정책을 통해 구현합니다.

3 우수 사례

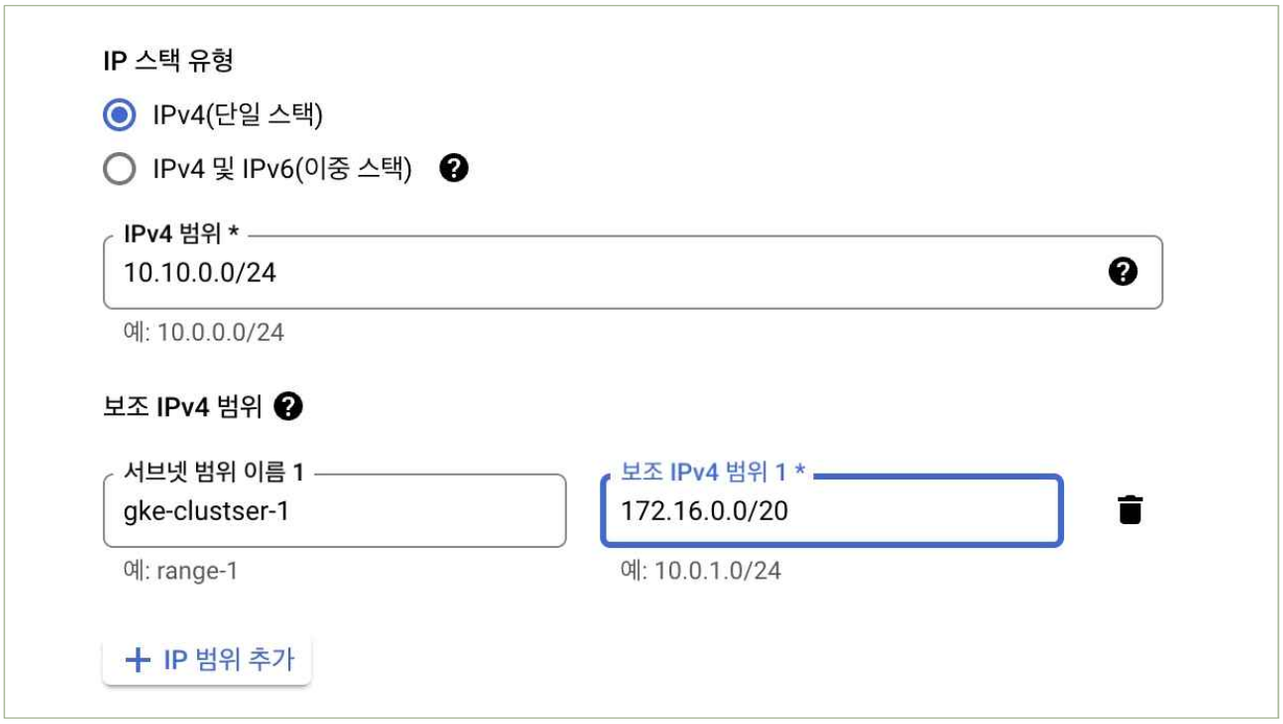
- ‘웹 콘솔 홈’ → ‘VPC 네트워크’ → ‘VPC 네트워크’ 로 이동합니다. 이후 **‘+VPC 네트워크 만들기’** 를 클릭하여 업무 목적에 따른 VPC 네트워크를 생성합니다.
  - VPC 네트워크 생성 시 업무나 운영의 목적이 잘 표현될 수 있도록 VPC 이름을 생성합니다. (예 : my-vpc1 보다는 dev-vpc와 같이 운영목적이 표현되는 이름을 권장합니다.)



| 그림 2-1-1 | VPC 네트워크 만들기

- 새 서브넷 설정에서 VPC 네트워크가 사용될 리전을 선택합니다. 그리고 IPv4 범위를 지정하여 VPC 네트워크에서 사용할 IP 주소 범위를 설정합니다.
  - 서브넷은 RFC 1918에 따른 비공개 IP 대역 사용이 권장됩니다. 비공개 용도로 공개 IP 대역을 설정할 수 있으나 권장되지 않습니다.

- Compute Engine(VM) 에서 여러 애플리케이션이 동작 되고 IP 주소 범위를 다르게 할당하여 구분을 하고자 할 때 보조 IP 주소 범위를 설정할 수 있습니다. 예를 들어 Google Kubernetes Engine (GKE)을 위한 서브넷에서 사용되는 경우입니다.



| 그림 2-1-2 | IP 주소 범위를 설정

- 단일 서브넷을 포함하는 VPC 네트워크를 생성할 수 있고, 또한 다수의 서브넷과 이러한 서브넷이 서로 다른 리전으로 설정 된 VPC 네트워크를 생성할 수도 있습니다. 그리고 이러한 서브넷들은 단일 VPC 내에서 통신이 가능한 환경으로 구성됩니다. 즉 하나의 VPC를 이용하여 다양한 글로벌 리전에 리소스를 배포하고 통신이 가능한 확장된 환경을 구성할 수 있습니다. 그러나 **서로 다른 VPC 간에는 통신할 수 없도록 분리되어 있는 네트워크**입니다.

| 그림 2-1-3 | VPC 네트워크 세부정보

- VPC 네트워크 생성 시 서브넷 생성 모드를 자동으로 선택할 경우 모든 리전에 /20 의 서브넷이 자동 생성 및 할당되며, 이는 모든 리전에 VM 을 배포하고 서로 간에 통신할 수 있도록 VPC 네트워크가 확장됩니다. 따라서 VPC 네트워크 생성 시 서브넷 생성 모드는 커스텀으로 설정하고 사용이 꼭 필요한 리전에만 서브넷을 생성합니다. (예 : asia-northeast3 / 서울 리전)
- 서로 다른 VPC 네트워크간의 연결이 필요할 경우 VPC 네트워크 피어링, HA VPN, 공유 VPC, Network Connectivity Center 중 하나를 이용하여 구성할 수 있습니다.
- '웹 콘솔 홈' → 'VPC 네트워크' → 'VPC 네트워크 피어링'로 이동합니다. 이후 **'연결 만들기'**를 클릭하여 연결이 필요한 VPC 네트워크 피어링을 설정합니다.

| 그림 2-1-4 | VPC 네트워크 피어링

4 참고 사항

- Google Cloud가 제공하는 VPC네트워크에 대해서 다음 링크에서 더 자세한 내용을 확인할 수 있습니다.
  - Virtual Private Cloud (VPC) overview
- Google Cloud가 제공하는 VPC네트워크 간의 피어링 정보는 다음 링크를 참고하시기 바랍니다.
  - VPC Network Peering | Google Cloud
- Google Cloud가 제공하는 방화벽 정보는 다음 링크를 참고하시기 바랍니다.
  - VPC firewall rules | Cloud NGFW

1 기준

식별번호	기준	내용
2.2.	내부망 네트워크 보안 통제	**클라우드 환경 내 내부망 구성 시 보안 통제 방안을 수립하고 적용하여야 한다.**

2 설명

- 클라우드 환경 내 내부망을 구성하는 경우 외부 침입, 비인가 접근 등으로 보호될 수 있도록 보안 통제 방안을 수립하고 적용하여야 한다.
  - VPC 등 네트워크 관련 기능을 통한 네트워크 접근 통제(인터넷망 등)
  - VPC 네트워크 방화벽 기능을 통한 네트워크 구성(인/아웃바운드 통제 등)
  - 내부망으로 구현한 가상자원(서버, 데이터베이스 등)에 공인IP 미할당
  - 방화벽 서비스를 통한 IP 통제 등

3 우수 사례

- 클라우드 환경 내 내부망은 서브넷을 이용하여 구성 됩니다. VPC 네트워크는 단일 서브넷을 포함할 수 있고, 또한 다수의 서브넷과 이러한 서브넷이 서로 다른 리전으로 설정된 VPC 네트워크를 생성할 수도 있습니다. 그리고 이러한 서브넷들은 단일 VPC 내에서 통신이 가능한 환경으로 구성됩니다. 그러나 서로 다른 VPC 간에는 통신할 수 없도록 분리 되어있는 네트워크입니다.
- 트래픽의 접근 통제는 방화벽 규칙을 사용합니다. 서브넷을 포함한 모든 VPC 네트워크 환경은 수신되는 트래픽에 대해 묵시적 거부 방화벽 규칙이 있어 기본적으로 모든 트래픽에 대한 접근을 차단하지만 외부로 송신하는 트래픽에 대해서는 묵시적인 허용 규칙이 있기 때문에 송신하는 트래픽에 대해서는 차단하지 않습니다. 따라서 서로 다른 VPC 네트워크 간의 통신뿐만 아니라 VPC 내부 및 외부와의 통신을 제어하기 위해서는 적절한 방화벽 규칙을 생성하여 반드시 필요한 트래픽의 송수신을 허용해야 합니다. 따라서 서로 다른 VPC 네트워크 간의 통신뿐만 아니라 VPC 내부의 리소스간 통신을 위해서도 적절한 방화벽 규칙을 생성하여 반드시 필요한 트래픽의 접근만을 허용해야 합니다.
  1. ‘웹 콘솔 홈’ → ‘네트워크 보안’ → ‘방화벽 정책’ 로 이동합니다. 이후 ‘**방화벽 규칙 만들기**’를 클릭하여 필요한 방화벽 규칙을 구성합니다.

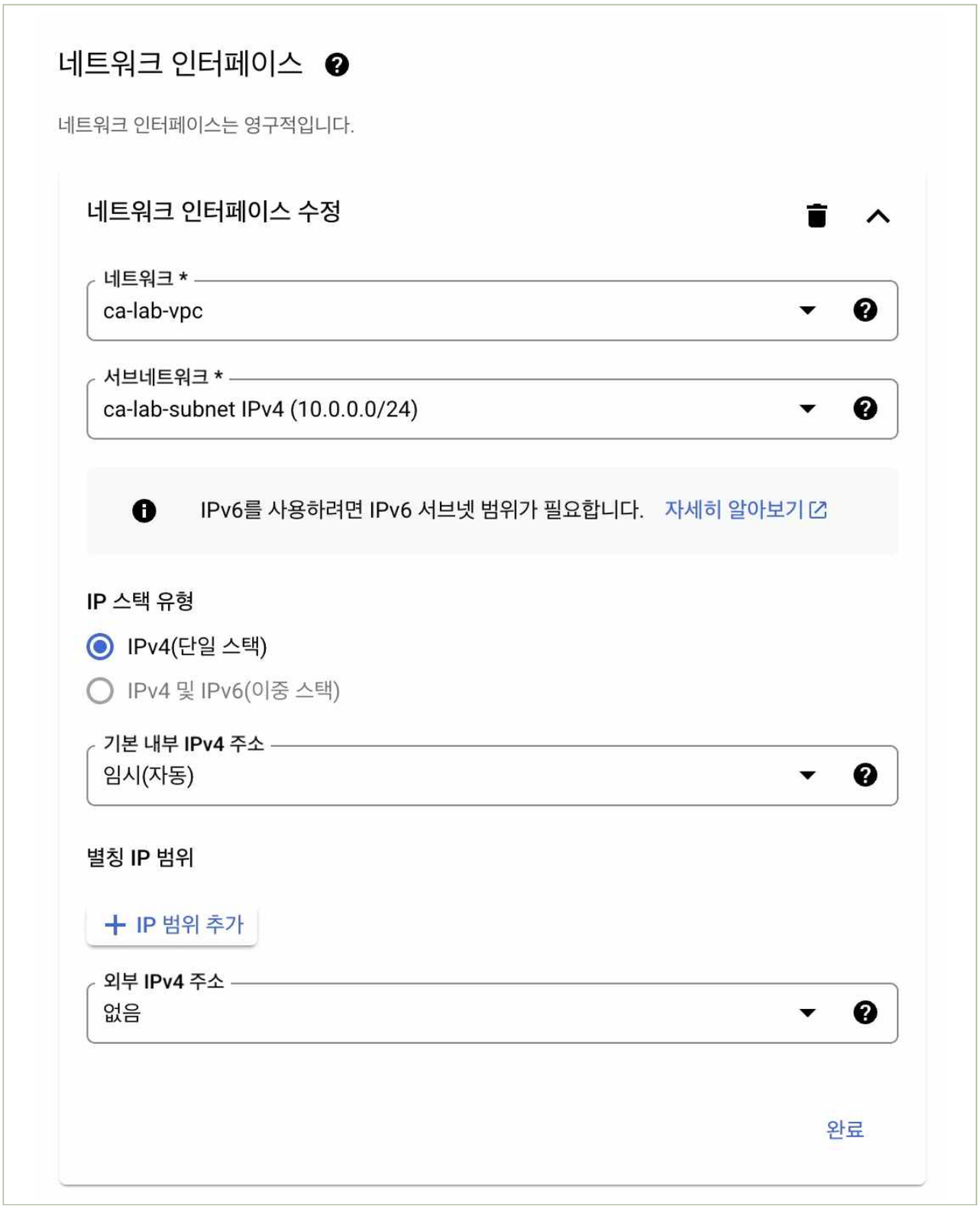
2. ‘로그’ 설정에서 ‘사용’을 선택하는 것을 권장합니다. 그러면 방화벽 정책에 일치할 경우 로그 정보를 생성합니다.
3. ‘네트워크’ 설정에서 해당 방화벽 규칙이 적용될 VPC 네트워크를 선택합니다.
4. ‘우선순위’는 다른 방화벽 규칙들과 비교하여 해당 방화벽 규칙이 평가될 순서를 설정합니다. ‘우선순위’의 값이 낮을 수록 해당 방화벽 규칙이 먼저 평가됩니다.
5. ‘트래픽 방향’ 설정에서 ‘수신’ 또는 ‘송신’을 선택합니다. ‘수신’은 외부에서 VPC 네트워크로 유입되는 트래픽을 의미하며, ‘송신’은 VPC 네트워크에서 외부로 나가는 트래픽을 의미합니다.
6. ‘일치 시 작업’에서 ‘허용’ 또는 ‘거부’를 선택합니다. 앞서 언급한 대로 VPC 네트워크 환경은 수신되는 트래픽에 대해 묵시적 거부 방화벽 규칙이 있으므로 필요한 ‘허용’ 규칙을 생성하고 관리하는 것이 VPC 네트워크 접근 통제의 기본 법칙입니다.

| 그림 2-2-1 | 방화벽 규칙 만들기

7. ‘대상’ 설정을 사용하여 해당 방화벽 규칙이 적용될 리소스를 제안하거나 선택할 수 있습니다. 예를 들어 아래 그림과 같이 대상 태그를 ‘web’이라고 지정할 경우, ‘web’이라는 태그를 가지고 있는 VM 인스턴스에 대해서만 해당 방화벽 규칙이 적용됩니다. ‘네트워크의 모든 인스턴스’를 선택할 경우 해당 VPC 네트워크의 모든 VM 인스턴스에 적용됩니다.
8. IP 정보, 프로토콜 및 포트 정보 설정을 사용하여 방화벽 규칙을 작성한 후 ‘만들기’ 버튼을 클릭하면 방화벽 규칙이 생성됩니다.

| 그림 2-2-2 | 방화벽 규칙 만들기

- 클라우드 환경의 리소스를 생성할 때 외부 IPv4 주소를 할당하지 않는 한 외부와 격리되어 내부망에서만 통신이 가능합니다. 예를 들어 아래와 같이 VM 인스턴스를 생성 시 '고급 옵션' → '네트워킹' → '네트워크 인터페이스'에서 '외부 IPv4 주소' 항목을 '없음'으로 설정합니다.



| 그림 2-2-3 | 네트워크 인터페이스

- 공인 IP를 리소스에 할당하지 못하도록 조직 관리자가 조직 정책을 이용하여 아래 그림과 같이 제한할 수 있습니다. 'IAM 및 관리자' → "조직 정책"에서 "constraints/compute.vmExternalIpAccess" 를 검색 후 해당 정책을 거부하도록 설정합니다. 이러한 설정은 조직의 판단에 따라 선택적으로 사용할 수 있습니다.

| 그림 2-2-4 | 외부 IP 조직 정책 설정

4 참고 사항

- Google Cloud 의 Compute Engine (VM 인스턴스) 설정은 아래 링크에서 보다 자세한 내용을 확인할 수 있습니다.
  - Create and start a Compute Engine instance
- Google Cloud가 제공하는 방화벽 정보는 다음 링크를 참고하시기 바랍니다.
  - VPC firewall rules | Cloud NGFW
- Google Cloud가 제공하는 조직 정책에 대한 자세한 내용과 설정은 다음 링크를 참고하시기 바랍니다.
  - How-to guides | Resource Manager Documentation | Google Cloud

1 기준

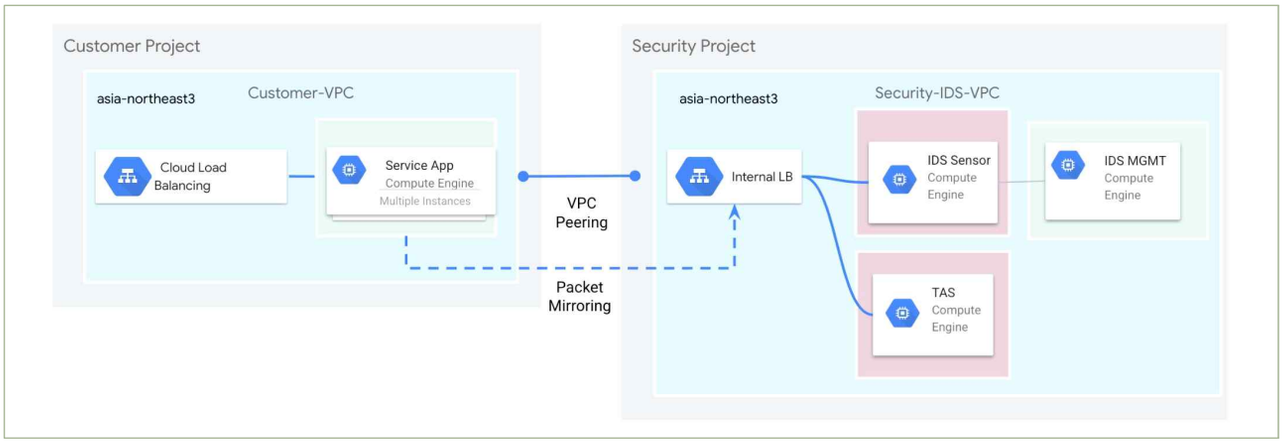
식별번호	기준	내용
2.3.	**네트워크 보안 관제 수행**	**클라우드 환경 내 금융회사 가상자원을 보호하기 위한 네트워크 보안 관제를 수행하여야 한다.**

2 설명

- 클라우드 환경 내 금융회사 가상자원을 보호하기 위한 네트워크 보안 관제를 수행하여야 한다.
  - Google Cloud는 패킷 미러링 방식으로 금융회사 보안 관제 서비스와 연동하여 관제를 수행할 수 있습니다.
  - 또한 Google Cloud는 Cloud Armor 서비스를 사용하여 가상자원 보호를 위한 네트워크 보안관제 및 DDoS방어 및 WAF 등의 기능을 구성할 수 있습니다.
  - GCE 및 GKE 서비스 등에 대하여 금융보안원에 가상화 방식의 패킷 미러링 데이터 전송을 통해 통합 보안관제 서비스를 구성하실 수 있습니다.

3 우수 사례

- 클라우드내에 발생하는 네트워크 트래픽은 '**패킷 미러링**' 기능을 이용하여 적절한 관제 솔루션과의 연동을 구성할 수 있습니다.

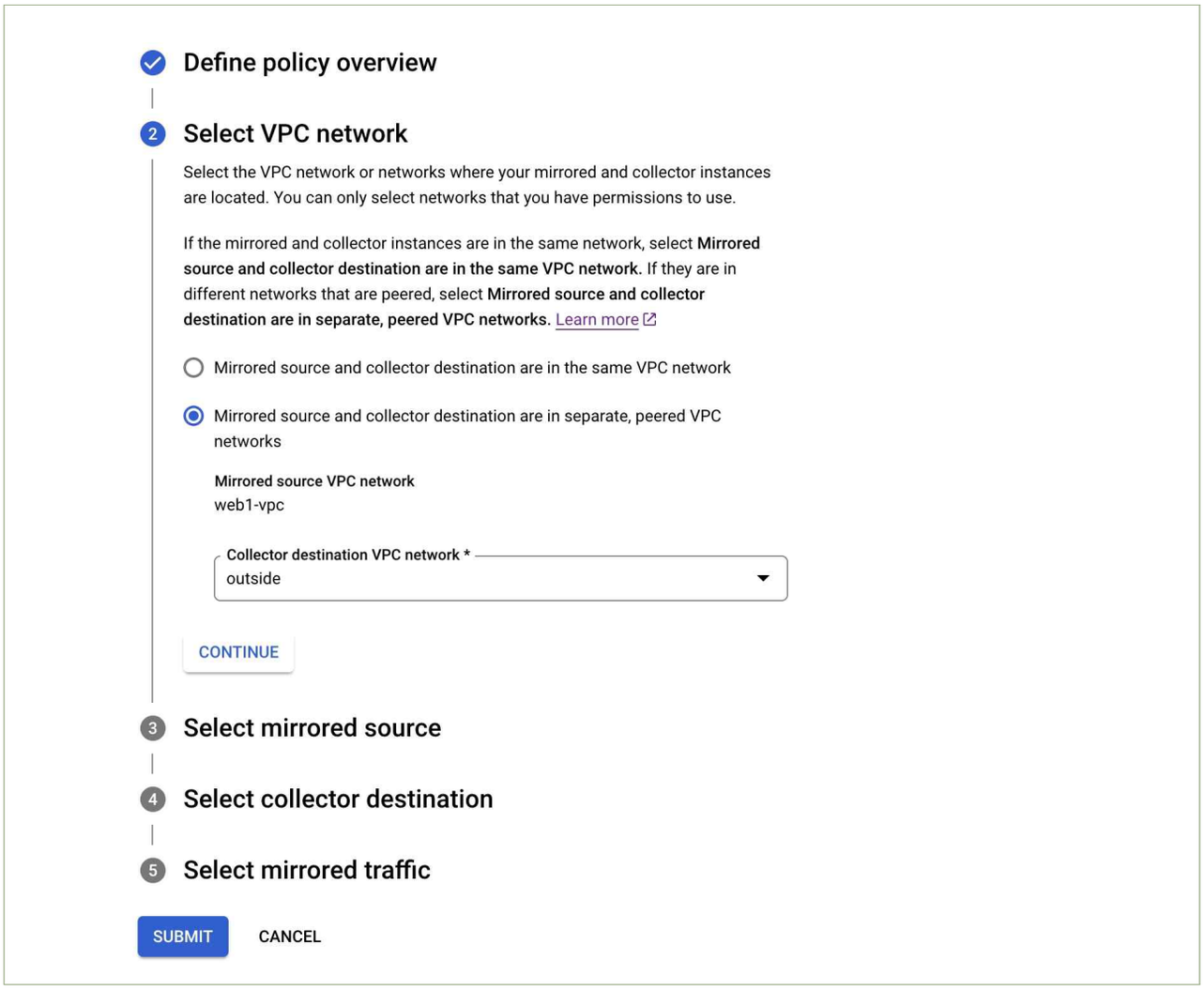


| 그림 2-3-1 | 패킷 미러링 구성도

- 'VPC 네트워크' → '패킷 미러링' → '정책 만들기' 버튼을 클릭하여 필요한 리소스에 대해 패킷 미러링을

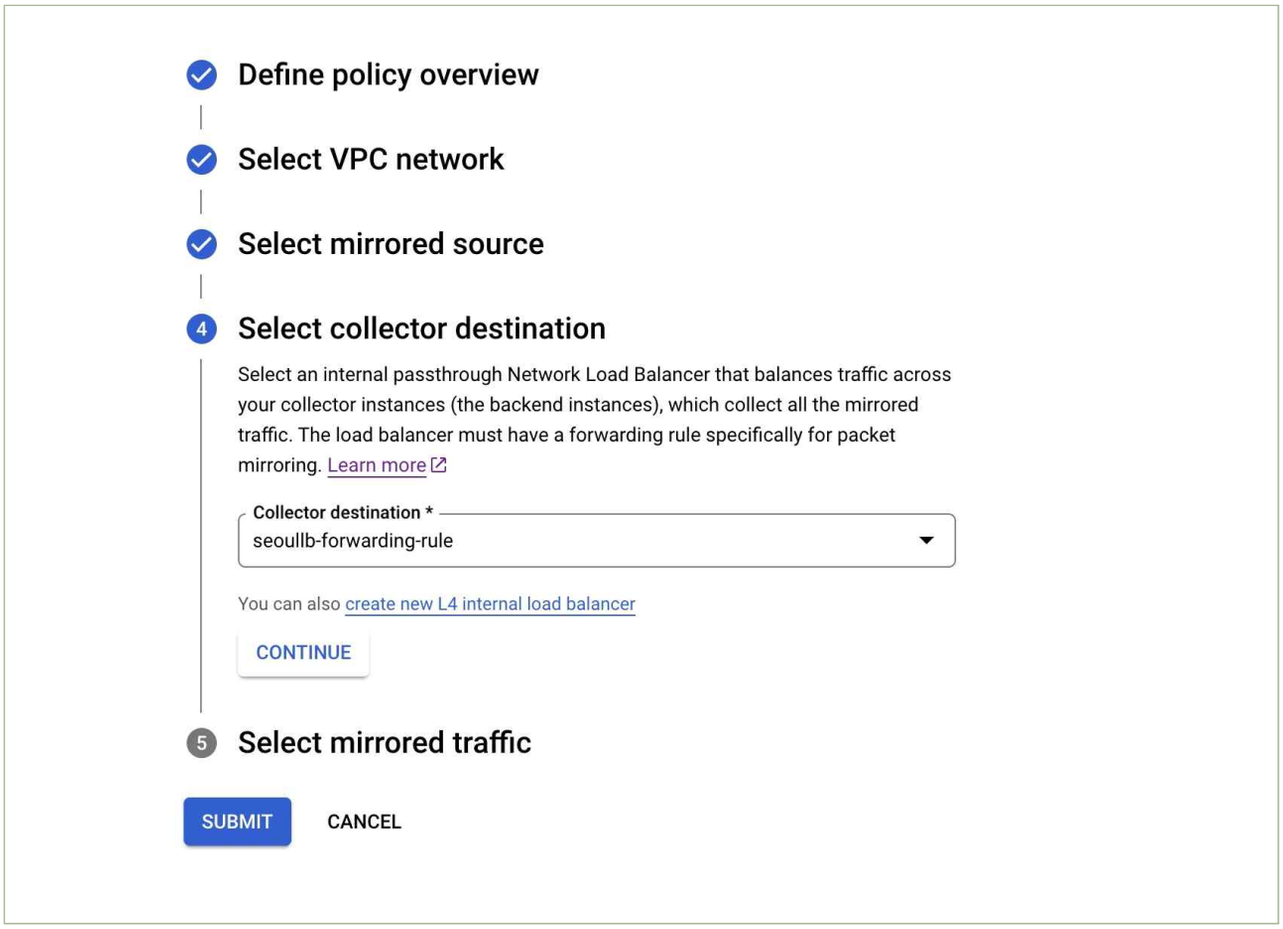
구성할 수 있습니다.

- '정책 개요 정의'에서 정책 이름과 패킷 미러링 할 리소스가 있는 리전을 선택합니다.
- 'VPC 네트워크 선택'에서 패킷 미러링 할 리소스의 VPC 네트워크와 미러링 트래픽을 수집할 리소스가 있는 VPC 네트워크를 선택합니다. 미러링과 수집기는 같은 VPC 네트워크에 있거나 다른 VPC 네트워크에 있을 수 있습니다. 만약 미러링과 수집기가 다른 VPC 네트워크에 있는 경우 VPC 피어링을 이용하여 VPC 네트워크 간 통신이 가능해야 합니다.



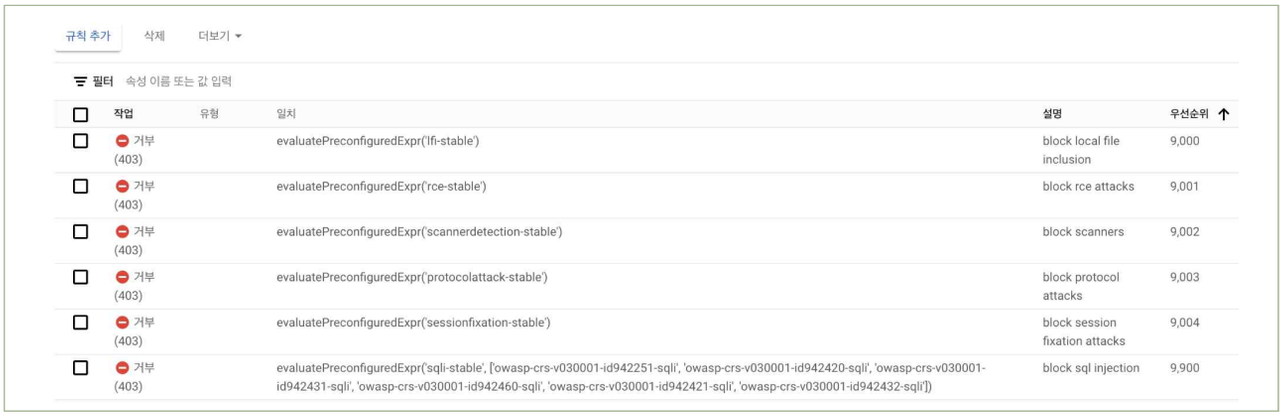
| 그림 2-3-2 | 패킷 미러링 구성 설정

- 패킷을 미러링 할 리소스와 수집기를 설정 합니다. 미러링 할 리소스는 단일 VM 인스턴스나 그룹을 지정할 수 있으며, 수집기의 경우 내부 패스스루 네트워크 부하 분산기를 선택해야 합니다.



| 그림 2-3-3 | 패킷 미러링 구성 설정

- Google Cloud 는 DDoS, WAF 보안을 위해 Cloud Armor 서비스를 사용할 수 있습니다. Google Cloud Armor를 사용하면 DDoS 공격과 교차 사이트 스크립팅(XSS), SQL 삽입(SQLi)과 같은 애플리케이션 공격을 포함한 여러 유형의 위협으로부터 Google Cloud 배포를 보호할 수 있습니다.
  - 보안 규칙은 크게 2가지인 Condition과 Action 설정으로 구성됩니다.
    - Condition 설정은 Cloud Armor가 보호하고 있는 애플리케이션과 리소스로 유입되는 트래픽 중에서, 어떠한 트래픽을 대상으로 보안 규칙을 적용할지 매치 조건을 선언하는 작업입니다.
    - 그리고 이렇게 조건과 일치하는 트래픽은 Action 설정을 이용하여 조치 방법을 결정할 수 있습니다. 허용/차단 설정이나 Redirect, Rate-limit 등 다양한 조치 방법을 구성할 수 있습니다.
    - '네트워크 보안' → 'Cloud Armor 정책' → '정책 만들기'를 클릭하여 Cloud Armor 정책을 생성합니다.
  - '규칙' → '규칙 추가'를 클릭하여 개별 보안 규칙을 추가합니다. 기본적인 IP 나 지역 기반 차단 정책뿐만 아니라 OWASP Top 10 등 WAF룰을 설정할 수 있습니다.



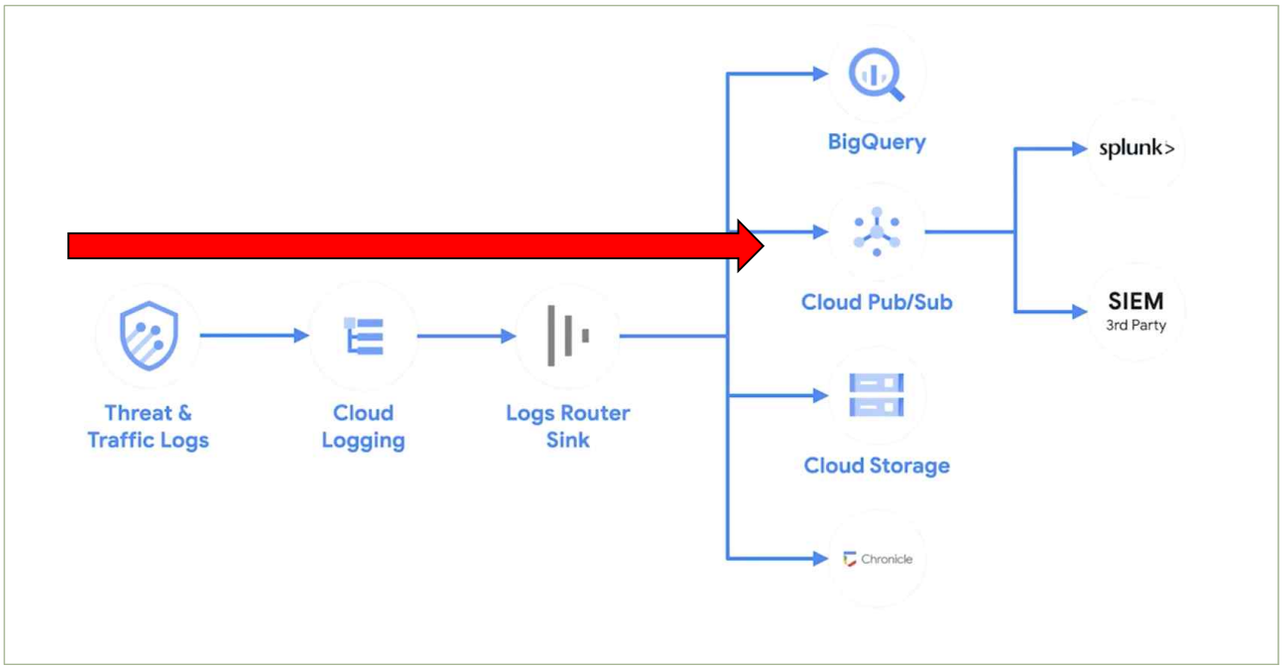
규칙 추가 삭제 더보기

필터 속성 이름 또는 값 입력

작업	유형	일치	설명	우선순위
거부 (403)		evaluatePreconfiguredExpr('lfi-stable')	block local file inclusion	9,000
거부 (403)		evaluatePreconfiguredExpr('rce-stable')	block rce attacks	9,001
거부 (403)		evaluatePreconfiguredExpr('scannerdetection-stable')	block scanners	9,002
거부 (403)		evaluatePreconfiguredExpr('protocolattack-stable')	block protocol attacks	9,003
거부 (403)		evaluatePreconfiguredExpr('sessionfixation-stable')	block session fixation attacks	9,004
거부 (403)		evaluatePreconfiguredExpr('sqli-stable', ['owasp-crs-v030001-id942251-sqli', 'owasp-crs-v030001-id942420-sqli', 'owasp-crs-v030001-id942431-sqli', 'owasp-crs-v030001-id942460-sqli', 'owasp-crs-v030001-id942421-sqli', 'owasp-crs-v030001-id942432-sqli'])	block sql injection	9,900

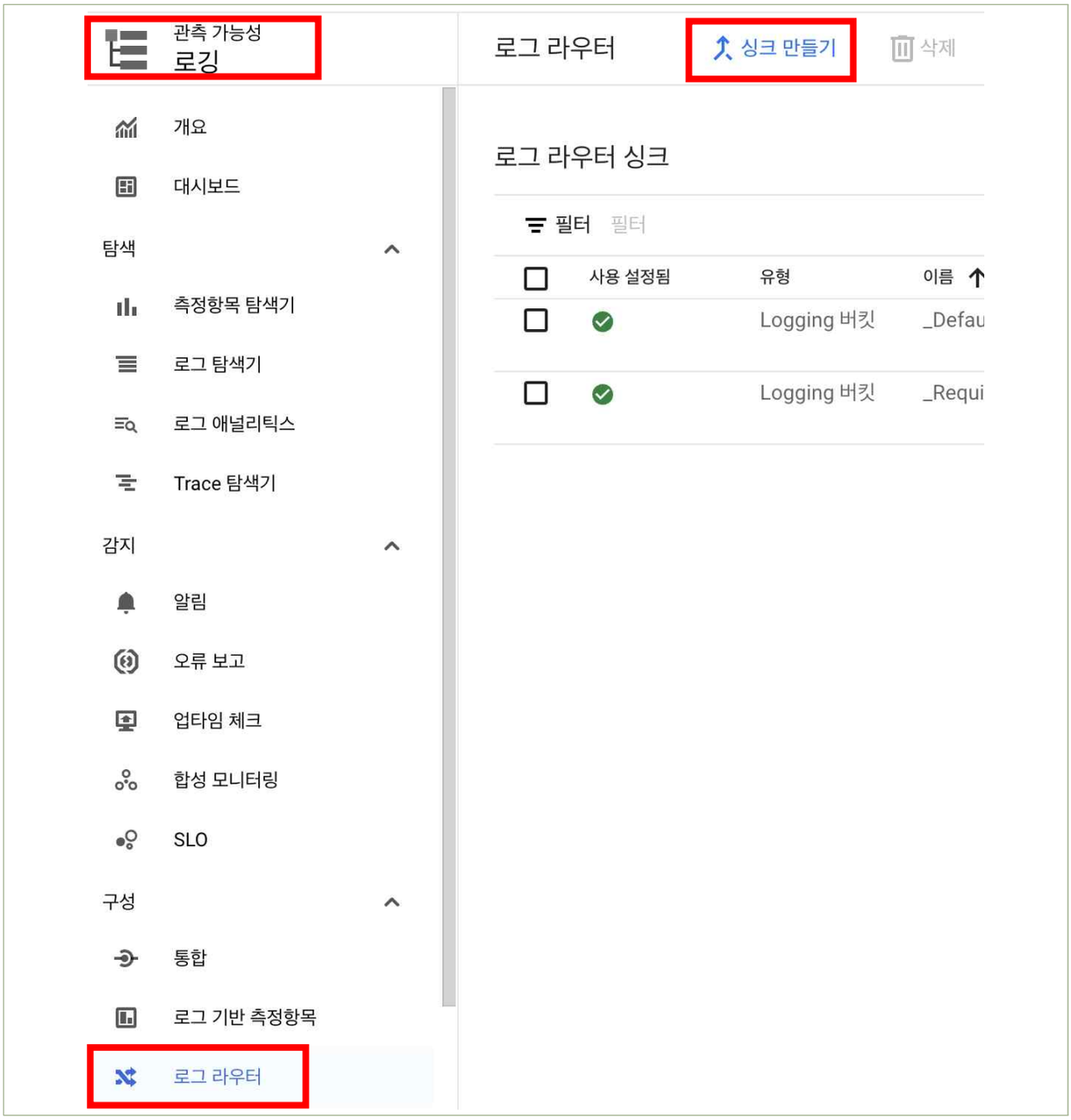
| 그림 2-3-4 | Cloud Armor 정책 설정

- Cloud Armor에 대한 네트워크 관제는 위협이나 트래픽에 대한 특이사항 발생 시 발생하는 Log정보를 Cloud Logging이라는 곳에 저장하고 처리하는 방식으로 진행됩니다. 발생되는 Log들은 Logs Router Sink 규칙을 구성하여 Log를 전달할 목적지와 방식을 지정합니다.



| 그림 2-3-5 | Cloud Armor 구성

- '웹 콘솔 홈' → '로깅' → '로그 라우터' 항목으로 이동하여 우상단에 '싱크 만들기'를 선택



| 그림 2-3-6 | Cloud Armor 관련 Cloud Logging 설정

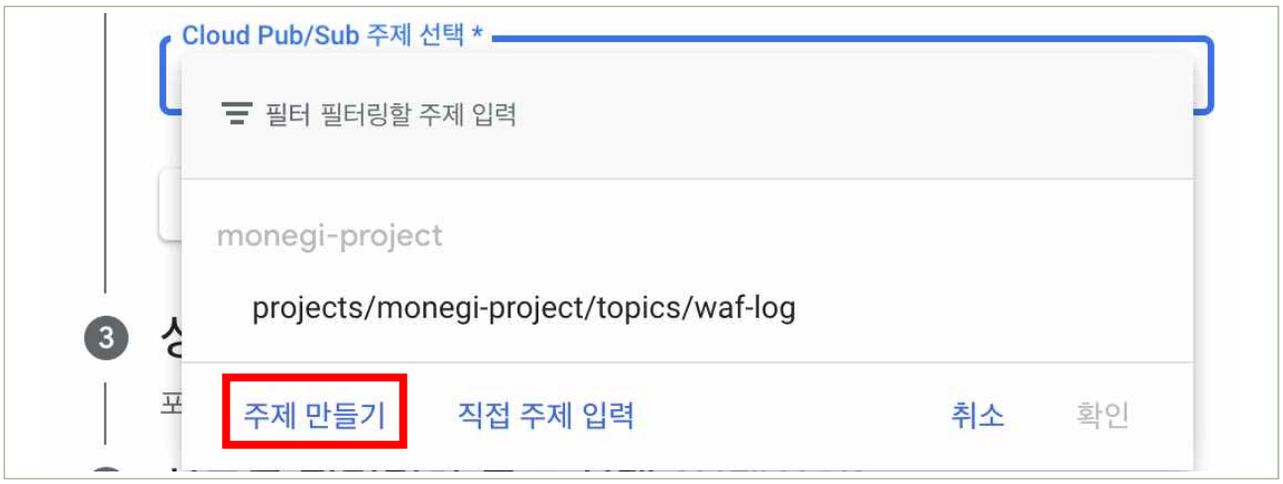
- 로그 라우팅 싱크의 이름과 설명을 기입하고 다음을 선택

| 그림 2-3-7 | Google Cloud Cloud Armor 관련 Cloud Logging 설정(싱크 이름)

- 로그를 전달할 대상을 선택, 외부 SIEM 등으로 보낼 때는 'Cloud Pub/Sub주제'를 선택

| 그림 2-3-8 | Cloud Armor 관련 Cloud Logging 설정(싱크 대상)

- 기존에 Pub/sub연결이 있다면 선택해도 되며, 없다면 신규로 '주제만들기' 선택



| 그림 2-3-9 | Cloud Armor 관련 Cloud Logging 설정(주체 만들기)

- Pub/sub 주제를 만들고 Log를 전달하는 구성을 완료하면, 이 주제를 구독할 온프레미스 SIEM을 구독자(Subscriber)로 연결

4 참고 사항

- Google Cloud의 패킷미러링 기능은 다음의 링크를 통해 더 자세한 정보를 확인할 수 있습니다.
  - Packet Mirroring | VPC | Google Cloud

- Google Cloud 의 Cloud Armor 에 대한 보다 자세한 내용과 설정 방법은 아래 링크를 참고하시기 바랍니다.
  - Product overview | Google Cloud Armor
  - [Cloud Armor 시리즈 1] Cloud Armor 정책의 종류와 이해
  - [Cloud Armor 시리즈 2] Cloud Armor 의 보안 규칙 사용하기 | Google Cloud 블로그
  - [Cloud Armor 시리즈 3] Cloud Armor 의 보안 이벤트 확인하기

- Google Cloud의 Pub/sub에 대한 보다 자세한 내용과 설정 방법은 아래 링크를 참고하시기 바랍니다.
  - https://cloud.google.com/logging/docs/export/pubsub#integrate-thru-pubsub

1 기준

식별번호	기준	내용
2.4.	공개용 웹서버 네트워크 분리	**클라우드 환경을 통한 공개용 웹서버 구현 시 내부통신망과 분리하여 내부통신망과 외부통신망 사이 별도의 독립된 통신망("이하 DMZ")을 구현하고 안전하게 보호하여야 한다.**

2 설명

- 클라우드 환경을 통한 공개용 웹서버의 경우 내부통신망과 분리하여 내부통신망과 외부통신망 사이 별도의 독립된 통신망에 구현하고 접근통제를 수행하여야 한다.

  - VPC 등 네트워크 분리 기능을 통한 DMZ 망 구축 후 공개용 웹서버 구현
    - 클라우드 환경에서의 네트워크는 VPC(Virtual Private Cloud) 단위로 구성되므로, 공개용 웹서버 구현을 위한 **별도의 독립된 DMZ VPC를 구성**합니다. 이 DMZ VPC의 경우에는 다른 서비스를 위한 내부 통신망을 위한 VPC와는 구분되어야 합니다.
    - 외부 통신을 위해서는 외부 자원과 통신을 허용하게 하는 구성이 필요합니다. 외부 공인 IP를 구성하여야 하여, 이 외부 IP할당 부분은 기본적으로 **DMZ VPC내에서만 허용하도록 관리**하여야 합니다.
  - 공개용 웹서버 직접 접근 시 통제(ACL 등)에 의한 중요단말기 등에서 접근하도록 관리
    - 공개용 웹서버를 관리적인 목적에 의해 직접 접근하여야 할 경우에는 사전에 정의된 중요단말기의 공인IP주소나 사설 IP를 식별하여 이를 선별적으로 허용해주어야 합니다. 이는 Cloud Firewall 규칙이나 정책으로 가능합니다.

3 우수 사례

- **(VPC 네트워크)** 네트워크 생성 시 DMZ VPC상에서만 외부 공인 IP를 구성하여 통신하도록 합니다. '웹 콘솔 홈' → 'VPC 네트워크' → 'VPC 네트워크'로 이동합니다. 이후 **'+VPC 네트워크 만들기'**를 클릭하여 VPC 네트워크를 생성합니다.

| 그림 2-4-1 | VPC 네트워크 만들기

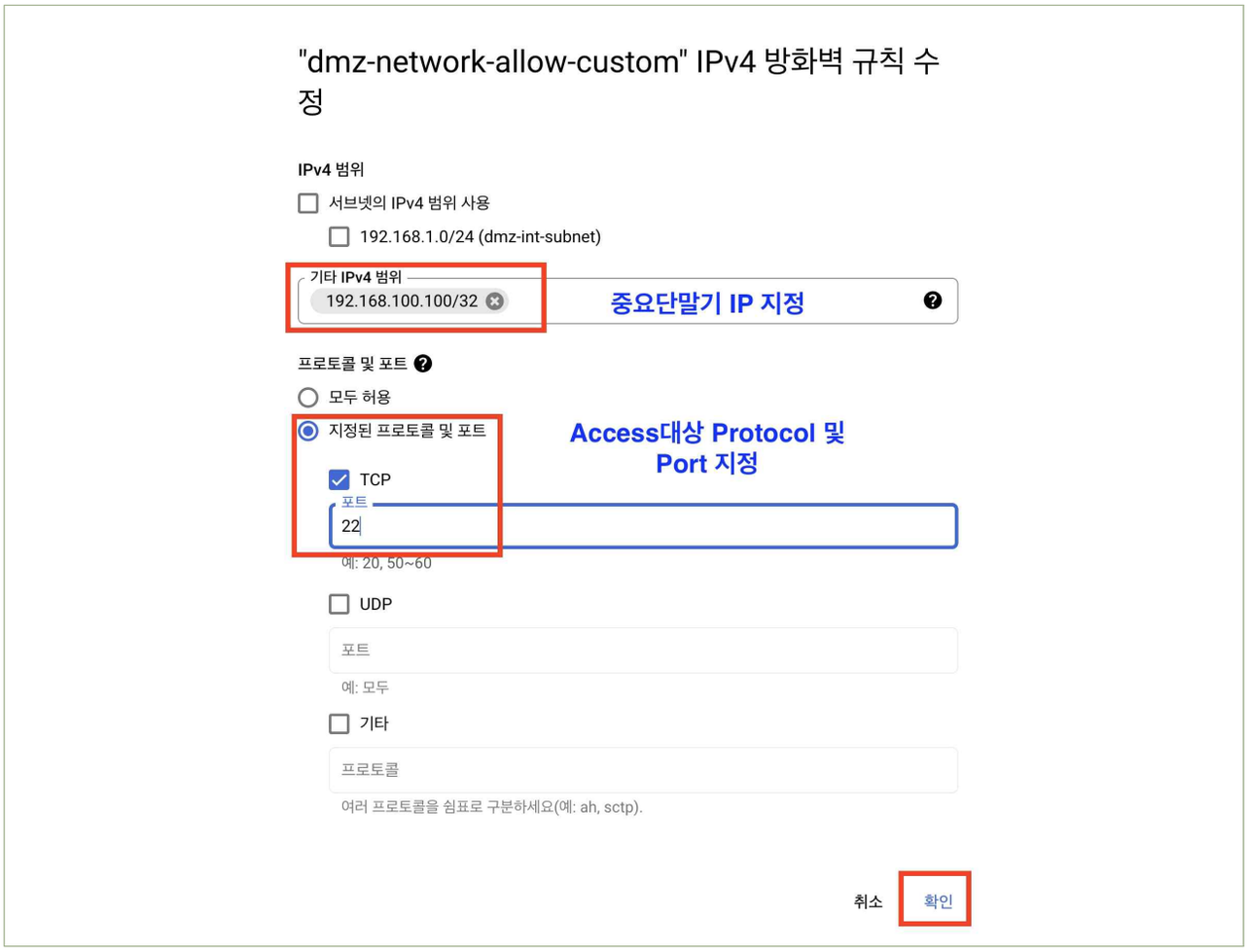
- VPC 네트워크를 구분할 '이름'과 '설명'을 적습니다. VPC 네트워크 ULA 내부 IPv6 범위에 관해서는 IPv6 통신이 필요 없을 시 사용하지 않아도 됩니다.

| 그림 2-4-2 | VPC 네트워크 만들기

- **새 서브넷** 섹션에서 서브넷에 다음 구성 매개변수를 지정합니다.
  - 서브넷 **이름**을 입력합니다.
  - **리전**을 선택합니다.
  - **IP 주소 범위**를 입력합니다. 이 범위는 서브넷의 기본 IPv4 범위입니다.
    RFC 1918 주소가 아닌 범위를 선택하는 경우 범위가 기존 구성과 충돌하지 않는지 확인합니다.
  - **비공개 Google 액세스**: 서브넷을 만들 때 또는 나중에 서브넷을 수정하여 서브넷에 비공개 Google 액세스 사용 여부를 선택합니다.
  - **흐름 로그**: 서브넷을 만들 때 또는 나중에 서브넷을 수정하여 서브넷에 VPC 흐름 로그 사용 여부를 선택합니다.
  - **완료**를 클릭합니다.
- 서브넷을 추가하려면 **서브넷 추가**를 클릭하고 이전 단계를 반복합니다. 네트워크를 만든 후에 네트워크에 서브넷을 더 추가할 수도 있습니다.
- **방화벽 규칙** 섹션의 **IPv4 방화벽 규칙**에서 사전 정의된 방화벽 규칙을 0개 이상 선택합니다. 이 규칙은 인스턴스에 연결하는 일반적인 사용 사례를 다룹니다.
  사전 정의된 규칙을 선택하지 않으면 네트워크를 만든 후 자체 방화벽 규칙을 만들 수 있습니다. 사전 정의된 각 규칙 이름은 만들려는 VPC 네트워크의 이름인 dmz-network로 시작합니다. **IPv4 방화벽 규칙** 탭에서 dmz-network**-allow-custom**라는 사전 정의된 인그레스 방화벽 규칙을 수정할 수 있습니다.

| 그림 2-4-3 | 방화벽 규칙

- 규칙이 포함된 행의 오른쪽에서 **수정**을 클릭하여 **중요단말기가 위치한 서브넷을 선택하고 IPv4 범위를 추가하고 프로토콜 및 포트를 지정**합니다. 예를 들어 중요단말기의 IP가 192.168.100.100이라면, 192.168.100.100/32을 구성하고, tcp 22번 포트만 허용하는 규칙을 만들어 줍니다.
  나중에 서브넷을 추가할 경우 dmz-network**-allow-custom** 방화벽 규칙은 자동으로 업데이트되지 않습니다. 새 서브넷에 대한 방화벽 규칙이 필요한 경우 방화벽 구성을 업데이트하여 규칙을 추가해야 합니다.



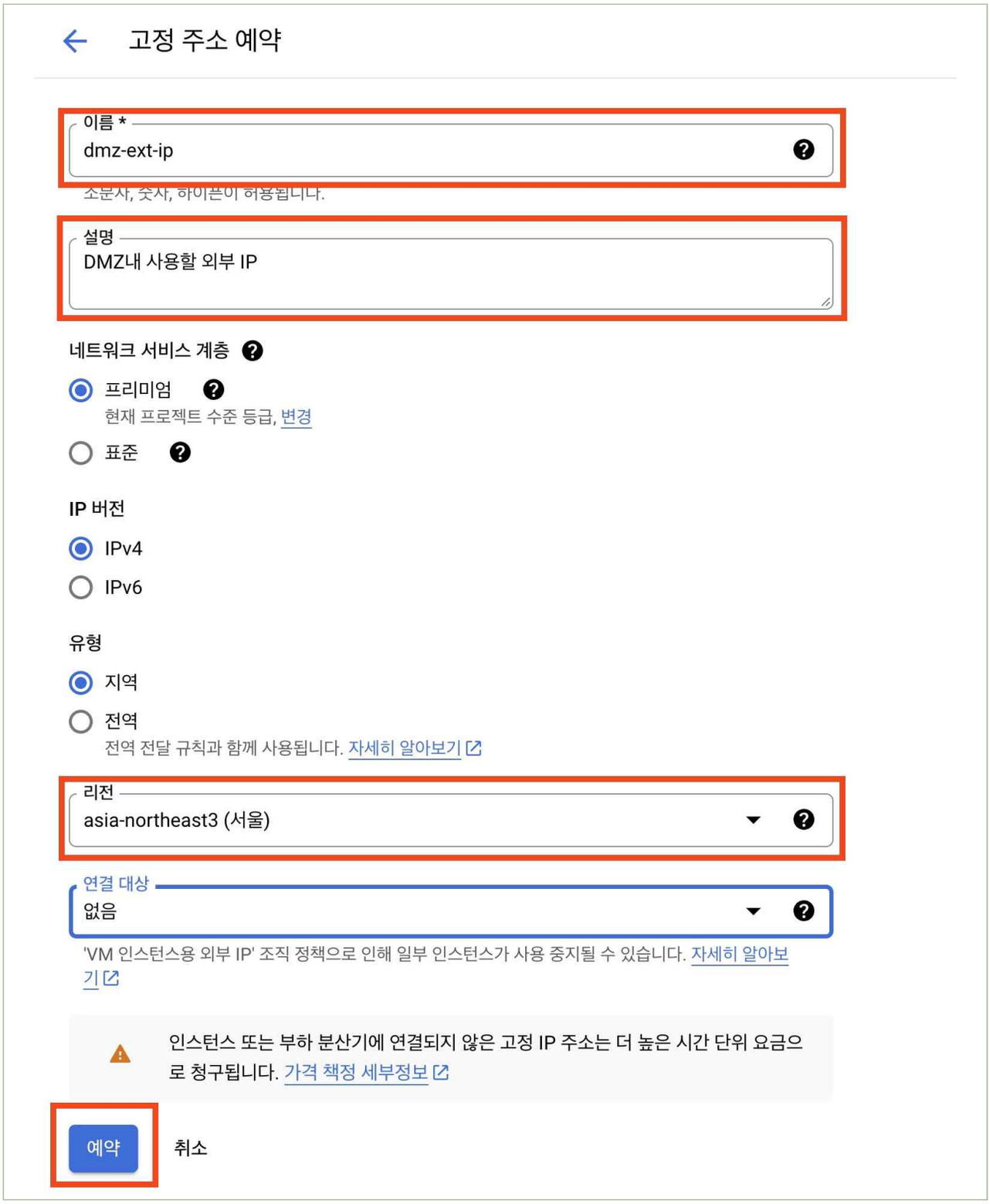
| 그림 2-4-4 | 방화벽 규칙 수정

- **만들기**를 클릭하여 VPC 네트워크 생성을 완료합니다.

- **(외부 IP 주소)** DMZ VPC 내 사용할 외부 IP주소를 예약합니다. 해당 VPC에서는 외부 통신을 위한 가상머신(VM, Google Compute Engine)이나 외부 부하분산기를 구성할 수 있습니다. 이 부분에 필요한 외부 IP는 미리 예약해서 사용할 수 있습니다. 외부 IP를 임시로 할당 받은 IP를 활용할 수 있지만, 가급적 고정 외부 IP를 구성하여, IP에 대한 분배 이력을 추적가능하게 하는 것을 권장합니다. '웹 콘솔 홈' → 'VPC 네트워크' → 'IP 주소'로 이동합니다. 이후 **외부 고정 IP 주소 예약**을 클릭하여 IP예약을 진행합니다.

| 그림 2-4-5 | VPC 네트워크

- 새 주소의 이름을 선택합니다.
- 네트워크 서비스 등급이 **프리미엄** 또는 **표준**인지 지정합니다. IPv6 고정 주소 예약은 프리미엄 등급에서만 지원됩니다.
- **IPv4** 또는 **IPv6** 주소 여부를 지정합니다.
- 이 IP 주소가 **리전** 또는 **전역**인지 지정합니다.
  - 전역 부하 분산기에 대해 고정 IP 주소를 예약하는 경우에는 **전역**을 선택한 다음 **예약**을 클릭합니다.
  - VM 또는 리전 부하 분산기에 대해 고정 IP 주소를 예약하는 경우에는 **리전**을 선택한 다음 주소를 만들 리전을 선택합니다.
- 리전 외부 IPv6 주소를 예약하는 경우에는 다음을 선택합니다.
  - **네트워크**: VPC 네트워크
  - **서브네트워크**: 고정 리전 IPv6 주소를 할당할 서브넷
  - **엔드포인트 유형**: **VM 인스턴스** 또는 **네트워크 부하 분산기** 선택
- 선택사항: VM에 대해 고정 외부 IP 주소를 예약하는 경우에는 **연결 대상** 목록에서 IP 주소를 연결할 VM을 선택합니다.
- **예약**을 클릭하여 IP 주소를 예약합니다.



| 그림 2-4-6 | 고정 주소 예약

- 예약을 완료한 해당 외부 IP를 추후 부하분산기나 VM인스턴스에서 활용할 수 있습니다.

4 참고 사항

- Google Cloud가 제공하는 VPC네트워크에 대해서 다음 링크에서 더 자세한 내용을 확인할 수 있습니다.
  - Virtual Private Cloud (VPC) overview

- 독립적으로 연결한 DMZ VPC 네트워크와 내부 통신망을 연결하고자 할 때는 다음 3가지 대표적인 방법을 활용할 수 있습니다.
  1. VPC 네트워크 Peering
     - VPC Network Peering | Google Cloud
  2. VPC 간 내부 VPN
     - HA VPN topologies | Google Cloud
  3. Network Security Appliance VM을 중앙에 두고 연결
     - Centralized network appliances on Google Cloud | Cloud Architecture Center

1 기준

식별번호	기준	내용
2.5.	**네트워크 사설 IP주소 할당 및 관리**	**클라우드 환경을 통한 내부망 네트워크 구현 시 사설 IP부여 등으로 보안을 강화하고, 내부IP 유출을 금지하여야 한다.**

2 설명

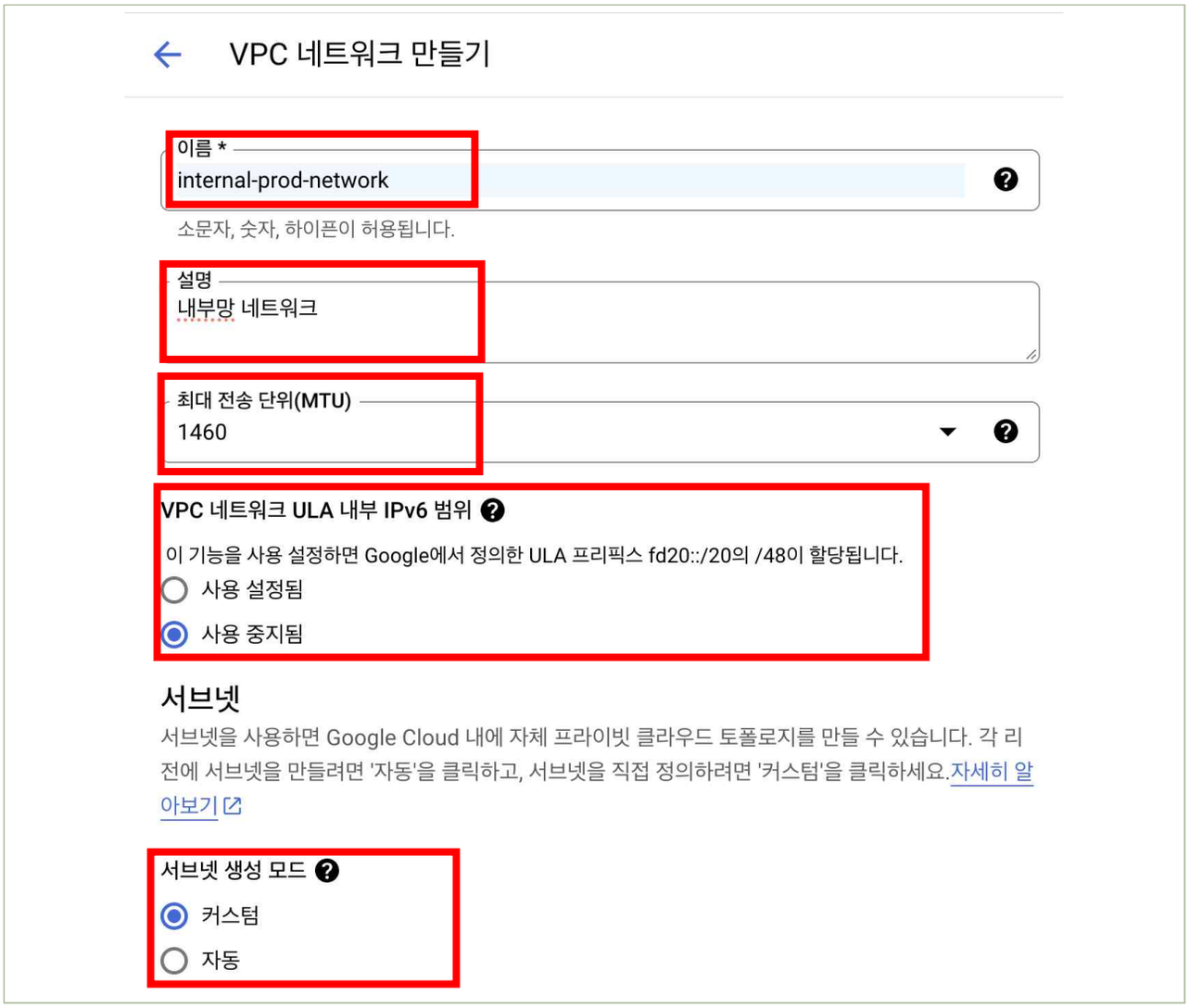
- 클라우드 환경 내 내부망 네트워크 구현 시 사설IP를 부여하고 주기적으로 현황을 검토하여야 한다.
  - 인터넷 게이트웨이, NAT 게이트웨이 등 관련 기능을 통해 사설IP부여 및 IP 관리 수행할 수 있습니다.
    a. VPC 네트워크는 '서브넷'이라는 하나 이상의 사설 IP 주소 범위로 구성됩니다. **서브넷은 리전 리소스**이며 서브넷과 연결된 IP 주소 범위가 있습니다. 기본적으로 모든 가상머신(VM) 기반 리소스는 사설 IP를 통하여 통신됩니다.
    b. VPC 네트워크를 만들면, 여기에 시스템에서 생성되는 IPv4 기본 경로(0.0.0.0/0)가 포함됩니다. **기본 경로는 VPC 네트워크에서 인터넷의 외부 IP 주소로의 경로를 정의**합니다. 네트워크를 **인터넷에서 완전히 분리**하거나 기본 경로를 커스텀 경로로 대체해야 하는 경우 **기본 경로를 삭제**할 수 있습니다.
      - IPv4만 해당: 인터넷 트래픽을 다른 다음 홉으로 라우팅하려면 기본 경로를 커스텀 정적 경로 또는 동적 경로로 바꿉니다. 예를 들어 다음 홉이 프록시 VM인 커스텀 정적 경로로 바꿀 수 있습니다.
    c. Google Cloud에서는 **Cloud NAT를 사용하여 사설 IP주소만으로 구성된 서브넷의 인스턴스가 VPC 네트워크 외부의 리소스에 연결할 수 있는 NAT 게이트웨이**를 만듭니다.
  - 사설 IP 할당 현황에 대한 주기적 검토 수행을 위해 VPC 네트워크 내 서브넷 화면 또는 내부 범위 화면에서 프로젝트 내 복수의 VPC 네트워크의 서브넷 할당 현황을 검토할 수 있습니다. 또한 '내부 범위'에서 사용할 사설IP 대역을 지정, 관리할 수 있습니다.

3 우수 사례

- **(VPC 네트워크 - 내부 IP 주소)** 내부 IP 주소는 인터넷에서 연결될 수 없으며 공개적으로 라우팅될 수 없습니다. 내부 IP 주소는 VPC 네트워크 피어링을 사용하여 연결된 VPC 네트워크, Cloud VPN, Cloud Interconnect, 라우터 어플라이언스를 사용하여 VPC 네트워크에 연결된 온프레미스 네트워크에서 사용됩니다. 내부 IP 주소가 있는 리소스는 모두 동일한 비공개 네트워크에 있는 것처럼 다른 리소스와 통신할 수 있습니다. 내부 IPv4 주소는 비공개 IPv4 주소이거나, 권장되지는 않지만 비공개로 사용되는 공개 IPv4 주소일 수 있습니다.
- **(VPC 네트워크 - 서브넷)** 네트워크를 사용하려면 네트워크에 한 개 이상의 서브넷이 있어야 합니다. 자동 모드 VPC 네트워크는 각 리전에 자동으로 서브넷을 만듭니다. 커스텀 모드 VPC 네트워크는 서브넷 없이 시작되므로 서브넷 만들기를 전적으로 제어할 수 있습니다. 한 리전에 두 개 이상의 서브넷을 만들 수 있습니다. 대부분의 경우, **커스텀 모드로 서브넷 없이 시작하고, 서브넷 만들기를 전적으로 제어하는 것을 권장**합니다.
  - Google Cloud에서 리소스를 만들 때 네트워크와 서브넷을 선택합니다. 인스턴스 템플릿 이외의 리소스를 만들 때는 영역(Zone) 또는 리전(Region)도 선택합니다. 영역을 선택하면 상위 리전도 암시적으로 선택됩니다. 서브넷은 리전 객체이므로 리소스에 선택한 리전에 따라 리소스에서 사용할 수 있는 서브넷이 결정됩니다.
  - 네트워크 생성 시 내부 VPC상에서 내부IP를 구성하여 통신하도록 합니다. '웹 콘솔 홈' → 'VPC 네트워크' → 'VPC 네트워크'로 이동합니다. 이후 **+VPC 네트워크 만들기**를 클릭하여 VPC 네트워크를 생성합니다.

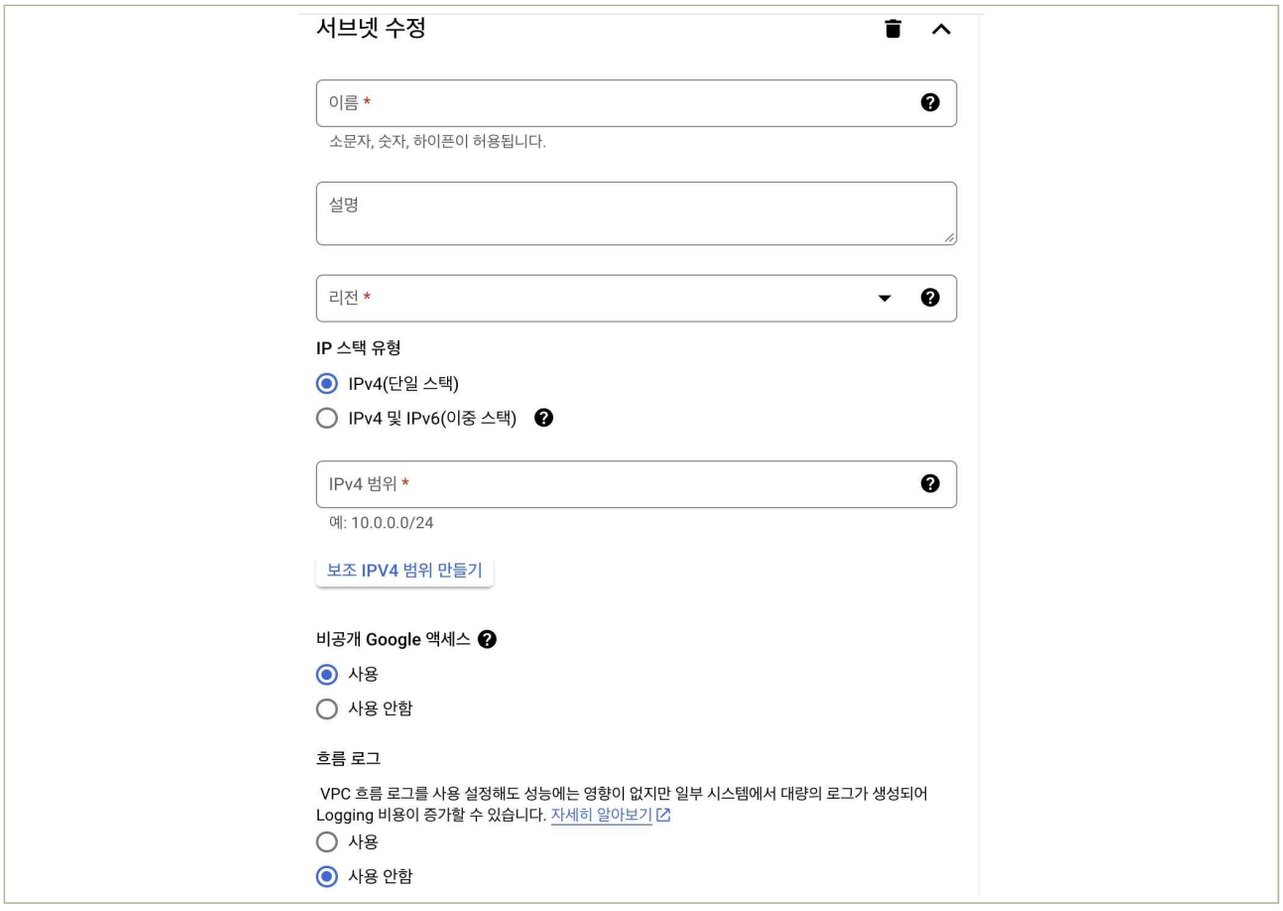
| 그림 2-5-1 | VPC 네트워크

  - VPC 네트워크 이름, 설명, 최대전송단위(MTU)를 구성합니다. VPC 네트워크 ULA 내부 IPv6 범위 기능은 IPv6가 별도로 필요하지 않다면 '사용 중지됨'으로 구성 유지합니다.
  - 서브넷 생성 모드는 앞서 확인한 것처럼 가급적 커스텀 모드로 시작합니다.



| 그림 2-5-2 | VPC 네트워크

- **새 서브넷** 섹션에서 서브넷에 다음 구성 매개변수를 지정합니다.
  a. 서브넷 이름을 입력합니다.
  b. **리전**을 선택합니다.
  c. **IP 주소 범위**를 입력합니다. 이 범위는 서브넷의 기본 IPv4 범위입니다.
  RFC 1918 주소가 아닌 범위를 선택하는 경우 범위가 기존 구성과 충돌하지 않는지 확인합니다.
  d. **비공개 Google 액세스**: 서브넷의 VM이 외부 IP 주소를 할당하지 않고도 Google 서비스에 액세스할 수 있는지 여부를 설정합니다.
  e. **흐름 로그**: 서브넷을 만들 때 또는 나중에 서브넷을 수정하여 서브넷에 VPC 흐름 로그를 사용할지 여부를 선택합니다.
  f. **완료**를 클릭합니다.



| 그림 2-5-3 | 서브넷 수정

- 서브넷을 추가하려면 **서브넷 추가**를 클릭하고 이전 단계를 반복합니다. 네트워크를 만든 후에 네트워크에 서브넷을 더 추가할 수도 있습니다.
- **방화벽 규칙** 섹션의 **IPv4 방화벽 규칙**에서 사전 정의된 방화벽 규칙을 0개 이상 선택합니다. 이 규칙은 인스턴스에 연결하는 일반적인 사용 사례를 다룹니다.
  사전 정의된 규칙을 선택하지 않으면 네트워크를 만든 후 자체 방화벽 규칙을 만들 수 있습니다.

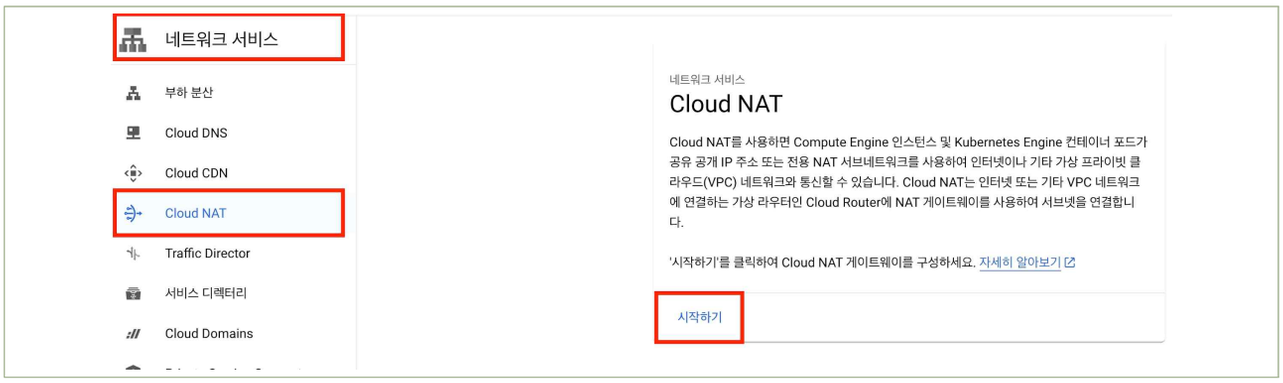
○ **(Cloud NAT)** VPC 네트워크의 동일한 서브넷에 NAT 서비스를 제공하는 공개(Public) NAT 및 비공개(Private) NAT 게이트웨이가 둘 다 있을 수 있습니다.

- Public NAT를 사용하면 공개 IP 주소가 없는 Google Cloud 리소스가 인터넷과 통신할 수 있습니다. 이러한 VM은 공유 공개 IP 주소 집합을 사용하여 인터넷에 연결합니다. Public NAT는 프록시 VM을 사용하지 않습니다. 대신 Public NAT 게이트웨이는 게이트웨이를 사용하여 인터넷에 대한 아웃바운드 연결을 만드는 각 VM에 외부 IP 주소 및 소스 포트 집합을 할당합니다.
- 네트워크 인터페이스에 외부 IP 주소가 없는 subnet-1에 VM-1이 있다고 가정해 보겠습니다. 그러나 VM-1은 중요한 업데이트를 다운로드하려면 인터넷에 연결해야 합니다. 인터넷에 연결할 수 있도록 subnet-1의 IP 주소 범위에 적용되도록 구성된 Public NAT 게이트웨이를 만들 수 있습니다. 이제

VM-1에서 subnet-1의 내부 IP 주소를 사용하여 트래픽을 인터넷에 전송할 수 있습니다.

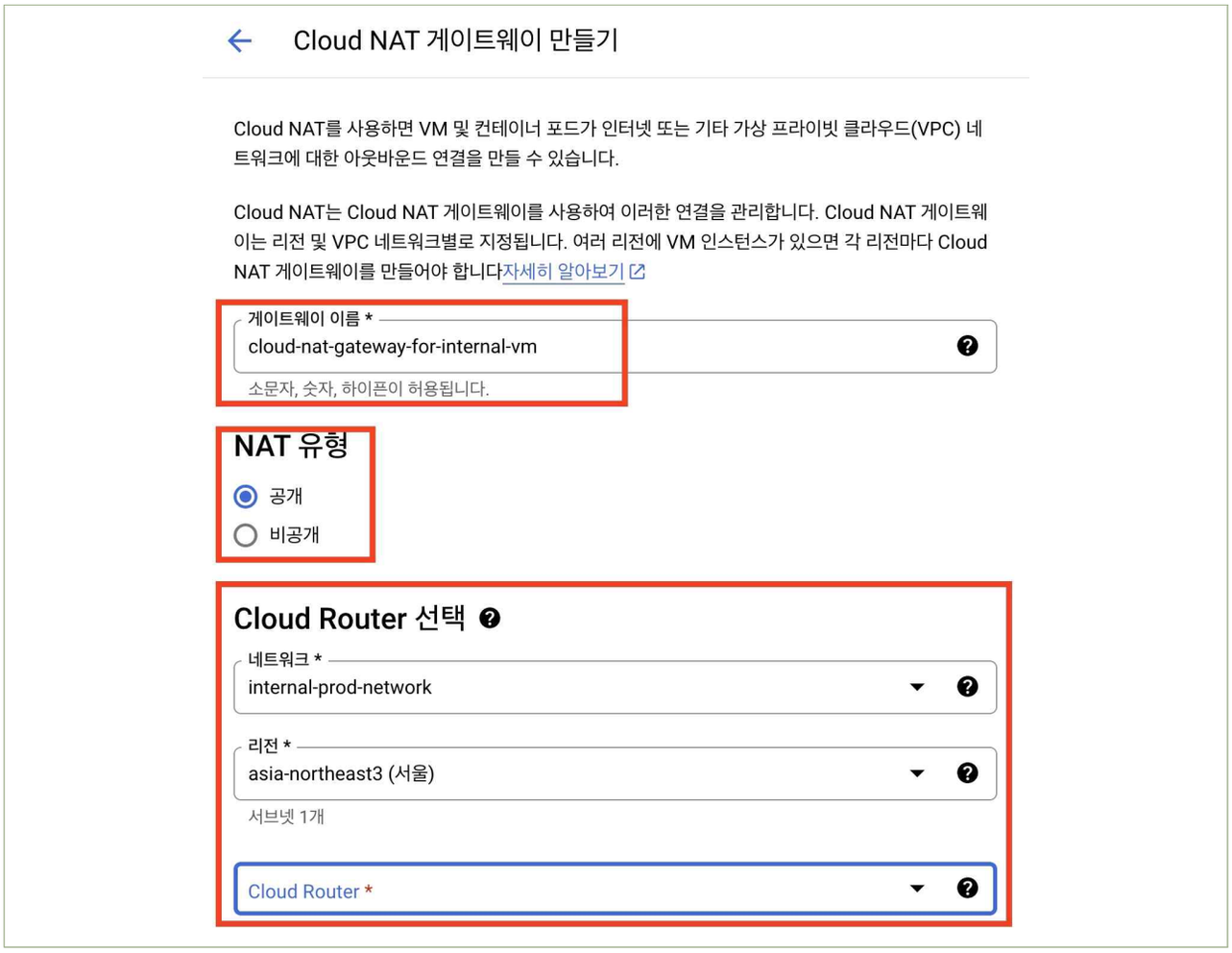
a. '웹 콘솔 홈' → '네트워크 서비스' → 'Cloud NAT'로 이동

b. 오른쪽 항목에 '시작하기' 선택



| 그림 2-5-4 | Cloud NAT

- '게이트웨이 이름', 'NAT 유형', Cloud NAT가 위치할 네트워크와 리전을 'Cloud Router 선택' 항목에서 지정



| 그림 2-5-5 | Cloud NAT 게이트웨이 만들기

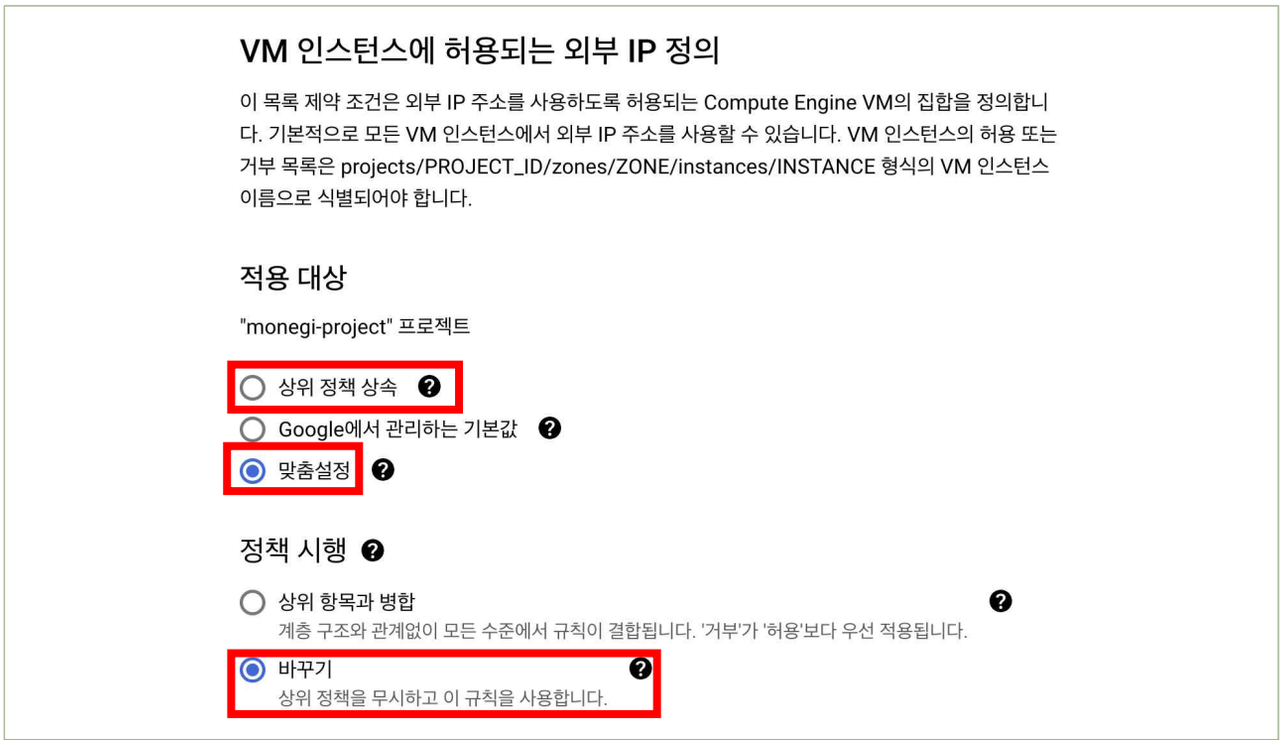
- Cloud Router가 만들어지지 않았다면, '새 라우터 만들기'을 선택하여 Cloud Router생성 후 진행

| 그림 2-5-6 | Cloud NAT 게이트웨이 만들기

- **(조직 정책)** 조직 정책 서비스는 조직의 클라우드 리소스를 중앙에서 프로그래매틱 방식으로 제어할 수 있는 기능을 제공합니다. 조직 정책 관리자는 전체 리소스 계층 구조에 대한 제한사항을 구성할 수 있습니다.
  - Google Cloud 조직정책에서는 사설 IP주소 할당에 대해서 여러 항목에 대해서 퍼블릭 인터넷으로 연결할 수 있는 가능성을 제어합니다. 제약 조건을 통해 외부 IP 주소를 사용하도록 허용되는 Compute Engine VM의 집합을 정의합니다. 기본적으로 모든 VM 인스턴스에서 외부 IP 주소를 사용할 수 있습니다.
  - '웹 콘솔 홈' → 'IAM 및 관리자' → '조직 정책'으로 이동
  - 오른쪽 필터 항목에 external IP항목으로 검색하여
    첫번째 'Define allowed external IPs for VM instances'선택

| 그림 2-5-7 | IAM 관리자

- 세부 항목에 대한 구성 이미 상위 정책에서 IP부여가 제한되어 있다면, '상위 정책 상속' 선택하며, 해당 프로젝트에서만 제한하고 싶다면 맞춤 설정을 구성하여 상위 정책과 다른 규칙으로 제한



| 그림 2-5-8 | VM 인스턴스에 허용되는 외부 IP 정의

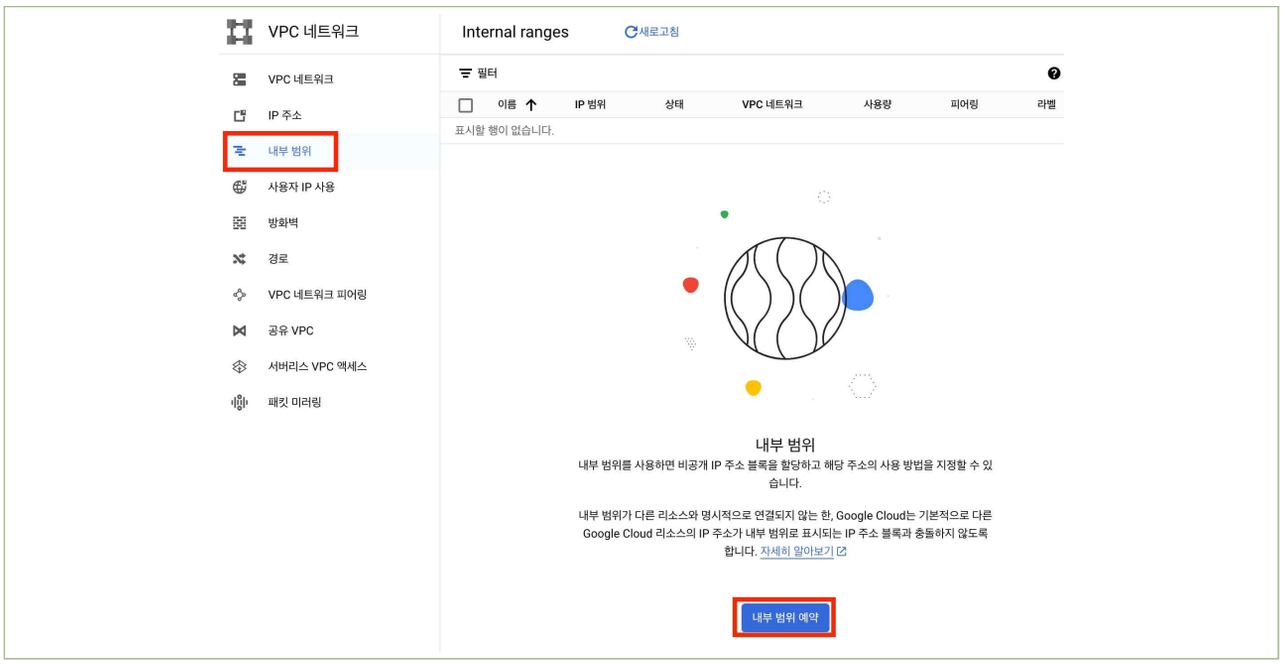
- 규칙 값은 모두 거부로 구성해야 External IP부여가 제한가능 하며, 정책설정까지 구성하여 완료되면, 수분 내로 조직정책 적용완료

| 그림 2-5-9 | 정책설정

- 이렇게 정책이 설정되면 프로젝트 내에서 가상머신을 만들 때 External IP를 구성하려고 하면 조직 정책에 의해 차단되었음을 알리고 External IP구성이 실패하게 됩니다.

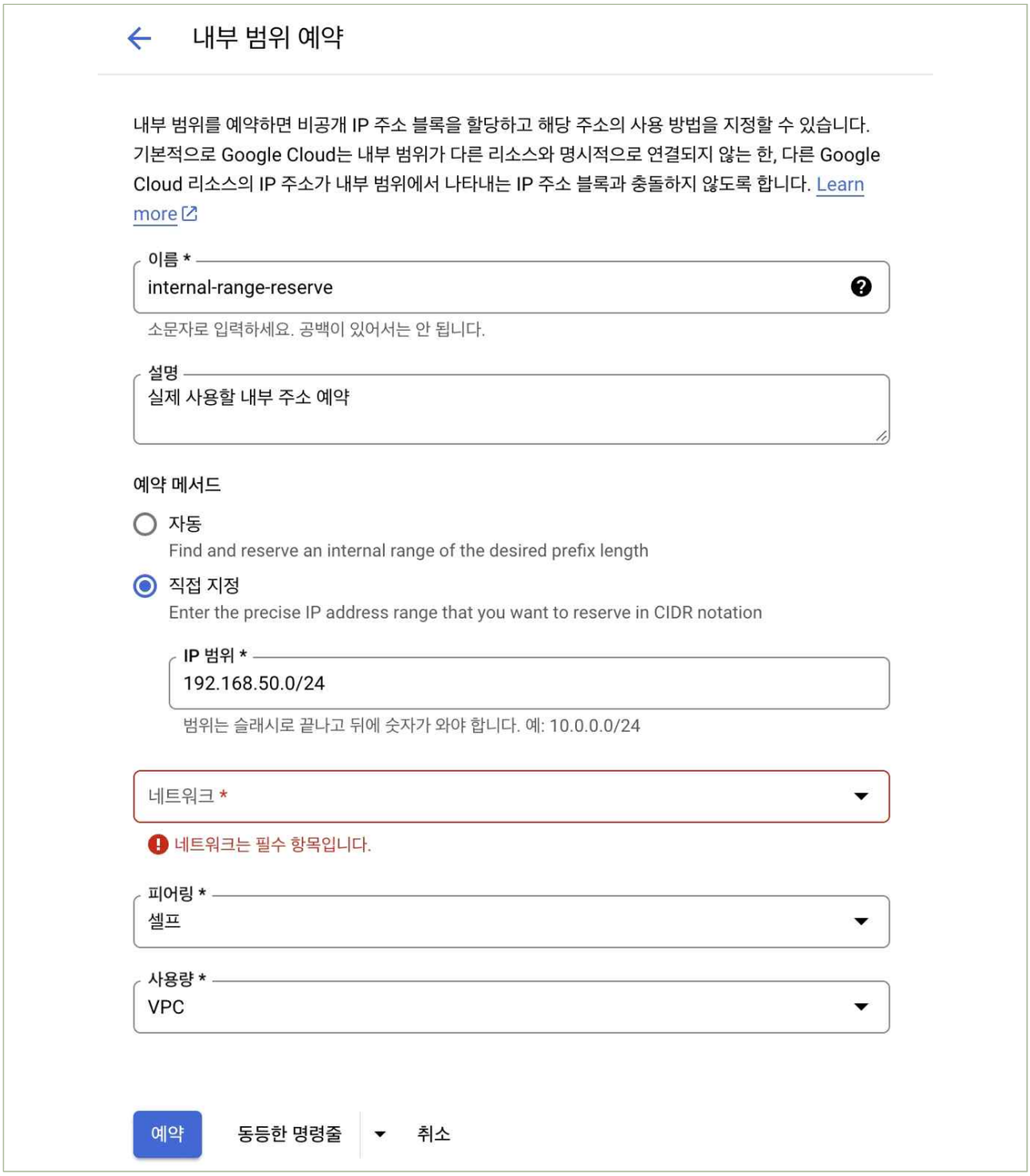
- **(내부 범위)** 내부 범위를 사용하면 사설(내부) IP 주소 블록을 할당하고 이러한 주소의 사용 방법을 지정할 수 있습니다. VPC 네트워크 피어링 및 공유 VPC와 같은 기능으로 인해 네트워크가 더 복잡해졌을 때 내부 범위를 사용하면 Virtual Private Cloud(VPC) 네트워크 토폴로지를 관리하는 데 도움이 될 수 있습니다.

  - Google Cloud 콘솔에서 내부 범위 페이지로 이동한 이후에 '내부 범위 예약'을 클릭합니다.



| 그림 2-5-10 | 내부 범위 예약

  - 이름을 입력합니다. 선택사항으로 설명을 입력합니다. 예약 메서드 섹션에서 직접 지정을 선택합니다.
  - IP 범위 필드에서 CIDR 표기법으로 내부 범위의 IP 주소 범위를 입력합니다.
  - 네트워크를 선택합니다.
  - 피어링 유형과 사용량 유형을 선택합니다.
  - 예약을 클릭합니다.



| 그림 2-5-11 | 내부 범위 예약

4 참고 사항

- Google Cloud가 제공하는 VPC네트워크와 사설IP주소에 대해서 다음 링크에서 더 자세한 내용을 확인할 수 있습니다.
  - Virtual Private Cloud (VPC) overview
  - Subnets | VPC | Google Cloud
  - IP addresses | VPC | Google Cloud
- Google Cloud가 제공하는 Cloud NAT에 대해서는 다음 링크에서 더 자세한 내용을 확인할 수 있습니다.
  - Cloud NAT overview
- Google Cloud가 제공하는 조직 정책에 대해서는 다음 링크에서 더 자세한 내용을 확인할 수 있습니다.
  - Introduction to the Organization Policy Service | Resource Manager Documentation | Google Cloud

1 기준

식별번호	기준	내용
2.6.	**네트워크(방화벽 등) 정책 주기적 검토**	**클라우드 서비스를 통해 구현한 네트워크 정책에 대해 주기적 검토를 수행하여야 한다.**

2 설명

- 클라우드 네트워크 관련 서비스 정책에 대한 적정성 여부를 주기적으로 검토하여야 한다.
  - 예시
    1) 방화벽 정책에 관한 주기적 검토 수행
    2) ACL 정책에 관한 주기적 검토 수행
    3) 보안그룹에 관한 주기적 검토 수행

3 우수 사례

- 금융회사 및 전자금융업자는 클라우드 서비스를 통해 구현한 네트워크 정책에 대해 주기적 검토를 수행
  - 금융회사에서는 '2. 네트워크 관리' 분야 내 내용을 참고하여 내부에서 방화벽, ACL, 보안그룹 등에 대해 검토

4 참고 사항

- Google Cloud가 제공하는 VPC네트워크와 사설IP주소에 대해서 다음 링크에서 더 자세한 내용을 확인할 수 있습니다.
  - Virtual Private Cloud (VPC) overview
  - Subnets | VPC | Google Cloud
  - IP addresses | VPC | Google Cloud

- Google Cloud가 제공하는 Cloud NAT에 대해서는 다음 링크에서 더 자세한 내용을 확인할 수 있습니다.
  - Cloud NAT overview
- Google Cloud가 제공하는 조직 정책에 대해서는 다음 링크에서 더 자세한 내용을 확인할 수 있습니다.
  - Introduction to the Organization Policy Service | Resource Manager Documentation | Google Cloud

3. 계정 및 권한 관리

3.1. 클라우드 계정 권한 관리
3.2. 이용자별 인증 수단 부여
3.3. 인사변경 사항 발생 시 계정 관리
3.4. 클라우드 가상자원 관리시스템 관리자 권한 추가인증 적용
3.5. 클라우드 가상자원 관리 시스템 로그인 규칙 수립
3.6. 계정 비밀번호 규칙 수립
3.7. 공개용 웹서버 접근 계정 제한

3 계정 및 권한 관리

1 기준

식별번호	기준	내용
3.1.	**클라우드 계정 권한 관리**	**클라우드 서비스 이용 시 업무 및 권한에 따라 계정을 관리하여야 한다.**

2 설명

- 클라우드를 이용하는 임직원의 업무 및 권한에 따라 계정을 관리하여야 한다.
  - Google Cloud는 계정의 생성, 변경 및 사용자 인증 등을 관리하는 관리 콘솔(admin.google.com)과 생성된 계정에 대하여 Google Cloud에서 어떠한 역할 또는 권한을 부여할지 관리하는 클라우드 콘솔(console.cloud.google.com)이 나누어져 있습니다.
  - Google Cloud는 임직원의 계정에 역할 또는 권한을 부여할 수 있는 Cloud IAM (Identity & Access Management)를 제공합니다.
  - 임직원은 클라우드에 접근할 계정이 있더라도 관리자가 IAM을 이용하여 임직원에게 권한을 부여하지 않는 경우 작업을 수행할 수 없습니다. 즉 IAM은 처음에 아무런 권한이 없는 것부터 시작하며, 관리자가 사용자에게 부여한 권한만을 사용자가 활용할 수 있기 때문입니다.

- 콘솔 최상위 관리자(ex. 최초 가입계정 등)은 서비스 운영에 활용하지 않아야 한다.
  - Google Workspace 또는 Cloud Identity에서 최초 가입한 계정은 Super Admin(최고 관리자) 역할을 할당받게 되며, 연결된 Google Cloud에서 Organization Admin(조직관리자) 역할을 자동 부여받습니다.
  - 따라서 최고 관리자 권한이 있는 사용자에게는 조직 노드의 Cloud IAM(Identity & Access Management) 정책을 수정할 수 있는 권한이 암시적으로 부여됩니다. 이 권한을 통해 최고 관리자는 조직 관리자 역할 또는 Google Cloud 조직의 다른 역할을 자신에게 할당할 수 있습니다.

- 그러므로 Super Admin권한을 가진 계정은 GCP의 일반 작업을 위한 계정으로 사용하지 않는 것을 권고합니다. GCP 서비스 운영을 위한 계정을 별도로 생성하고, Google Workspace 또는 Cloud Identity의 Super Admin을 부여받은 계정은 GCP 서비스 운영에 사용되지 않아야 하며 별도의 관리/백업용으로 2~3개 정도만 할당하여 비상용으로 사용하는 것을 권장합니다.

3 우수 사례

- Google Cloud에서 사용자에게 부여할 수 있는 권한은 매우 많습니다. 이를 모두 개별적으로 부여하는 번거로움을 해소하기 위해서, Google Cloud는 사용자에게 개별 권한을 부여하는 것이 아니라 업무 성격에 맞는 권한들을 묶은 역할(Role)을 부여합니다.
  - 역할은 소유자(Owner), 편집자(Editor), 뷰어(Viewer) 등의 기본역할과 가상머신 관리자, 가상머신 생성자 등 특정 리소스별로 지정한 사전정의 역할(pre-defined role)로 구분합니다. 소유자, 편집자와 같은 기본역할은 클라우드 자원을 구별하지 않고 권한을 행사할 수 있으므로 **사전정의 역할을** 사용자에게 할당해서 최소 권한 원칙을 구현해야 합니다.

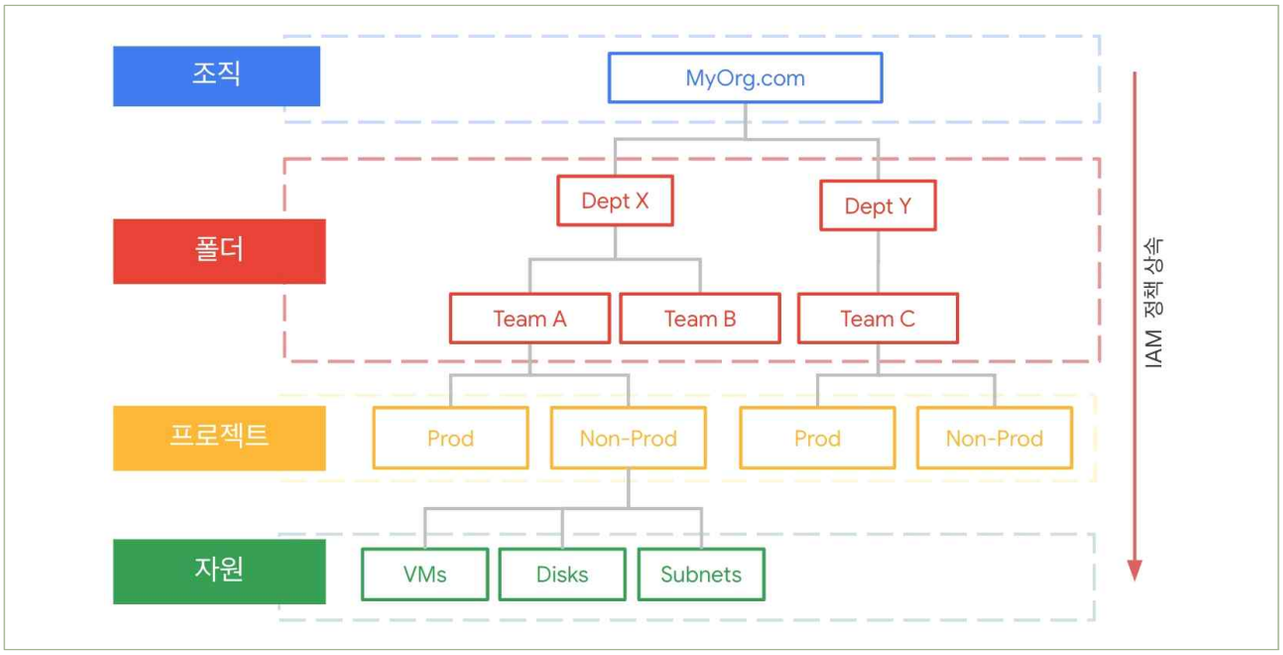
- **(Cloud IAM)** '웹 콘솔 홈' → 'IAM 및 관리자' → 'IAM'으로 이동합니다.
  - **+액세스 권한부여**를 클릭하여 사용자/그룹에게 허용권한을 부여합니다.

| 그림 3-1-1 | 액세스 권한 부여

- 역할을 부여할 구성원을 선택합니다. 이곳에는 사용자 또는 그룹을 지정할 수 있습니다. 역할 지정에서는 선택한 구성원이 필요한 최소 권한을 부여해야 합니다.

| 그림 3-1-2 | 주 구성원 추가

- Google Cloud에서 IAM을 이용한 역할 지정은 조직, 폴더, 프로젝트별 수준에서 개별적으로 부여할 수 있습니다.
  - 조직, 폴더 프로젝트에 부여한 역할 지정은 자동적으로 하위 노드에 상속됩니다. 그러므로 특정 사용자에게 조직 수준에서 역할을 지정했다면 해당 사용자는 조직의 모든 리소스에 대한 역할을 얻게 되며 이는 보안상 권고하지 않는 방식입니다.
  - Google Cloud 운영 특성상 프로젝트 수준이 IAM의 최소 단위로 인식하므로, 일반 이용자는 프로젝트 수준에서 역할을 지정하고 클라우드 관리 업무를 수행하는 사용자에게 조직, 폴더 수준에서 역할을 지정해야 합니다.



| 그림 3-1-3 | IAM 정책 상속

4 참고 사항

- Google Cloud가 제공하는 Cloud IAM의 모든 상세 기능은 다음 링크에서 더 자세한 내용을 확인할 수 있습니다.
  - https://cloud.google.com/iam/docs/overview?hl=ko
- 계정 및 조직 계획을 위한 권장사항은 다음 링크에서 더 자세한 내용을 확인할 수 있습니다.
  - https://cloud.google.com/architecture/identity/best-practices-for-planning?hl=ko

1 기준

식별번호	기준	내용
3.2.	이용자별 인증수단 부여	클라우드 서비스를 이용하는 임직원(이용자)별 인증 수단을 할당하여야 한다.

2 설명

- 클라우드 서비스를 이용하는 임직원(이용자)별 인증 수단을 부여하여야 하며, 필요 시 추가인증을 적용할 수 있어야 한다.(외부직원 포함)
  - Google Cloud는 사용자별 인증수단을 적용하기 위해서 사용자별 계정과 비밀번호를 가장 기본적인 인증 수단으로 사용합니다.
  - Google Cloud에서는 이용자별, 조직 단위별로 추가 인증 정책을 적용할 수 있습니다. 즉, 업무 중요도별로 추가 인증 적용 여부와 추가 인증 형식을 결정할 수 있습니다.
  - 보안 강화를 위해서 사용자별로 추가 인증을 적용할 수 있습니다. Google Cloud에서 사용할 수 있는 추가 인증은 휴대전화를 이용한 SMS, 전화 통화, Google Authenticator을 이용한 OTP가 있으며 하드웨어 타입의 보안 토큰도 사용할 수 있습니다.

3 우수 사례

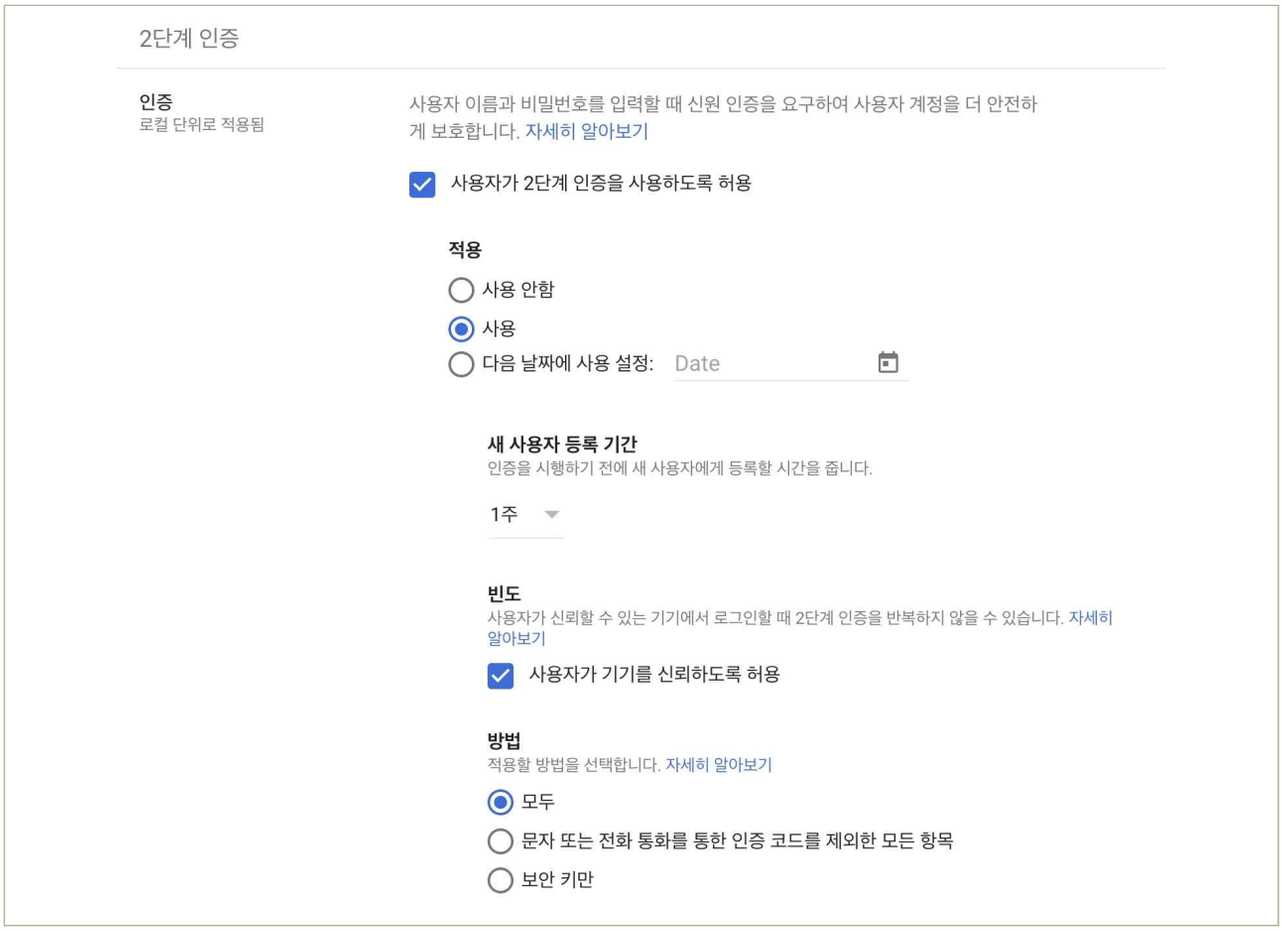
- **(2단계 인증)** '구글 어드민 콘솔 홈' → '보안' → '인증' → '2단계 인증'으로 이동합니다.
  - 조직 단위를 선택해서 단위(Organization Unit)마다 별도의 2단계 인증 정책을 적용할 수 있습니다.
- 2단계 인증의 설정 내역
  - 사용자가 2단계 인증을 사용하도록 허용 : 사용자가 개별적으로 2단계 인증을 활성화 시킬 수 있는 옵션을 제공합니다. 만일 이 옵션을 끄고 다음의 적용에서 "사용안함"으로 설정하면 기업 사용자 누구도 2단계 인증을 사용하지 못합니다. 그러므로 이 옵션은 항상 활성화 시켜 놓아야 합니다.
  - 적용
    - 사용 안함: 조직 차원에서 2단계 인증을 사용하지 않는 것입니다.
    - 사용: 조직 차원에서 사용자에게 2단계 인증을 강제하려면 이 옵션을 선택해야 합니다.

- 다음 날짜에 사용 설정: 설정한 날짜부터 2단계 인증이 강제 적용됩니다. 이 옵션은 사용자에게 2단계 인증을 설정할 수 있는 기한을 주고 실제 2단계 인증이 시작되는 날짜를 지정하는 것입니다.

- 새 사용자 등록 기간: 새로운 사용자가 등록되면 2단계 인증이 적용되지 않았기 때문에 로그인이 실패합니다. 이 경우 신규 사용자에게 2단계 인증을 등록할 시간을 줘야 합니다. 아래 그림에서 1주는 사용자가 1주일 안에 2단계 인증을 설정할 수 있는 시간을 제공하는 것입니다.

- 빈도: 2단계 인증을 다시 요청할 수 있는 방법을 정하는 것입니다. “사용자가 기기를 신뢰하도록 허용” 옵션을 활성화시키면 사용자가 등록한 기기는 2단계 인증을 더 이상 요청하지 않습니다. 이 활성화를 켜놓으면 로그인 시 항상 2단계 인증을 요구합니다.

- 방법
  - 모두 : 2단계 인증으로 휴대전화 문자(SMS), 구글 Authenticator을 이용한 OTP, 보안 키를 모두 사용할 수 있습니다.
  - 문자 또는 전화 통화를 통한 인증코드를 제외한 모든 항목: 구글 Authenticator를 이용한 OTP와 보안키를 적용합니다.
  - 보안 키만: 하드웨어 토큰인 보안 키만 2단계 인증으로 사용할 수 있습니다. 2단계 인증 방식 중에 가장 강력한 보안성을 제공합니다.



| 그림 3-2-1 | 2단계 인증

4 참고 사항

- Google Cloud의 2단계 인증의 상세한 내역은 다음 링크에서 상세한 정보를 얻으실 수 있습니다.
  - https://support.google.com/cloudidentity/answer/175197?hl=ko

1 기준

식별번호	기준	내용
3.3.	**인사변경 사항 발생 시 계정 관리**	**사용자의 인사변경(휴직, 전출, 퇴직 등) 발생 시 지체 없이 사용자 계정 삭제, 중지 등의 조치를 수행하여야 한다.**

2 설명

- 클라우드를 이용하는 임직원의 인사변경 사항 발생 시 이를 클라우드 환경에도 반영해야 합니다. Google Cloud에서는 업무 효율성을 위해서 이용자의 계정 삭제 및 중지 기능, 계정 비밀번호 변경 기능을 제공하고 있습니다.
  - 사용자의 계정이 더 이상 사용되지 않을 때 해당 계정을 삭제할 수 있습니다.
  - 필요에 따라서 사용자의 계정을 일시 정지시킬 수 있습니다.
  - 보안 강화를 위해서 사용자에게 신규 비밀번호를 부여할 수 있습니다. 비밀번호는 자동 생성하거나 관리자가 직접 생성할 수 있습니다.
  - 비밀번호를 관리자가 생성하는 경우 사용자에게 로그인 과정에서 새로운 비밀번호로 변경하도록 강제할 수 있습니다.

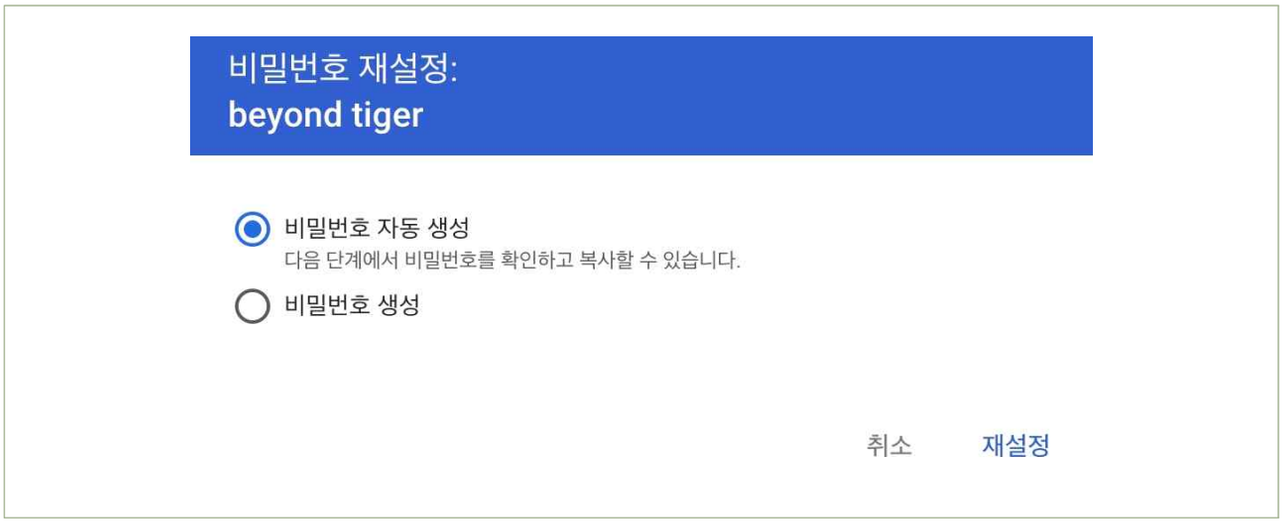
3 우수 사례

- **(사용자 삭제)** '구글 어드민 콘솔 홈' → '디렉터리' → '사용자'로 이동합니다.
  - 작업 대상 이용자를 선택하고 원하는 작업을 선택합니다.
  - 일시 중지를 선택하면 사용자 계정의 사용이 중지됩니다.

| 그림 3-3-1 | 사용자 삭제

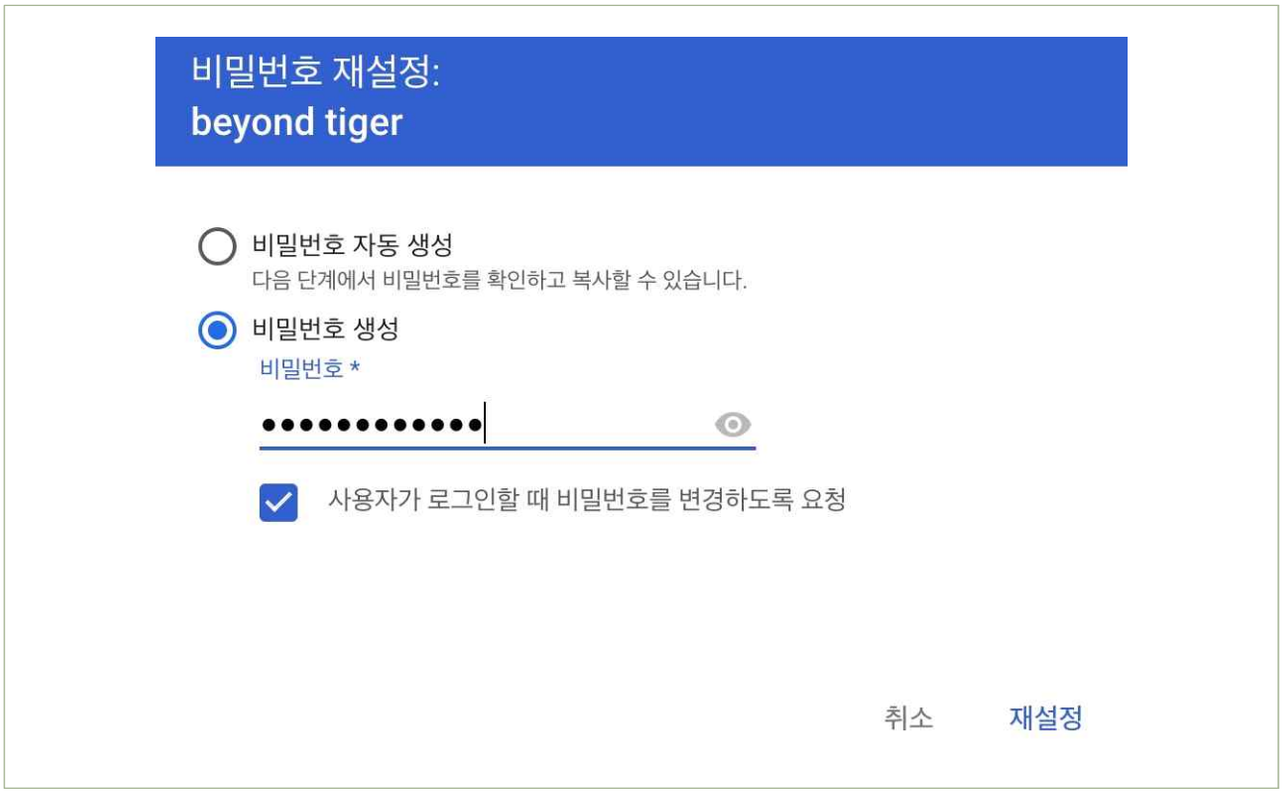
- 사용자 삭제는 해당 계정을 삭제하는 것입니다.

비밀번호 재설정



| 그림 3-3-2 | 비밀번호 재설정

- Google Cloud는 비밀번호 재설정에 두 가지 선택사항을 제공합니다.
  비밀번호 자동 생성: 안전한 비밀번호를 프로그램이 자동으로 생성하는 것입니다.



| 그림 3-3-3 | 비밀번호 재설정

- 비밀번호 생성: 관리자가 비밀번호를 수동으로 입력하는 것입니다.
- 사용자가 로그인할 때 비밀번호를 변경하도록 요청을 선택하면 관리자가 입력한 비밀번호로 클라우드 환경에 로그인하면 비밀번호를 변경하라는 안내문이 나옵니다. 이때 이용자가 비밀번호 변경을 수행하면 관리자가 지정한 비밀번호를 덮어쓰고 이용자가 신규로 비밀번호를 설정한 효과를 가집니다.

4 참고 사항

- Google Cloud에서 사용자 계정 삭제 및 중지 등의 방법은 다음 링크에서 상세한 정보를 얻으실 수 있습니다.
  - https://support.google.com/cloudidentity/answer/6329207?hl=ko

1 기준

식별번호	기준	내용
3.4.	**클라우드 가상자원 관리 시스템 관리자 권한 추가인증 적용**	**클라우드 서비스 관리자 권한으로 로그인 시 추가인증 수단을 적용하여야 한다.**

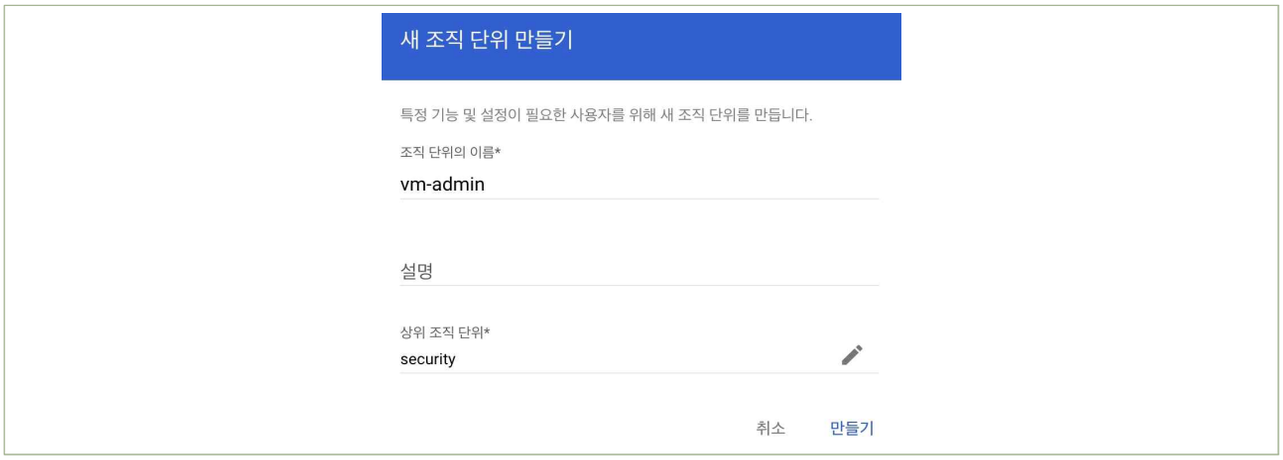
2 설명

- 클라우드 환경(콘솔 등)에 관리자 권한으로 로그인 시 추가인증 수단을 적용해서 관리자 권한을 가진 이용자의 로그인 보안을 강화시킬 수 있습니다.
  - Google Cloud는 추가 인증 방안으로 SMS 인증, OTP, 보안키 방식을 제공합니다.

- Google Cloud는 이용자 계정이 기본적으로 보유하는 권한이 존재하지 않습니다. 모든 권한은 신규로 부여받아야 합니다. 그러므로 관리자 계정이 아닌 관리 권한을 보유한 이용자 계정을 구분하고 이러한 계정의 로그인 보안을 강화시켜야 합니다.

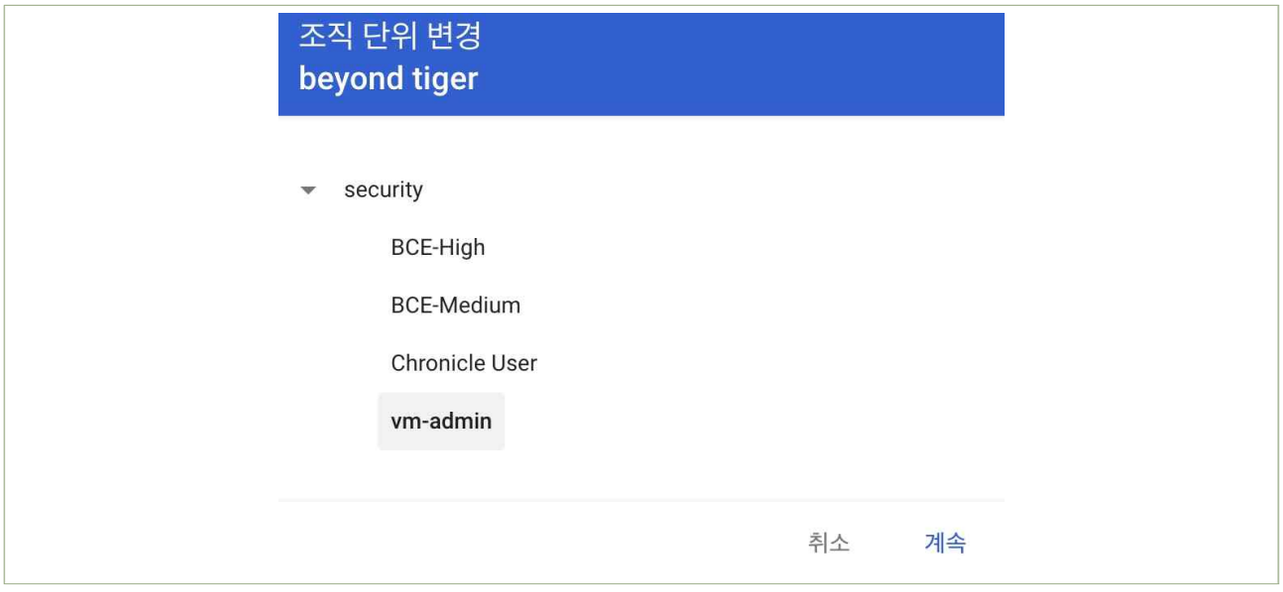
3 우수 사례

- **(조직 단위 생성)** 이용자 계정마다 2단계 인증을 적용시킬 수 있습니다. 하지만 이 경우 관리 권한 보유 계정이 증가할수록 통제가 어렵다는 단점이 존재합니다. 이런 경우를 위해서 이용자가 아닌 조직 단위를 설정하고 해당 조직에 정책을 적용시키는 방법을 사용하는 것이 좋습니다.
  - ‘구글 어드민 콘솔 홈’ → ‘디렉터리’ → ‘조직단위'로 이동하여 조직 단위 만들기를 선택합니다.
  - 가상머신 관리 권한을 보유한 계정 들을 위한 조직단위를 생성합니다.



| 그림 3-4-1 | 새 조직 단위 만들기

- **(이용자 정보 변경)** '구글 어드민 콘솔 홈' → '디렉터리' → '사용자'로 이동하여 관리 권한을 보유한 계정을 선택합니다. 이후 해당 계정의 조직 단위 변경을 실시하여 관리 권한 통제용 조직 단위로 변경합니다.
  - 이제 이용자는 vm-admin 조직 단위의 구성원이 되었으며 해당 조직 단위에 적용된 보안 정책을 상속받습니다.

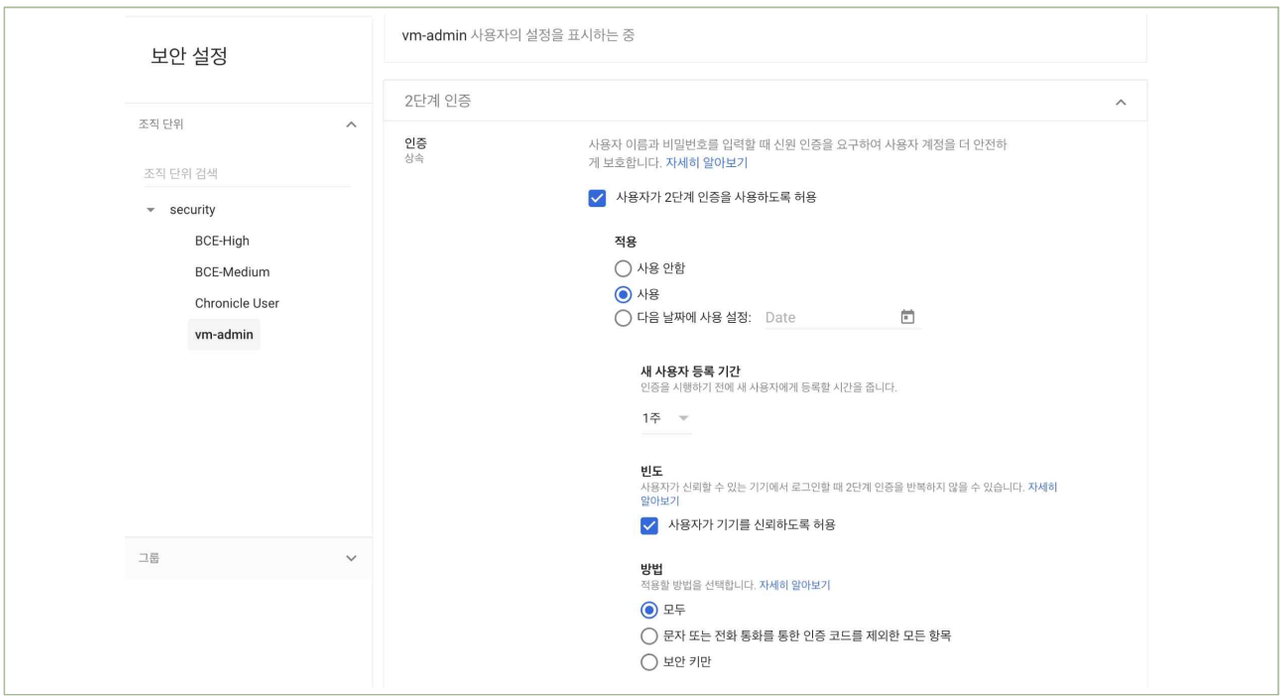


| 그림 3-4-2 | 조직 단위 변경

- **(2단계 인증)** '구글 어드민 콘솔 홈' → '보안' → '인증' → '2단계 인증'으로 이동합니다.
  - 조직 단위에서 vm-admin을 선택하고 별도의 2단계 인증 정책을 적용합니다.
- 2단계 인증의 설정 내역
  - 사용자가 2단계 인증을 사용하도록 허용 : 사용자가 개별적으로 2단계 인증을 활성화 시킬 수 있는

옵션을 제공합니다. 만일 이 옵션을 끄고 다음의 적용에서 “사용안함”으로 설정하면 기업 사용자 누구도 2단계 인증을 사용하지 못합니다. 그러므로 이 옵션은 항상 활성화 시켜 놓아야 합니다.

- 적용에서는 사용을 선택하여 2단계 인증을 강제합니다.
  - 다음 날짜에 사용 설정: 설정한 날짜부터 2단계 인증이 강제 적용됩니다. 이 옵션은 사용자에게 2단계 인증을 설정할 수 있는 기한을 주고 실제 2단계 인증이 시작되는 날짜를 지정하는 것입니다.
- 새 사용자 등록 기간: 새로운 사용자가 등록되면 2단계 인증이 적용되지 않았기 때문에 로그인이 실패합니다. 이 경우 신규 사용자에게 2단계 인증을 등록할 시간을 줘야 합니다. 아래 그림에서 1주는 사용자가 1주일 안에 2단계 인증을 설정할 수 있는 시간을 제공하는 것입니다.
- 빈도: 2단계 인증을 다시 요청할 수 있는 방법을 정하는 것입니다. “사용자가 기기를 신뢰하도록 허용” 옵션을 활성화 시키면 사용자가 등록한 기기는 2단계 인증을 더 이상 요청하지 않습니다. 이 활성화를 켜놓으면 로그인 시 항상 2단계 인증을 요구합니다.
- 방법
  - 모두 : 2단계 인증으로 휴대전화 문자(SMS), 구글 Authenticator을 이용한 OTP, 보안 키를 모두 사용할 수 있습니다.
  - 문자 또는 전화 통화를 통한 인증코드를 제외한 모든 항목: 구글 Authenticator를 이용한 OTP와 보안키를 적용합니다.
  - 보안 키만: 하드웨어 토큰인 보안 키만 2단계 인증으로 사용할 수 있습니다. 2단계 인증 방식 중에 가장 강력한 보안성을 제공합니다.



| 그림 3-4-3 | 2단계 인증

4 참고 사항

- Google Cloud의 2단계 인증의 상세한 내역은 다음 링크에서 상세한 정보를 얻으실 수 있습니다.
  - https://support.google.com/cloudidentity/answer/175197?hl=ko

1 기준

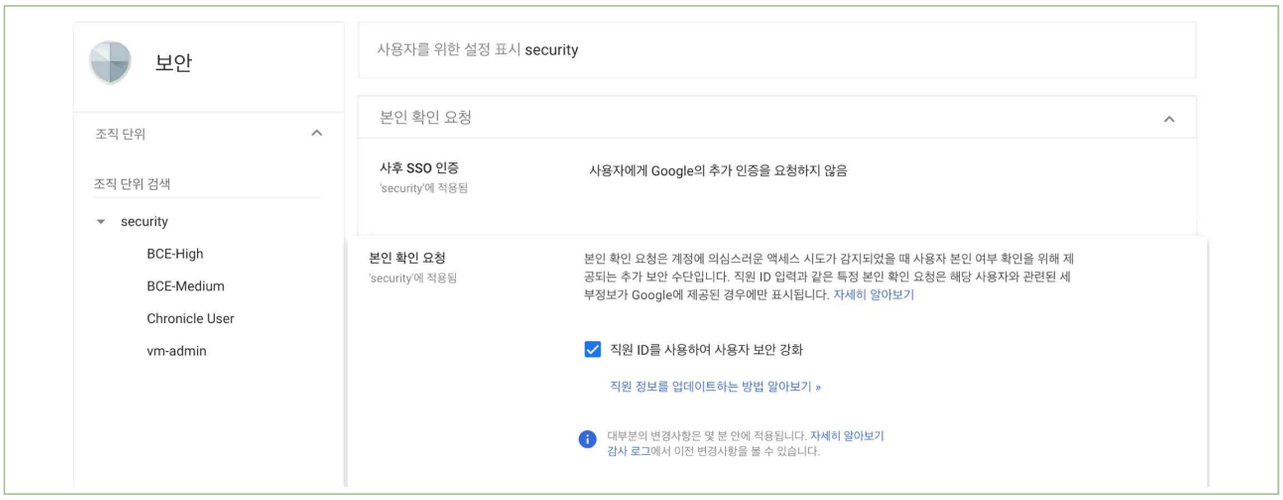
식별번호	기준	내용
3.5.	**클라우드 가상자원 관리 시스템 로그인 규칙 수립**	**이용자는 패스워드 무작위 대입 공격등에 대응하기 위해 가상자원 관리 시스템 계정에 대한 안전한 로그인 규칙을 수립하여야 한다.**

2 설명

- 클라우드 환경(콘솔 등)에 로그인 시 안전한 로그인 규칙을 설정할 수 있습니다.
  - Google Cloud는 이용자 계정에 의심스러운 엑세스 시도가 감지되었을 때 본인 여부 확인을 위해서 추가 정보를 요구합니다.
  - 구글은 로그인 과정에서 본인인지 알 수 없는 사용자가 계정에 액세스하려고 시도하면 이를 감지하여 차단합니다. 주로 비정상적인 로그인 활동(평소와 다른 위치 또는 기기에서 로그인 시도)를 감지했을 때 로그인 시도를 차단하고 이를 사용자에게 통보합니다.

3 우수 사례

- **(본인확인요청 설정)** '구글 어드민 콘솔 홈' → '보안' → '인증' → '본인 확인' 요청에서 본인 확인 요청을 설정합니다. 전체 조직 또는 조직 단위로 설정이 가능합니다.



| 그림 3-5-1 | 본인 확인 요청

4 참고 사항

- Google Cloud의 로그인 관련 보안의 내역은 다음 링크에서 상세한 정보를 얻으실 수 있습니다.
  - https://support.google.com/cloudidentity/topic/7558944?hl=ko

1 기준

식별번호	기준	내용
3.6.	**계정 비밀번호 규칙 수립**	**클라우드 가상자원 관리 시스템 로그인 계정 생성 시 비밀번호 규칙을 수립하여 적용하여야 한다.**

2 설명

- Google Cloud는 클라우드를 이용하는 임직원의 비밀번호 정책을 구성할 수 있는 기능을 제공합니다.
  - 조직 전체에 적용하는 단일 비밀번호 정책을 수립하거나 조직 단위별로 고유의 정책을 수립할 수 있습니다.
  - 주기적으로 안전한 비밀번호 만들기 등의 교육을 통해서 이용자들의 보안 수준을 향상시켜야 합니다.
  - Google Cloud의 비밀번호는 문자, 숫자, 기호를 조합하여 만들 수 있습니다. 취약한 비밀번호(예: password123), 이전에 사용한 적이 있는 비밀번호, 공백으로 시작하거나 끝나는 비밀번호는 사용할 수 없습니다.

3 우수 사례

- **(비밀번호 관리)** '구글 어드민 콘솔 홈' → '보안' → '인증' → '비밀번호 관리'로 이동합니다.
  - Google Cloud의 비밀번호 정책은 조직 전체 또는 개별 조직별로 설정할 수 있습니다.
  - 타사 ID 공급자를 이용하여 인증을 수행하는 경우는 비밀번호 관리 정책이 적용되지 않을 수 있습니다.
  - 안전한 비밀번호 적용을 선택하여 비밀번호 강도를 조정해야 합니다.
  - 비밀번호 길이는 영문 글자로 최소 8자에서 최대 100자까지 설정할 수 있습니다.
  - 모든 비밀번호 정책은 이용자의 현재 비밀번호에는 적용되지 않습니다. 이용자가 비밀번호를 변경할 때 적용됩니다. 만일 비밀번호 정책 변경사항을 즉시 적용하려면 **다음 로그인 시 비밀번호 정책 시행**을 선택합니다. 이 항목을 선택하는 경우 시스템은 이용자의 다음 로그인시에 비밀번호 정책에 맞는 비밀번호로 변경할 것을 요청합니다.
  - 이용자가 사용한 비밀번호의 재사용을 허용하려면 재사용 항목을 선택합니다. 보안을 위해서 해당 항목은 선택하지 않는 것을 권고합니다.

- 비밀번호의 변경 주기를 설정하려면 만료에서 해당 항목을 선택합니다. 30일, 60일, 90일, 180일, 365일과 만료일 없음에서 선택할 수 있습니다. 90일을 설정하는 것이 일반적입니다.

| 그림 3-6-1 | 비밀번호 관리

4 참고 사항

- Google Cloud가 제공하는 비밀번호 관리 기능은 다음 링크에서 더 자세한 내용을 확인할 수 있습니다.
  - https://support.google.com/accounts/answer/32040?hl=ko

1 기준

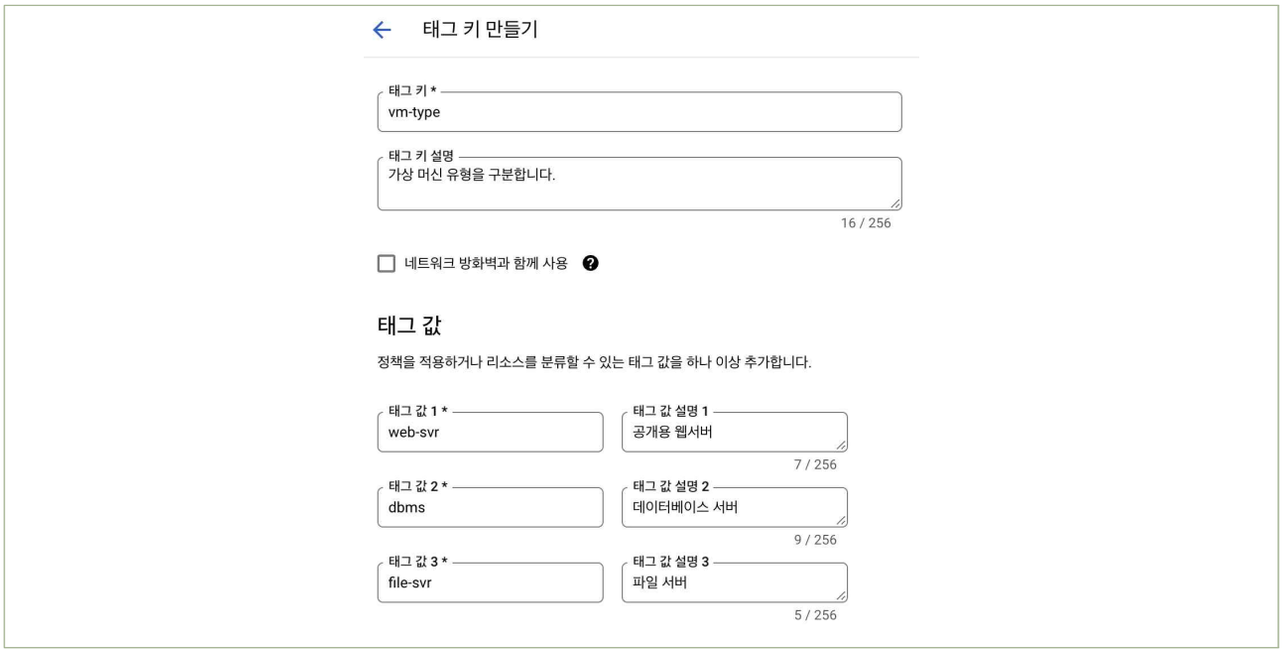
식별번호	기준	내용
3.7.	**공개용 웹서버 접근 계정 제한**	**클라우드를 통해 공개용 웹서버를 운영하는 경우 접근 계정을 적절하게 제한하여야 한다.**

2 설명

- 클라우드 환경을 통해 공개용 웹서버를 운영하는 경우 접근 계정을 적절하게 제한해야한다.
  - 계정 관리 기능을 통해 공개용 웹서버만 접근 가능한 계정을 개인별 부여하여 관리한다.
  - 공개용 웹서버에 접근 가능한 계정으로 로그인 시 추가인증 수단을 적용한다.

3 우수 사례

- 공개용 웹서버용 VPC를 별도 생성하고 해당 VPC에만 공개용 웹서버를 연결합니다.
- Google Cloud에서는 공개용 웹서버외에 다른 가상 머신이 동일 프로젝트에 존재하는 경우 계정만으로는 공개용 웹서버와 타 VM을 구별하여 접근통제를 구현할 수 없습니다. 이런 경우는 태그와 IAM 조건 기능을 조합하여 원하는 기능을 구현할 수 있습니다.
- **(태그 생성 및 부여)** 공개용 웹서버를 구분할 수 있는 태그를 먼저 생성합니다. ‘클라우드 콘솔 홈' → ‘IAM 및 관리자’ → ‘태그'로 이동하여 만들기를 선택합니다.
  - 태그 키는 태그를 지정하는 키입니다. 예제에서는 vm-type라는 키를 생성했습니다. 키는 소문자와 ‘-’만 사용할 수 있습니다.



| 그림 3-7-1 | 태그 키 만들기

- 태그 키를 만든 다음에는 공개용 웹서버에 생성한 태그를 지정해야 합니다. 공개용 웹서버 가상머신의 수정상태로 진입하고 태그를 선택합니다.
- Google Cloud는 프로젝트 단위로 동작하므로 태그의 범위도 프로젝트로 선택하고 키와 값을 목록에서 선택합니다.

| 그림 3-7-2 | 태그 설정

- (IAM 조건) 공개용 웹서버를 관리하는 이용자에게 Compute Admin 역할을 부여합니다. 그리고 옆에 **+ IAM 조건 추가**를 클릭합니다. IAM 조건은 특정 조건에 부합될 때만 부여한 역할이 적용됩니다.

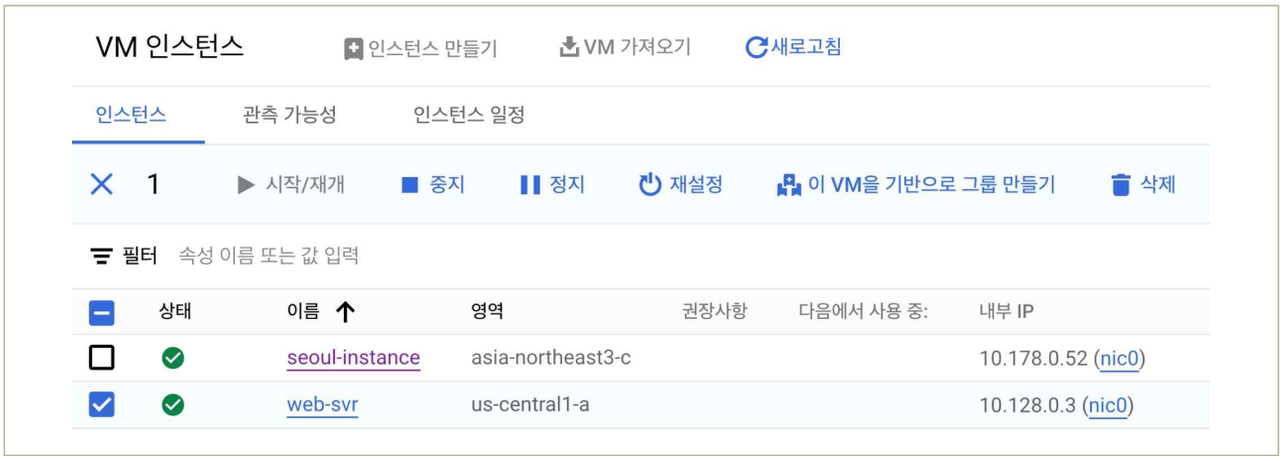
| 그림 3-7-3 | IAM 조건 추가

- 조건 추가 페이지에서 제목을 입력합니다. 조건 빌더에서 조건 유형은 태그를 선택하고 작업자는 값 ID가 있음을 선택합니다. 이전에 생성한 태그 페이지에서 키 ID와 web-svr에 할당된 값 ID를 복사해서 가져옵니다.

| 그림 3-7-4 | 태그 키 입력

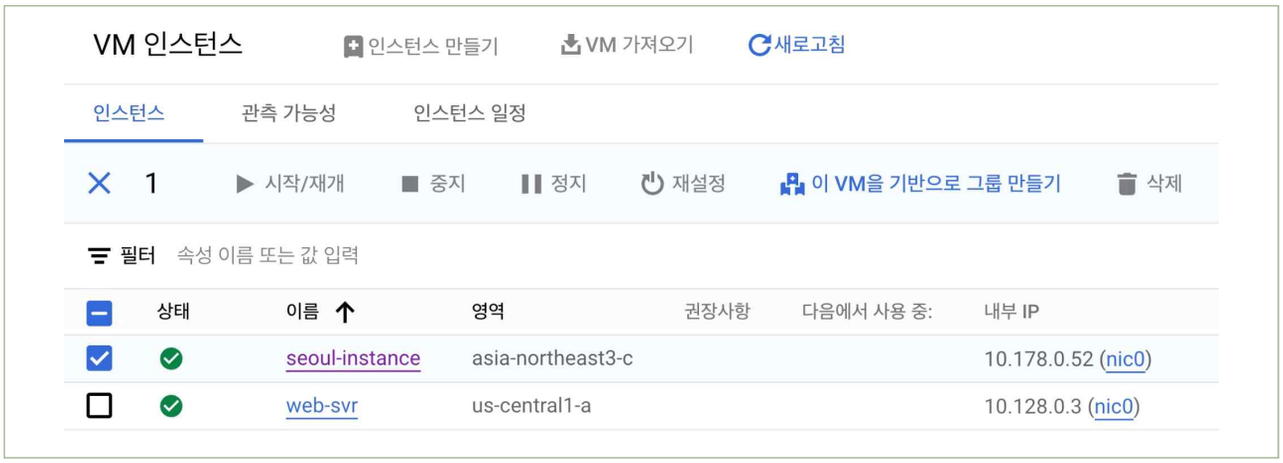
- 모든 입력을 완료하면 IAM 조건을 저장하고 IAM 역할 부여도 저장합니다.

- 이제 해당 이용자는 공개용 웹서버 태그가 부착된 가상머신만을 관리할 수 있게 됩니다.



| 그림 3-7-5 | IAM 조건이 맞는 경우

- IAM에서 compute 관리자 역할을 부여받은 이용자와 IAM 조건이 맞는 경우 공개용 웹서버 가상머신을 선택하면 중지, 정지 삭제 등의 작업을 수행할 수 있습니다.



| 그림 3-7-6 | IAM 조건이 맞지 않는 경우

- IAM 조건에 맞지 않는 서버인 seoul-instance를 선택하면 중지, 정지 및 삭제 등의 버튼이 비활성화됩니다. 이것은 해당 이용자가 compute 관리자 권한을 가지고 있을지라도 IAM 조건이 태그가 다른 서버에 접근하는 것을 차단하기 때문입니다.

4 참고 사항

- Google Cloud가 제공하는 Cloud IAM의 모든 상세 기능은 다음 링크에서 더 자세한 내용을 확인할 수 있습니다.

  - https://cloud.google.com/iam/docs/overview?hl=ko

4. 암호키 관리

4.1. 암호화 적용 가능 여부 확인
4.2. 암호키 관리 방안 수립
4.3. 암호키 서비스 관리자 권한 통제
4.4. 사용될
4.5. 안전한 암호화 알고리즘 적용

4 암호키 관리

1 기준

식별번호	기준	내용
4.1.	암호화 적용 가능 여부 확인	관련 법령(전자금융거래법, 신용정보법 등)에 따른 암호화 대상이 저장 및 처리되는 가상자원(서버, 스토리지 등)에 대한 암호화 기능 적용 여부를 확인하여야 한다.

2 설명

- 관련 법령(전자금융거래법, 개인정보보호법, 신용정보법 등)에 따라 암호화가 필요한 대상이 저장 및 처리되는 가상자원에 대해서는 암호화 적용을 고려하여야 한다.
  - Google은 사용자가 조치를 취하지 않아도 하나 이상의 암호화 메커니즘을 사용하여 저장된 모든 고객 콘텐츠를 암호화합니다. 고객이 직접 암호화 키관리를 하려면 KMS 통해서 할 수 있으며, Google Cloud Platform의 키 관리 서비스인 Cloud Key Management Service(Cloud KMS)를 통해 Google Cloud 서비스 및 자체 애플리케이션에서 사용할 암호화 키를 만들고 관리할 수 있습니다.
  - KMS와 통합되는 GCP 서비스는 다음 링크에서 확인할 수 있습니다.
    (호환 서비스 | Cloud KMS 문서)
  - 소프트웨어 또는 하드웨어 키(Cloud HSM 키)를 생성하거나, 기존 키를 Cloud KMS로 가져올 수 있으며, 호환 가능한 외부 키 관리(EKM) 시스템에서 외부 키를 연결할 수 있습니다.

3 우수 사례

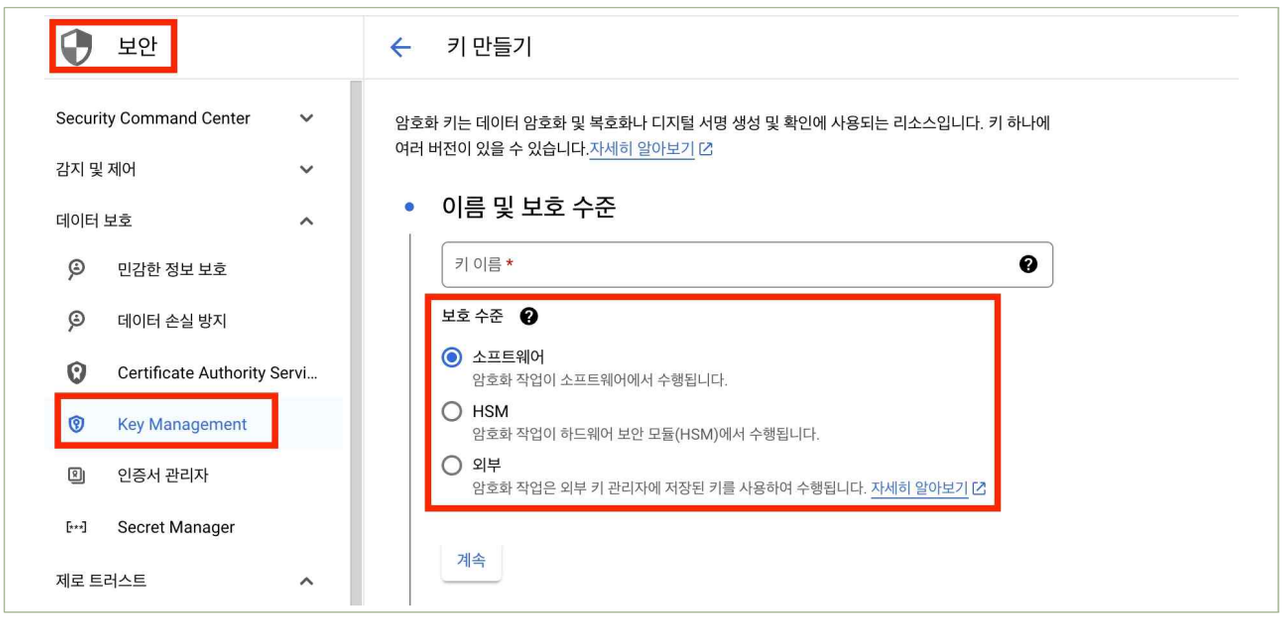
- 암호화 적용 유형
  - Google Cloud 기본 암호화
    - 고객 데이터를 저장하는 모든 Google Cloud 서비스

- Google Cloud 서비스에 저장된 고객 데이터를 자동으로 암호화합니다.
- 암호화를 위한 구성이 필요하지 않고 무료로 제공됩니다.
- 키를 자동으로 순환하고 데이터를 다시 암호화합니다.
- AES-256을 사용한 암호화를 지원합니다.

- 고객 관리 암호화 키(CMEK) - 소프트웨어(Cloud KMS 키) 및 하드웨어(Cloud HSM 키)
  - 자동 키 순환 일정, IAM 역할 및 권한을 제어하고 키 버전을 사용 설정, 중지, 폐기합니다.
  - 암호화 및 복호화에 대칭 및 비대칭 키를 지원합니다.
  - 대칭 키를 자동으로 순환합니다.
  - 여러 일반적인 알고리즘을 지원합니다.
- 외부 키 관리자(Cloud EKM 키), 고객 제공 암호화키(CSEK) 등 다른 암호화 유형은 참고사항에 연결된 문서를 참고하시기 바랍니다.

암호화 적용을 위한 키생성

- Cloud Console → 보안 → 데이터보호 카테고리 중 Key Management
- 보호수준(Protection Level): 보호 수준에 따라 암호화 작업 방식을 크게 다음 3가지 중 하나로 결정(SW 방식, 하드웨어 보안모듈 방식(HSM), 외부 키관리자)



| 그림 4-1-1 | 키 만들기

4 참고 사항

- 외부 키 관리자(Cloud EKM 키), 고객 제공 암호화키(CSEK) 등 전체 암호화 적용 유형
  - Cloud Key Management Service 개요 | Cloud KMS Documentation
- 저장 데이터의 기본 암호화
  - 기본 저장 데이터 암호화 | Documentation
- Cloud HSM: 클라우드에 호스팅되는 하드웨어 보안 모듈(HSM) 서비스
  - https://cloud.google.com/kms/docs/hsm?hl=ko
- 컨피덴셜 컴퓨팅: 민감한 정보 또는 워크로드를 처리하는 VM에 사용 중 데이터(메모리 데이터) 암호화를 제공하며 다음 3가지 서비스에서 사용 가능
  - Compute Engine
  - GKE
  - Dataproc

1 기준

식별번호	기준	내용
4.2.	**암호키 관리 방안 수립**	**암호화 기능 이용 시 암호키 관리 방안을 수립하여야 한다.**

2 설명

- (**키 계층구조**) 암호화 키를 관리하기 위하여 Cloud KMS에서는 키링, 키, 키버전의 계층적 구조를 가지고 있습니다.
  - **키**: 특정 데이터의 암호화를 위해 사용되는 암호키이며, 시점에 따라 여러 버전을 가질수 있습니다.
  - **키링**: 목적에 따라 구분된 키의 그룹입니다. 키링은 프로젝트에 속하며 키링에 적용된 IAM 정책을 키가 상속받습니다.
  - **키버전**: 특정 시점의 키와 연관된 암호키를 의미합니다. 버전은 1부터 순차적으로 번호가 매겨집니다. 키가 rotation되면 새 키버전이 만들어집니다.

| 그림 4-2-1 | 키 계층구조

- (키순환) 대칭 암호화키의 경우 보안을 위하여 주기적으로 그리고 자동적으로 키를 순환하는 것이 권장합니다.
  - 암호키를 순환하면 동일한 키 버전으로 암호화되는 메시지 수를 제한함으로써 암호화 분석을 통한 공격을 방지하는 데 도움이 됩니다.
  - 키가 손상되더라도 정기적으로 키를 순환하면 손상에 취약한 실제 메시지 수가 제한됩니다. 키 버전이 손상되었다고 의심될 경우에는 이를 사용 중지하고 가능한 한 빨리 키 액세스 권한을 취소해야 합니다.

- (키 폐기) 키버전을 폐기하면 암호키가 영구적으로 삭제됩니다. 따라서 암호키가 폐기되면 해당 키버전으로 암호화된 데이터를 복호화할 수 없습니다.

- 키폐기는 되돌릴 수 없으므로 Cloud KMS는 키버전을 즉시 폐기할 수 없습니다. 대신 키버전 폐기를 예약합니다. 키버전은 구성 가능한 시간 동안 폐기 예약상태로 유지됩니다. 폐기 예약 기간 중에 키버전을 복원하여 폐기를 취소할 수 있습니다.
- 키버전을 폐기해도 키이름 및 키버전 번호와 같은 세부정보는 삭제되지 않습니다.

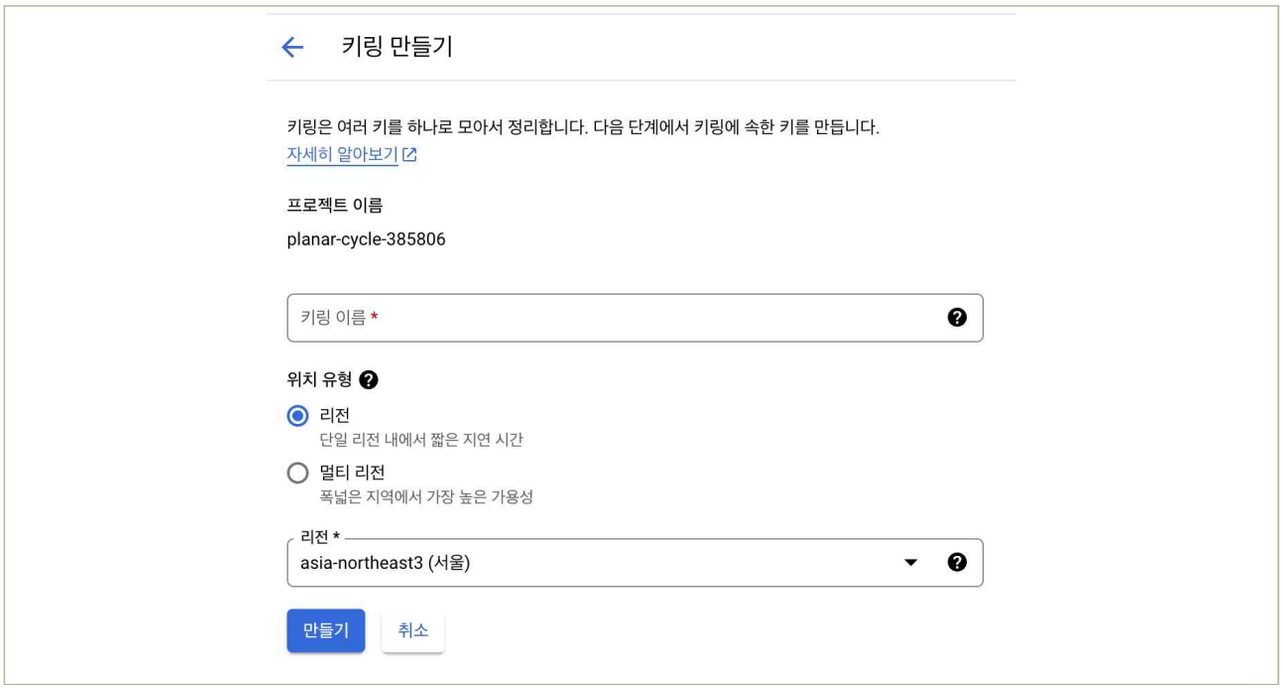
- (키버전 사용중지) 암호키를 폐기하지 않고도 키버전 사용중지 기능을 통해 키사용을 중단할 수 있습니다.
  - 키를 폐기할 필요는 없으나, 키사용을 일시적으로 중단할 필요가 있는 경우 사용할 수 있습니다.
  - 키가 사용 중지된 기간 동안에는 해당 암호키로 암호화된 데이터에 액세스할 수 없습니다. 데이터에 액세스하려면 키버전을 다시 사용 설정해야 합니다.
  - 키를 폐기하기 전에 사용 중지하는 것은 키가 사용 중이 아닌지 확인하는 데 도움이 되기 때문에 권장됩니다. 키 폐기 사용 중지 키 제한 제약조건을 사용하면 키 폐기를 예약하기 전에 키가 사용 중지되도록 요구할 수 있습니다.

- (안전한 암호화키 보관) Cloud KMS에서 생성된 암호화키 또는 고객이 기존에 보유한 암호화키를 Cloud KMS로 가져온 경우 등 암호화키는 Cloud KMS 안에서만 보관되고 Cloud KMS 영역 밖으로 나가지 않습니다.
  - 외부키관리(Cloud EKM)의 경우 고객이 구성한 외부 키관리자에 의해 암호화키가 보관됩니다.

3 우수 사례

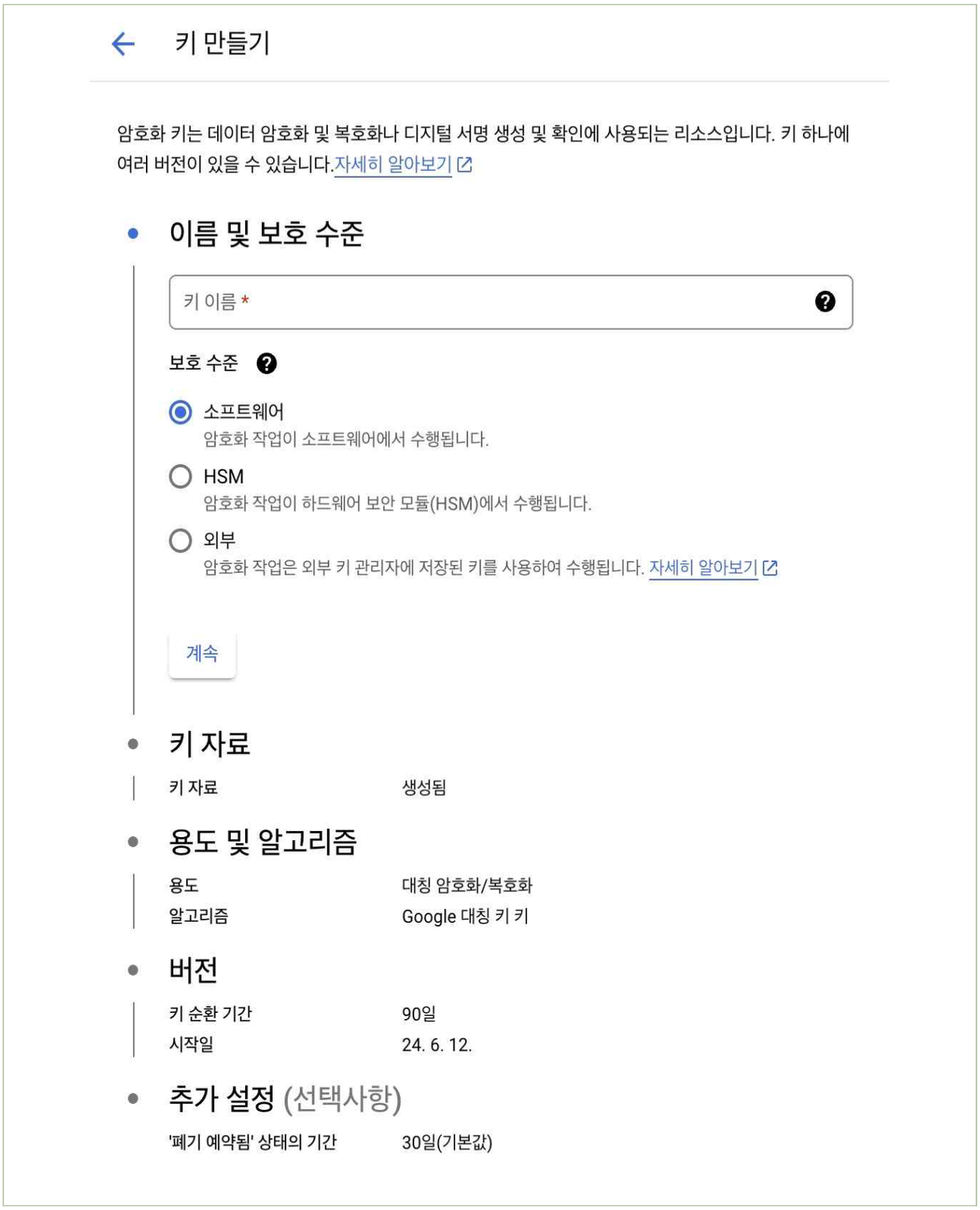
◦ 키링 및 키 만들기

- 키링 만들기



| 그림 4-2-2 | 키링 만들기

– 키 만들기



| 그림 4-2-3 | 키 만들기

키순환

– 키순환 주기 설정

| 그림 4-2-4 | 키순환 주기 설정

– 키순환 현황

| 그림 4-2-5 | 키순환 현황

- 키폐기

| 그림 4-2-6 | 키폐기

- 키버전 사용설정 및 사용중지

  - 사용설정

| 그림 4-2-7 | 키버전 사용설정

  - 사용중지

| 그림 4-2-8 | 키버전 사용중지

4 참고 사항

- Cloud Key Management Service - Deep Dive

  - Cloud Key Management Service—Deep Dive

1 기준

식별번호	기준	내용
4.3.	**암호키 서비스 관리자 권한 통제**	**클라우드 암호키 서비스 이용 시 관리자 권한은 최소인원에게 부여하고 모니터링하여야 한다.**

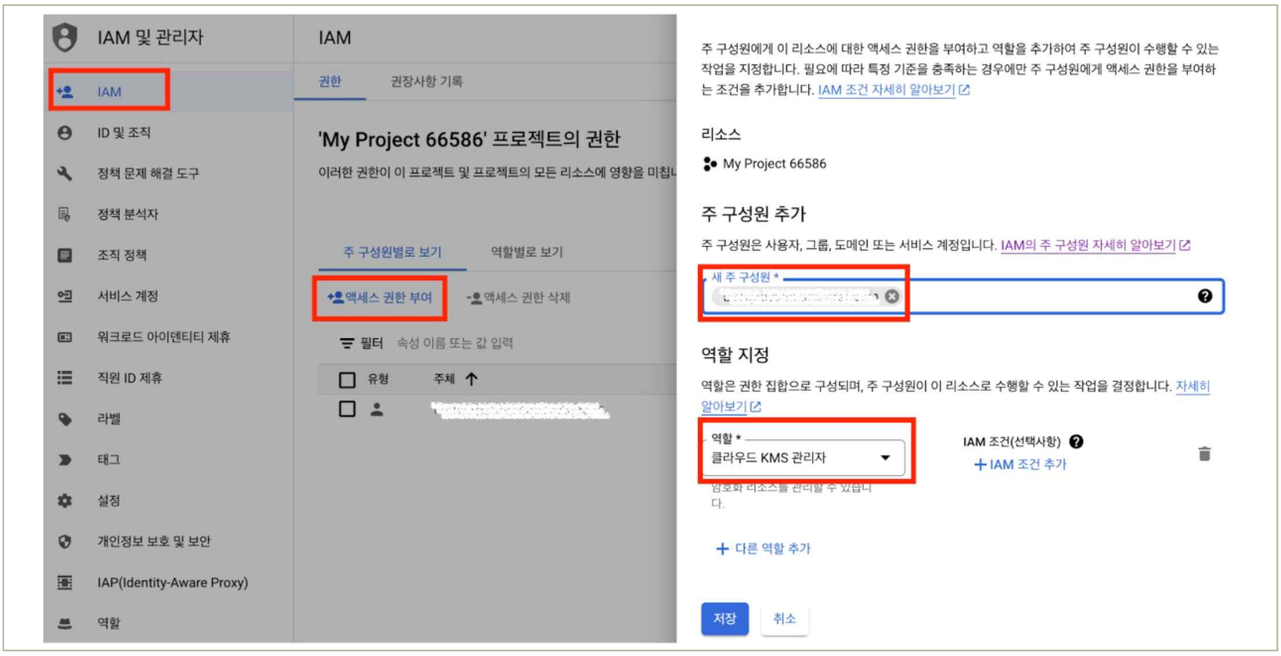
2 설명

- 클라우드 환경 내 암호키 관리 서비스 이용 시 암호키 서비스 관리자 권한을 적절하게 통제하여야 한다.
  - Identity and Access Management(IAM) 역할을 부여를 통해 암호키와 키링과 같은 Cloud KMS 리소스에 대한 액세스를 관리를 통해 암호키 관리자 권한을 통제할 수 있습니다.
  - Cloud KMS 리소스 액세스 관리를 위해 IAM의 사전정의된 역할(Predefined Roles)를 활용하여 암호키 관리 서비스 관리자 권한을 최소인원에게 부여할 수 있습니다.
  - 사용자가 생성하는 각 키, 키링, 프로젝트 등 Cloud KMS 리소스에 대한 관리자를 별도로 지정할 수 있으며, 이를 위해서는 Identity and Access Management(IAM) 역할을 부여해야 합니다. 이를 통해 키 순환 또는 데이터 암호화와 같은 특정한 암호화 작업을 수행하는 기능을 부여하거나 제한할 수 있습니다. Cloud KMS 리소스에 대한 IAM 역할을 부여는 아래와 같이 단계적으로 수행할 수 있습니다.
    - 키(직접 역할 부여)
    - 해당 키링의 모든 키로 상속되는 키링에 역할부여
    - 프로젝트의 모든 키로 상속되는 Google Cloud 프로젝트에 역할부여
    - 폴더 내 모든 프로젝트의 모든 키로 상속되는 Google Cloud 폴더에 역할부여
    - 조직의 폴더에 있는 모든 키로 상속되는 Google Cloud 조직에 역할부여
  - 또한 암호키 순환 또는 데이터 암호화와 같이 특정한 암호화 작업을 수행하는 권한을 부여하거나 제한할 수 있습니다.

- Cloud Audit Logs 또는 IAM 정책 분석 기능을 통하여 암호키 관리자 권한 부여현황에 대해 상시 모니터링을 수행할 수 있습니다.

3 우수 사례

- IAM을 통해 Cloud KMS 관리자 역할 부여(프로젝트, 폴더 또는 조직 단위)
  - IAM → **+액세스 권한 부여** → '새 주 구성원'에 사용자 등 추가 → 역할에 Cloud KMS 관리자' 선택 → 저장

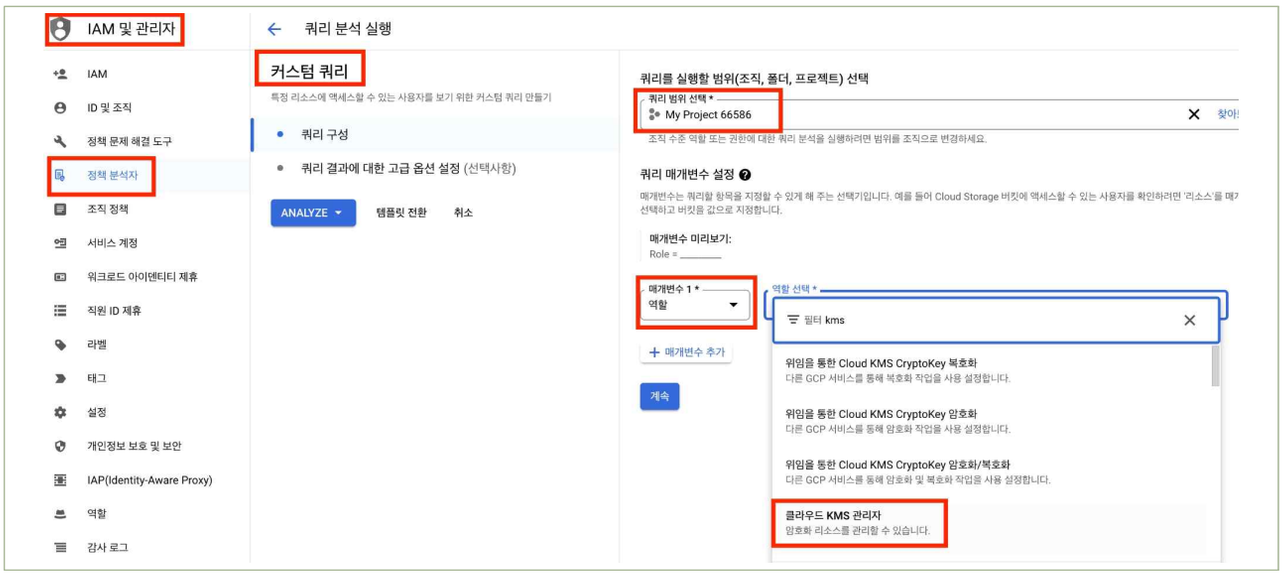


| 그림 4-3-1 | IAM 통한 Cloud KMS 관리자 역할 부여

  - 그 외 키링 및 키 단위에서 Cloud KMS 역할 부여는 '4.4 암호키 호출 권한 관리'를 참고하시기 바랍니다.

- 정책 분석자 기능을 활용하여 암호키 관리자 권한 부여현황을 확인할수 있습니다.
  - IAM 및 관리자 → 정책 분석자 → 커스텀 쿼리 선택
  - 쿼리를 실행할 범위(조직, 폴더, 프로젝트)를 선택 → 매개변수에 '역할' 선택 → 역할선택에서 '클라우드 KMS 관리자' 선택

- ANALYZE 버튼 클릭하여 '쿼리실행' 선택



| 그림 4-3-2 | 관리자 권한 부여현황

- 쿼리 결과를 확인하여 관리 권한 모니터링

| 그림 4-3-3 | 권한 모니터링

- (권장사항) Cloud KMS를 별도의 프로젝트에서 구성하여 좀 더 안전하게 Google Cloud를 사용할 수 있습니다.
  - Cloud KMS는 기존 프로젝트에서 실행될 수 있으나, 이 경우 해당 프로젝트에 대한 owner 액세스 권한을 가진 사용자가 해당 프로젝트에서 Cloud KMS의 키를 관리(하고 이 키를 사용하여 암호화 작업을 수행)할 수 있습니다. 이는 키 또한 프로젝트에 속하여 있기 때문에 프로젝트의 owner가 키까지 관리할 수 있게 되기 때문입니다.

- 이렇게 하는 대신 Cloud KMS를 별도의 프로젝트(예: your-key-project)에서 실행하면 분리 요구사항의 엄격한 정도에 따라 다음 중 하나를 수행할 수 있습니다.
- 프로젝트 수준에서 owner role 없이 암호키 관리를 위한 프로젝트를 생성하고 조직 수준에서 부여된 조직 관리자를 지정합니다. owner와 달리 조직 관리자는 키를 직접 관리하거나 사용할 수 없습니다.
- 조직 관리자의 업무 범위는 키를 관리하고 사용할 수 있는 사용자를 제한하는 IAM 정책 설정으로 제한됩니다.

4 참고 사항

- Cloud KMS에 대한 사전 정의된 역할
  - 권한 및 역할 | Cloud KMS 문서
- Cloud KMS의 액세스 관리를 위한 일반 가이드라인
  - 권한 및 역할 | Cloud KMS 문서

1 기준

식별번호	기준	내용
4.4.	암호키 호출 권한 관리	클라우드 암호키 호출 권한을 관리하여야 한다.

2 설명

- 클라우드 암호키 호출에 관한 사항(암호화, 복호화, 암호키 변경, 삭제 등)은 이용자의 권한 및 업무에 따라 적절하게 부여하고 관리하여야 한다.
  - 암호키를 키용도(Key purpose) 및 사용목적에 따라 특정한 키를 생성하고, 각 키에 IAM 역할(role)을 부여하여 호출에 대한 권한을 관리할 수 있습니다.
  - 키 및 키링과 같은 Cloud KMS 리소스에 대한 액세스를 관리하려면 Identity and Access Management(IAM) 역할을 부여해야 합니다. 이를 통해 키 순환 또는 데이터 암호화와 같 특정한 암호화 작업을 수행하는 기능을 부여하거나 제한할 수 있습니다. Cloud KMS 리소스에 대한 IAM 역할을 부여는 아래와 같이 단계적으로 수행할 수 있습니다.
    - 키(직접 역할 부여)
    - 해당 키링의 모든 키로 상속되는 키링에 역할부여
    - 프로젝트의 모든 키로 상속되는 Google Cloud 프로젝트에 역할부여
    - 폴더 내 모든 프로젝트의 모든 키로 상속되는 Google Cloud 폴더에 역할부여
    - 조직의 폴더에 있는 모든 키로 상속되는 Google Cloud 조직에 역할부여

- Cloud 감사로그를 통하여 Cloud KMS의 암호키 호출 권한 현황에 대한 모니터링을 할수 있습니다. Cloud 감사로그는 관리자 활동 감사 로그와 데이터 액세스 감사 로그로 구분됩니다.
  - (관리자 활동 감사 로그) 메타데이터 또는 구성 정보를 쓰는 '관리자 쓰기' 작업이 포함되고, 관리자 활동 감사 로그에 대한 사용 중지는 할 수 없습니다.
  - (데이터 액세스 감사 로그) 메타데이터 또는 구성 정보를 읽는 '관리자 읽기' 작업이 포함됩니다. 또한 사용자가 제공한 데이터를 읽거나 쓰는 '데이터 읽기' 및 '데이터 쓰기' 작업도 포함됩니다. 데이터 액세스 감사 로그를 받으려면 이를 명시적으로 사용 설정해야 합니다.

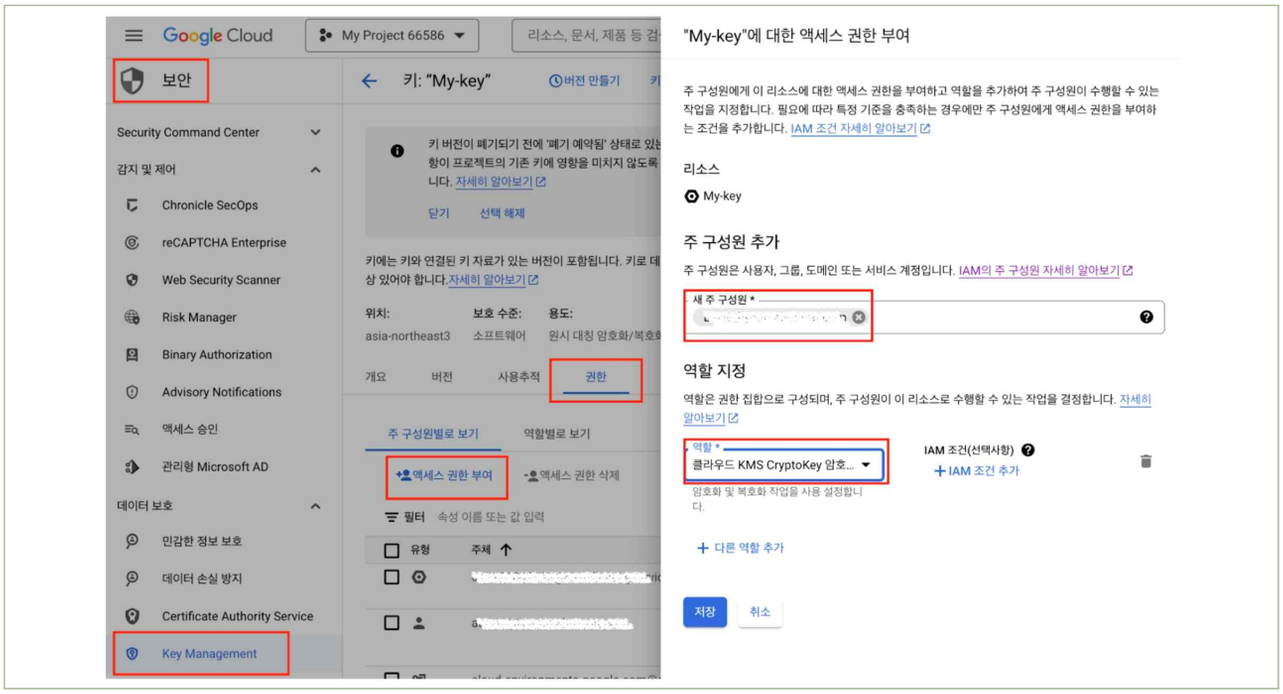
감사 로그 카테고리	Cloud KMS 작업
	cloudkms.projects.locations.keyRings.create cloudkms.projects.locations.keyRings.setIamPolicy cloudkms.projects.locations.keyRings.cryptoKeys.create cloudkms.projects.locations.keyRings.cryptoKeys.patch cloudkms.projects.locations.keyRings.cryptoKeys.setIamPolicy cloudkms.projects.locations.keyRings.cryptoKeys.updatePrimaryVersion cloudkms.projects.locations.keyRings.cryptoKeys.cryptoKeyVersions.create cloudkms.projects.locations.keyRings.cryptoKeys.cryptoKeyVersions.destroy cloudkms.projects.locations.keyRings.cryptoKeys.cryptoKeyVersions.patch cloudkms.projects.locations.keyRings.cryptoKeys.cryptoKeyVersions.restore cloudkms.projects.locations.keyRings.importJobs.create cloudkms.projects.locations.keyRings.importJobs.setIamPolicy
	cloudkms.projects.locations.get cloudkms.projects.locations.list cloudkms.projects.locations.keyRings.get cloudkms.projects.locations.keyRings.getIamPolicy cloudkms.projects.locations.keyRings.list cloudkms.projects.locations.keyRings.testIamPermissions cloudkms.projects.locations.keyRings.cryptoKeys.get cloudkms.projects.locations.keyRings.cryptoKeys.getIamPolicy cloudkms.projects.locations.keyRings.cryptoKeys.list cloudkms.projects.locations.keyRings.cryptoKeys.testIamPermissions cloudkms.projects.locations.keyRings.cryptoKeys.cryptoKeyVersions.get cloudkms.projects.locations.keyRings.cryptoKeys.cryptoKeyVersions.list cloudkms.projects.locations.keyRings.importJobs.get cloudkms.projects.locations.keyRings.importJobs.getIamPolicy cloudkms.projects.locations.keyRings.importJobs.list cloudkms.projects.locations.keyRings.importJobs.testIamPermissions kmsinventory.organizations.protectedResources.search(미리보기) kmsinventory.projects.cryptoKeys.list(미리보기) kmsinventory.projects.locations.keyRings.cryptoKeys.getProtectedResourcesSummary (미리보기)
	cloudkms.projects.locations.keyRings.cryptoKeys.decrypt cloudkms.projects.locations.keyRings.cryptoKeys.encrypt cloudkms.projects.locations.keyRings.cryptoKeys.cryptoKeyVersions.asymmetricDecrypt cloudkms.projects.locations.keyRings.cryptoKeys.cryptoKeyVersions.asymmetricSign cloudkms.projects.locations.keyRings.cryptoKeys.cryptoKeyVersions.getPublicKey

3 우수 사례

- IAM을 통해 Cloud KMS 관리자 역할 부여(프로젝트, 폴더 또는 조직 단위)
  - IAM → **+액세스 권한 부여** → '새 주 구성원'에 사용자 등 추가 → 역할에 '클라우드 KMS CryptoKey 암호화/복호화' 등 선택 → 저장

| 그림 4-4-1 | IAM을 통한 Cloud KMS 관리자 역할 부여

- Cloud KMS 키에 대해 특정 사용자에게 키호출 관련 역할부여
  - 개별 키에 대한 IAM 권한을 부여하려면 IAM 메뉴가 아닌 Cloud KMS 메뉴에서 설정
  - 보안 → Key Management → 키링선택 → 키선택 → 권한 탭 → 액세스 권한 부여 → 새 구성원 추가 → 역할지정



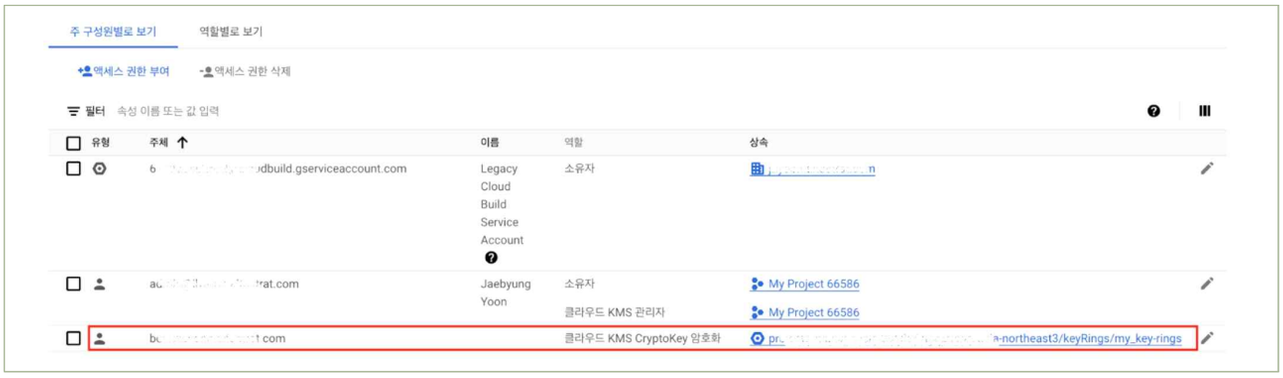
| 그림 4-4-2 | 개별 키에 대한 IAM 권한을 부여

- Cloud KMS 키링에 대해 특정 사용자에게 키호출 관련 역할부여

  - 개별 키링에 대한 IAM 역할 부여는 CLI 형태로 실행 필요

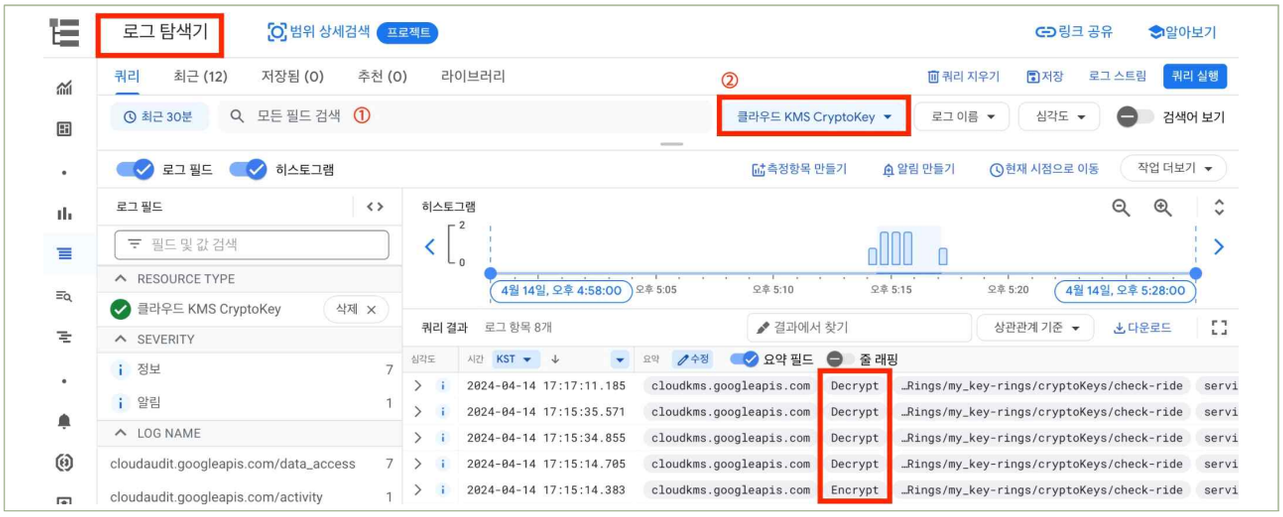
```
gcloud kms keyrings add-iam-policy-binding "keyring" \
--location "location" \
 --member "principal-type":"principal-email" \
 --role roles/"role"
```

  - CLI 방식으로 역할 부여한 후 키링에 IAM 역할이 부여된 화면



| 그림 4-4-3 | 키링에 IAM 역할 부여 현황

- Cloud Console에서 로그 탐색기를 이용하여 암호키 관리 및 호출에 대한 내역을 확인할 수 있음
  - 로깅 → 로그 탐색기
  - ① 모든 필드 검색에 kms 등 검색어를 입력하거나 ② 리소스 선택에서 '클라우드 KMS CryptoKey' 등을 선택하고, 적절한 검색 시간(예: 최근 30일 등)을 선택하여 암호키 호출내역(예: Encrypt 또는 Decrypt 등) 확인



| 그림 4-4-4 | 암호키 관리 및 호출에 대한 내역

4 참고 사항

- IAM으로 암호화키 역할 관리
  - IAM으로 액세스 제어 | Cloud KMS Documentation

1 기준

식별번호	기준	내용
4.5.	안전한 암호화 알고리즘 적용	암호화 기능 이용 시 안전한 암호화 알고리즘을 적용하여야 한다.

2 설명

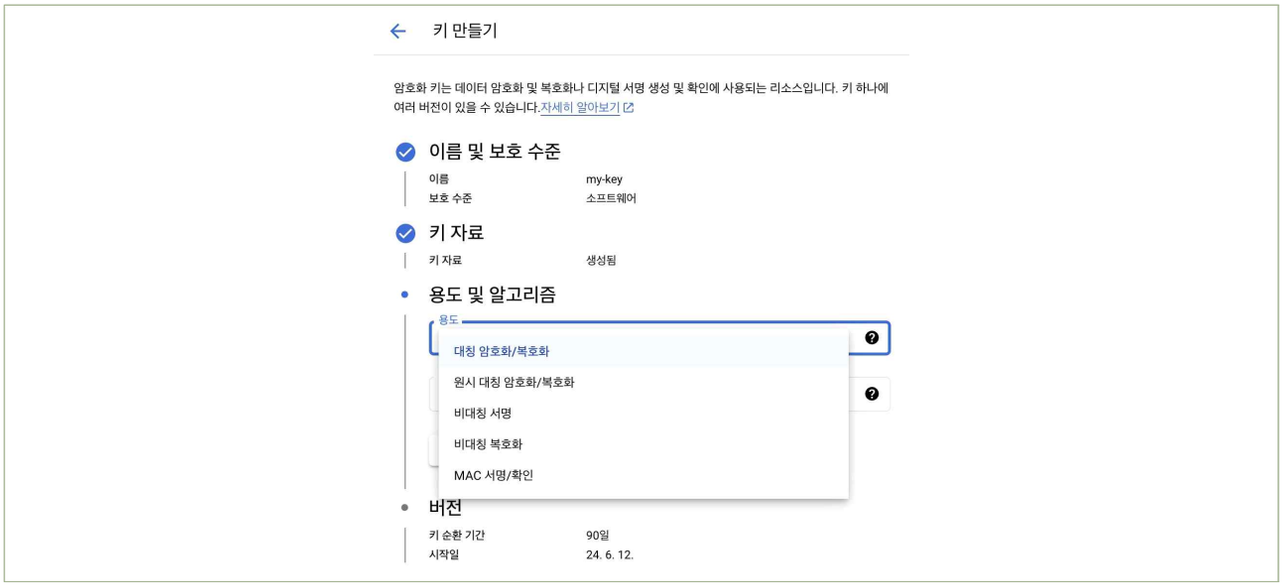
- 암호화 기능 이용 시 안전한 암호화 알고리즘을 적용이 필요합니다. Google Cloud는 암호화 알고리즘을 키용도(Key purpose)에 따라 다음의 5가지로 분류하고, 각 키용도에 따른 선택가능한 알고리즘을 제공하고 있습니다.
  - 대칭 암호화/복호화(Symmetric encryption) : Google 대칭 암호화 알고리즘
  - 원시 대칭 암호화/복호화(Raw symmetric encryption): AES알고리즘(128 bit 및 256 bit)
  - 비대칭 서명(Asymmetric signing): 타원곡선알고리즘, RSA알고리즘(PSS, PKCS#1 v1.5)
  - 비대칭 암호화/복호화(Asymmetric encryption): RSA알고리즘(OAEP)
  - MAC 서명/확인(MAC signing): HMAC알고리즘

시나리오	키 용도(SDK)	키 용도(API)	지원되는 메서드
대칭적 암호화	encryption	ENCRYPT_DECRYPT	cryptoKeys.encrypt, cryptoKeys.decrypt
원시 대칭 암호화	raw-encryption	RAW_ENCRYPT_DECRYPT	cryptoKeys.rawEncrypt, cryptoKeys.rawDecrypt
비대칭 서명	asymmetric-signing	ASYMMETRIC_SIGN	cryptoKeyVersions.asymmetricSign, cryptoKeyVersions.getPublicKey
비대칭 암호화	asymmetric-encryption	ASYMMETRIC_DECRYPT	cryptoKeyVersions.asymmetricDecrypt, cryptoKeyVersions.getPublicKey
MAC 서명	mac-signing	MAC	cryptoKeyVersions.macSign, cryptoKeyVersions.macVerify

3 우수 사례

- 키용도(Key purpose) 및 알고리즘 선택: 보안 → Key Management → 키링 선택(또는 키링 만들기) → 키 만들기

  - 키용도 선택



| 그림 4-5-1 | 키용도 선택

  - 알고리즘 선택

| 그림 4-5-2 | 알고리즘 선택

4 참고 사항

- 키 용도 및 알고리즘

  - 키 용도 및 알고리즘 | Cloud KMS Documentation

5. 로깅 및 모니터링 관리

5.1. 가상자원 이용(생성, 삭제, 변경 등)에 관한 행위추적성 확보
5.2. 가상자원 이용 행위추적성 증적 모니터링
5.3. 이용자 가상자원 모니터링 기능 확보
5.4. API 사용(호출대상, 호출자, 호출일시 등)에 관한 행위추적성 확보
5.5. 네트워크 관련 서비스(VPC, 보안그룹, ACL 등)에 관한 행위추적성 확보
5.6. 계정 변동사항에 대한 행위추적성 확보
5.7. 계정 변경사항에 관한 모니터링 수행

5 로깅 및 모니터링 관리

1 기준

식별번호	기준	내용
5.1.	**가상자원 이용(생성, 삭제, 변경 등)에 관한 행위추적성 확보**	**이용자의 가상자원(서버, 데이터베이스, 스토리지 등) 이용 관련 행위추적성(로그 등)을 확보하여야 한다.**

2 설명

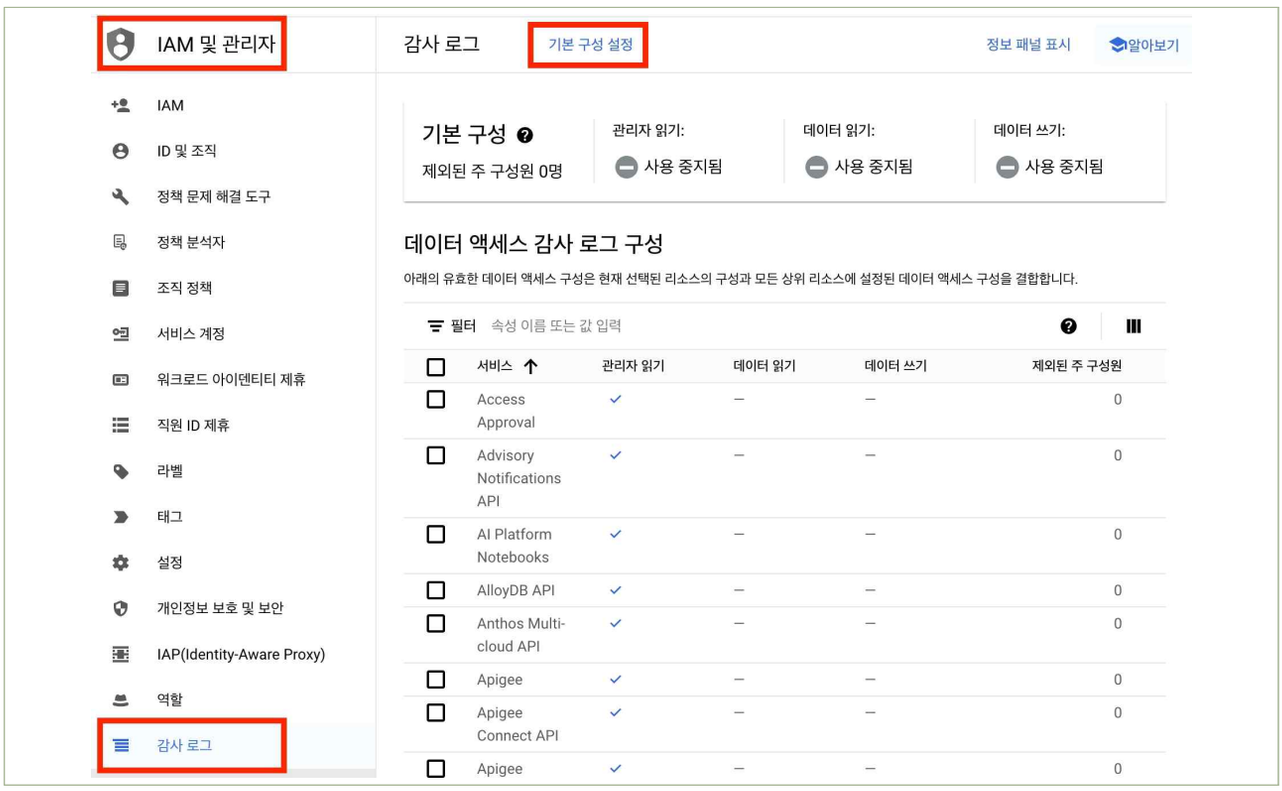
- 이용자의 가상자원 이용 관련 일련의 행위에 대한 추적성을 확보할 수 있는 방안이 마련되어야 한다.
  - 가상자원 변경사항에 관한 행위(생성, 변경, 삭제 등)
  - 가상자원에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록
  - 가상자원을 사용한 일시, 사용자 및 가상자원의 형태(서버, 데이터베이스, 스토리지 등)를 확인할 수 있는 접근기록
  - 가상자원 내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 엑세스 로그 등 접근기록

- (Cloud Logging) Google Cloud 서비스는 Google Cloud 리소스 내의 관리 활동과 액세스를 기록하는 감사 로그를 작성합니다. 감사 로그는 Google Cloud 리소스 내에서 '누가 언제 어디서 무엇을 했는가?'라는 질문에 답하는 데 도움을 주고, 시스템에서 취약점 발생 또는 데이터 오용 가능성을 모니터링할 수 있습니다. 감사로그 유형은 4가지로, 관리자 활동 감사 로그, 데이터 액세스 감사 로그, 시스템 이벤트 감사 로그, 정책 거부 감사 로그로 구성됩니다.
  - **관리자 활동 감사 로그** : 관리자 활동 감사 로그에는 API 호출이나 리소스의 구성 또는 메타데이터를 수정하는 기타 작업과 관련된 로그 항목이 포함됩니다. 예를 들어 사용자가 VM 인스턴스를 만들거나 Identity and Access Management 권한을 변경하면 로그가 기록됩니다.
  - **데이터 액세스 감사 로그** : 데이터 액세스 감사 로그에는 리소스의 구성 또는 메타데이터를 읽는 API 호출뿐만 아니라 사용자가 제공한 리소스 데이터를 생성, 수정 또는 호출하는 API 정보를 포함합니다.

- **시스템 이벤트 감사 로그** : 시스템 이벤트 감사 로그는 리소스 구성을 수정하는 Google Cloud 작업의 로그 항목을 포함합니다.
- **정책 거부 감사 로그** : 정책 거부 감사 로그는 보안 정책 위반으로 인해 Google Cloud 사용자 또는 서비스 계정에 대해 액세스를 거부할 때 기록됩니다.
- **가상자원 내 전산자료의 처리 로그 :** 금융회사에서는 가상자원으로 구성한 정보처리시스템 내 전산자료(소스코드, 고객정보, 회사정보 등)에 대한 처리 로그(전산자료의 수정 및 삭제, 접근 등)를 수집하여야 한다.

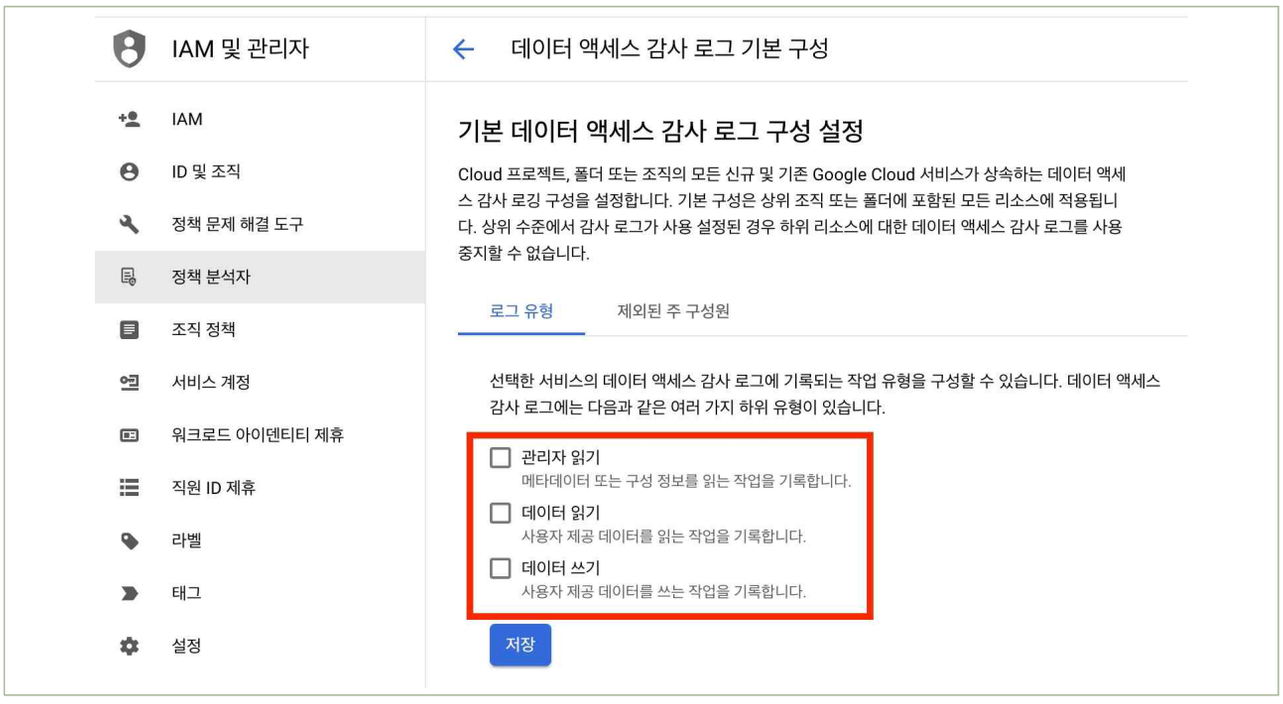
3 우수 사례

- 데이터 액세스 감사 로그(BigQuery 데이터 액세스 감사 로그 제외)는 크기가 클 수 있으므로 기본적으로 사용 중지되어 있습니다. BigQuery 이외의 Google Cloud 서비스에 대해 데이터 액세스 감사 로그를 남기려면 로그를 명시적으로 사용 설정해야 합니다.
  - 데이터 액세스 감사 로그를 활성화 하려면 'IAM 및 관리자' → '감사 로그' → '기본 구성 설정



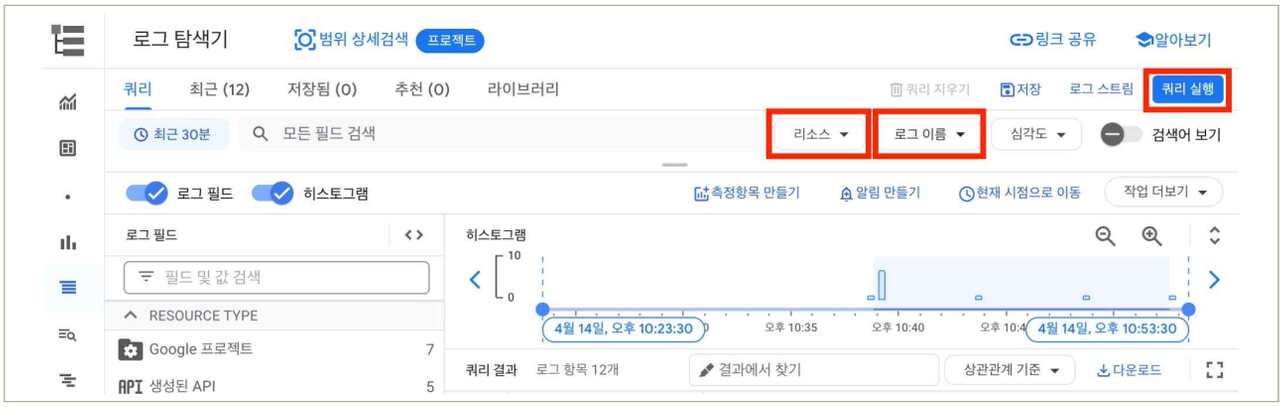
| 그림 5-1-1 | 감사 로그 구성

- 데이터 액세스 감사로는 '관리자 읽기', '데이터 읽기' 및 '데이터 쓰기' 유형이 있으며 각 유형에 대해 선택적으로 활성화 가능



| 그림 5-1-2 | 데이터 액세스 감사 로그 기본 구성

- (로그 탐색기) 로그를 검색하기 위해서는 로그 탐색기를 활용하여 리소스별, 로그 생성시간별로 선택하여 검색할 수 있습니다.
  - '로깅' → '로그 탐색기'로 이동한다. → 쿼리 빌더 창에서 다음을 수행한다.
  - **리소스 유형**에서 감사 로그를 확인할 Google Cloud 리소스를 선택한다.
  - **로그 이름**에서 확인할 감사 로그 유형을 선택한다.
    - 관리자 활동 감사 로그의 경우 **activity**를 선택한다.
    - 데이터 액세스 감사 로그의 경우 **data_access**를 선택한다.
    - 시스템 이벤트 감사 로그의 경우 **system_event**를 선택한다.
    - 정책 거부 감사 로그의 경우 **정책**을 선택한다.
  - **쿼리 실행**을 클릭한다.



| 그림 5-1-3 | 로그 탐색기

4 참고 사항

- Cloud 감사 로그 개요
  - Cloud 감사 로그 개요 - Logging
- Cloud Logging 개요
  - Cloud Logging 개요
- 감사로그를 생성하는 서비스 목록
  - 감사 로그가 있는 Google Cloud 서비스

1 기준

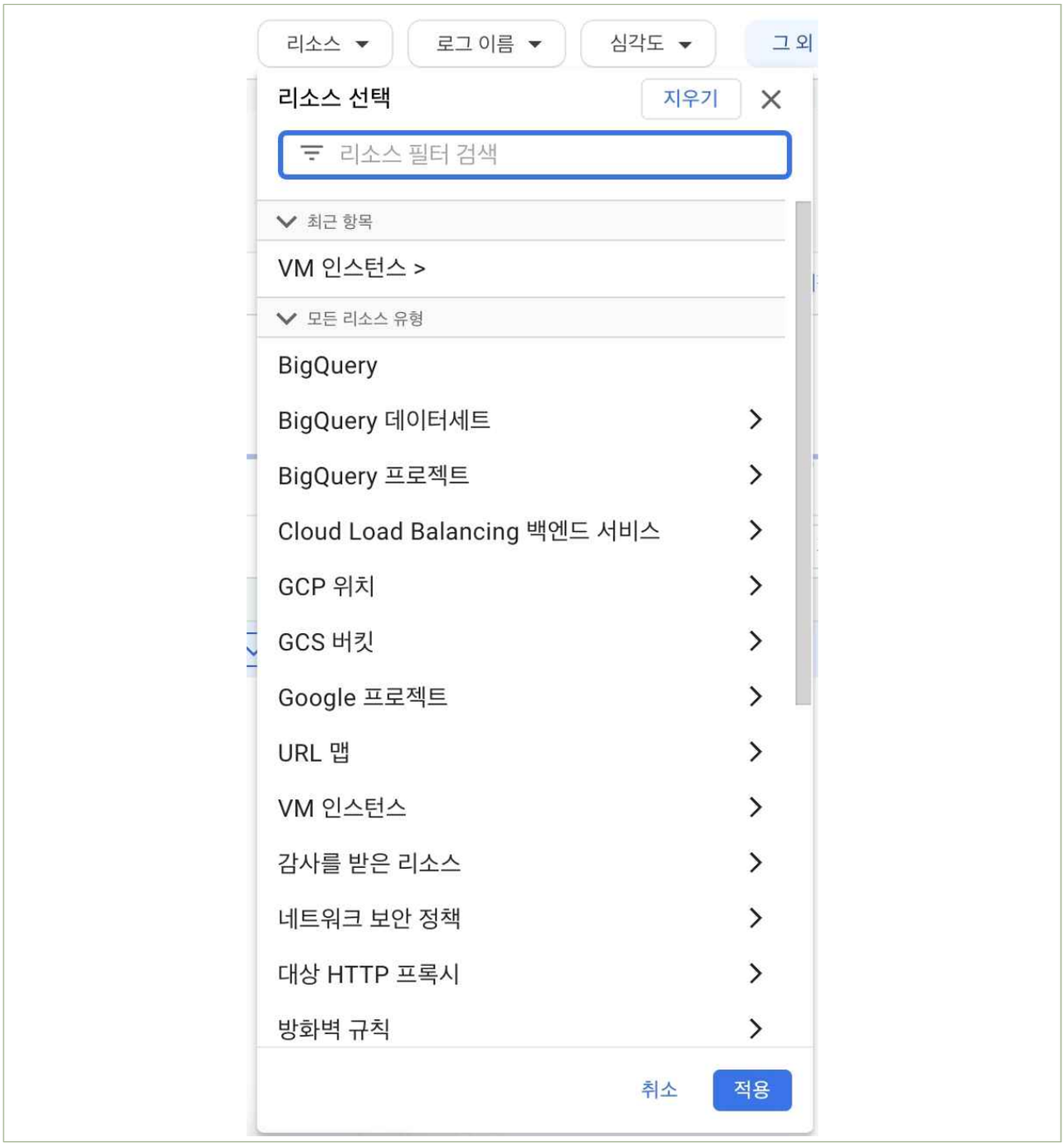
식별번호	기준	내용
5.2.	**가상자원 이용 행위추적성 증적 모니터링**	**가상자원 이용에 관한 행위추적성 증적에 대해 모니터링 및 주기적 검토를 수행하여야 한다.**

2 설명

- 클라우드 가상자원 이용에 관한 행위추적성 증적에 대해 모니터링 및 주기적 검토를 수행하여야 한다.
  - 클라우드 가상자원 이용에 관한 행위추적성 증적(ex. 감사로그 등)에 대한 상시 모니터링 수행
  - 금융회사 내부규정등 관련 규정을 통해 수립된 검토 기간에 맞추어 클라우드 가상자원 이용에 관한 행위추적성 증적에 대한 주기적 검토 수행

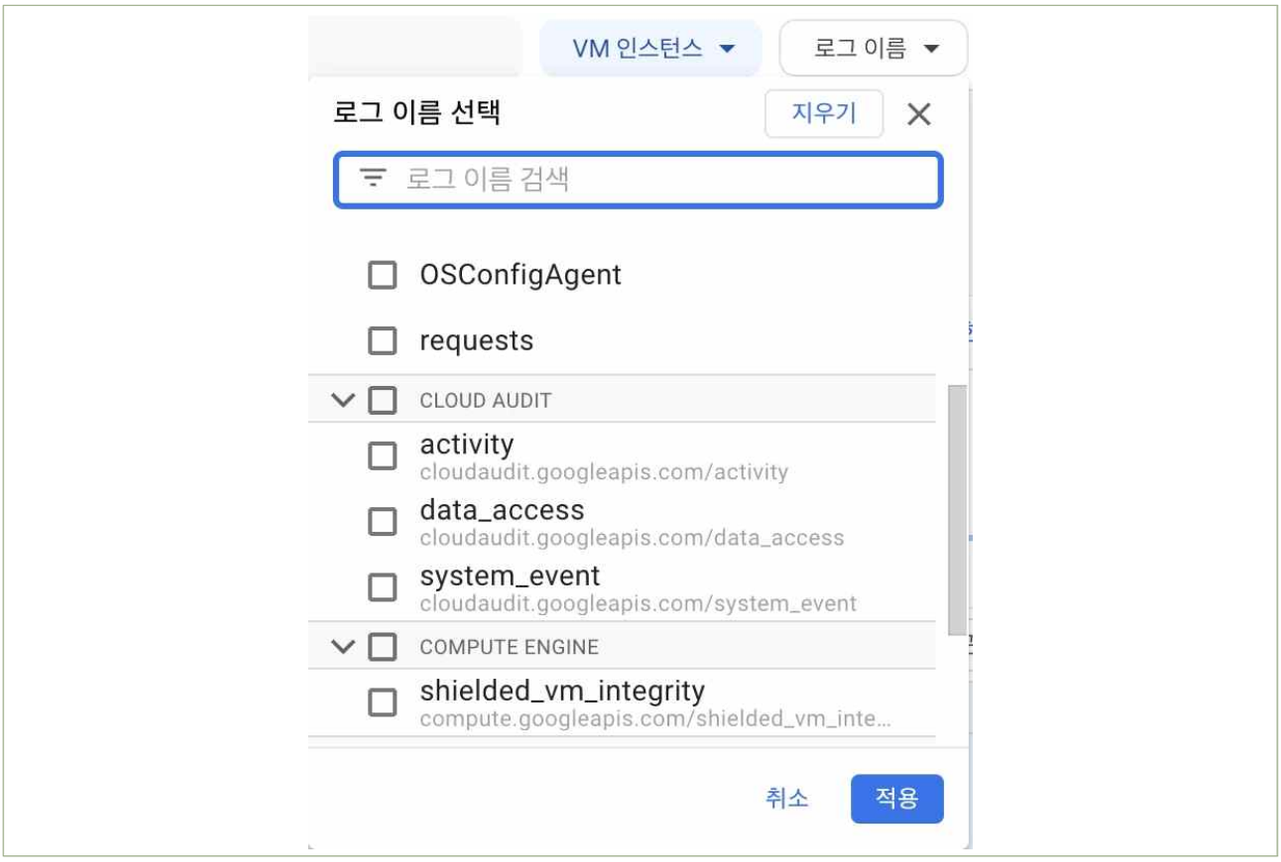
3 우수 사례

- (로그 탐색기) '로깅' → '로그 탐색기'로 이동한다. → 이후 '리소스' 항목에서 모니터링이 필요한 서비스를 선택하고 '로그 이름' 항목에서 확인하려는 행위를 선택하여 로그를 확인할 수 있다.
  1. Google Cloud 콘솔의 탐색 패널에서 로깅을 선택 한 후 로그 탐색기를 선택합니다.
  2. 기존 Google Cloud 프로젝트, 폴더 또는 조직을 선택합니다.
  3. 특정 리소스의 감사 로그 유형을 확인하려면 작업을 수행합니다.
     - 리소스 항목에서 감사 로그를 확인할 Google Cloud 리소스를 선택합니다.



| 그림 5-2-1 | 로그 탐색기 리소스 선택

- 로그 이름 항목에서 확인할 감사 로그 유형을 선택합니다.
  - 관리자 활동 감사 로그의 경우 activity를 선택합니다.
  - 데이터 액세스 감사 로그의 경우 data_access를 선택합니다.
  - 시스템 이벤트 감사 로그의 경우 system_event를 선택합니다.
  - 정책 거부 감사 로그의 경우 정책을 선택합니다.



| 그림 5-2-2 | 감사 로그 유형 선택

- (주기적 검토) 위 단계를 통해 확인된 로그에 대해 금융회사에서는 주기적 검토를 수행한다.
  1. 인가받지 않은 가상자원 접속, 생성, 변경, 삭제 등

4 참고 사항

- VM에서 발생한 상세한 로그를 확인하기 위해서는 Agent를 설치하여야 합니다. 다음 링크에서 Agent에 대한 설명 및 설치 방법을 확인할 수 있습니다.

  - Google Cloud Observability 에이전트

- 운영 에이전트를 사용하여 Compute Engine 가상 머신(VM) 인스턴스에 설치된 Apache 웹 서버에서 수집된 syslog 로그를 수집하고 보는 방법

  - 빠른 시작: 운영 에이전트를 사용하여 Apache에서 로그 수집 | Cloud Logging

1 기준

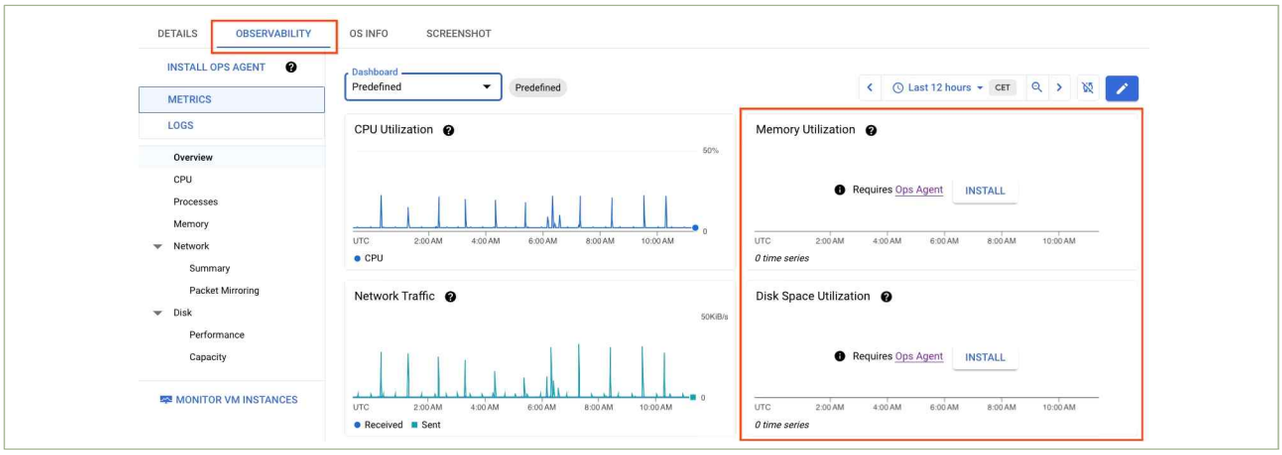
식별번호	기준	내용
5.3.	**이용자 가상자원 모니터링 기능 확보**	**이용자 가상자원 운용에 관한 모니터링 기능을 확보하여야 한다.**

2 설명

- 이용자 가상자원 가용성 확보 및 장애대응을 위한 모니터링 기능을 확보하여야 한다.
  - 가상자원 상태 모니터링(사용량, 트래픽 용량 등)
  - 가상자원 장애 모니터링(장애 발생 시 담당자 공지 등)
  - 가상자원 장애 발생 시 장애상황기록부 작성 등
  - 가상자원 네트워크 정책 변경(삭제 등) 모니터링

3 우수 사례

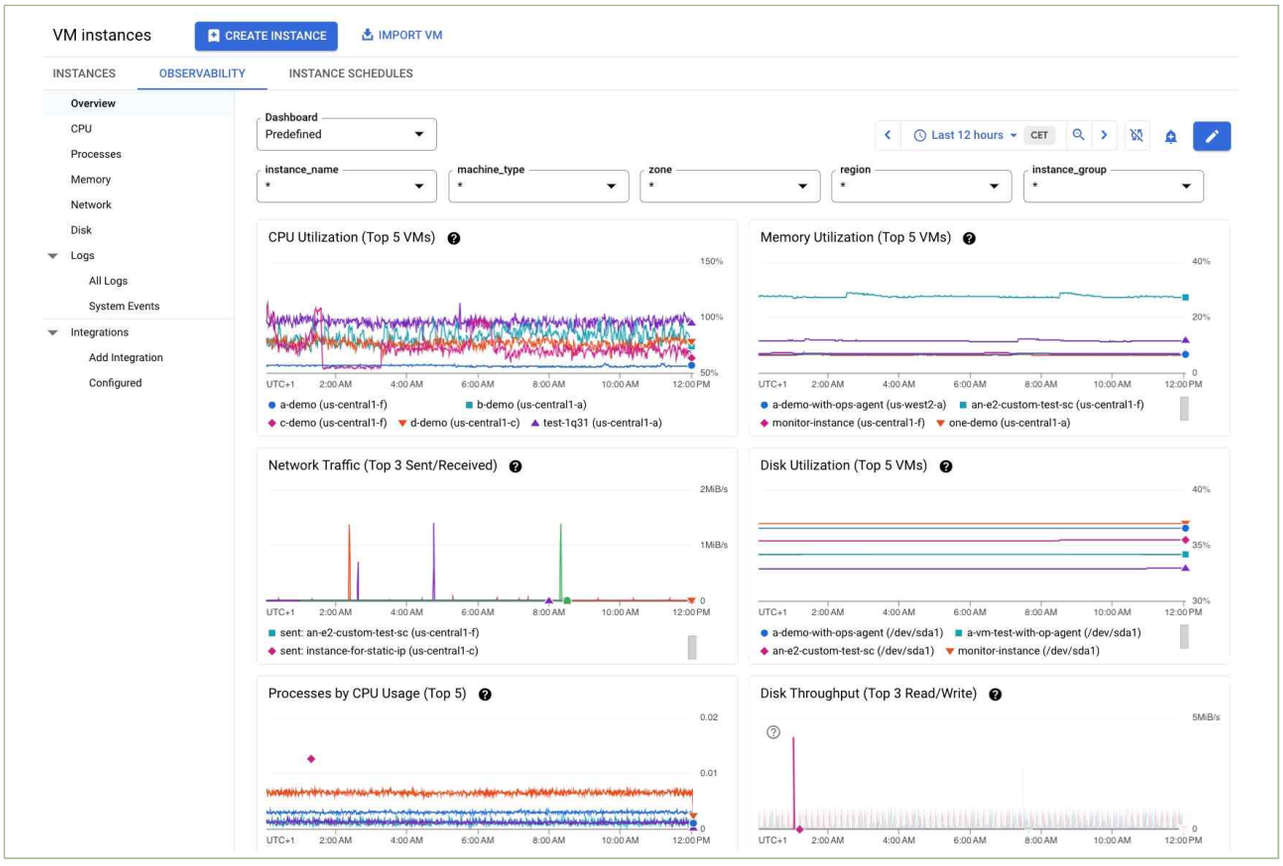
- 가상자원 생성 후 CPU 사용률 및 네트워크 트래픽과 같은 기본 측정항목을 모니터링할 수 있습니다. 다만, 메모리 및 프로세스 사용률에 대한 측정항목은 운영 에이전트를 설치해야 확인할 수 있습니다.
  - 단일 VM의 측정항목을 보려면 다음을 수행합니다.
    1. Google Cloud 콘솔에서 **VM 인스턴스** 페이지로 이동합니다.
    2. VM을 선택하여 **세부정보** 페이지를 엽니다.
    3. **관측 가능성** 탭을 클릭하여 VM에 대한 정보를 표시합니다.
    4. 선택사항: 1시간의 기본 기간을 모니터링할 기간으로 재설정합니다.



| 그림 5-3-1 | 측정 항목

- 여러 VM의 관측 가능성 측정항목 보기

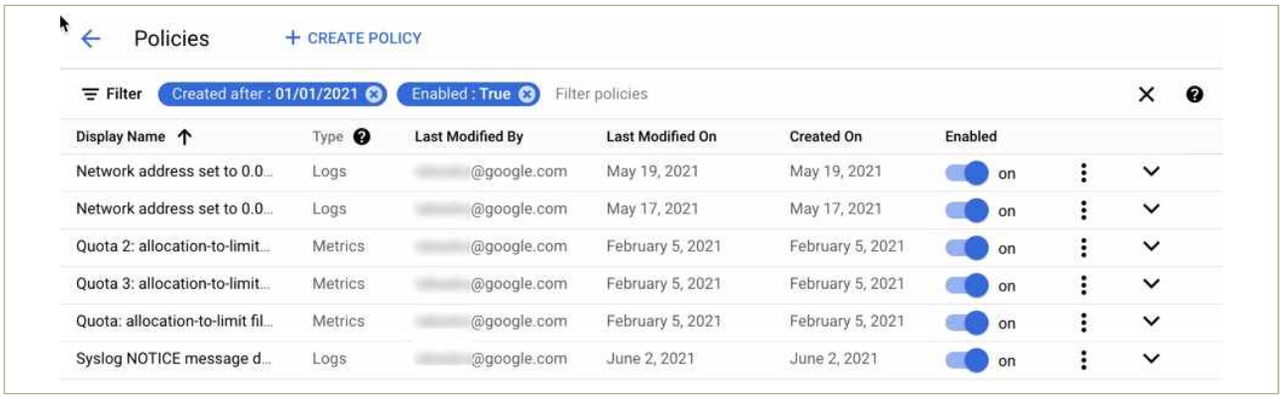
1. Google Cloud 콘솔에서 **VM 인스턴스** 페이지로 이동합니다.
2. **관측 가능성** 탭을 클릭합니다.
3. 선택사항: 1시간의 기본 기간을 모니터링할 기간으로 재설정합니다.
4. 다음 옵션 중 하나 이상을 사용해서 결과를 필터링합니다.
   - ID
   - 이름
   - 머신 유형
   - 영역
   - 리전
   - 인스턴스 그룹
   - 라벨
   - 상태



| 그림 5-3-2 | 여러 VM의 관측 가능성 측정항목 보기

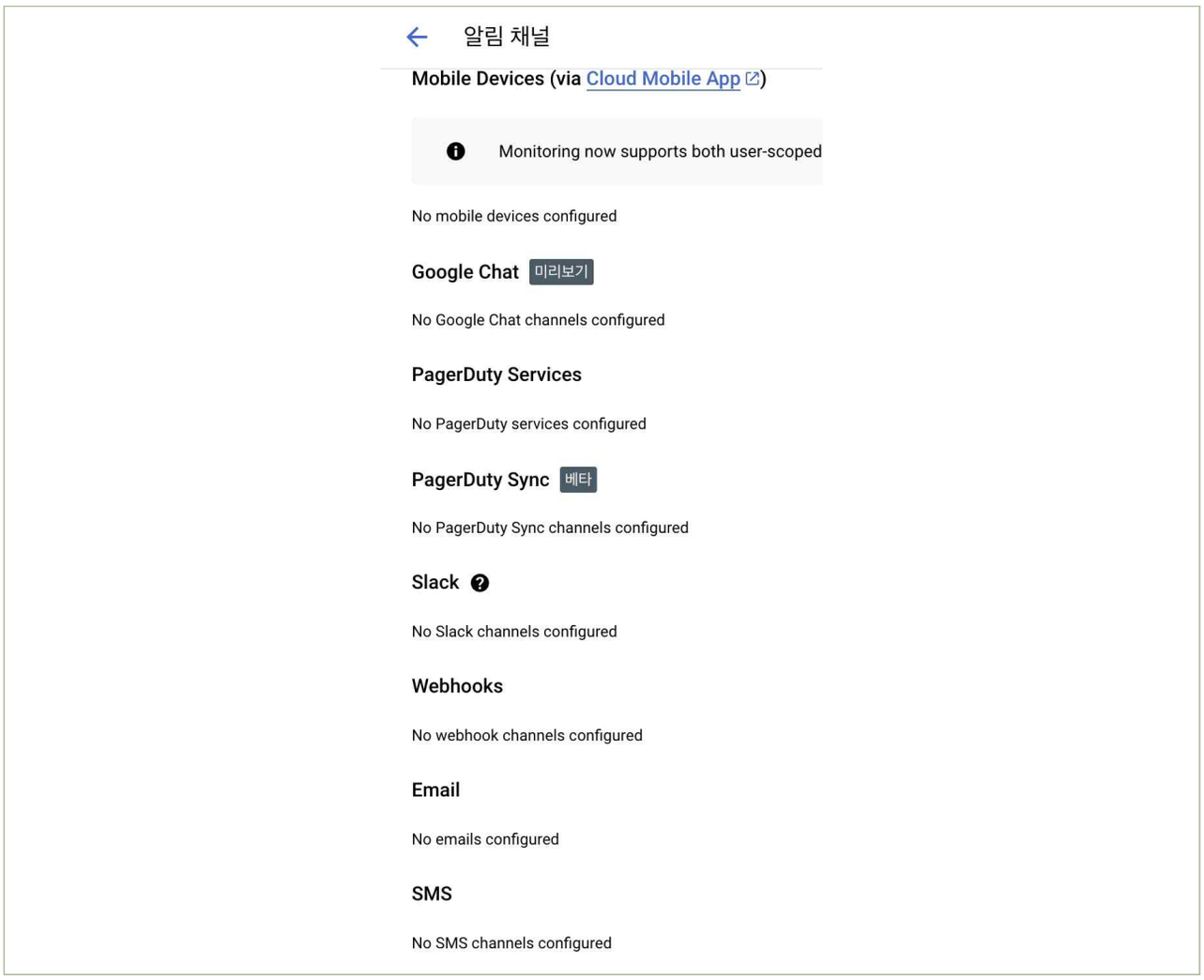
- 로그 모니터링 방법에는 로그 기반 알림과 로그 기반 측정항목 알림 두 가지 종류가 있습니다.
  - 로그 기반 측정 알림 : 시간 경과에 따른 변경사항을 알리는 알림 정책을 만들수 있습니다.
  - 로그 기반 알림 : 특정 이벤트가 로그에 나타날 때마다 알림을 제공합니다.

- 알림 정책 만들기 및 관리
  1. Google Cloud 콘솔의 탐색 패널에서 **Monitoring**을 선택한 후 **알림**을 선택합니다.
  2. **모든 정책 보기**를 선택합니다.
  3. 로그 기반 알림은 **유형** 열의 Logs 값과 함께 목록에 표시됩니다. 로그 기반 측정항목을 포함한 측정항목 기반 알림은 **유형** 열의 Metrics 값과 함께 목록에 표시됩니다. 다음 스크린샷은 정책 목록의 일부를 보여줍니다.



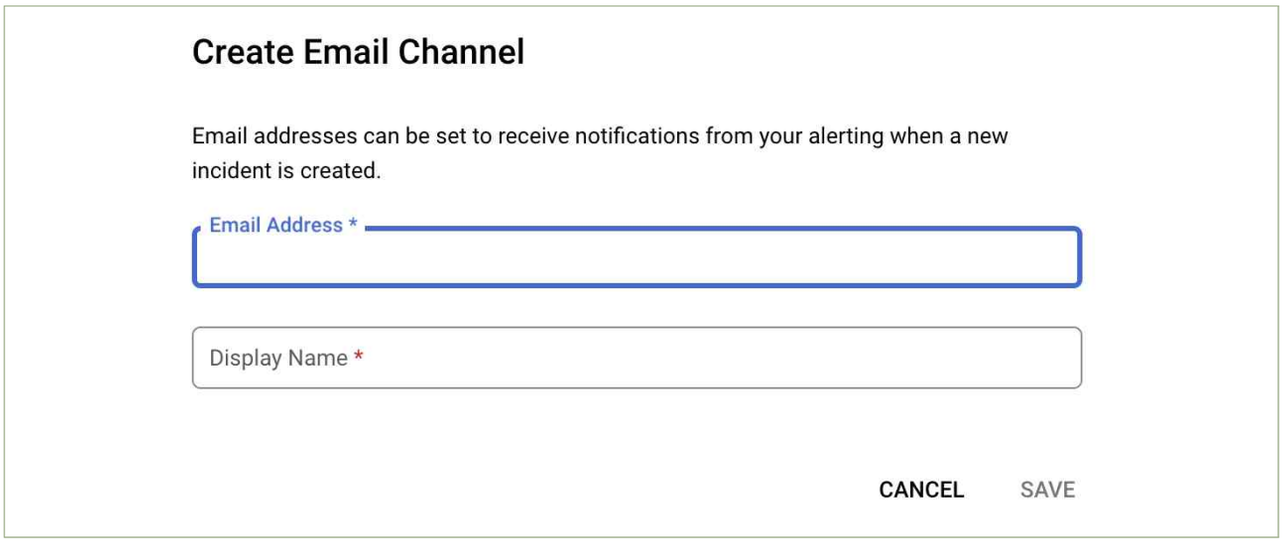
| 그림 5-3-3 | 알림 정책 만들기 및 관리

- 알림 채널 : 측정항목 기반 및 로그 기반 알림에서 Monitoring이 지원하는 모든 알림 채널에 알림을 보낼 수 있습니다. 이러한 채널을 알림 정책에 사용하려면 먼저 채널을 구성해야 합니다.
  알림을 보낼 수 있는 채널은 Email / SMS / Webhooks / Slack / Google Chat등 다양합니다.
  아래는 이메일 알림 채널 생성하는 예제입니다.



| 그림 5-3-4 | 알림 채널

1. Google Cloud 콘솔의 탐색 패널에서 **Monitoring**을 선택한 후 **알림**을 선택합니다.
2. **알림 채널 수정**을 클릭합니다.
3. **이메일** 섹션에서 **새로 추가**를 클릭합니다.
4. 단일 이메일 주소와 설명을 입력합니다.
5. **저장**을 클릭합니다.



| 그림 5-3-5 | 이메일 알림 채널 생성

4 참고 사항

- 로그 모니터링
  - 로그 모니터링 - Logging
- 알림 채널 만들기
  - 알림 채널 만들기 및 관리 | Cloud Monitoring

1 기준

식별번호	기준	내용
5.4.	**API 사용(호출대상, 호출자, 호출일시 등)에 관한 행위추적성 확보**	**API 사용 이력에 대한 행위추적성(로그 등)을 확보하여야 한다.**

2 설명

- API 사용 이력에 대한 행위추적성을 확보하여야 한다.
  - API 호출에 관한 정보(호출대상, 호출자, 호출일시 등)

3 우수 사례

- (로그 탐색기) '로깅' → '로그 탐색기'로 이동한다. → 이후 '리소스' 항목에서 '생성된 API'를 선택하여 API 사용 관련 행위 추적성을 확보할 수 있습니다.
  - API 로그는 서비스별로, Method별로 분리해서 로그 확인이 가능합니다.
    1. 해당 결과에 호출 대상, 호출자, 호출일시가 나타남을 알 수 있습니다.

| 그림 5-4-1 | 로그 탐색기

| 그림 5-4-2 | 로그 탐색 결과

4 참고 사항

- Google Cloud 콘솔의 로그 탐색기를 사용하여 중요한 로그를 쉽게 찾을 수 있는 추천 쿼리
  - 샘플 쿼리 - Logging

1 기준

식별번호	기준	내용
5.5.	**네트워크 관련 서비스(VPC, 보안그룹, ACL 등)에 관한 행위추적성 확보**	**이용자의 클라우드 네트워크 서비스 이용 시 발생하는 사항에 대한 행위추적성(로그 등)을 확보하여야 한다.**

2 설명

- 클라우드 환경에서 네트워크 서비스(VPC, NAT 등) 사용 시 발생하는 사항에 대한 행위추적성(로그 등)을 확보하여야 한다.
  - 네트워크 서비스 이용에 관한 사항(VPC, NAT 규칙 생성 및 변경 등) 등

3 우수 사례

- VPC flow 로그는 VPC네트워크에서 전송 또는 수신되는 네트워크 흐름을 기록합니다. 이 로그를 통하여 네트워크 모니터링 및 실시간 보안 분석에 사용할 수 있다.
  - 네트워크 모니터링 : VPC flow 로그는 네트워크 처리량과 성능에 관한 실시간 정보를 제공합니다. 다음과 같은 작업을 수행할 수 있습니다.
    - VPC 네트워크 모니터링
    - 네트워크 진단 수행
    - VM 및 애플리케이션별로 흐름 로그를 필터링하여 트래픽 변화 파악
    - 용량 예측을 위한 트래픽 증가 파악
  - 네트워크 사용량 파악 및 네트워크 트래픽 비용 최적화 : VPC 흐름 로그를 사용하여 네트워크 사용량을 분석할 수 있습니다. 다음의 네트워크 흐름을 분석할 수 있습니다.
    - 리전 및 영역 간의 트래픽
    - 인터넷의 특정 국가로 가는 트래픽
    - 최상위 네트워크 소비자

- 네트워크 증거 수집 : 네트워크 포렌식용으로 VPC 흐름 로그를 활용할 수 있습니다. 예를 들어 이슈가 발생하면 다음 항목을 검사할 수 있습니다.
  - 어떤 IP로 누구와 언제 통신했는지
  - 모든 손상된 IP(들어오고 나가는 모든 네트워크 흐름 분석)
- 실시간 보안 분석
  - Pub/Sub를 통해 실시간 스트리밍 API를 활용하고 SIEM(Security Information and Event Management) 시스템과 통합할 수 있습니다. 실시간 모니터링, 이벤트, 분석, 보안 알림의 연관성을 제공할 수 있습니다.

- 서브넷 생성 시 VPC flow 로그 사용 설정
  1. Google Cloud 콘솔에서 **VPC 네트워크** 페이지로 이동합니다.
  2. 서브넷을 추가할 네트워크를 클릭합니다.
  3. **서브넷 추가**를 클릭합니다.
  4. **흐름 로그**에서 **사용**을 선택합니다.
  5. 로그 샘플링 및 집계를 조정하려는 경우 **로그 구성**을 클릭하고 다음을 조정합니다.
     - **집계 간격**
     - 최종 로그 항목에 메타데이터를 포함할지 여부. 기본적으로 **메타데이터 포함**에는 모든 필드가 포함됩니다.
     - **샘플링 레이트**. 100%는 모든 항목이 유지됨을 의미합니다.
  6. 기타 필드를 상황에 맞게 지정합니다.
  7. **추가**를 클릭합니다.

- Cloud NAT 로깅을 사용하면 NAT를 사용하는 네트워크 연결이 생성되는 로그를 생성할 수 있다.
  1. Google Cloud콘솔에서 Cloud NAT 페이지로 이동한다.
  2. NAT 게이트웨이를 클릭한다.
  3. 수정을 클릭한다.
  4. 고급 구성을 클릭한다.
  5. Logging 섹션에서 다음중 하나를 선택한다.
     - 로깅 없음 : 로깅 중지한다.
     - 변환 및 오류 : 모든 로그를 Logging으로 보낸다.
     - 변환만 : 연결이 생성될 때만 로그를 보내며 삭제된 패킷은 로깅하지 않는다.
     - 오류만 : 사용할 수 있는 포트가 없어서 패킷이 삭제될 때 로그를 보내며 새 연결은 로깅하지 않는다.

4 참고 사항

- NAT 로깅
  - https://cloud.google.com/nat/docs/monitoring?hl=ko
- VPC flow 로깅
  - https://cloud.google.com/vpc/docs/flow-logs?hl=ko

1 기준

식별번호	기준	내용
5.6.	**계정 변동사항에 대한 행위추적성 확보**	**클라우드 계정 변동사항에 대한 행위추적성(로그 등)을 확보하여야 한다.**

2 설명

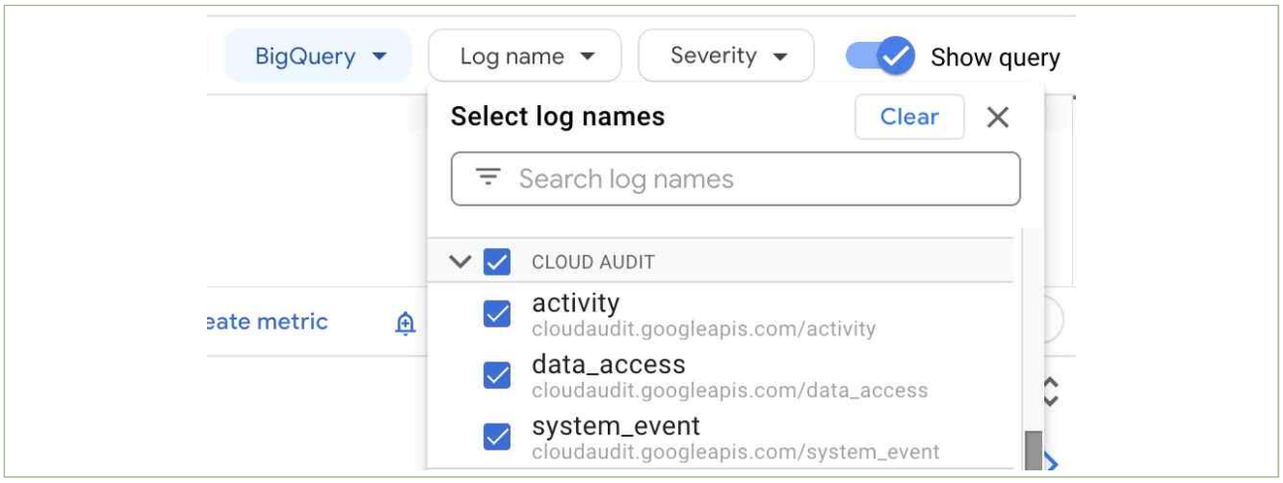
- 클라우드 계정에 대한 행위추적성(로그 등)을 확보하여야 한다.
  - 클라우드 가상자원 관리시스템 접속 계정 생성, 변경, 삭제에 관한 사항
  - 클라우드 가상자원(서버, 데이터베이스 등) 접속 계정 생성, 변경, 삭제에 관한 사항

3 우수 사례

- 클라우드 계정 변동 사항에 대한 행위 추적성 확보는 IAM 감사 로그를 통해 가능하고 아래 유형의 감사 로그가 존재합니다.
  - 관리자 활동 감사 로그 : 메타정보 및 구성 정보를 쓰는 'admin write' 관련 로그를 저장합니다.(예. CreateRole / DeleteRole / UpdateRole/CreateServiceAccount)
  - 데이터 액세스 감사 로그 : 메타정보 및 구성 정보를 읽는 'admin read' 관련 로그를 저장하고(예.GetRole/ListRoles) 사용자가 제공한 데이터를 읽거나 쓰는 '데이터 읽기' 및 '데이터 쓰기' 작업 로그도 저장합니다.

- 관리자 활동 감사 로그를 통하여, '누가,언제,어디서,무엇을 했는지'를 확인할 수 있으며, 이를 통하여 가상자원 관련 계정 변동 사항에 대한 행위 추적성을 확보할 수 있습니다.

- (로그 탐색기) '로깅' → '로그 탐색기'로 이동합니다.
  1. 리소스 유형에서 감사 로그를 확인할 Google Cloud 리소스를 선택
     - 관리자 활동 감사 로그의 경우 activity를 선택
     - 데이터 액세스 감사 로그의 경우 data_access를 선택
     - 시스템 이벤트 감사 로그의 경우 system_event를 선택
     - 정책 거부 감사 로그의 경우 정책을 선택
  2. **쿼리 실행**을 클릭합니다.

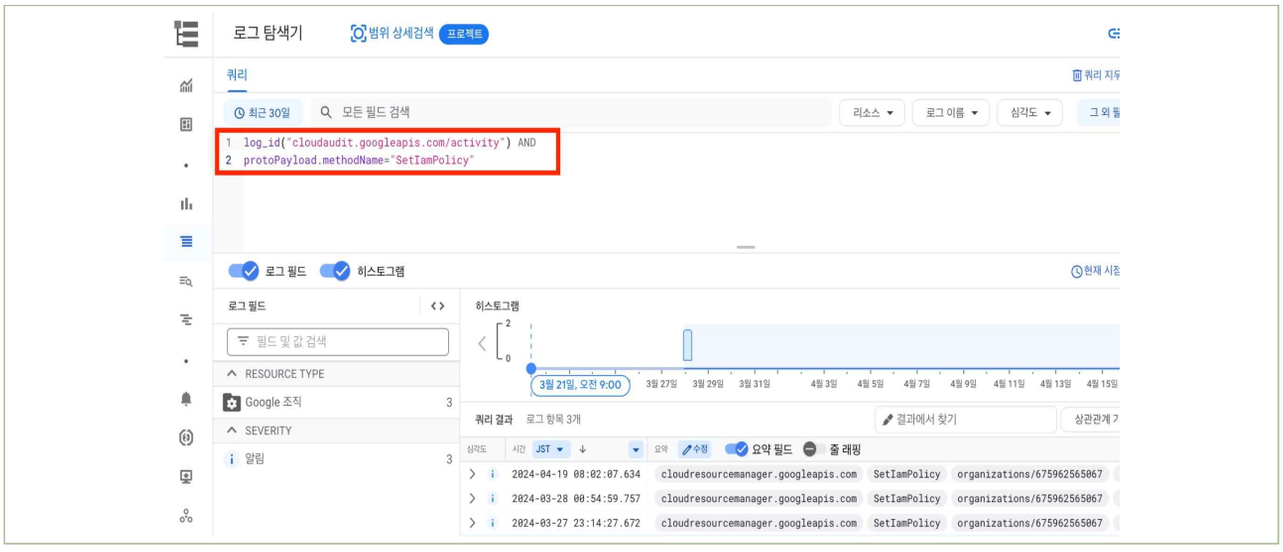


| 그림 5-6-1 | 로그 탐색기

- 로그 탐색기를 통해 계정에 부여된 역할 또는 권한의 변동에 대해 필터를 사용하여 로그 탐색기를 통해 모니터링하는 방법은 아래와 같습니다.

  - 로그탐색기 → 필터에서 아래 내용 추가후 쿼리실행

```
log_id("cloudaudit.googleapis.com/activity") AND
protoPayload.methodName="SetIamPolicy")
```



| 그림 5-6-2 | 로그 탐색기 쿼리 실행

4 참고 사항

- IAM 감사 로깅
  - IAM 감사 로깅 | IAM 문서
- Google 관리 콘솔(admin.google.com)에서 Google Cloud 서비스와 데이터 공유하기(로그 전달)
  - Google Cloud 서비스와 데이터 공유하기
- Identity and Access Management(IAM) 관련 샘플 쿼리
  - 샘플 쿼리 - Logging

1 기준

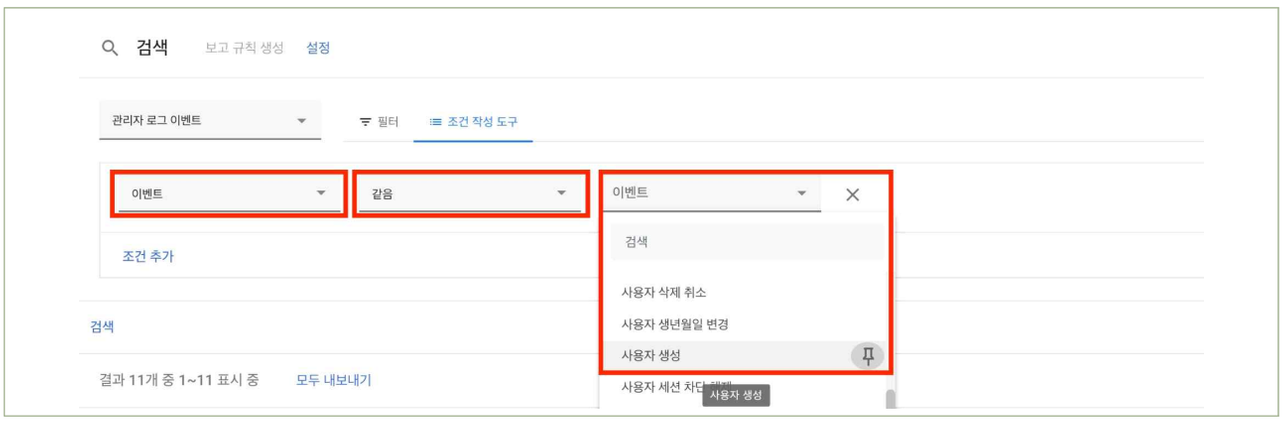
식별번호	기준	내용
5.7.	**계정 변경사항에 관한 모니터링 수행**	**클라우드 서비스 이용 계정 변경사항(생성, 삭제 등)에 관한 로깅 및 모니터링을 수행하여야 한다.**

2 설명

- 클라우드 서비스 이용 계정 변경사항에 관한 모니터링을 수행하여야 한다.
  - 계정 변경사항 관한 상시 모니터링은 1차적으로 Google 관리 콘솔(admin.google.com)에서 수행가능합니다.
  - Google 관리 콘솔(admin.google.com)에서 제공하는 로그 이벤트를 Google Cloud와 공유하면 Google Cloud의 로그 탐색기를 통해 전자금융감독규정 및 금융회사 내부규정 등에 수립된 주기에 맞추어 주기적 검토 수행할 수 있습니다.

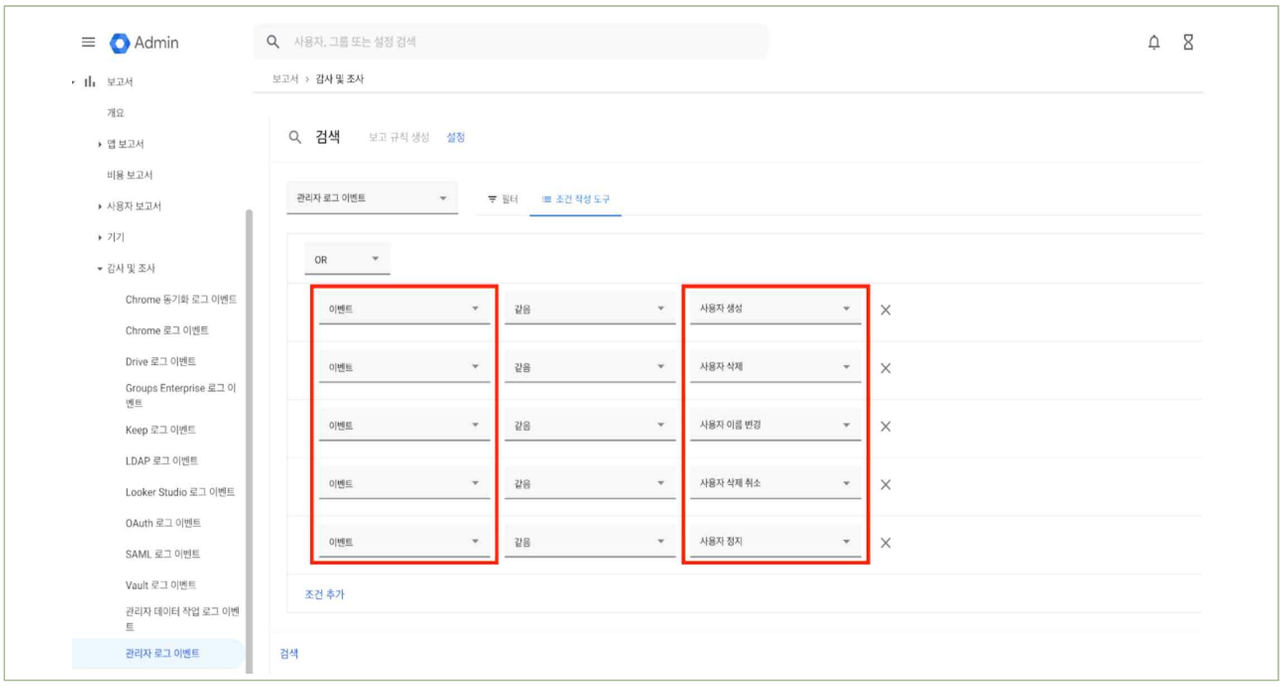
3 우수 사례

- 계정 생성, 삭제 등 계정 변경 사항은 Google 관리 콘솔(admin.google.com)에서 모니터링 가능
  - Google 관리 콘솔(admin.google.com) → 보고서 → 감사 및 조사 → 관리자 로그 이벤트
  - 조건추가 → '속성'에서 이벤트 선택 → '연산자 선택'에서 같음 선택 → '이벤트'에서 사용자 설정 하위에 있는 사용자 생성, 사용자 삭제 등을 선택



| 그림 5-7-1 | Google 관리 콘솔(admin.google.com)에서 모니터링

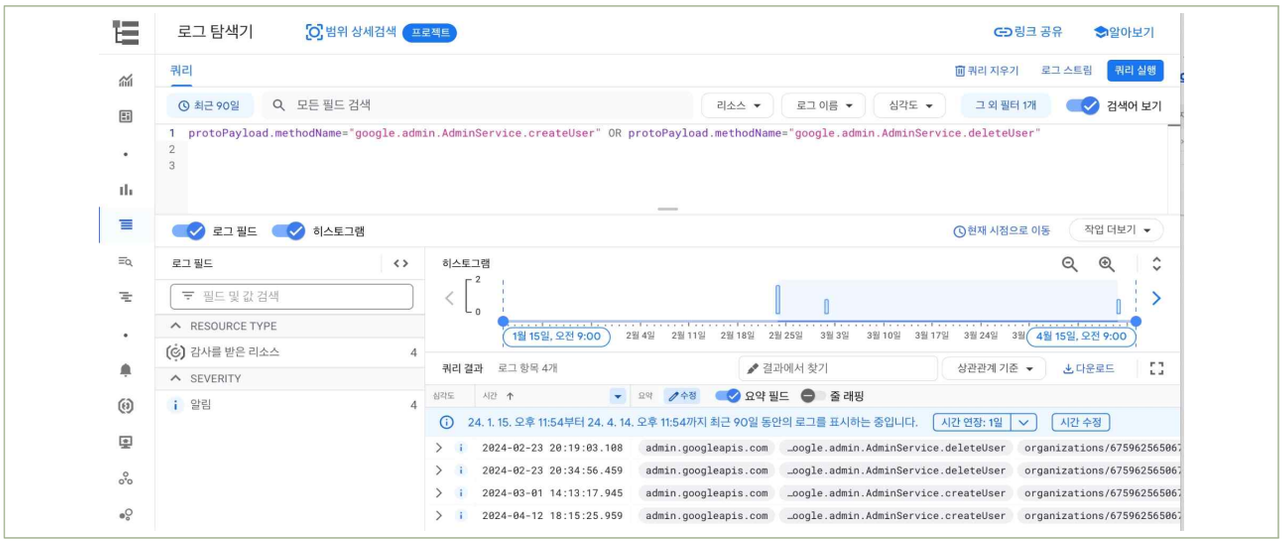
- 필요시 조건 추가하여 모니터링 할 이벤트를 추가(OR 조건으로 추가시 한번에 모니터링 가능)하고 검색 클릭



| 그림 5-7-2 | 모니터링 할 이벤트를 추가

- Google 관리 콘솔(admin.google.com)에서 제공하는 로그 이벤트를 Google Cloud와 공유하면 로그 탐색기를 통해 계정 생성, 삭제 등을 모니터링 할 수 있습니다.
  - 공유 방법은 참고사항의 링크를 참고하시기 바랍니다.
  - 로그탐색기 → 필터에서 아래 내용 추가 후 쿼리실행

```
protoPayload.methodName="google.admin.AdminService.createUser" OR
protoPayload.methodName="google.admin.AdminService.deleteUser“
```



| 그림 5-7-3 | 로그 탐색기 통한 계정 관련 사항 모니터링

- 그 외 Google 관리 콘솔(admin.google.com)에서 제공하는 계정 중지, 삭제취소 등을 모두 검색하려면 아래의 필터를 사용하시기 바랍니다.

```
protoPayload.serviceName="admin.googleapis.com"
```

4 참고 사항

- IAM 감사 로깅
  - IAM 감사 로깅 | IAM 문서
- Google 관리 콘솔(admin.google.com)에서 제공하는 로그 이벤트를 Google Cloud와 공유
  - Google Cloud 서비스와 데이터 공유하기

6. API 관리

6.1. API 호출 시 인증 수단 적용
6.2. API 호출 시 무결성 검증
6.3. API 호출 시 인증키 보호대책 수립
6.4. API 이용 관련 유니크 값 유효기간 적용
6.5. API 호출 구간 암호화 저장

6 API 관리

1 기준

식별번호	기준	내용
6.1.	API 호출 시 인증 수단 적용	클라우드 가상자원 관리를 위한 API 를 안전하게 호출하기 위한 인증수단을 적용하여 보안성을 강화해야 한다.

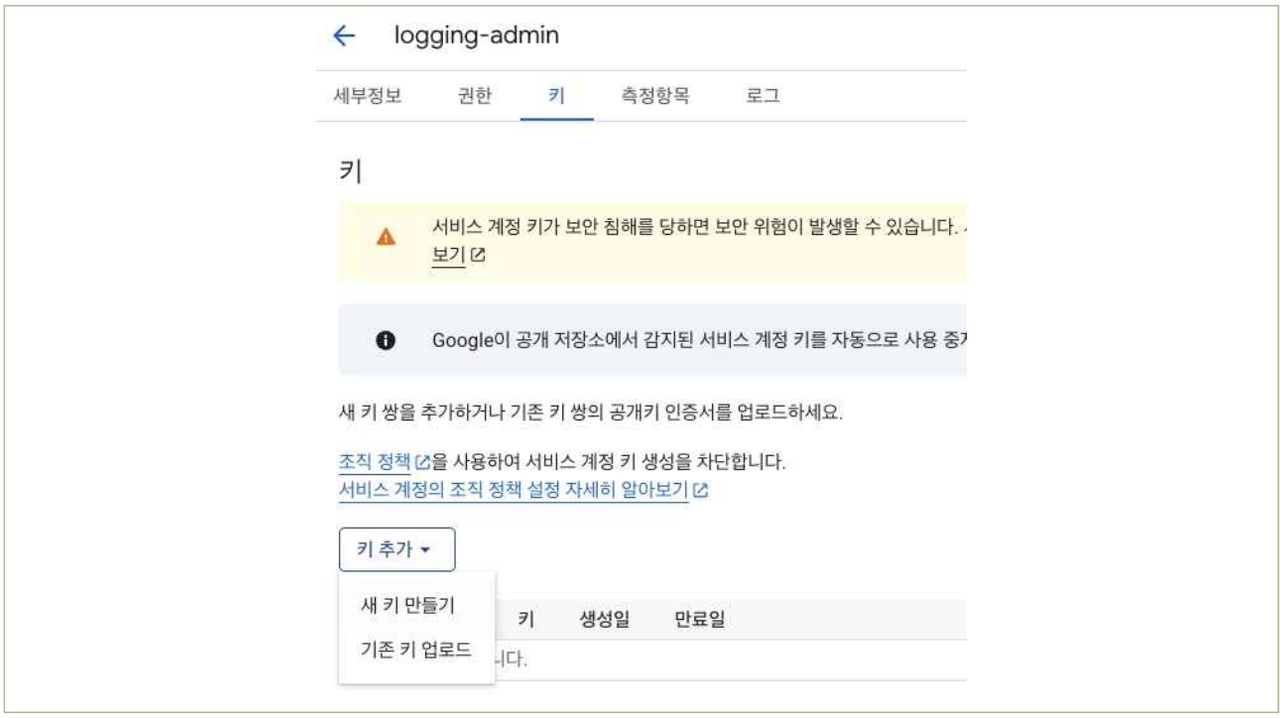
2 설명

- Google Cloud 외부에서 API를 호출하여 클라우드 자원을 사용하려면 반드시 인증을 거쳐야 합니다. Google Cloud는 다음 세 가지 방식으로 인증을 지원합니다.
  - Google Cloud 사용자 계정을 통한 인증
  - 서비스 계정 키를 이용한 인증
  - API 키를 이용한 인증

- API를 호출하는 경우는 프로그램 방식으로 접근하는 것이므로 서비스 계정 키와 API 키를 이용한 인증을 많이 사용하므로 두 가지 방식을 설명합니다.

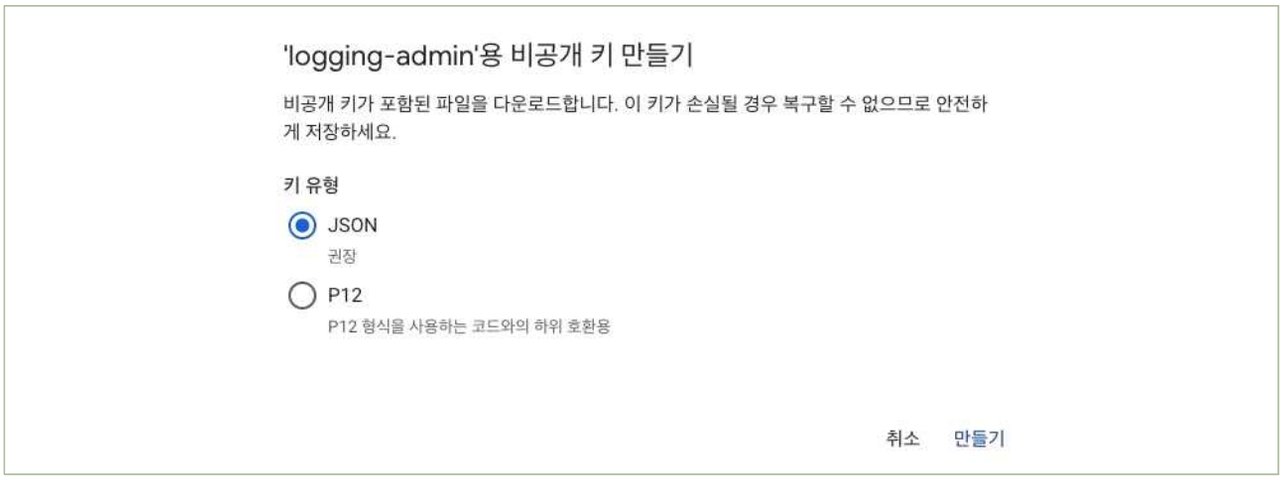
- **서비스 계정 키를 이용한 인증**
  - 서비스 계정 키는 암호화된 문자열로서 서비스계정에서 사용하는 인증방식입니다. 서비스 계정은 사용자가 아닌 프로그램 또는 클라우드 리소스가 사용하는 계정입니다. 이런 특성으로 서비스 계정에는 다중인증을 적용할 수 없습니다.
  - 서비스 계정은 Google Cloud가 관리하는 서비스 계정과 사용자가 관리하는 서비스 계정으로 구분합니다. Google Cloud가 관리하는 서비스 계정은 Google Cloud 내부에서만 사용이 가능합니다. 사용자 PC에서 Google Cloud API 호출을 하는 경우에 서비스 계정을 사용하며, 이때 사용자 관리 서비스 계정을 사용해야 합니다. 사용자 관리 서비스 계정 키는 Google Cloud 프로젝트에서 생성하고, 계정마다 최대 10개의 키를 생성할 수 있습니다.

- Google Cloud 웹 콘솔 -〉 IAM 및 관리자 -〉 서비스 계정 메뉴에서 계정을 선택하고 키 항목에서 그림과 같이 새 키 만들기를 선택합니다.



| 그림 6-1-1 | 서비스 계정 키 생성

- 이후 키 만들기 화면에서 JSON을 선택하고 만들기를 클릭하면 키 생성 후 사용자 컴퓨터에 자동으로 내려받기가 됩니다.

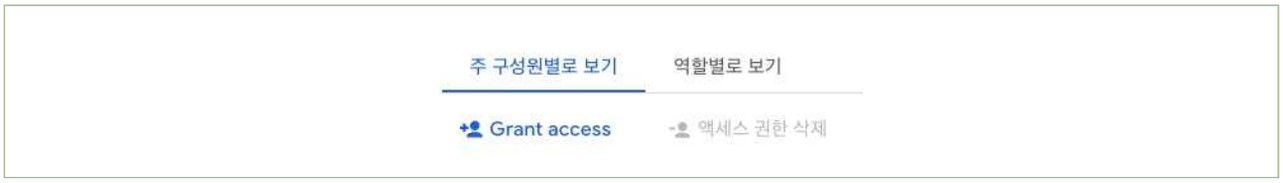


| 그림 6-1-2 | 서비스 계정 키 생성 형식 지정

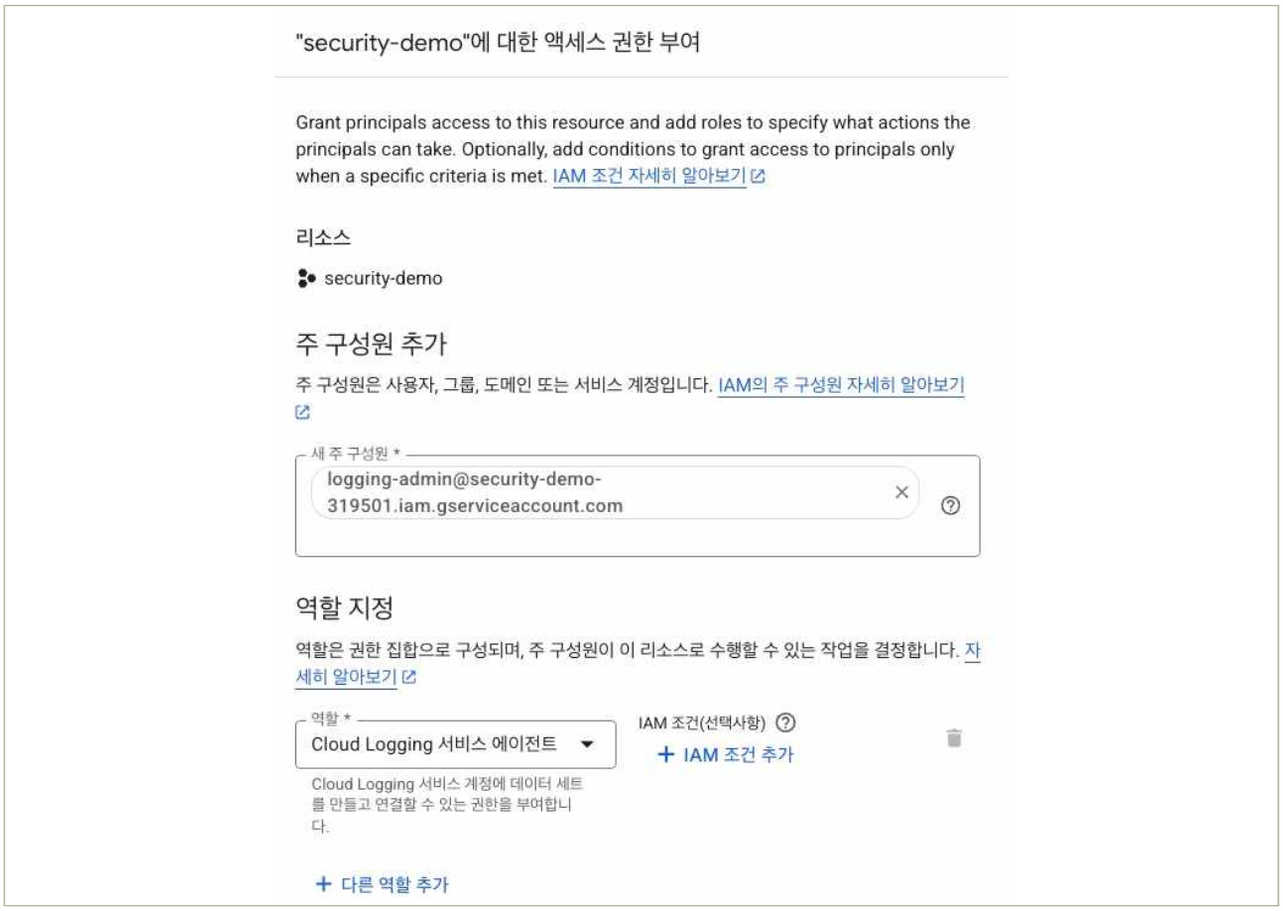
- 내려받은 키의 위치를 확인합니다. 인증이 필요한 컴퓨터에 서비스 계정키를 위치시키고 다음과 같이 환경 변수를 설정합니다.

GOOGLE_APPLICATION_CREDENTIALS = [내려받은 서비스 계정키 파일]

- 이후 프로그램을 실행시키면 해당 키를 이용하여 Google Cloud 인증이 자동으로 진행되고 IAM 권한에 따라 API를 호출할 수 있습니다.
- 서비스 계정은 일반 사용자 계정과 동일하게 취급합니다. 서비스 계정이 특정 역할을 수행하려면 Google Cloud에서 IAM에 등록하여 사용해야 합니다. 서비스 계정을 생성하고 IAM에서 서비스 계정에게 업무에 필요한 역할을 부여하지 않으면 인증이 성공하더라도 API 호출이 실패합니다. 그러므로 서비스 계정에게 최소한의 필요 권한을 IAM에서 할당해야 합니다.
- 웹 콘솔 -> IAM 및 관리자 -> IAM으로 이동합니다. Grant Access를 클릭하여 서비스 계정에게 필요한 역할을 부여할 수 있습니다.



| 그림 6-1-3 | IAM에 역할 추가 버튼



| 그림 6-1-4 | IAM에 계정 및 역할 추가하기

API 키를 이용한 인증

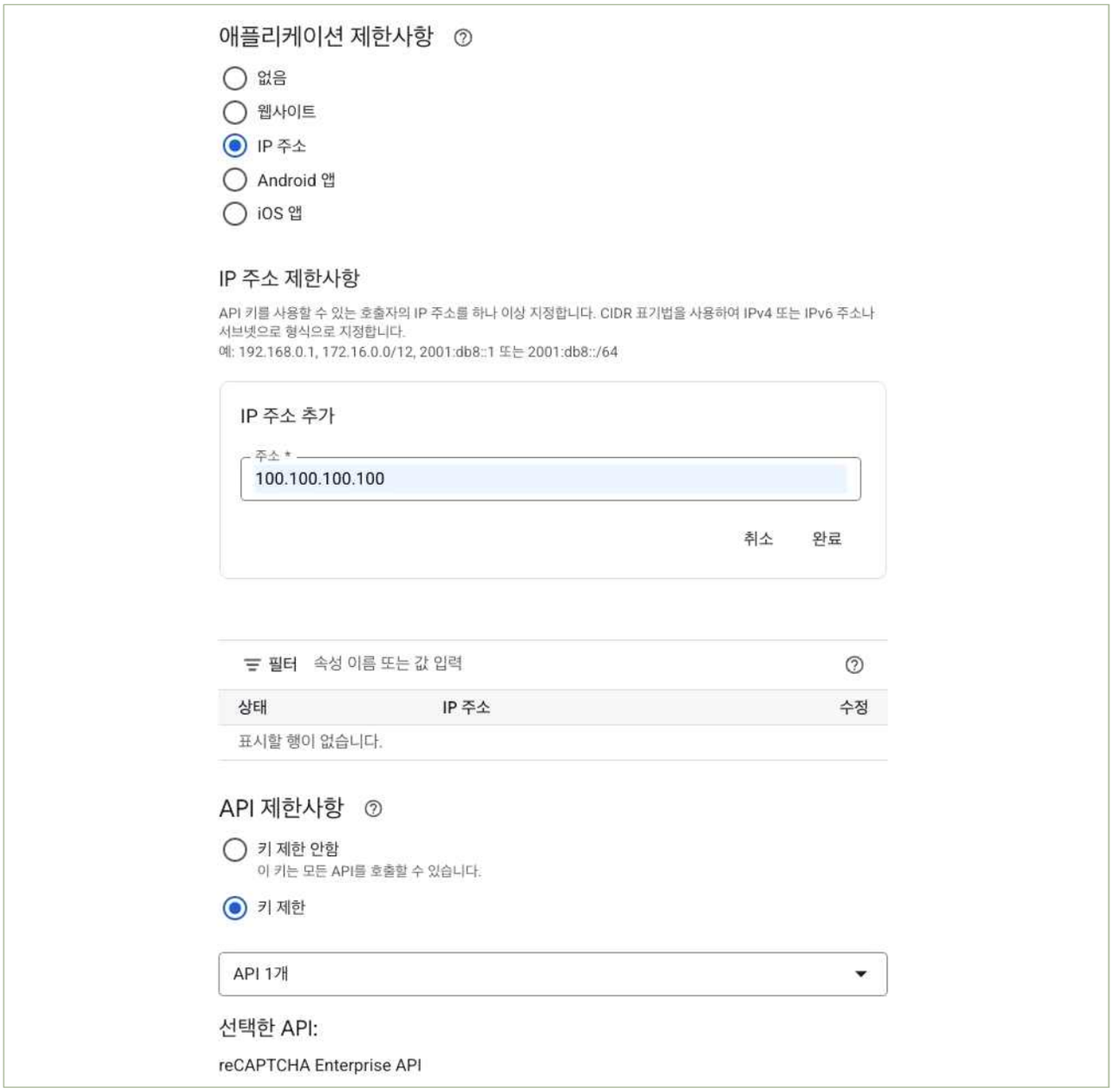
- API키는 특정 API를 호출할 수 있는 일종의 패스워드입니다. API를 호출할 때 API 키를 같이 전송하여 인증을 수행합니다. 다음은 API 키를 생성하는 절차입니다.
- Google Cloud 웹 콘솔 -〉 API 및 서비스 -〉 사용자 인증 정보 메뉴로 이동하여 사용자 인증 정보 만들기 -〉 API 키를 클릭하여 생성합니다. API 키를 생성하면 자동으로 키를 생성하고 생성 결과를 보여줍니다.

| 그림 6-1-5 | API 키 생성 완료

- 생성한 API키는 처음에는 아무런 제약이 없습니다. 그러므로 키 사용 대상 및 권한을 제한하도록 반드시 다음과 같은 설정절차를 완료해야 합니다.
- 애플리케이션 제한사항은 총 네 가지 항목입니다.
  - 웹사이트 - 특정 웹사이트에서만 API를 호출하도록 설정합니다.
  - IP 주소 - 특정 IP 대역에서만 호출이 가능하도록 설정합니다.
  - Android 앱 - 안드로이드 앱 패키지 이름과 SHA-1 인증서 지문을 추가하여 해당 API 사용을 안드로이드 앱으로 제한합니다.
  - iOS 앱 - 각 앱의 번들 ID를 추가하여 iOS 앱에서만 API를 호출할 수 있게 합니다.

API 제한 사항

- 제한사항은 해당 키로 호출할 수 있는 API를 지정하는 것입니다. 기본적으로 생성한 키는 모든 API를 호출할 수 있습니다. 만일 해당 API 키가 유출된 경우 모든 API를 호출하는 위험이 존재합니다. 그러므로 필요한 API만을 호출하도록 제한을 해야 합니다.
- 예시 그림에서는 IP가 100.100.100.100인 출발지에서 reCAPTCHA Enterprise API만을 호출할 수 있도록 키 제한을 설정하였습니다.



| 그림 6-1-6 | API 키 보안 설정

3 우수 사례

- 서비스 계정 키는 유출시 보안 위험을 초래할 수 있습니다. 특히 서비스 계정키에 많은 권한을 부여하면 유출시 더 큰 피해가 발생할 수 있습니다. Google Cloud에서 서비스 계정키는 아래와 같은 사용을 지켜야 합니다.
  - 서비스 계정을 리소스로 관리합니다.
    - 서비스 계정을 이용하여 직접 인증하지 않고 필요한 계정이 서비스 계정을 한시적으로 사용할 수 있도록 설정합니다.

- 단일 목적 서비스 계정을 만듭니다.
  - 서비스 계정 하나로 다수의 서비스를 실행시키지 않아야 합니다. 특정 목적에 맞는 서비스 계정을 생성하고 필요한 권한만 부여해서 최소 권한으로 서비스 계정을 동작시켜야 합니다.
- 이름 지정 및 문서 규칙을 따르세요.
  - 서비스 계정에 고유의 이름 규칙을 만들어서 해당 서비스 계정을 목적을 쉽게 식별할 수 있어야 합니다.
- 사용하지 않는 서비스 계정을 식별하고 사용 중지합니다.
  - 서비스 계정은 프로그램이 사용하므로 일반적으로 자동으로 중지하지 않습니다. 사용자는 서비스 계정 사용 현황을 파악해서 사용중지를 해야 합니다.
- 사용하지 않는 서비스 계정을 삭제하기 전에 사용 중지합니다.
  - 서비스 계정은 프로그램이 사용하는 계정이므로 함부로 삭제하는 경우 프로그램이 오동작할 수 있습니다. 그러므로 삭제하기 전에 중지를 시켜서 영향을 파악해야 합니다. 이후 중지 이후에도 별다른 영향이 없다면 삭제하면 됩니다.

4 참고 사항

- 위 내용에 대한 좀 더 자세한 정보는 아래에 링크에서 확인하실 수 있습니다.
  - https://cloud.google.com/docs/authentication?hl=ko
  - https://cloud.google.com/iam/docs/best-practices-service-accounts?hl=ko
  - https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts?hl=ko

1 기준

식별번호	기준	내용
6.2.	API 호출 시 무결성 검증	클라우드 가상자원 관리를 위한 API 호출 시 무결성을 보장하여야 한다.

2 설명

- Google Cloud는 API 호출과정에서 데이터의 손실, 유출 등을 방지하기 위해서 모든 전송구간 통신에 암호화를 필수로 적용합니다. 모든 API 호출은 반드시 HTTPS를 사용해서 호출해야 합니다.
  - Google Cloud에서 제공하는 클라이언트 라이브러리를 사용하여 호출하는 경우 전송 중인 데이터 암호화가 라이브러리에서 자동으로 처리됩니다.
  - 자체 gRPC 클라이언트를 사용하는 경우 gRPC 인증 가이드의 안내에 따라 Google에 인증해야 합니다. 이때 TLS 통신은 필수입니다.

3 우수 사례

- Google Cloud의 API 호출시 HTTPS 통신은 기본 기능이라서 별도의 설정이 존재하지 않습니다. 소스코드, curl과 같은 도구를 이용하여 호출하는 경우 사용하는 API 도메인 주소를 사용하면 됩니다. 예를 들어 클라우드 스토리지에 접속하고자 하는 경우 다음 예제와 같이 도메인 앞에 https://를 붙여서 https://storage.googleapis.com를 호출하면 됩니다.

4 참고 사항

- 위 내용에 대한 좀 더 자세한 정보는 아래에 링크에서 확인하실 수 있습니다.
  - https://cloud.google.com/security/encryption-in-transit?hl=ko

1 기준

식별번호	기준	내용
6.3.	**API 호출 시 인증키 보호대책 수립**	**API 호출 시 인용되는 유니크 값(ex. 보안키 등)은 안전하게 보관 및 관리하여야 한다.**

2 설명

- 기업에서 사용하는 API 키 또는 보안 키는 외부에 노출되지 않도록 보안을 철저하게 관리해야 합니다. 이러한 키가 클라우드 내부에 위치하는 경우 키를 안전하게 보관하는 서비스를 사용하여 키 값을 소스코드에서 직접 사용하지 못하게 합니다.

- Google Cloud는 API 키 또는 보안 키의 안전한 보관을 위해 Secret Manager 서비스를 제공합니다. Secret Manager는 데이터베이스, 저장소 등에 접근하는 인증 정보를 안전하게 보관하는 보안 저장소입니다.

- API 키, 보안키가 사용자 영역에 존재한다면 클라우드 서비스가 아닌 자체적으로 비밀 관리 프로그램을 사용해야 합니다. Secret Manager 역시 클라우드 서비스이므로 이를 접속하기 위한 인증이 추가로 필요하기 때문입니다. 만일 사용자 프로그램이 Google Cloud에서 동작하고 외부 API를 호출하는 경우라면 Secret Manager를 사용할 수 있습니다.

3 우수 사례

1. Google Cloud 웹 콘솔 -> 보안 -> Secret Manager 메뉴로 이동합니다.
2. 보안 비밀 만들기를 선택하여 새로운 보안 비밀을 생성합니다.
   a. 보안 비밀값이 포함된 파일을 업로드하거나 사용자가 직접 입력할 수 있습니다.
   b. 타 클라우드 또는 온프레미스 접속용 API 키 파일을 업로드할 수 있습니다.
3. 보안 비밀의 순환 주기, 만료일을 추가로 설정할 수 있습니다.

| 그림 6-3-1 | 보안 비밀 설정

- 보안 비밀을 생성한 이후에는 해당 보안 비밀값 대신 보안 비밀 이름을 사용합니다. 프로그램 소스 코드에서는 객체 이름을 이용하여 보안 비밀값을 사용합니다. 공격자에게 소스 코드가 탈취되더라도 코드에는 객체 이름만 있어 보안 비밀값을 안전하게 지킬 수 있습니다.

4 참고 사항

- 위 내용에 대한 좀 더 자세한 정보는 아래에 링크에서 확인하실 수 있습니다.
  - https://cloud.google.com/secret-manager/docs/overview?hl=ko

1 기준

식별번호	기준	내용
6.4.	**API 이용관련 유니크값 유효기간 적용**	**클라우드 가상자원 관리를 위해 API 기능 이용시, 세션 유효기간 및 유니크값(보안키 등)에 대한 만료기간을 설정하여야 한다.**

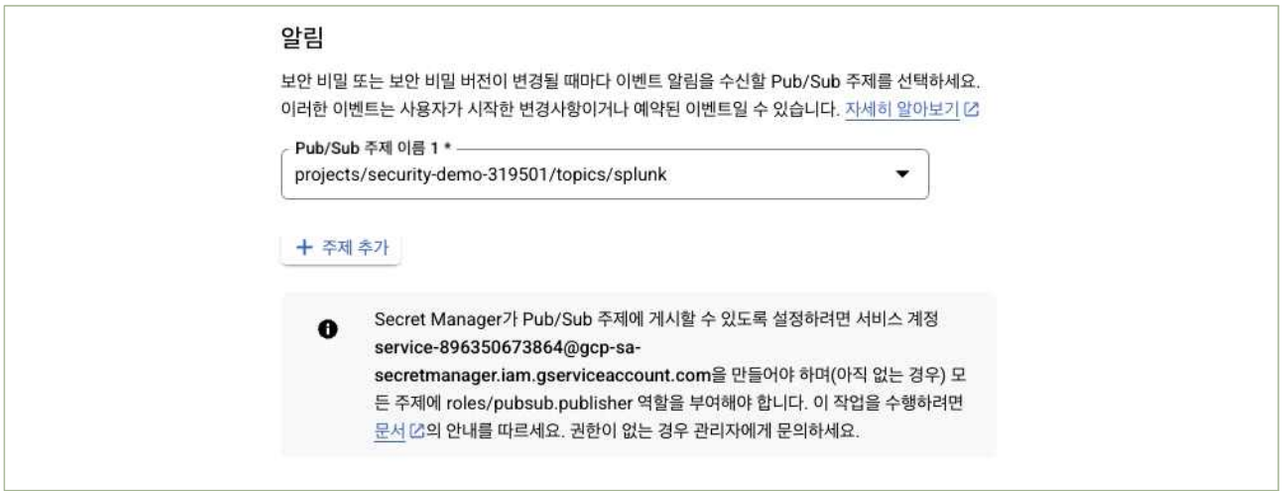
2 설명

- API 세션 및 서명값에 대한 유효기간 설정하고, 유니크값(보안키 등)유출 방지 대책으로 만료기간을 적용하여야 한다.
  - Google Cloud API 키는 만료기간 설정을 지원하지 않습니다. 또한 사용자별 권한 통제를 제어할 수 없습니다. 그러므로 API 키 사용을 최대한 자제하는 것이 보안상 좋습니다.
  - API 키가 만료 기간을 지원하지 않지만 보안 비밀 관리자(Secret Manager)에 저장하여 만료일을 설정할 수 있습니다.
  - Google Cloud 웹 콘솔 -〉 Secret Manager -〉 보안 비밀 만들기를 선택합니다.
  - 생성 옵션에서 회전, 알림과 만료일을 설정합니다. 회전은 보안 비밀(API 키값)을 새 값으로 변경하는 것을 의미하며 만료일은 해당 객체의 만료일을 지정하는 것입니다. 알림은 이러한 행위를 관리자에게 통보하도록 설정하는 것입니다.
  - 보안 비밀의 회전은 아래 그림과 같이 설정합니다.

| 그림 6-4-1 | 보안 비밀 순환주기 설정

  - 순환주기는 30일, 90일, 맞춤 설정 등의 옵션이 있습니다. 클라우드 관리자가 필요한 값을 설정합니다. 순환 주기를 설정했다면 알림 역시 설정하여 순환 주기 도래를 관리자에게 통보해야

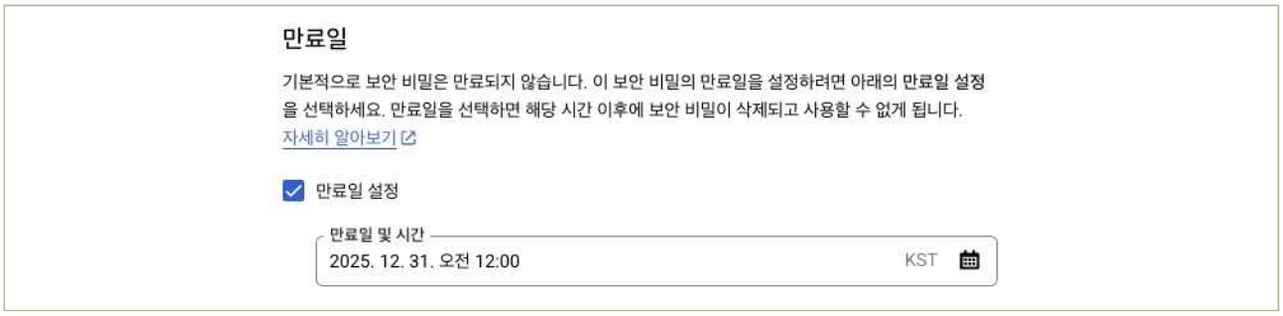
합니다. 보안비밀 값은 자동으로 생성 및 변경되지 않습니다. 그러므로 지정된 일자에 관리자에게 순환하도록 통보하는 기능을 알림에서 제공하고 있습니다.



| 그림 6-4-2 | 알림 설정

- 보안 비밀 관련 이벤트가 발생할 때마다 지정한 Pub/Sub 주제로 해당 이벤트를 전송합니다. 보안 비밀 업무를 수행하는 서비스 계정에게 지정한 Pub/Sub 주제에 이벤트를 게시할 권한을 부여해야 합니다.

만료일 설정



| 그림 6-4-3 | 만료일 설정

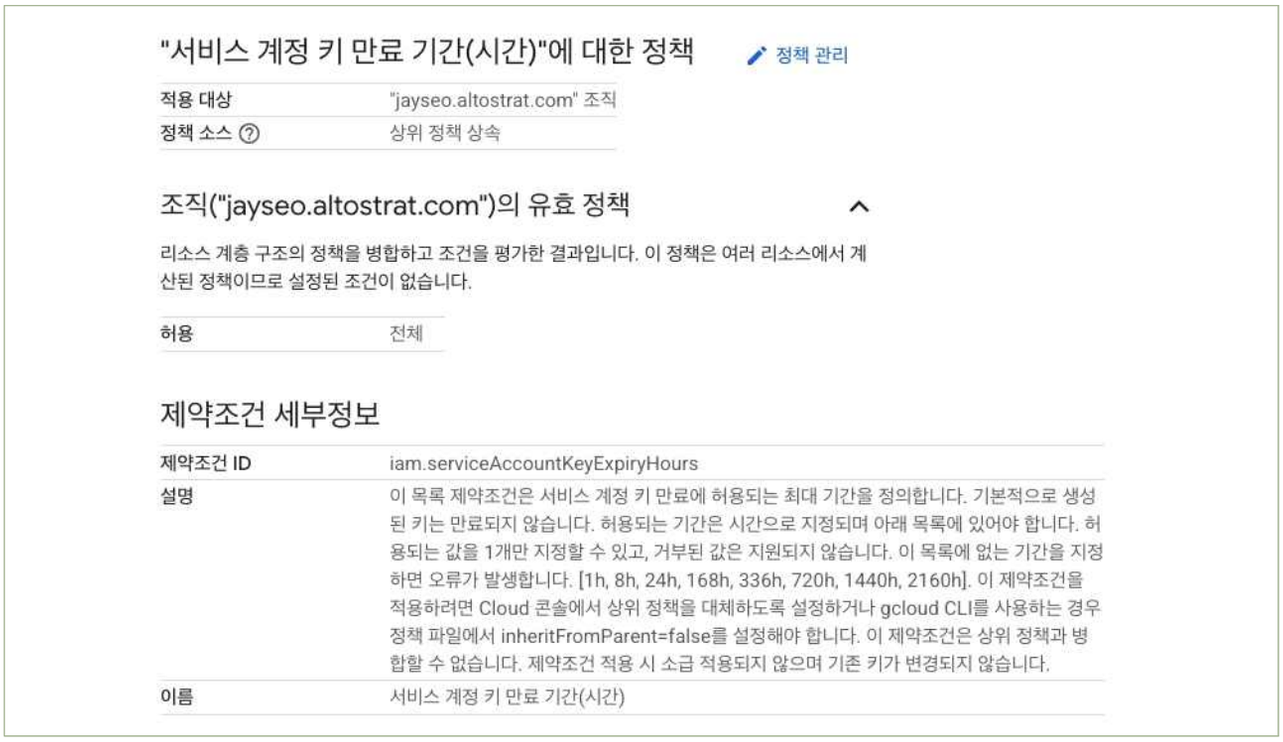
- 만료일을 설정하면 해당 보안비밀에 저장된 API 키 및 서비스 계정키는 더 이상 사용할 수 없습니다. 자동화 업무에 API 키와 서비스 계정 키를 연결했다면 만료일 이후 해당 업무가 정상 동작하지 않을 수 있으니 관리자는 만료일 설정에 주의하셔야 합니다.

서비스 계정 키 만료일 지정

- 서비스 계정키는 만료일을 지정할 수 있습니다. 개별적으로 설정하는 것이 아니라 클라우드를 사용하는 모든 사용자에게 조직 정책으로 강제화시킬 수 있습니다. Google Cloud에서는 조직 정책(Organization Policies)에서 이 항목을 설정할 수 있습니다. 이 정책을 수정하려면 Google

Cloud 조직 수준에서 조직 정책 관리자 역할을 가지고 있어야 합니다.

- Google Cloud 웹 콘솔 -> IAM 및 관리자 -> 조직 정책으로 이동합니다. 정책 목록에서 서비스 계정 키 만료 기간(시간) iam-serviceAccountKeyExpiryHours를 선택합니다. 다음 화면을 볼 수 있습니다.

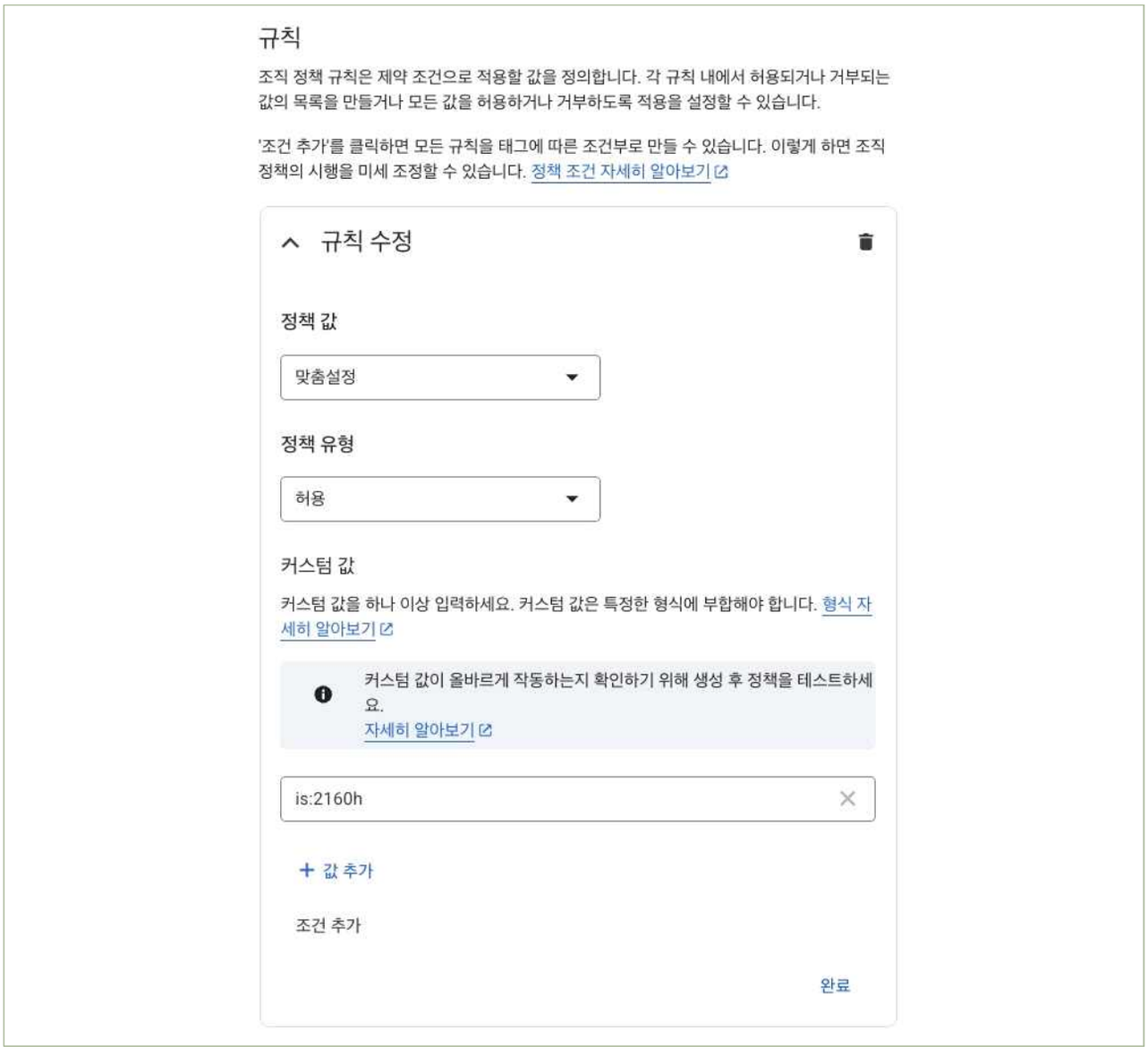


| 그림 6-4-4 | 서비스 계정키 만료 시간 설정 화면

- 현재 화면은 정책을 적용하지 않은 상태이며 이 정책에서는 서비스 계정키를 생성할 때 만료일을 지정하지 않습니다. 화면 우측 상단의 정책 관리를 클릭합니다. 이 정책을 수정하려면 조직 정책 관리자 역할을 보유하고 있어야 합니다.

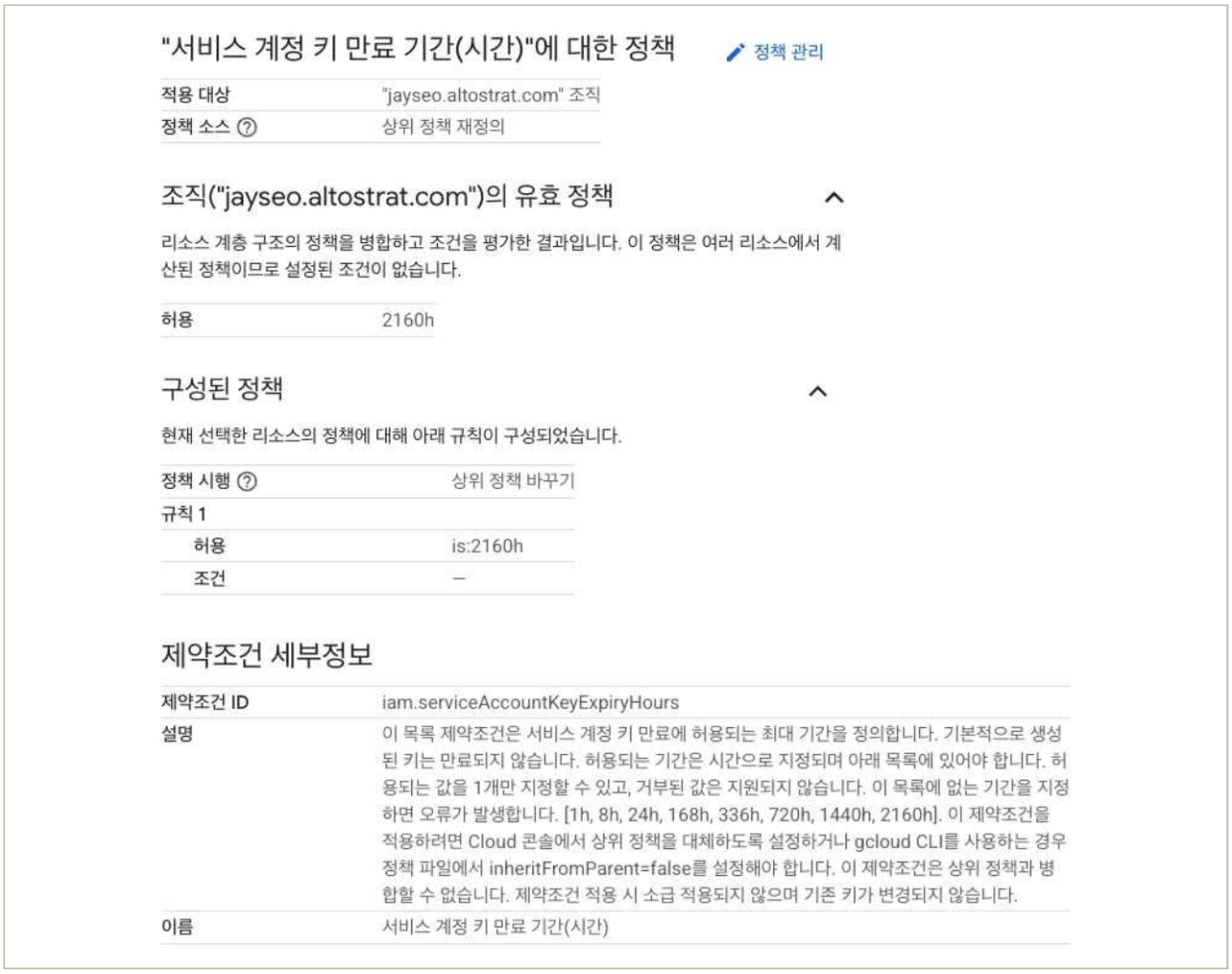
| 그림 6-4-5 | 정책 기본값 설정

- 만료일을 지정하는 것은 기존의 값을 덮어쓰는 개념이므로 상위정책 재정의, 바꾸기로 각각 선택합니다.
- 규칙 설정은 그림 6-5-6과 같이 설정한다. 만료일은 일이 아닌 시간으로 계산하여 값을 입력한다. 예제에서는 만료시간을 2160h 즉, 2160 시간이며 이는 약 90일의 기간입니다.
- 커스텀 값은 is:2160h로 입력하고 반드시 완료 버튼을 클릭해야 해당 값이 규칙에 반영됩니다.



| 그림 6-4-6 | 규칙 설정

- 모든 설정을 완료한 후 정책설정을 클릭하여 다음 화면이 보이는지 확인합니다.



| 그림 6-4-7 | 서비스 계정 만료일 정책 완료

- 서비스 계정키의 만료일은 조직 정책을 설정한 이후에 생성하는 서비스 계정키에만 적용됩니다. 그러므로 해당 정책을 클라우드 환경 초기에 설정하여 모든 서비스 계정키가 만료일에 영향을 받게 설정해야 합니다.

3 우수 사례

- API 키 및 서비스 계정키는 클라우드 외부에서 클라우드 자원을 호출할 때 필요한 인증수단입니다. 애플리케이션이 클라우드 내에서 동작하는 경우 두 인증수단을 사용할 필요가 없습니다. 그러므로 사용자 애플리케이션을 클라우드에서 직접 동작하는 것이 보안상 가장 좋은 방법입니다.
  애플리케이션을 클라우드에서 동작하지 못하는 경우는 API 키 또는 서비스 계정키를 이용해서 클라우드 자원을 사용합니다. 두 방법 각각은 다른 보안 설정을 지원합니다.

  - Google Cloud의 API 키는 만료일 설정이 없습니다. 그러므로 Secret Manager와 같은 보안비밀

관리자에 API 키를 저장하여 만료일, 순환 주기를 설정해야 합니다.

- APIKI에 호출 주소, 호출 가능 프로그램, 대상 API 제한 등을 설정하여 키 사용을 제한해야 합니다.
- 서비스 계정키는 조직 정책에서 만료일을 지정하여 조직 내 모든 서비스 계정에 적용시켜야 합니다.
- 서비스 계정은 IAM에서 꼭 필요한 역할만 부여하여 과도한 권한 사용을 방지해야 합니다.
- 조직 정책에서 반드시 서비스 계정 키 노출 응답을 그림 6-5-8과 같이 설정합니다.

| 그림 6-4-8 | 서비스 계정 키 노출 응답 설정

- is:DISABLE_KEY는 외부에 키가 노출되는 경우 Google Cloud가 자동으로 이를 탐지해서 키를 즉시 만료시킵니다. 서비스 계정키는 개발과정에서 노출되는 경우가 많으므로 이 정책을 이용하여 발생 가능한 사고를 예방하는 것이 좋습니다.

4 참고 사항

- 위 내용에 대한 좀 더 자세한 정보는 아래에 링크에서 확인하실 수 있습니다.
  - API 키 관리 권장사항: https://cloud.google.com/docs/authentication/api-keys-best-practices?hl=ko
  - 서비스 계정 사용 권장사항: https://cloud.google.com/iam/docs/best-practices-service-accounts?hl=ko

1 기준

식별번호	기준	내용
6.5.	API 호출 구간 암호화 적용	**클라우드 가상자원 관리를 위한 API 호출 시 암호화된 통신구간을 적용하여야 한다.**

2 설명

- API를 통한 클라우드 가상자원 관리 수행 시 네트워크 트래픽 보호를 위한 암호화된 통신구간을 적용하여야 한다.(또는 확인하여야 한다.)
  - Google은 모든 전송 구간에 암호화 통신을 강제 적용하고 있습니다. 사용자가 HTTP로 접속하더라도 강제로 HTTPS로 전환하여 암호통신을 수행합니다.

3 우수 사례

- Google Cloud의 API 호출시 HTTPS 통신은 기본 기능이라서 별도의 설정이 존재하지 않습니다. 소스코드, curl과 같은 도구를 이용하여 호출하는 경우 사용하는 API 도메인 주소를 사용하면 됩니다. 예를 들어 클라우드 스토리지에 접속하고자 하는 경우 다음 예제와 같이 도메인 앞에 https://를 붙여서 https://storage.googleapis.com를 호출하면 됩니다.

4 참고 사항

- 위 내용에 대한 좀 더 자세한 정보는 아래에 링크에서 확인하실 수 있습니다.
  - https://cloud.google.com/security/encryption-in-transit?hl=ko

7. 스토리지 관리

7.1. 스토리지 접근 관리
7.2. 스토리지 권한 관리
7.3. 스토리지 업로드 파일 제한

7 스토리지 관리

1 기준

식별번호	기준	내용
7.1.	**스토리지 접근관리**	**스토리지 목적에 따라 외부 공개 차단 등 적절한 접근통제를 수행하여야 한다.**

2 설명

- Google Cloud Storage는 다양한 접근 통제 메커니즘을 제공하여 버킷과 객체에 대한 액세스를 세밀하게 관리할 수 있도록 지원합니다. 접근통제 목록(Access Control List)를 통한 방법과 특정 역할에 기반한 IAM 통제 방안이 있으며 사용자들에게 역할기반으로 접근 권한을 부여하는 균일한 버킷 수준 액세스를 적용하는 것이 바람직합니다.
  - IAM (Identity and Access Management): 프로젝트, 버킷, 폴더 수준에서 사용자 및 서비스 계정에 특정 역할(예: Storage 객체 뷰어, Storage 객체 생성자, Storage 관리자)을 부여하여 권한을 제어합니다. 이는 Cloud Storage 접근 통제의 기본이자 가장 권장되는 방식입니다.
  - ACL (Access Control Lists): 개별 객체 또는 버킷에 대한 접근 권한을 보다 세밀하게 제어할 때 사용합니다. IAM과 함께 사용될 수 있지만, 단순성을 위해 균일한 버킷 수준 액세스를 사용하는 것이 좋습니다. 균일한 버킷 수준 액세스를 활성화하면 ACL이 비활성화되고 IAM 권한만 적용됩니다.
  - 공개 액세스 방지 (Public Access Prevention): 이 기능은 버킷과 객체가 실수로 인터넷에 공개되는 것을 방지합니다. 활성화되면 allUsers 또는 allAuthenticatedUsers를 통한 접근이 차단됩니다. 이는 민감한 데이터를 보호하는 데 매우 효과적입니다.

- 그림 7-1-1은 스토리지 버킷 생성 시 버킷에 적용하는 객체 액세스를 제어하는 방식을 선택하는 화면입니다. 인터넷에서 접속하는 것을 방지하기 위해서 “이 버킷에 공개 액세스 방지 적용”이 기본적으로 설정되어 있습니다. 만일 해당 버킷을 인터넷에서 접속이 가능한 버킷으로 만들려면 이 선택을 해제하면 됩니다.

| 그림 7-1-1 | 스토리지에서 객체 엑세스를 제어하는 방식 선택

3 우수 사례

- Google Cloud의 스토리지는 인터넷 접속이 기본적으로 차단합니다.
- 스토리지 버킷에 allUsers 구성원을 추가하면 인터넷 접속이 허용됩니다. allUsers구성원을 허용하기 이전에 반드시 인터넷 공개가 필요한지 확인해야 합니다.

| 그림 7-1-2 | 인터넷 공개 설정 주의

4 참고 사항

- 위 내용에 대한 좀 더 자세한 정보는 아래에 링크에서 확인하실 수 있습니다.
  - 공개 액세스 방지 사용: https://cloud.google.com/storage/docs/using-public-access-prevention?hl=ko

1 기준

식별번호	기준	내용
7.2.	**스토리지 권한 관리**	**스토리지 목적에 따라 읽기, 쓰기 등의 권한을 관리하여야 한다.**

2 설명

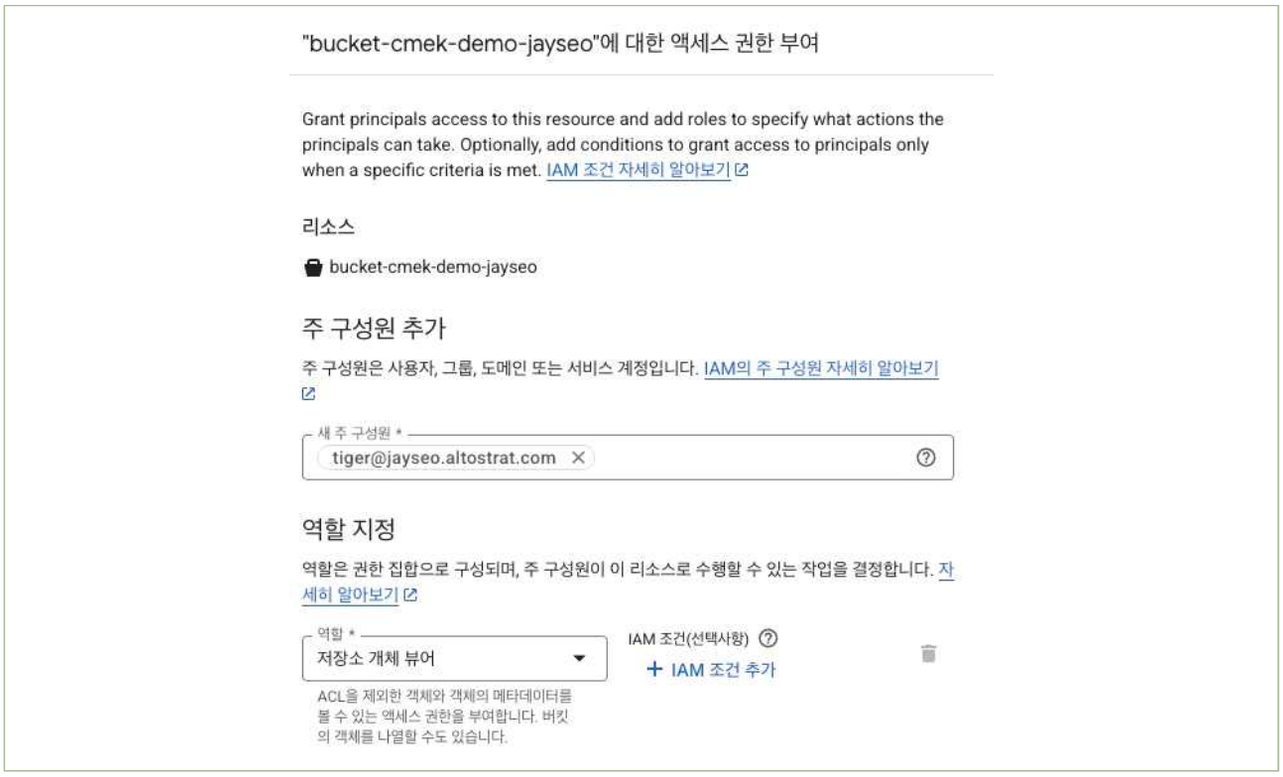
- Google Cloud는 스토리지 버킷에 균일한 액세스 제어를 이용해서 사용자 계정별 접근 권한을 통제할 수 있습니다. 버킷 생성 후 사용자별 권한을 부여하는 방법은 다음과 같습니다.
  - Google Cloud 웹콘솔 -〉 Cloud Storage -〉 버킷으로 이동합니다.
  - 권한을 설정할 버킷을 선택하면 상단에 권한 버튼이 활성화됩니다.

| 그림 7-2-1 | 권한 부여 대상 버킷 선택

  - 버킷을 선택한 후 권한 버튼을 클릭하면 사용자에게 권한을 추가할 수 있는 정보창이 화면 우측에 나타납니다. 해당 정보창에서 사용자별 권한을 추가할 수 있습니다.

| 그림 7-2-2 | 버킷에 사용자 권한 추가하기

- 주 구성원을 추가를 클릭하면 IAM과 동일한 사용자 계정 및 권한 설정 화면이 나타납니다.



| 그림 7-2-3 |

- 사용자 또는 그룹에게 권한을 부여하고 저장 버튼을 클릭합니다.

3 우수 사례

- 클라우드 스토리지 접근통제는 다음과 같은 원칙으로 운영해야 합니다.
  - 최소 권한의 원칙: 사용자나 서비스 계정에는 업무 수행에 필요한 최소한의 권한만 부여합니다.
  - 균일한 버킷 수준 액세스 사용: 가능하면 균일한 버킷 수준 액세스를 사용하여 ACL 관리를 단순화하고 IAM을 통해 일관된 접근 통제를 적용합니다.
  - 공개 액세스 방지 적극 활용: 민감한 데이터를 저장하는 버킷에는 반드시 공개 액세스 방지 기능을 활성화합니다.
  - 정기적인 권한 검토: 주기적으로 IAM 정책과 ACL 설정을 검토하여 불필요하거나 과도한 권한이 부여되지 않았는지 확인합니다.
  - 로깅 및 모니터링: Cloud Audit Logs 및 Storage 사용 로그를 활용하여 접근 시도 및 변경

사항을 모니터링하고 의심스러운 활동을 감지합니다.

4 참고 사항

- 위 내용에 대한 좀 더 자세한 정보는 아래에 링크에서 확인하실 수 있습니다.
  - Cloud Storage IAM 부여 : https://cloud.google.com/storage/docs/access-control/iam-roles?hl=ko
  - Cloud Storage 접근제어: https://cloud.google.com/storage/docs/access-control?hl=ko

1 기준

식별번호	기준	내용
7.3.	**스토리지 업로드 파일 제한**	**스토리지 목적에 따른 확장자 파일만 업로드 될 수 있도록 업로드 가능 파일을 제한하여야 한다.**

2 설명

- Google Cloud는 파일 확장자 기반 업로드 제한 기능을 제공하지 않습니다.

3 우수 사례

4 참고 사항

8. 백업 및 이중화 관리

8.1. 클라우드 이용에 관한 행위추적성 증적(로그 등) 백업
8.2. 행위추적성 증적 (로그 등) 백업 파일 무결성 검증
8.3. 금융회사 전산자료 백업
8.4. 금융회사 전산자료 백업 파일 무결성 검증
8.5. 행위추적성 증적 전산자료 등 백업에 관한 기록 및 관리
8.6. 백업파일 원격 안전지역 보관
8.7. 주요 전산장비 이중화

8 백업 및 이중화 관리

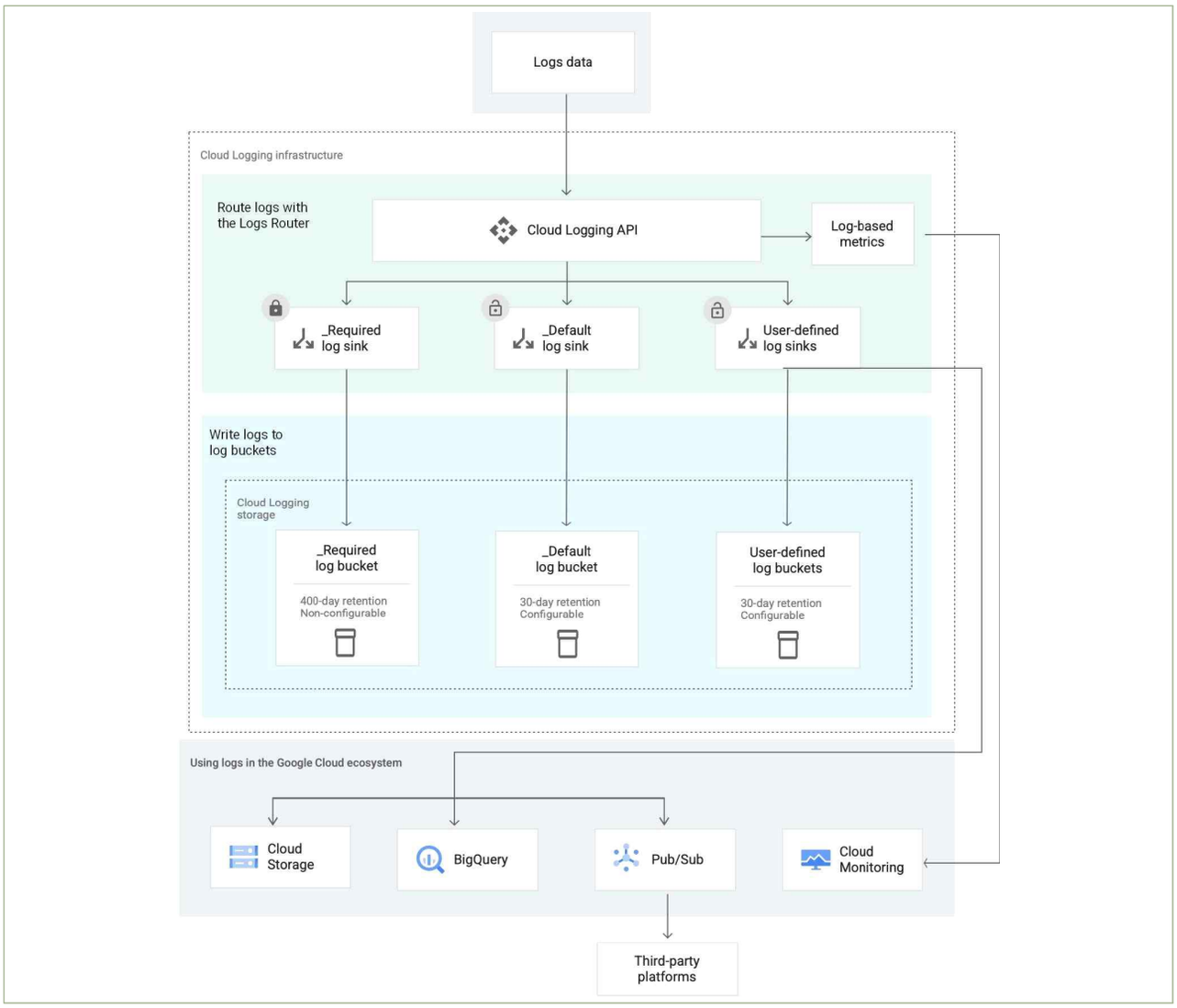
1 기준

식별번호	기준	내용
8.1.	**클라우드 이용에 관한 행위추적성 증적(로그 등) 백업**	**금융회사가 클라우드 이용 시 발생하는 다양한 행위추적성 증적(가상자원, API, 네트워크서비스, 스토리지 관리, 계정 및 권한관리 등)의 보관기간 확보 등을 위해 백업을 수행(1년이상 보관)하여야 한다.**

2 설명

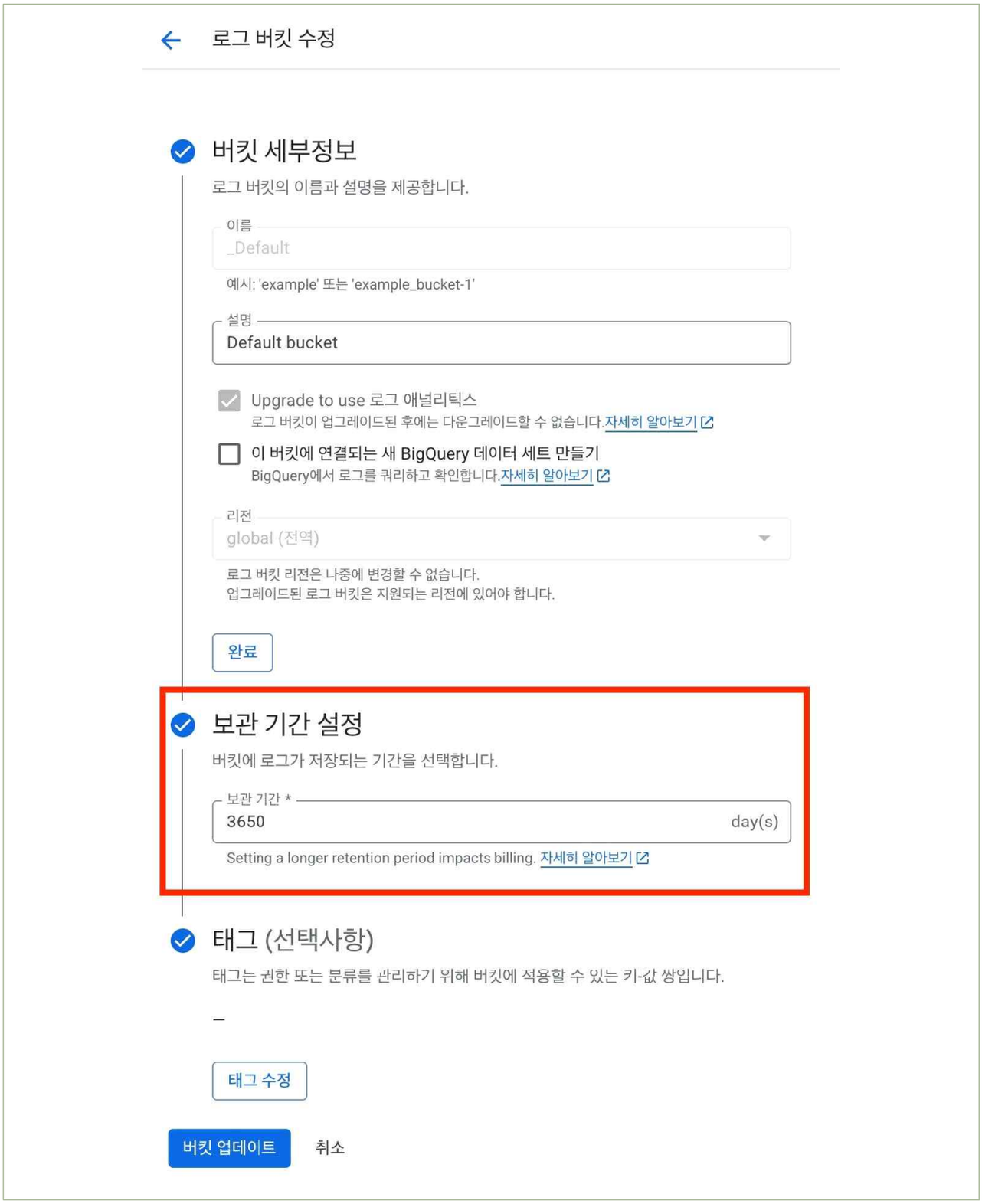
- 금융회사가 클라우드 이용 시 발생하는 다양한 행위추적성 증적에 대해 백업을 수행(1년이상 보관)하여야 한다.
  - 보관 규제 요건(1년 이상 보관)을 충족하며 효과적으로 로그를 관리하기 위해 다음 사항을 고려해야 합니다.
    - 로깅 범위 정의: 관련 규제 및 내부 정책에 따라 감사 로그가 필요한 Google Cloud 리소스 및 활동(예: VM 생성/삭제, IAM 정책 변경, 스토리지 객체 액세스 등)을 명확히 식별합니다.
    - 데이터 액세스 로그 활성화: 관리자 활동 로그는 기본적으로 활성화되어 있지만, 스토리지 객체 읽기/쓰기, BigQuery 쿼리 실행 등 민감한 작업에 대한 추적성을 확보하려면 해당 서비스에서 데이터 액세스 로그를 명시적으로 활성화해야 합니다. (비용 영향 검토 필요)
    - 로그버킷별 보유기간 설정: Cloud Logging 서비스는 다음 유형의 로그 항목을 _Required 버킷, _Default 버킷 및 사용자정의 버킷의 3종의 버킷으로 분류하여 저장합니다. 가장 기본적인 _Required 버킷은 다음 사항을 저장하며, _Required 버킷의 로그 항목을 400일 동안 보관합니다. 이 보관 기간은 변경할 수 없습니다.
      - (_Required 버킷 저장 항목) 관리 활동 감사 로그, 시스템 이벤트 감사 로그, Google Workspace 관리자 감사 로그, Enterprise 그룹스 감사 로그, 로그인 감사 로그
      - (_Default 버킷 및 사용자정의 버킷) 그 외의 로그 버킷은 기본 30일 동안 보관하며, 로그버킷 보관기간을 3,650일까지 연장하거나 또한 모든 로그 버킷에 대해 로그 싱크를 구성하여 그 이상 장기 보관할 수 있습니다.

- 로그 싱크 구성: Cloud Logging에서 로그 라우터 싱크를 설정하여 필요한 감사 로그를 장기 보관용 스토리지로 안전하게 라우팅합니다.
  - 대상: 비용 효율적인 장기 보관을 위해 Cloud Storage 버킷을 대상으로 지정하는 것이 일반적이며, 보안 강화를 위해 별도의 감사용 프로젝트에 Cloud Storage 버킷을 생성하는 것을 고려할 수 있습니다.
  - 필터링: 로그 싱크에서 제공하는 포함/제외 필터를 사용하여 필요한 로그만 정확하게 내보내도록 구성하여 스토리지 비용을 최적화하고 분석을 효과적으로 할 수 있습니다.
  - 형식: 일반적으로 로그는 JSON 형식으로 내보내집니다.



| 그림 8-1-1 | 로그 라우팅 및 스토리지

- 보관 정책 설정 및 적용
  - Cloud Storage: 객체 수명 주기 관리 규칙을 설정하여 일정 기간(예: 1년) 후 로그 파일을 자동으로 저렴한 스토리지 클래스(Archive 등)로 이동시키거나, 보관 기간 만료 후 삭제하도록 구성합니다. 금융 규제상 로그의 불변성이 요구될 경우, Cloud Storage 버킷 잠금 기능을 사용하여 지정된 기간 동안 로그 파일의 삭제 및 수정을 방지합니다. (Cloud Storage 보관 정책 설정 및 적용은 8.2 참조)
  - Cloud Logging 버킷: 필요한 경우 Cloud Logging 자체의 커스텀 보관 기간 설정을 활용할 수도 있습니다 (최대 3650일).

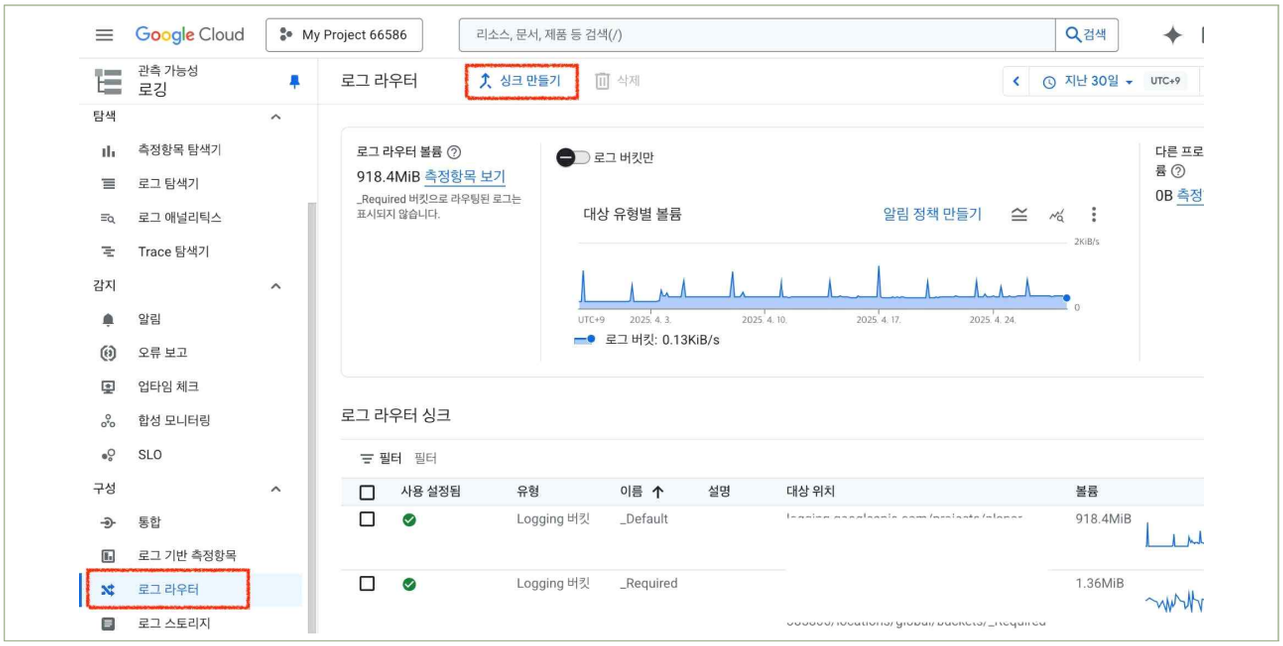


| 그림 8-1-2 | 로그 버킷 보관 기간 커스텀 설정

3 우수 사례

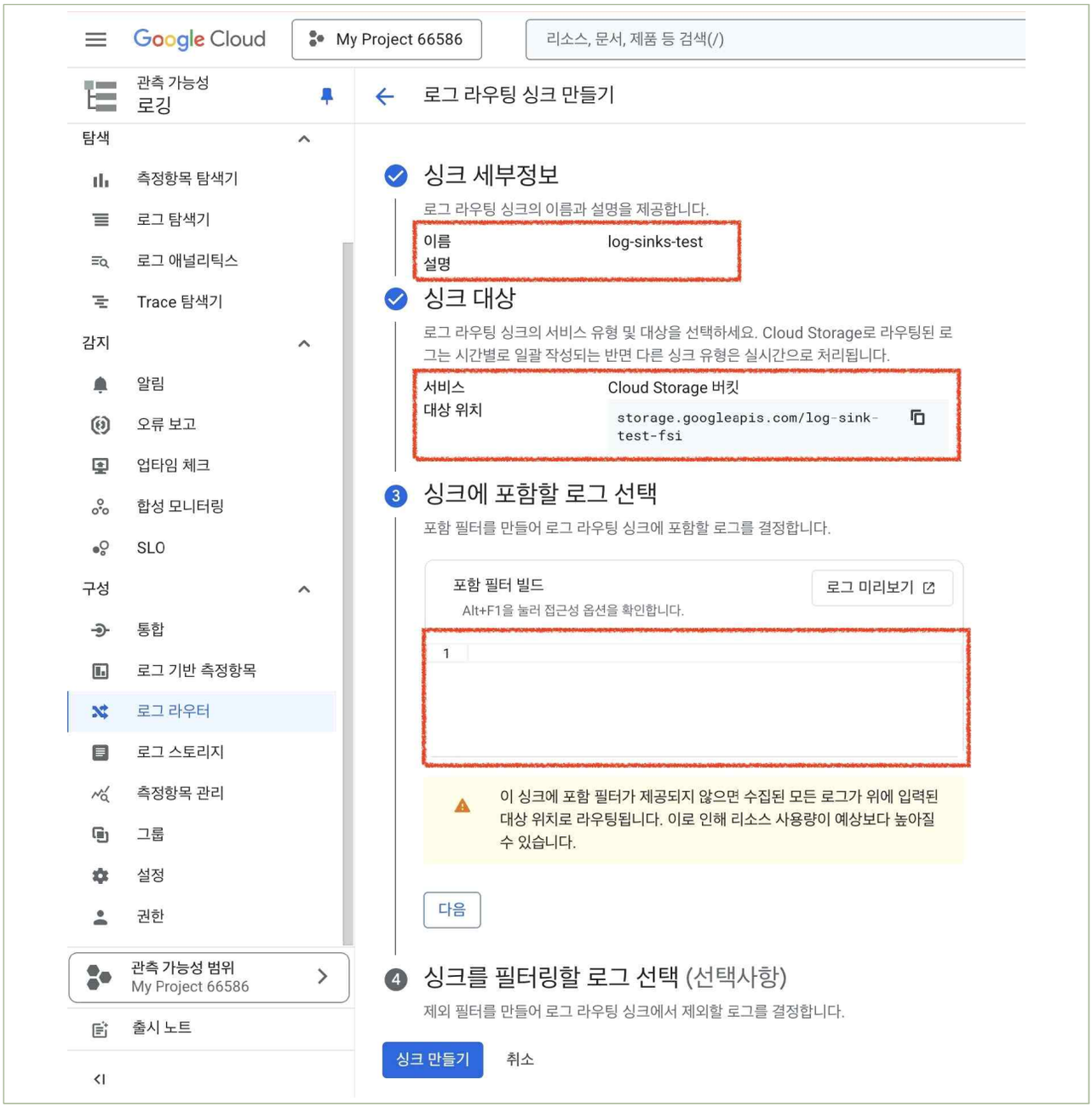
◦ 로그 싱크 만들기

- 로그 라우터 메뉴에서 “싱크 만들기”를 클릭합니다. 이 과정을 통해 로그 라우터 싱크를 설정하여 필요한 감사 로그를 장기 보관용 스토리지로 안전하게 라우팅할 수 있습니다.



| 그림 8-1-3 | 로그 싱크 만들기

- 싱크 이름과 싱크 대상 및 필터링 정보를 설정하여 로그 싱크 설정을 완료합니다.



| 그림 8-1-4 | 로그 싱크 세부설정

4 참고 사항

- Cloud Logging 기본 사항 참고
  - 금융분야 상용 클라우드컴퓨팅서비스 보안 관리 참고서(Google Cloud)의 5. 로깅 및 모니터링 관리 챕터의 5.1 가상자원 이용(생성, 삭제, 변경 등)에 관한 행위추적성 확보 부분 참고
- 로그 라우팅 및 로그 스토리지
  - https://cloud.google.com/logging/docs/routing/overview?hl=ko

- 로그 보관 기간
  - 기본 보관기간: https://cloud.google.com/logging/quotas?hl=ko#logs_retention_periods
  - 커스텀 설정: https://cloud.google.com/logging/docs/buckets?hl=ko#custom-retention

1 기준

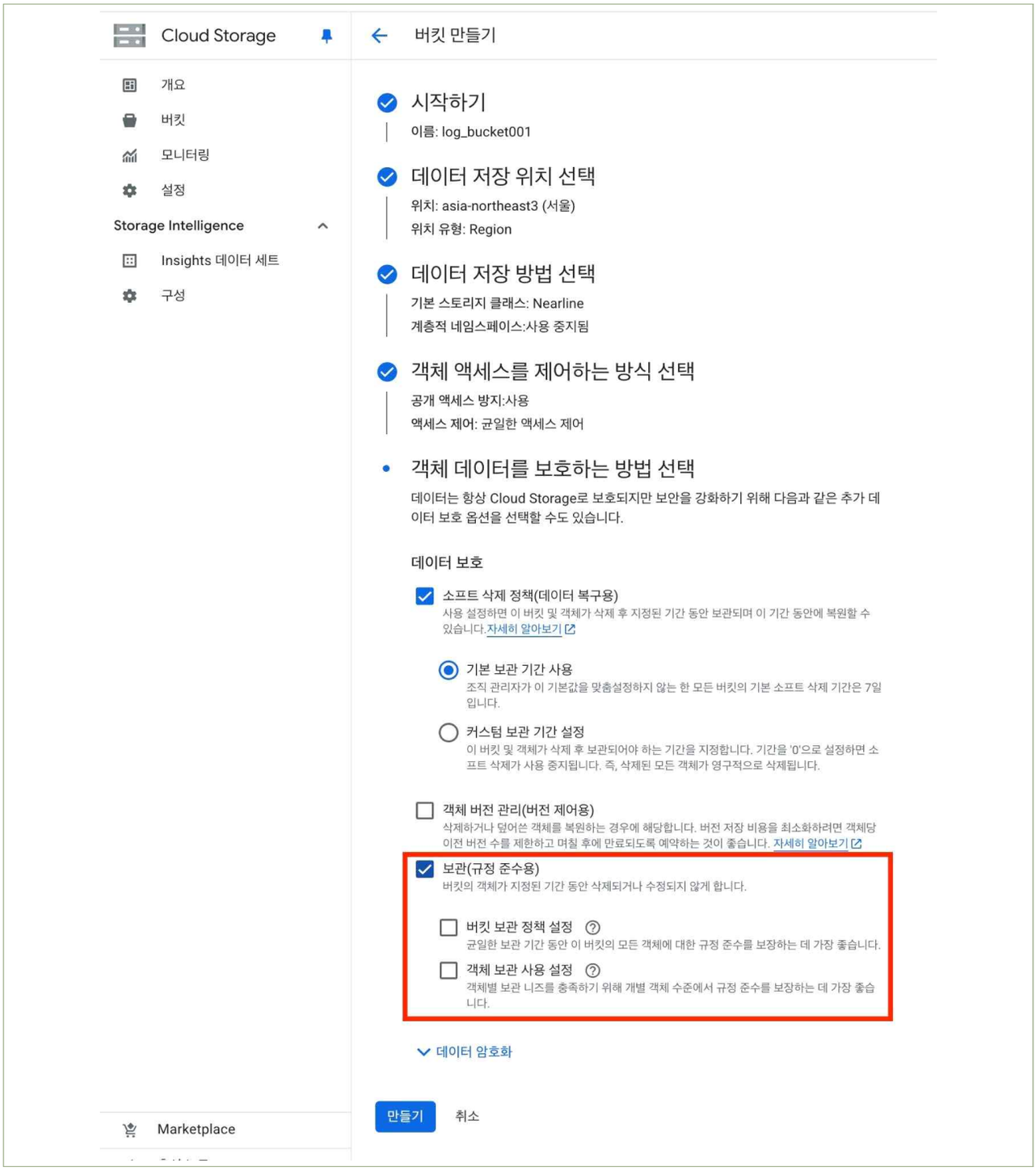
식별번호	기준	내용
8.2.	**행위추적성 증적(로그 등) 백업 파일 무결성 검증**	**백업을 통해 보관되고 있는 행위추적성 파일에 대한 무결성이 보장되어야 한다.**

2 설명

- Cloud Logging의 로그버킷에 저장된 로그는 기록된 후 내용이 변경될 수 없으며, 삭제도 설정된 보관 기간이 만료되어야 삭제가 자동으로 수행됩니다. 따라서 로그에 대한 조회기능만 제공하며, 로그에 대한 변경이나 보관기간 만료 전에 삭제 기능은 제공하지 않습니다.
- 로그라우팅을 통해 Cloud Storage에 로그를 저장한 경우 다음과 같은 기능을 통해 무결성을 확보할 수 있습니다.
  - 버킷 잠금 (Bucket Lock):
    - Cloud Storage 버킷의 버킷 잠금을 통해 버킷의 객체를 보관해야 하는 기간을 제어할 수 있습니다. 이 기능을 사용하면 버킷의 보관 정책을 잠글 수 있어 정책이 축소되거나 삭제되는 것을 영구 방지할 수 있습니다.
    - Cloud Storage 버킷 잠금
  - Cloud Storage 객체 잠금 (Object Lock):
    - 객체 보관 잠금 기능을 사용하면 Cloud Storage 버킷 내 객체에 보관 구성을 설정할 수 있습니다. 보관 구성은 객체를 보관해야 하는 기간을 제어하며 보관 기간 축소 또는 삭제를 영구 방지하는 옵션을 지정할 수 있습니다.
    - Cloud Storage 객체 잠금
  - 해시 값을 통한 무결성 검증 및 훼손 시 알림:
    - Cloud Storage는 객체 업로드 시 자동으로 MD5 또는 CRC32c 해시 값을 계산하고 메타데이터로 저장합니다. 이 MD5_hash 또는 CRC32c_hash는 수정이 불가능합니다. 따라서 필요시 Cloud Functions 등을 이용해 스케줄링 기반으로 백업된 로그 파일의 해시 값을 주기적으로 검증하여 파일의 무결성을 검증할 수 있습니다.
    - 또한 무결성 검증결과 훼손된 경우 Cloud Monitoring 또는 Cloud Pub/Sub을 활용하여 알림을 설정할 수 있습니다.
    - Cloud Storage 객체 메타데이터

3 우수 사례

- 로그 저장을 위한 Cloud Storage 버킷에서 보관 설정
  - 로그를 저장하기 위해 Cloud Storage 버킷을 생성시, 데이터 보호 방법으로 “보관(규정 준수용)”을 선택한 후 “버킷 보관 정책 설정” 또는 “객체 보관 사용 설정”을 활성화



| 그림 8-2-1 | Cloud Storage 버킷의 보관 설정

4 참고 사항

- Cloud Storage 객체 checksum
  - https://cloud.google.com/storage/docs/metadata?hl=ko#checksums
- 객체 버전 관리
  - https://cloud.google.com/storage/docs/object-versioning?hl=ko
- 수정할 수없는 메타데이터
  - https://cloud.google.com/storage/docs/metadata?hl=ko#fixed
- 데이터 보호, 백업, 복구 옵션
  - https://cloud.google.com/storage/docs/protection-backup-recovery-overview?hl=ko

1 기준

식별번호	기준	내용
8.3.	**금융회사 전산자료 백업**	**관련 법령(전자금융거래법, 전자금융감독규정 등)에 따라 백업이 필요한 금융회사 전산자료에 대해 백업을 수행하여야 한다.**

2 설명

- 금융회사 클라우드 이용 시 관련 법령(전자금융거래법, 전자금융감독규정 등)에 따라 백업이 필요한 전산자료에 대해서는 백업을 수행하여야 하며, 중요업무인 경우 클라우드서비스와 관련한 중요 설정파일 및 가상 시스템 이미지도 백업 대상에 포함하여야 합니다.(중요도에 따라 1년이상 보관)
- Google Cloud는 금융분야 규정 준수 및 안정적인 데이터 보호를 위한 다양한 백업 기능을 제공합니다.

  - **Persistent Disk** 스냅샷:
    - Compute Engine VM 인스턴스의 Persistent Disk(데이터 디스크 포함)를 특정 시점으로 백업합니다.
    - 자동 스냅샷 예약 기능을 통해 정기적인 백업을 설정할 수 있습니다.
    - 초기 스냅샷 이후 변경된 블록만 저장하는 증분 백업 방식을 사용하여 비용 효율적입니다.
    - 스냅샷은 기본적으로 동일 리전에 저장되지만, 리전 간 스냅샷 복사 기능을 통해 재해 복구 대비가 가능합니다.
    - Persistent Disk 스냅샷
  - **Machine Images:**
    - VM 인스턴스의 디스크 데이터뿐만 아니라 인스턴스 설정, 메타데이터, 권한 등 전체 구성을 포함하여 백업합니다.
    - 중요 업무 시스템의 전체 상태를 백업하고 신속하게 복구해야 할 때 유용합니다.
    - 머신 이미지
  - **Cloud Storage:**
    - 객체 스토리지 서비스로, 다양한 유형의 전산 자료(파일, 데이터베이스 덤프, 로그 등)를 내구성 높게 저장할 수 있습니다.
    - 스냅샷, 머신 이미지 외 별도 백업 데이터(예: 설정 파일)를 저장하는 용도로 활용 가능합니다.
    - 데이터 접근 빈도와 보관 기간에 따라 Standard, Nearline, Coldline, Archive 등 다양한

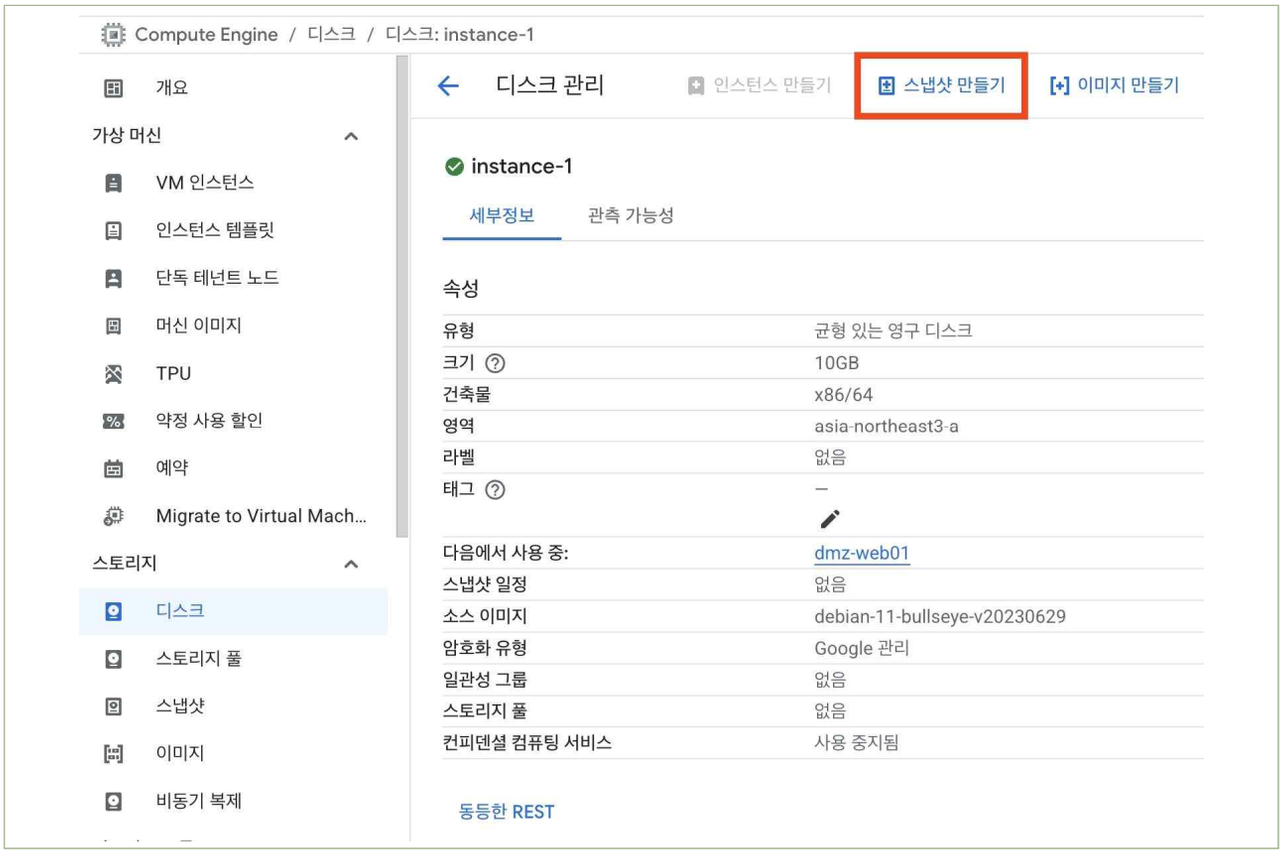
스토리지 클래스를 제공하여 비용을 최적화할 수 있습니다. (Archive는 1년 이상 장기 보관에 적합)

- 객체 수명 주기 관리 정책을 통해 자동으로 데이터를 다른 스토리지 클래스로 이동시키거나 삭제할 수 있어 규정된 보관 기간 준수에 용이합니다.
- Cloud Storage
- 스토리지 클래스
- 객체 수명 주기 관리

- **Backup and DR:**
  - 중앙 집중식 관리 인터페이스를 통해 데이터베이스, 파일 시스템, VM 등 다양한 워크로드에 대한 애플리케이션 인식 백업 및 복구를 제공하는 관리형 서비스입니다.
  - 데이터베이스 등의 경우 애플리케이션 정합성을 보장하는 백업이 가능합니다.
  - 정책 기반 자동화, 보고, 감사 기능을 제공하여 운영 부담을 줄여줍니다.
  - Backup and DR

3 우수 사례

- Compute Engine VM 인스턴스의 Persistent Disk를 특정 시점으로 백업
  - VM 인스턴스가 포함된 프로젝트를 선택한 후, 이름 열에서 백업할 디스크가 있는 VM의 이름을 클릭하여 VM의 상세 사항을 살펴봅니다.
  - 부팅 디스크를 백업하려면 부팅 디스크 섹션에서 부팅 디스크 이름을 클릭하고, 연결된 데이터 디스크를 백업하려면 추가 디스크에서 디스크의 이름을 클릭합니다.
  - 디스크를 클릭한 후 아래 그림과 같은 “스냅샷 만들기”를 클릭합니다.

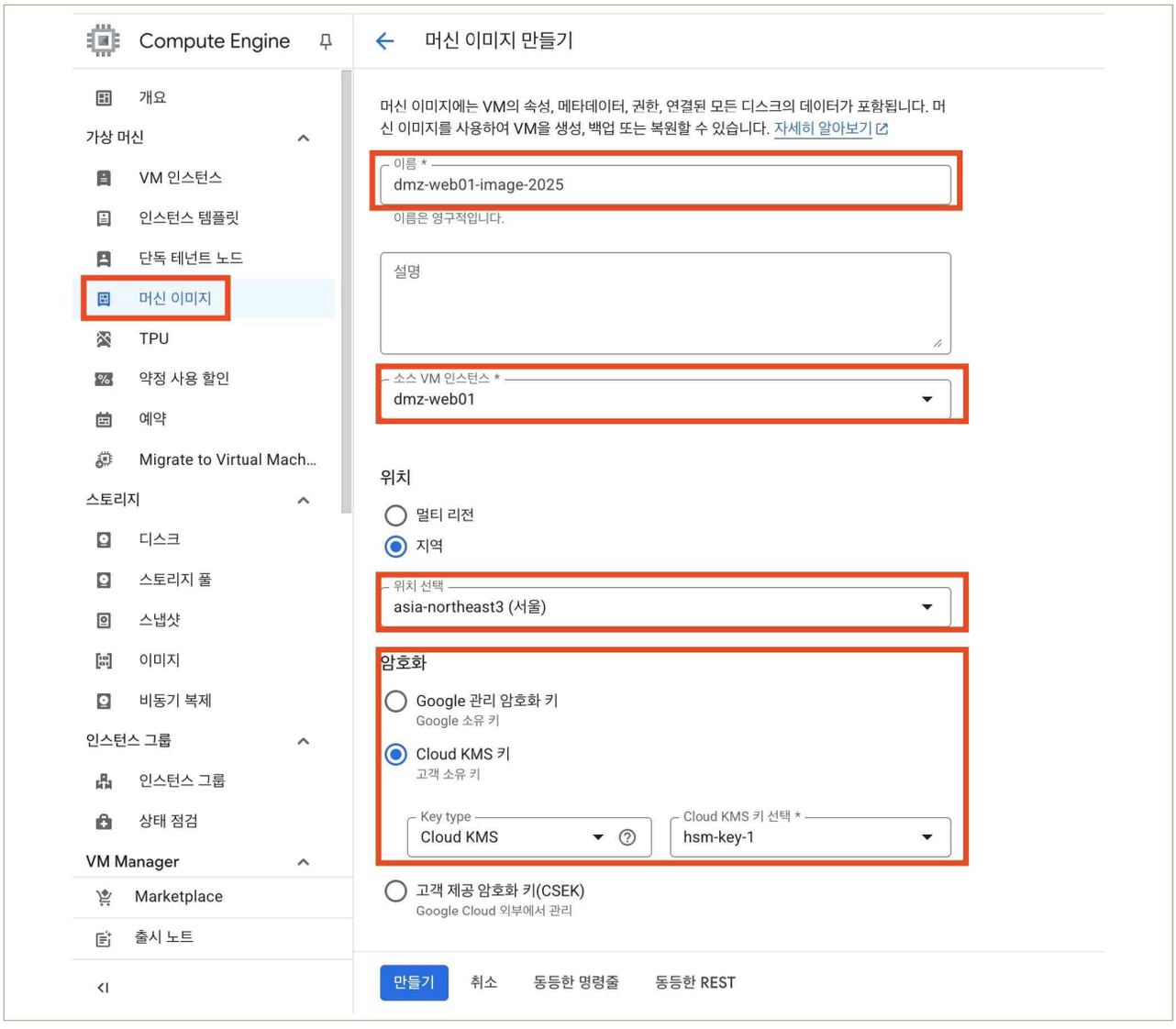


| 그림 8-3-1 | Compute Engine VM 스냅샷 만들기

- 머신 이미지(**Machine Images**)를 사용하여 Compute Engine에서 실행되는 VM 인스턴스에 대한 여러 디스크에 관련된 모든 구성, 메타데이터, 권한, 데이터를 백업합니다.
  - 머신 이미지 메뉴에서 “머신 이미지 만들기”를 선택합니다.

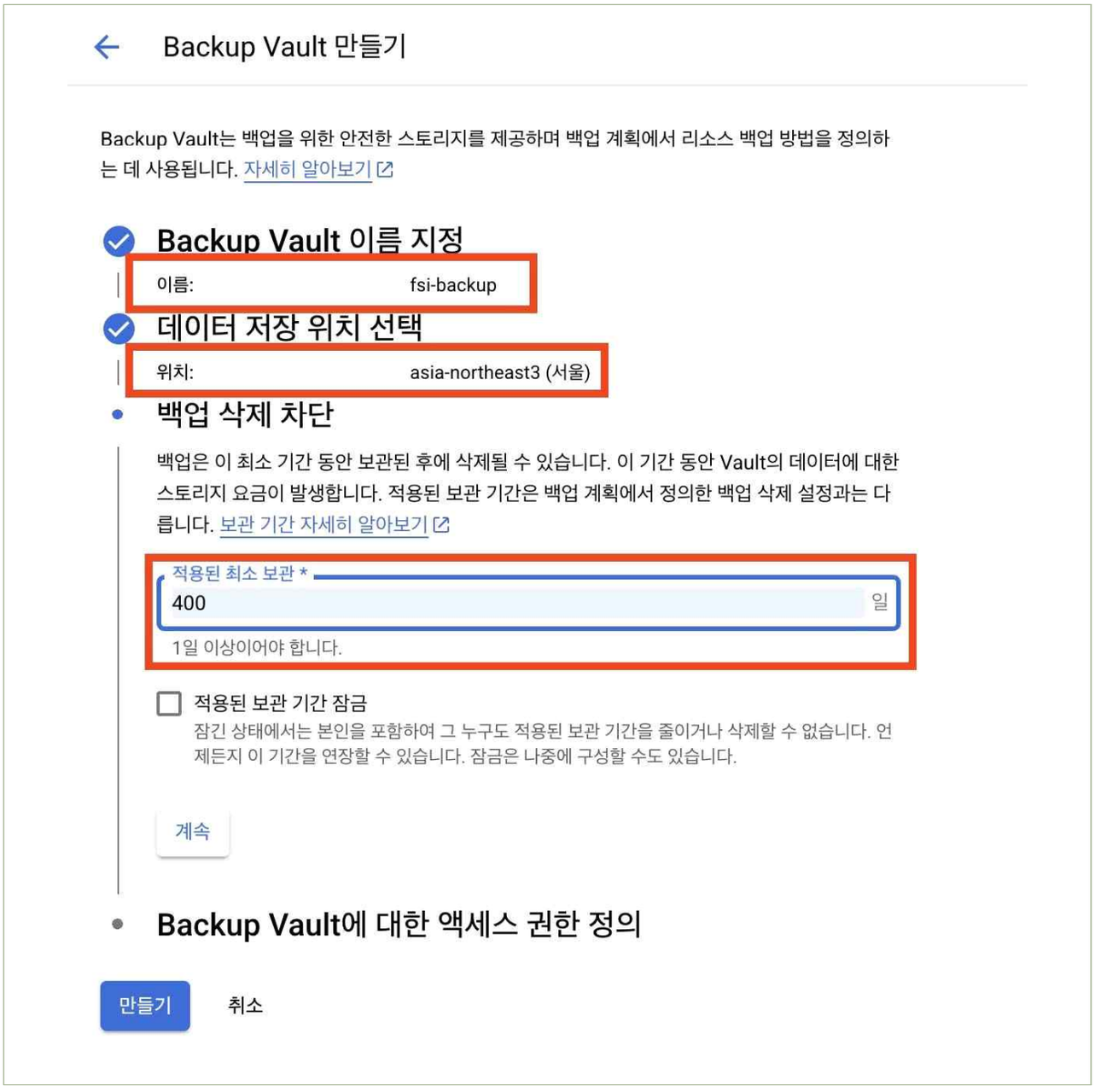
| 그림 8-3-2 | Compute Engine VM 이미지 만들기

  - 생성하려는 이미지의 이름, 백업대상 VM 인스턴스(소스 VM 인스턴스), 저장위치, 암호화 설정을 하고 이미지를 만듭니다.



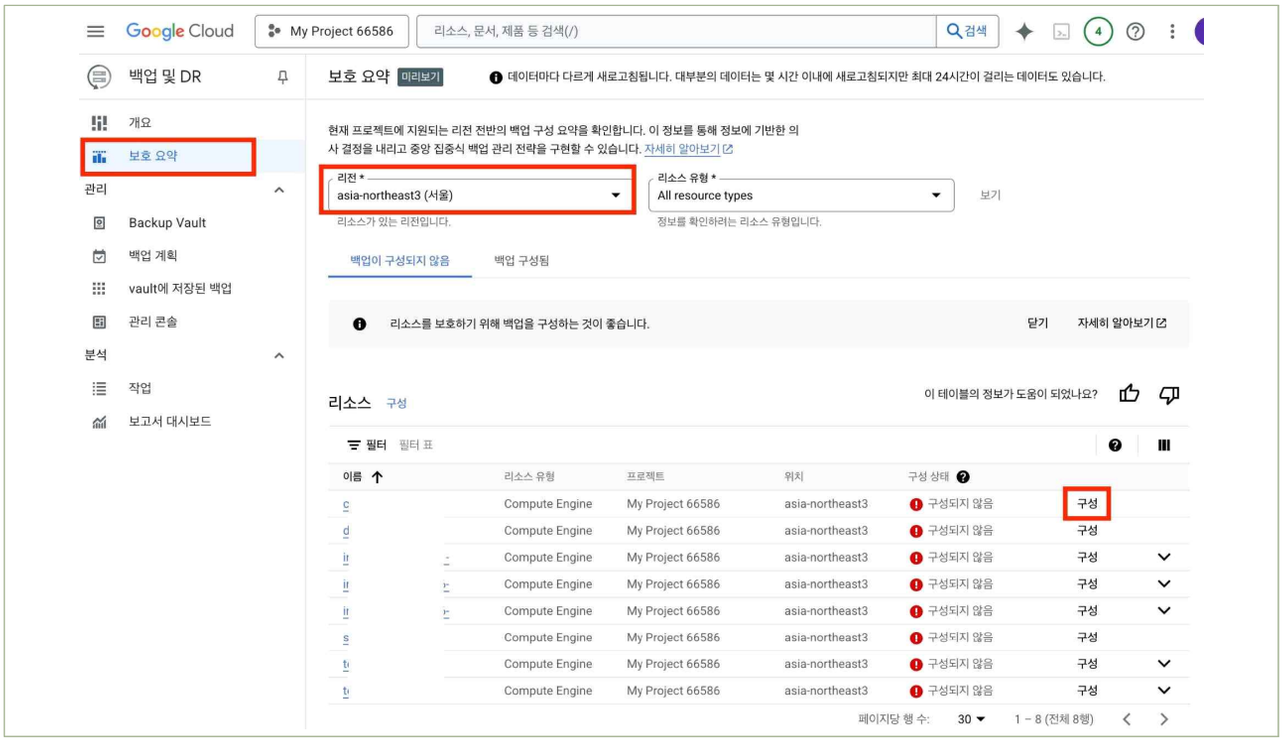
| 그림 8-3-3 | Compute Engine VM 이미지 만들기 상세설정

- Backup and DR 서비스를 이용한 백업
  - Backup Vault를 서울리전(asia-northeast3)에 생성하여 백업수행



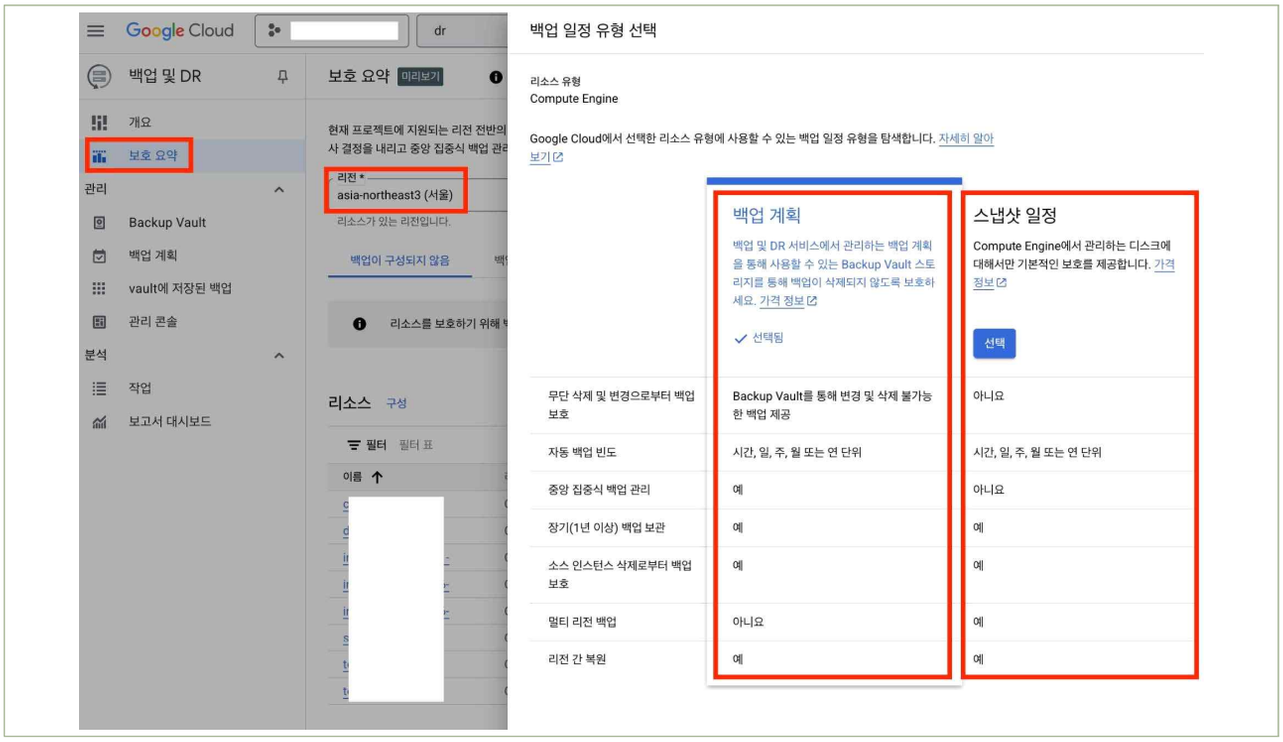
| 그림 8-3-4 | Backup Vault 만들기

- Backup and DR(백업 및 DR) 메뉴의 보호요약에서 리전을 선택하여 리소스 리스트 참조하여, 백업에 추가할 리소스의 “구성” 항목을 클릭하여 상세 화면 호출



| 그림 8-3-5 | 백업 대상 리소스 선택

– “백업 일정 유형 선택” 항목에서 필요한 항목 지정



| 그림 8-3-6 | 백업 대상 리소스 선택

4 참고 사항

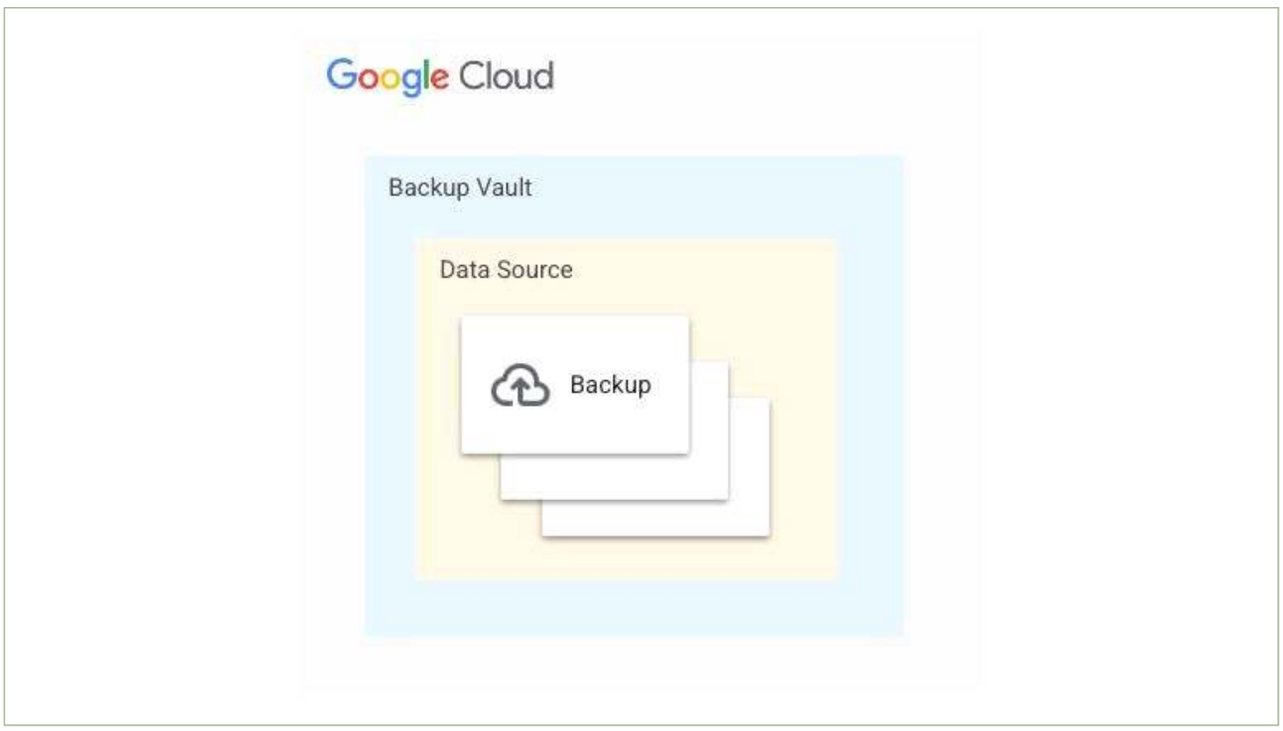
- Persistent Disk 볼륨의 스냅샷 만들기
  - https://cloud.google.com/compute/docs/disks/create-snapshots?hl=ko#create_snapshots
- 머신 이미지 만들기
  - https://cloud.google.com/compute/docs/machine-images/create-machine-images?hl=ko
- 백업 및 DR 서비스 개요
  - https://cloud.google.com/backup-disaster-recovery/docs/concepts/backup-dr?hl=ko

1 기준

식별번호	기준	내용
8.4.	**금융회사 전산자료 백업 파일 무결성 검증**	**백업을 통해 보관되고 있는 전산자료에 대한 무결성이 보장되어야 한다.**

2 설명

- Backup Vault를 사용하면 지정된 기간이 지나기 전에는 백업이 만료될 수 없도록 하고 실수 또는 악의적인 삭제로부터 보호하는 데 도움이 되는 적용된 최소 보관 기간을 지정할 수 있습니다.



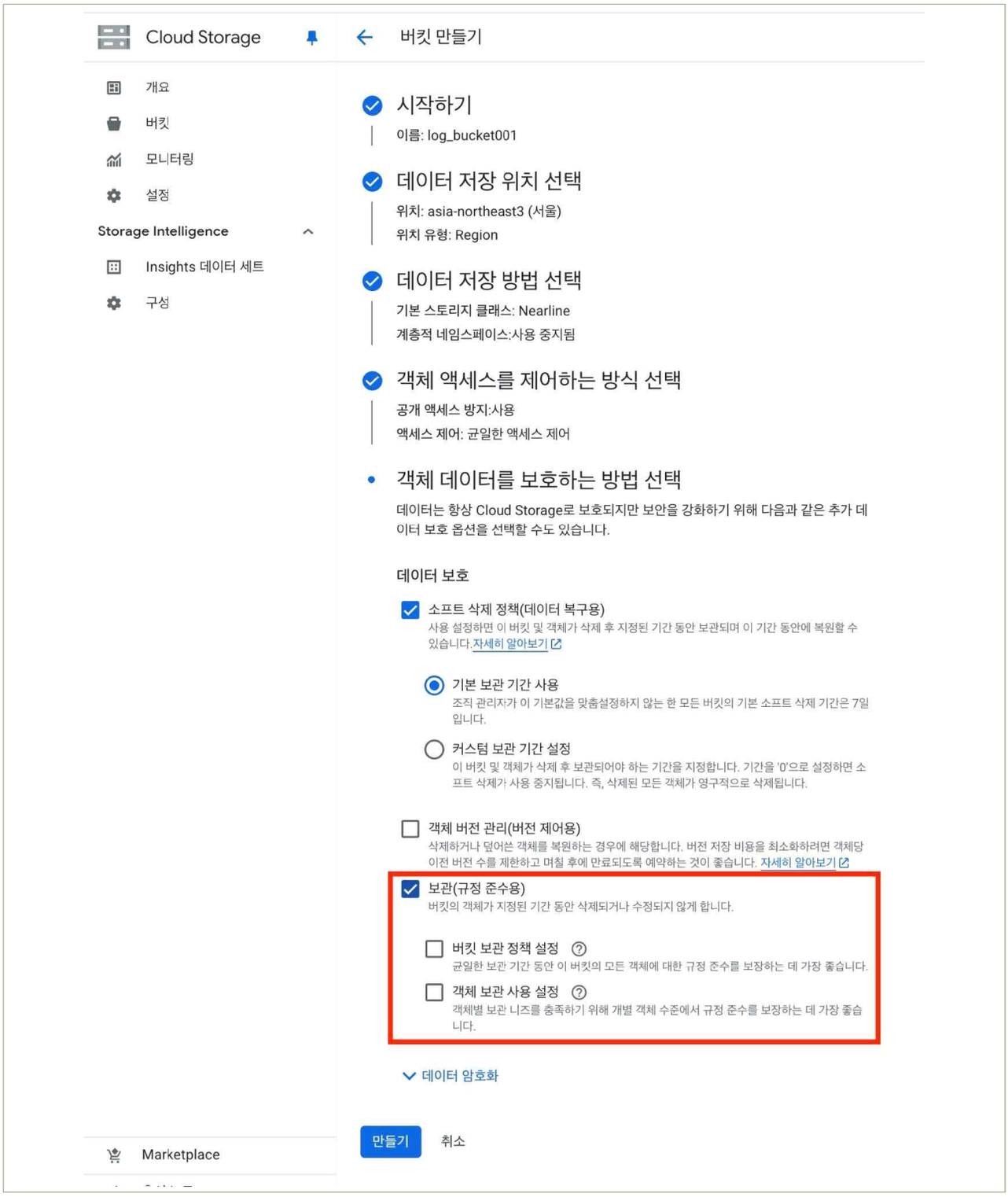
| 그림 8-4-1 | Backup Vault 리소스 모델

- 전산자료 백업자료를 Cloud Storage에 로그를 저장한 경우 다음과 같은 기능을 통해 무결성을 확보할 수 있습니다.
  - 버킷 잠금 (Bucket Lock):
    - Cloud Storage 버킷의 버킷 잠금을 통해 버킷의 객체를 보관해야 하는 기간을 제어할 수 있습니다. 이 기능을 사용하면 버킷의 보관 정책을 잠글 수 있어 정책이 축소되거나 삭제되는 것을 영구 방지할 수 있습니다.
    - Cloud Storage 버킷 잠금

- Cloud Storage 객체 잠금 (Object Lock):
  - 객체 보관 잠금 기능을 사용하면 Cloud Storage 버킷 내 객체에 보관 구성을 설정할 수 있습니다. 보관 구성은 객체를 보관해야 하는 기간을 제어하며 보관 기간 축소 또는 삭제를 영구 방지하는 옵션을 지정할 수 있습니다.
  - Cloud Storage 객체 잠금
- 해시 값을 통한 무결성 검증 및 훼손시 알림:
  - Cloud Storage는 객체 업로드 시 자동으로 MD5 또는 CRC32c 해시 값을 계산하고 메타데이터로 저장합니다. 이 MD5_hash 또는 CRC32c_hash는 수정이 불가능합니다. 따라서 필요시 Cloud Functions 등을 이용해 스케줄링 기반으로 백업된 로그 파일의 해시 값을 주기적으로 검증하여 파일의 무결성을 검증할 수 있습니다.
  - 또한 무결성 검증결과 훼손된 경우 Cloud Monitoring 또는 Cloud Pub/Sub을 활용하여 알림을 설정할 수 있습니다.
  - Cloud Storage 객체 메타데이터

3 우수 사례

- 전산자료 백업 파일 저장을 위한 Cloud Storage 버킷에서 보관 설정
  - 로그를 저장하기 위해 Cloud Storage 버킷을 생성시, 데이터 보호 방법으로 “보관(규정 준수용)”을 선택한 후 “버킷 보관 정책 설정” 또는 “객체 보관 사용 설정”을 활성화



| 그림 8-4-2 | Cloud Storage 버킷의 보관 설정

- 전산자료 백업 파일 저장을 위한 Backup Vault 사용에 대해서는 8.2의 우수사례 참고

4 참고 사항

- 변경할 수 없고 지울 수 없는 백업을 위한 Backup Vault
  - https://cloud.google.com/backup-disaster-recovery/docs/concepts/backup-vault?hl=ko
- Cloud Storage 객체 checksum
  - https://cloud.google.com/storage/docs/metadata?hl=ko#checksums
- 객체 버전 관리
  - https://cloud.google.com/storage/docs/object-versioning?hl=ko
- 수정할 수 없는 메타데이터
  - https://cloud.google.com/storage/docs/metadata?hl=ko#fixed
- 데이터 보호, 백업, 복구 옵션
  - https://cloud.google.com/storage/docs/protection-backup-recovery-overview?hl=ko

1 기준

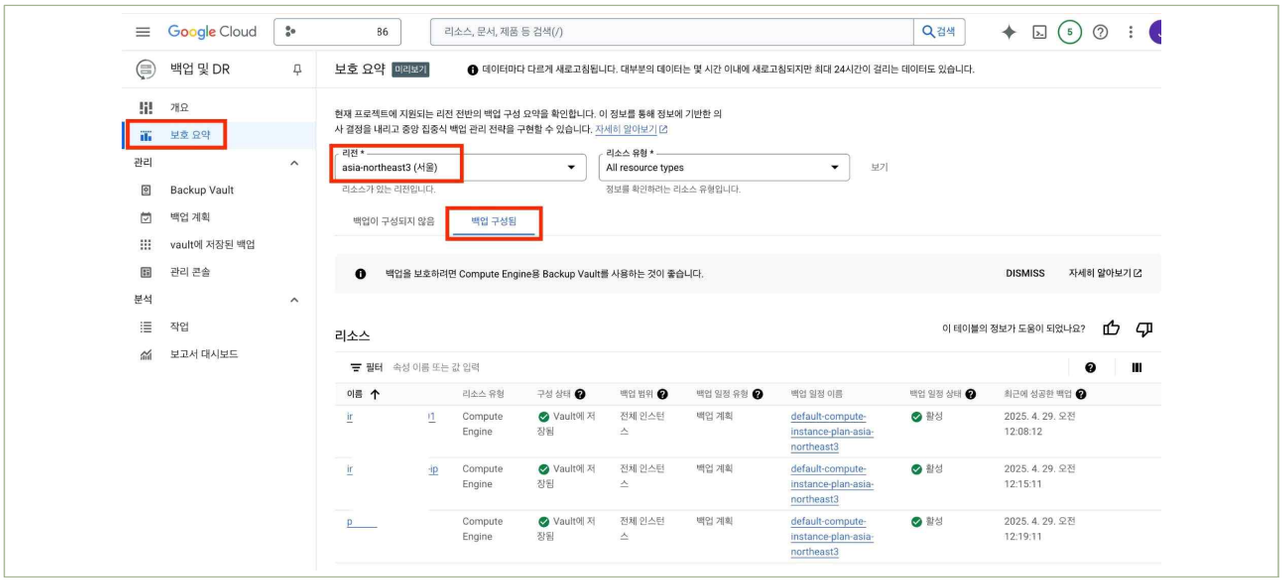
식별번호	기준	내용
8.5.	**행위추적성 증적 및 전산자료등 백업에 관한 기록 및 관리**	**행위추적성 증적 및 금융회사 전산자료 백업 시 백업내역을 기록하고 관리하여야 한다.**

2 설명

- 행위추적성 증적 및 전산자료 등 백업 시 백업내역을 기록하고 관리하여야 한다.
  - Cloud Audit Logs 활성화 및 활용:
    - 관리자 활동 로그는 기본 활성화 상태를 유지합니다.
    - 백업 실행 및 데이터 접근 추적이 중요한 Compute Engine(스냅샷 관련), Cloud Storage(백업 파일 저장 관련) 등의 서비스에 대해서는 데이터 접근 로그(특히 쓰기 작업)를 활성화하여 상세한 백업 실행 기록(백업 내역)을 확보합니다.
  - 로그 중앙 관리 및 장기 보관: Cloud Logging을 사용하여 모든 백업 관련 로그(Audit Logs, 애플리케이션 백업 로그 등)를 중앙에서 관리합니다. 규정에서 요구하는 보관 기간 이상으로 로그를 보존해야 하는 경우, 로그 싱크를 구성하여 Cloud Storage의 저비용 스토리지 클래스나 BigQuery로 로그를 내보내 보관합니다. (8.1 참조)
  - 백업 및 DR 서비스를 통한 백업내역 현황 관리할 수 있습니다.

3 우수 사례

- 백업 구성에 대한 현황 확인
  - 백업 및 DR → 보호 요약 → 리전 선택 후, “백업 구성됨” 탭을 선택하여 백업 구성 상태와 최근 백업 현황을 파악



| 그림 8-5-1 | 백업 구성 현황

- Cloud Audit Logs 및 로그 보관기간 관련 사항에 대해서는 8.1 참조

4 참고 사항

- 백업 관리자를 위한 도구
  - https://cloud.google.com/backup-disaster-recovery/docs/backup-admin/protection-summary?hl=ko
- Cloud Logging 기본 사항 참고
  - 금융분야 상용 클라우드컴퓨팅서비스 보안 관리 참고서(Google Cloud)의 5. 로깅 및 모니터링 관리 챕터의 5.1 가상자원 이용(생성, 삭제, 변경등)에 관한 행위추적성 확보 부분 참고
- 로그 라우팅 및 로그 스토리지
  - https://cloud.google.com/logging/docs/routing/overview?hl=ko

1 기준

식별번호	기준	내용
8.6.	**백업파일 원격 안전지역 보관**	**금융회사는 전산자료 등 중요도에 따라 중요도가 높은 파일에 대해선 원격 안전지역에 소산하여 보관하여야 한다.**

2 설명

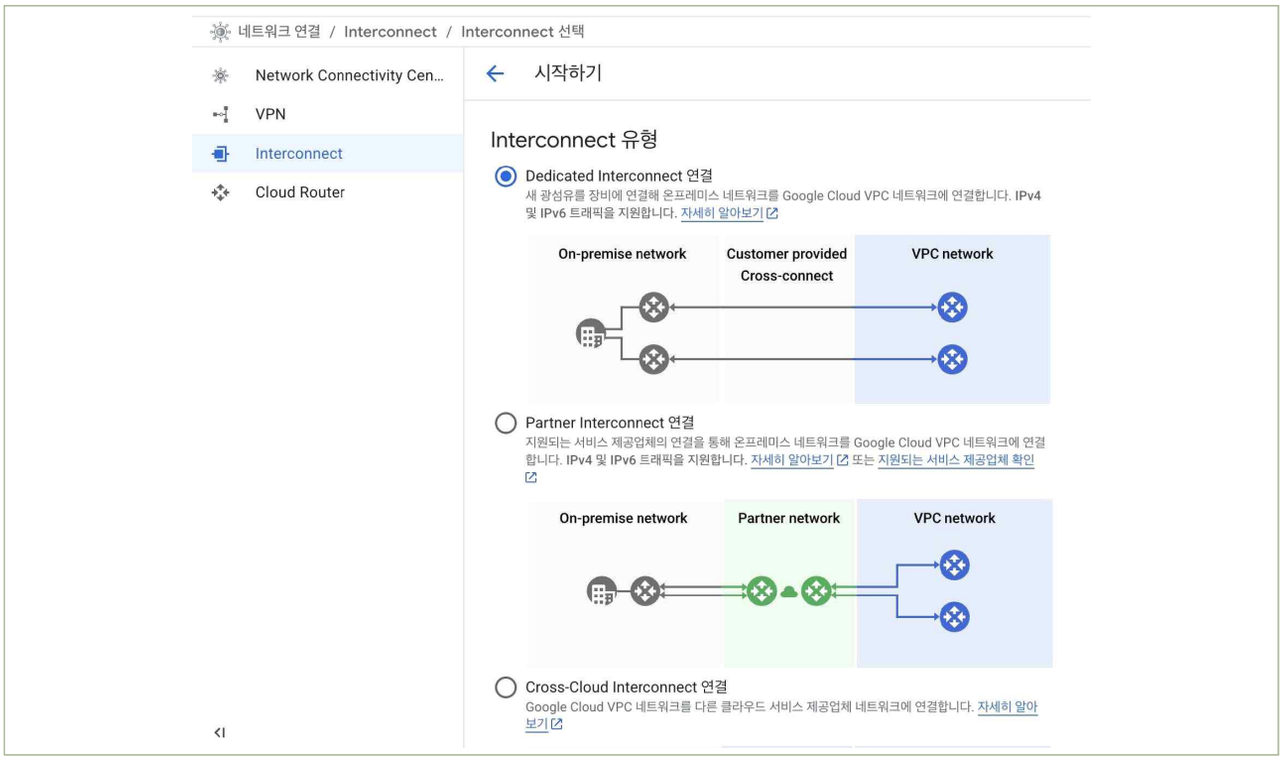
- 금융회사는 중요도에 따라 전산자료 등 중요도가 높은 파일에 대해서는 원격 안전지역에 소산하여 보관하여야 한다.
  - 소산의 방식은 퍼블릭 클라우드에 저장된 전산자료를 금융회사 자체 데이터센터로 소산할 수 있고, 반대로 금융회사 자체 데이터센터에 저장된 전산자료를 퍼블릭 클라우드에 소산할 수도 있습니다. 또한 특정 클라우드에 저장된 전산자료를 다른 클라우드에 저장하는 방식도 고려해 볼 수 있습니다. 이런 소산을 위하여 Google Cloud는 다양한 연결과 데이터 전송 도구를 지원하고 있습니다.
  - 네트워크 연결 (Cloud Interconnect / Cloud VPN):
    - 금융회사의 자체 데이터센터와 Google Cloud 간에 안정적이고 안전한 비공개 네트워크 연결을 제공합니다. 이를 통해 Google Cloud에 저장된 백업 데이터를 금융회사의 원격 안전 지역 데이터센터로 전송(소산)하거나 금융회사 자체 데이터센터의 백업 데이터를 Google Cloud로 안전하게 전송할 수 있습니다.
    - Cloud Interconnect는 네트워크를 확장하여 Google Cloud를 포함할 수 있는 다음과 같은 옵션을 제공합니다.
      - Dedicated Interconnect는 온프레미스 네트워크와 Google 네트워크 간에 물리적인 직접 연결을 제공합니다.
      - Partner Interconnect는 지원되는 서비스 제공업체를 통해 온프레미스 네트워크와 VPC 네트워크 간의 연결을 제공합니다.
      - Cross-Cloud Interconnect는 다른 클라우드의 네트워크와 Google 네트워크 간에 물리적인 직접 연결을 제공합니다.
    - Cloud VPN은 IPsec VPN 연결을 통해 동종 앱 네트워크를 가상 프라이빗 클라우드(VPC) 네트워크에 안전하게 확장합니다.

- 데이터 전송 도구 (Storage Transfer Service):
  - Cloud Storage에 저장된 백업 파일을 외부(금융회사 데이터센터 등)로 다운로드하거나 전송하는 데 사용되는 도구 및 서비스입니다. 대규모 데이터 전송을 관리하고 자동화할 수 있습니다.

3 우수 사례

Cloud Interconnect 만들기

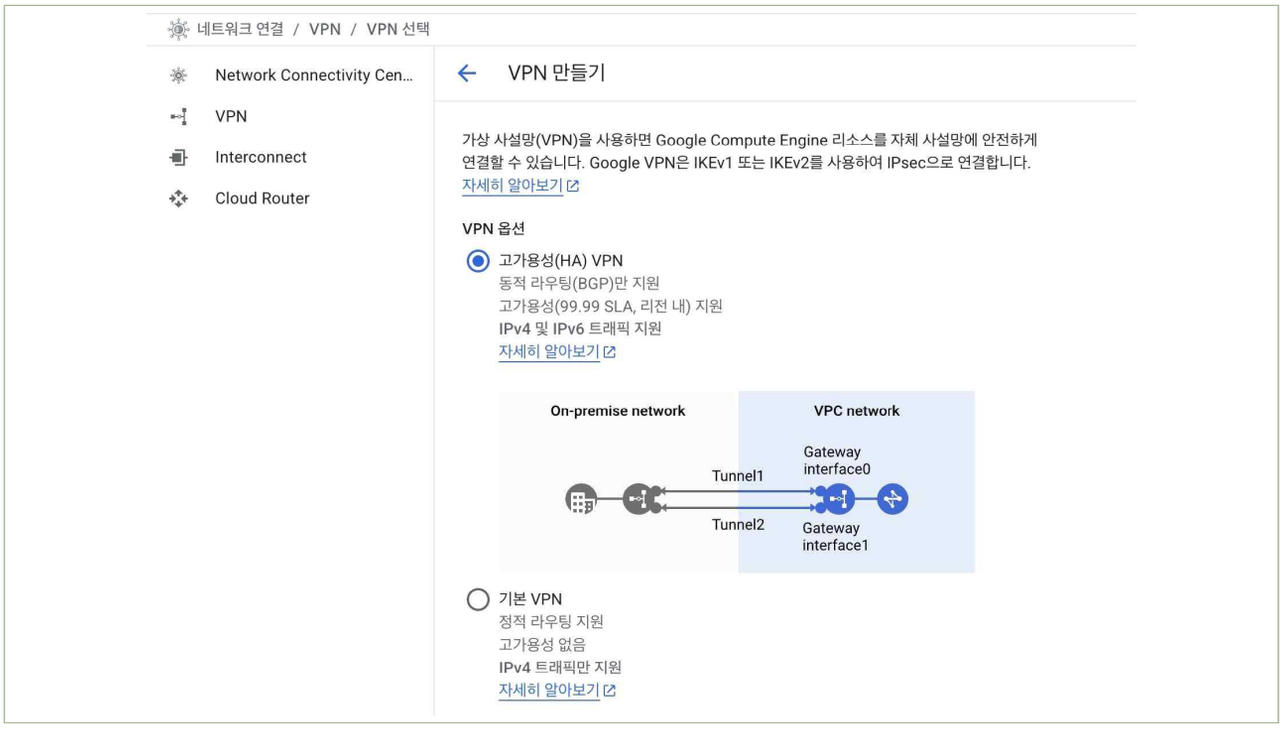
- Network Connectivity Center → Interconnect → ‘ + VLAN 연결 만들기’ 또는 ‘ + 물리적 연결 설정’



| 그림 8-6-1 | Cloud Interconnect 설정

Cloud VPN 만들기

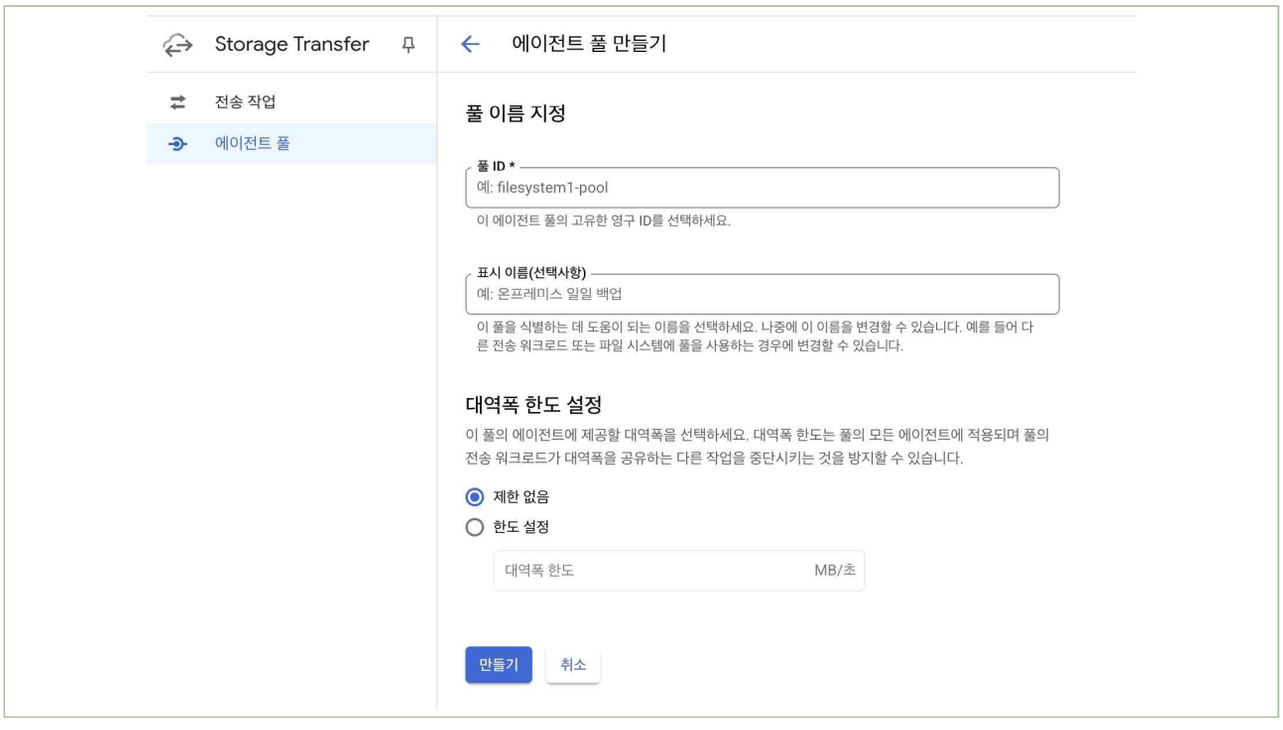
- Network Connectivity Center → VPN → VPN 연결 만들기



| 그림 8-6-2 | Cloud VPN 설정

Storage Transfer 설정

- Storage Transfer → 에이전트 풀 → '+ 풀 만들기'



| 그림 8-6-3 | Storage Tranfer 설정

4 참고 사항

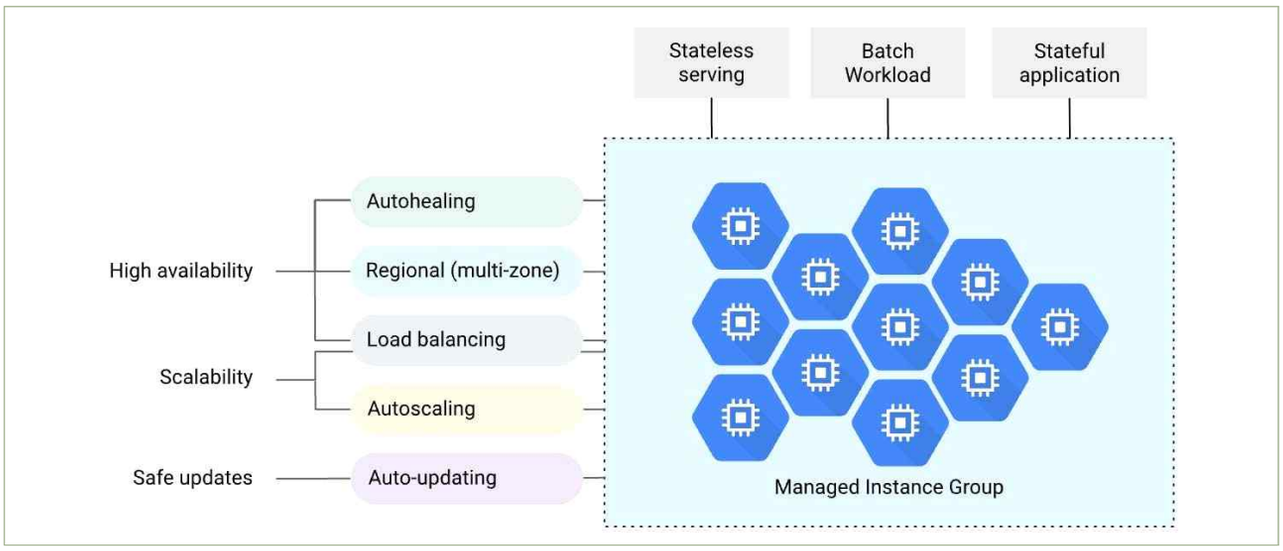
- Cloud Interconnect
  - https://cloud.google.com/network-connectivity/docs/interconnect/concepts/overview?hl=ko
- Cloud VPN
  - https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview?hl=ko
- Storage Transfer Service 개요
  - https://cloud.google.com/storage-transfer/docs/overview?hl=ko
- 백업자료 소산방안 클라우드 전환 관련 법령해석
  - https://better.fsc.go.kr/fsc_new/replyCase/LawreqDetail.do?stNo=11&muNo=171&muGpNo=75&lawreqIdx=4200

1 기준

식별번호	기준	내용
8.7.	주요 전산장비 이중화	**금융회사는 클라우드 환경을 통한 인프라 구성 시 주요 전산장비를 이중화하여야 한다.**

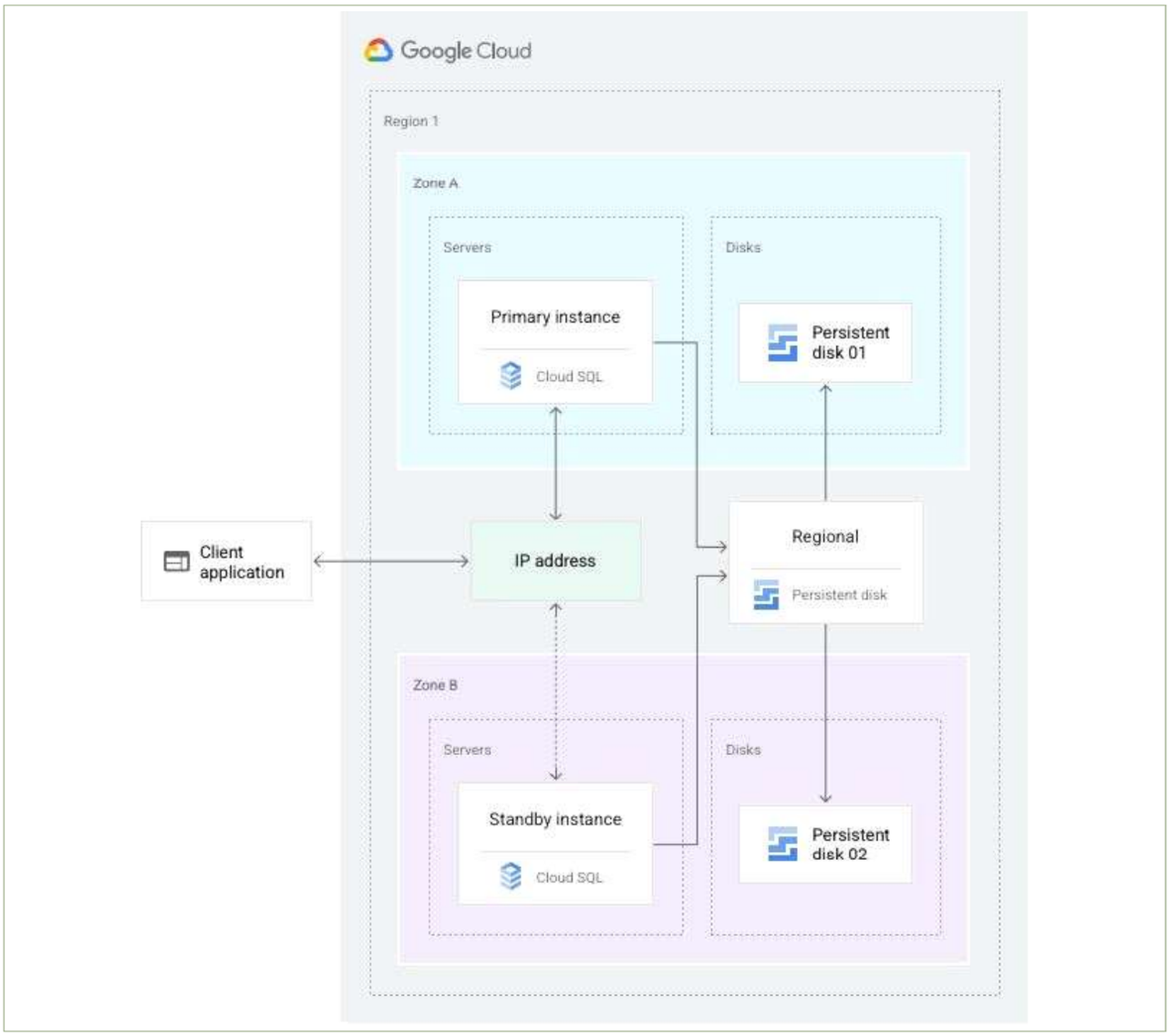
2 설명

- 금융회사는 클라우드 환경을 통한 인프라 구성 시 가상화 기능을 이용하여 주요 전산장비를 이중화하여야 한다.
  - Google Cloud는 가상화 기술을 기반으로 다양한 서비스와 기능을 통해 단일 장애 지점(Single Point of Failure)을 제거하고 고가용성(High Availability, HA) 및 재해 복구(Disaster Recovery, DR) 환경을 구축하여 서비스 연속성을 보장합니다.
  - **Managed Instance Groups (MIGs):**
    - MIGs: 여러 VM 인스턴스를 논리적인 그룹으로 관리하며 자동 확장(Auto-scaling), 자동 복구(Auto-healing), 자동 업데이트 기능을 제공합니다.
    - Regional MIGs: 여러 가용 영역(Zone)에 걸쳐 VM 인스턴스를 분산 배포하여 단일 영역 장애 시에도 서비스 가용성을 유지합니다. 이는 "원격 안전지역"(최소 Zone 수준)을 고려한 이중화의 기본입니다.



| 그림 8-7-1 | MIG 기능과 일반적인 워크로드의 개요

- **Cloud SQL (관리형 관계형 데이터베이스):**
  - 고가용성(HA) 구성: 주 인스턴스와 다른 영역(Zone)에 위치한 동기식 대기 인스턴스를 구성합니다. 주 인스턴스 장애 시 자동으로 대기 인스턴스로 장애 조치(Failover)됩니다. (Zone 수준 이중화)
  - 리전 간 읽기 복제본(Cross-Region Read Replicas): 다른 리전에 비동기식 복제본을 생성하여 읽기 성능을 확장하고, 재해 복구 시 수동으로 승격하여 사용할 수 있습니다. (Region 수준 이중화 고려)



| 그림 8-7-2 | Cloud SQL 이중화 개요

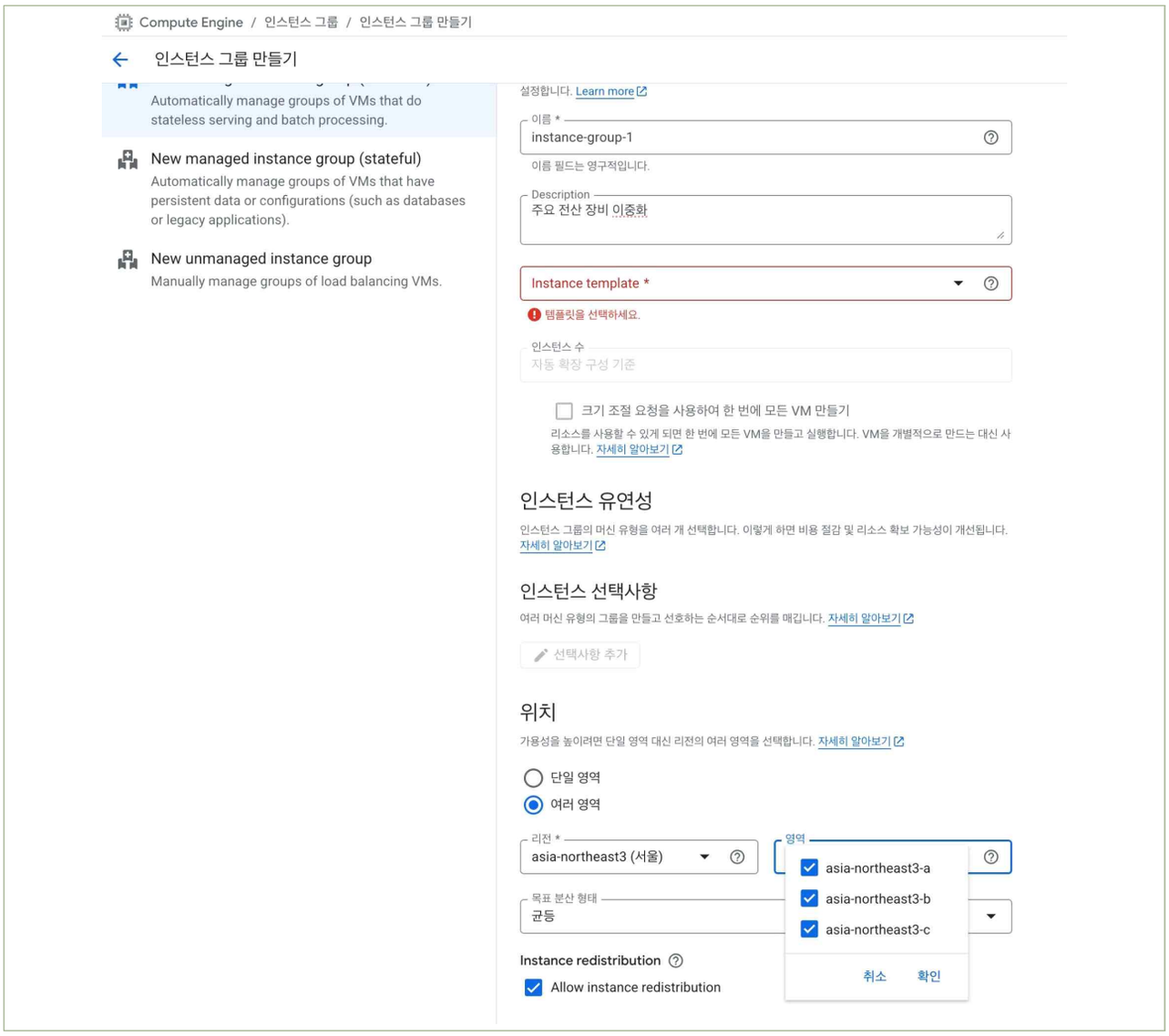
- **Cloud Storage (오브젝트 스토리지):**
  - Cloud Storage는 스토리지에 기록된 객체를 최소 2개 이상의 서로 다른 가용성 영역에 중복해서 저장한 후에야 쓰기 작업이 성공한 것으로 간주합니다. 즉 별도의 설정을 하지 않아도 기본적으로 복제가 이루어지고 있습니다.(기본복제)

- 이중/멀티 리전 버킷은 데이터를 최소 두 개 이상의 지리적으로 분리된 리전에 자동으로 복제하여 극단적인 재해 상황에서도 데이터 손실을 최소화하고 높은 가용성을 제공합니다.
- 버킷 간 복제: 경우에 따라 두 번째 버킷에 데이터 사본을 유지할 수 있습니다. 버킷 간 복제는 신규 객체와 업데이트된 객체를 비동기식으로 소스 버킷에서 대상 버킷으로 복사합니다.

3 우수 사례

VM 인스턴스 그룹 만들기

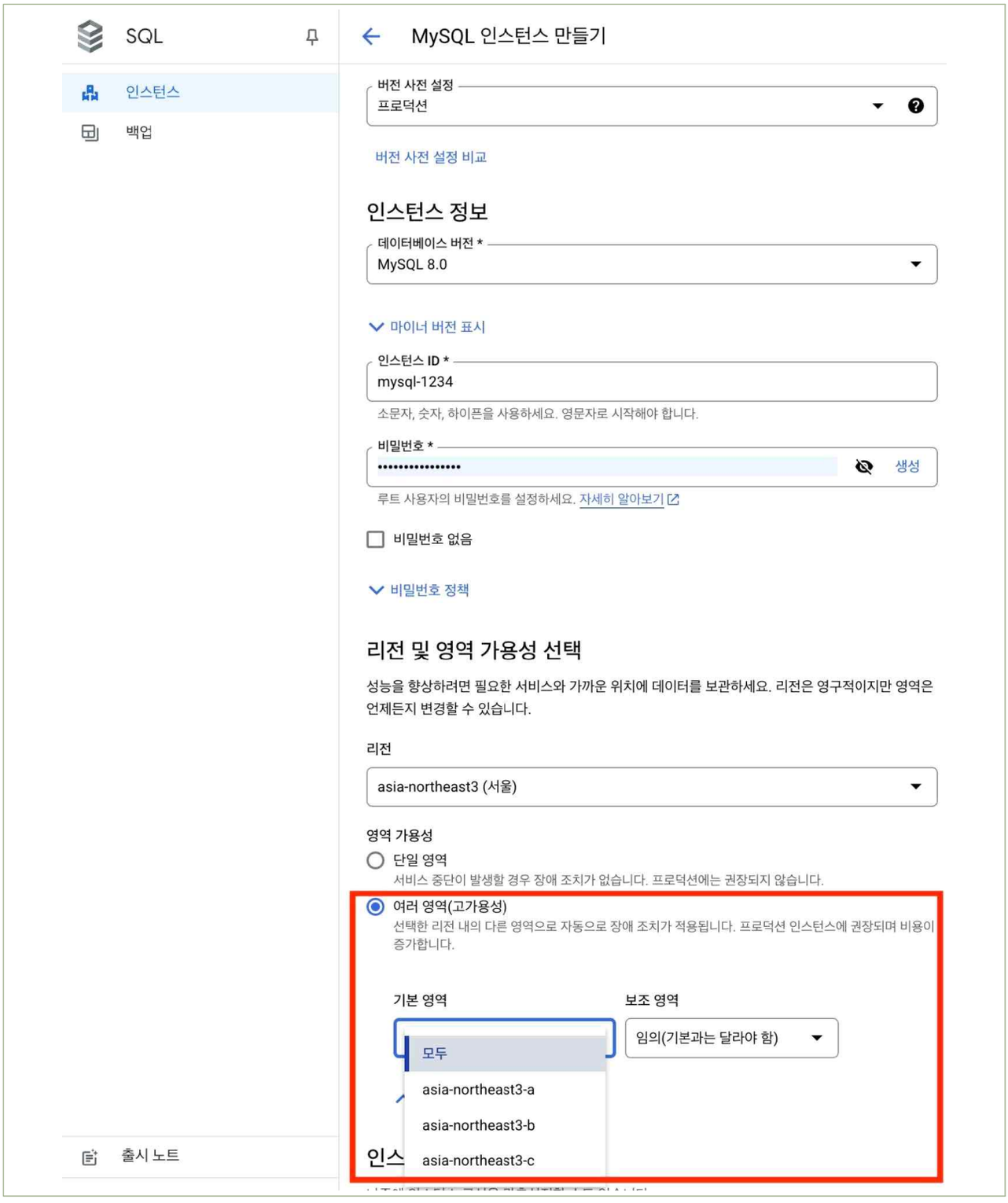
- Compute Engine → 인스턴스 그룹 → 인스턴스 그룹 만들기



| 그림 8-7-3 | 인스턴스 그룹 만들기

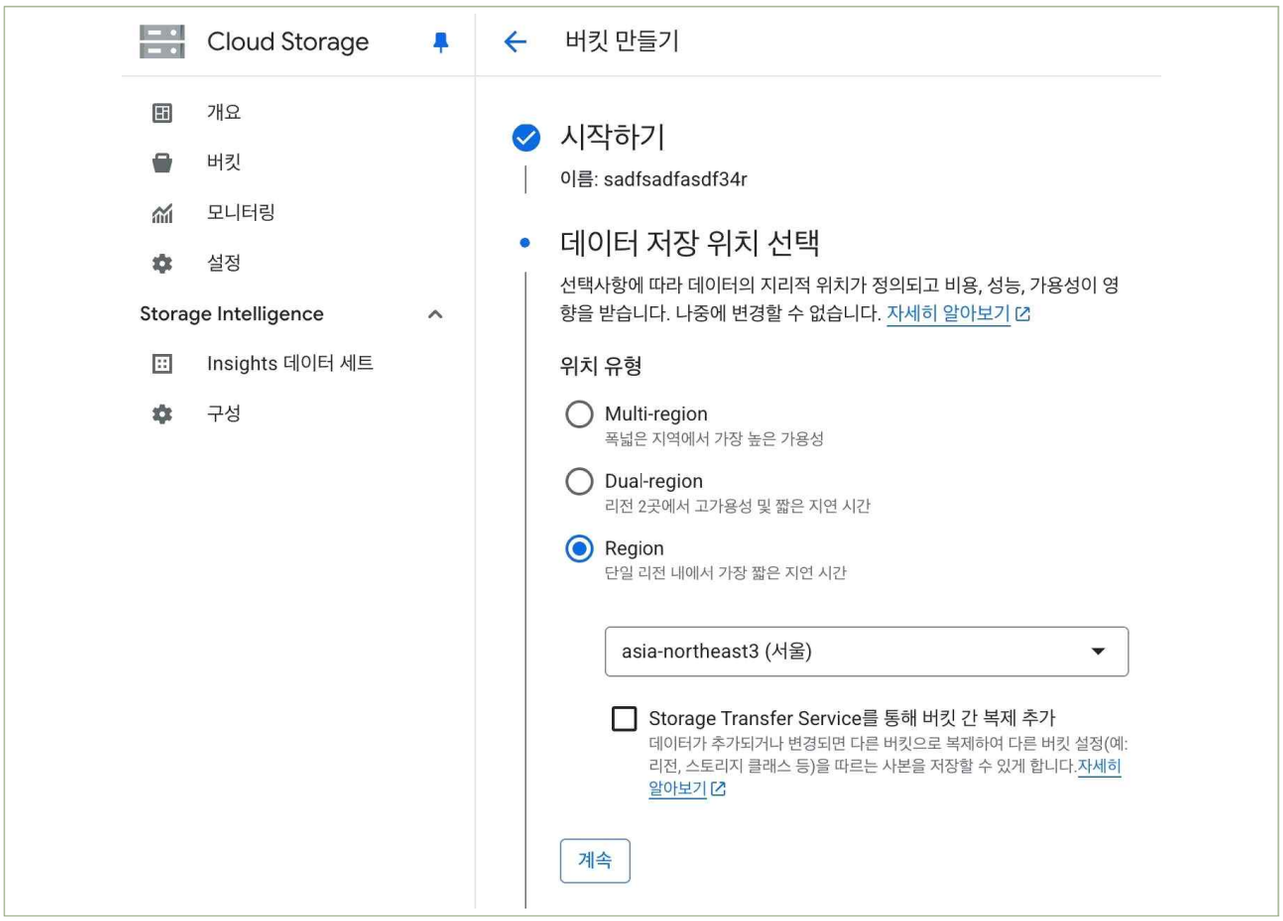
고가용성 SQL 인스턴스 만들기

- SQL → 인스턴스 → 인스턴스 만들기 → 리전 및 영역 가용성 선택



| 그림 8-7-4 | 고가용성 SQL 인스턴스 만들기

- **Cloud Storage**
  - Cloud Storage → 버킷 → 버킷 만들기 → 데이터 저장 위치 선택 선택



| 그림 8-7-5 | Cloud Storage 저장 위치

4 참고 사항

- Managed Instance Groups (MIGs) 개요
  - https://cloud.google.com/compute/docs/instance-groups?hl=ko
- 고가용성 SQL 인스턴스
  - https://cloud.google.com/sql/docs/mysql/configure-ha?hl=ko#ha-create
- Cloud Storage 데이터 가용성 및 내구성
  - https://cloud.google.com/storage/docs/availability-durability?hl=ko
  - https://cloud.google.com/storage/docs/locations?hl=ko#considerations

금융분야 상용 클라우드컴퓨팅서비스 보안 관리 참고서 (Google Cloud)

발 행 일	2025년 10월
발 행 인	금융보안원(원장 박상원)
공 동 발 행 인	Google Cloud
금 융 보 안 원	
클라우드대응부	부장 김제광
클라우드기획팀	팀장 장지현 차장 정희선 과장 김용규 과장 안성현 과장 마승영 대리 최주섭 대리 송창석 주임 전동현 주임 전하은
발 행 처	금융보안원
	02-3495-9000
	경기도 용인시 수지구 대지로 132

〈비 매 품〉

금융분야
상용 클라우드컴퓨팅서비스 보안 관리 참고서